Security Target Lite

Tachograph Generation V2

CONTENT

FIGURES

TABLES

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	Tachograph Generation V2 Security Target
Version :	1.3
ST Reference :	D1432172
Origin :	Gemalto
IT Security Evaluation scheme :	SERMA Safety & Security
IT Security Certification scheme :	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

Product Name/ TOE Name :	Smart Tachograph G2 on MultiApp V4.0.1
Security Controllers :	**M7892 G12**
TOE Reference :	Tachograph Generation V2 on MultiApp V4.0.1
TOE Version :	2.0.1.G
TOE documentation :	Guidance [AGD]

The TOE identification is provided by the Card Production Life Cycle Data (CPLCD). These data are available by executing a dedicated command.

1.3 SECURITY TARGET OVERVIEW

The TOE is the micro-module made of the Integrated Circuit (IC) and its embedded software (ES). The ES encompasses the MultiApp V4.0.1 javacard platform and the Tachograph Generation V2 Application. It includes the associated embedded data of the smart card working on the micro-controller unit in accordance with the functional specifications.

The plastic card is outside the scope of this Security Target.

This Security Target defines the security objectives and requirements for the Digital Tachograph Card based on the requirements and recommendations of the EU Regulation 165/2014).

The Security Target is based on the Protection Profile: Digital Tachograph – Tachograph Card [PP-TACHO-CARD].

The Security Target defines the security requirements for the TOE. The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the Tachograph application and data during its life cycle.

The main objectives of this ST are:

- To introduce the TOE and the Tachograph Generation V2 application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

1.4 REFERENCES, GLOSSARY AND ABBREVIATIONS

1.4.1 External references

Reference	Title - Reference
[CC]	Common Criteria references
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 rev 5, April 2017
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2012-09-002, version 3.1 rev 5, April 2017
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2012-09-003, version 3.1 rev 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2012-09-004, version 3.1 rev 5, April 2017
[ISO]	ISO references
[ISO 7816]	ISO 7816-X documents
[ISO9797-2].	ISO/IEC 9796: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
[PP]	Protection Profiles
[PP-TACHOCARD]	Digital Tachograph –Tachograph Card (TC PP) Protection Profile BSI-CC-PP-0091-2017 Version 1.0
[PP-IC-0084]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014
[TACHO]	Tachograph references
	ANNEX I C - Requirements for construction, testing, installation, and inspection
	Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on Tachographs in road transport
	APPENDIX 2 - TACHOGRAPH CARDS SPECIFICATION
	APPENDIX 10 - SECURITY REQUIREMENTS
	APPENDIX 11 - COMMON SECURITY MECHANISMS
[5]	Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components
[6]	Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’, 05.08.2002, Annex I B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)
[7]	A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-Systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011

[NXP]	Protection Profiles
[ST-IC]	Security Target Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12 Revision 1.7 as of 2016-11-16
[CR-IC]	Certification Report, M7892 D11 & G12 BSI-DSZ-CC-0891-V2-2016
[JCS]	Javacard references
[JCAPI304]	Java Card 3.0.4 Application Programming Interface (API) Specification, Classic Edition-– September 2011 – Published by Oracle
[JCRE304]	Java Card 3.0.4 Runtime Environment (JCRE) Specification, Classic Edition – September 2011 – Published by Oracle
[JCVM304]	Java Card 3.0.4 Virtual Machine (JDVM) Specification, Classic Edition-– September 2011 – Published by Oracle
[GP]	Global Platform references
[GP221]	GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification v 2.2 – Amendment D Version 1.0 Public Release April 2009
[MISC]	Miscellaneous
[RSA-PKCS#1]	PKCS#1 v2.1 RSA Cryptography Standard
[DSS]	FIPS PUB 186-4 Digital Signature Standard, ECDSA signing algorithm
[AES]	FIPS PUB 197 Advanced Encryption Standard
[SP800-67]	SP800-67 Triple Data Encryption Algorithm (TDEA)
[FIPS180-4]	FIPS PUB 180-4 Secure Hash Standard
[HMAC]	RFC 5869: HMAC based Extract and Expand Key Derivation Function
[SP800-38 A]	NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of operation

1.4.2 Internal references

Reference	Title - Reference
[AGD]	**Guidance Documentation**
[AGD-OPE]	**Operational user Guidance** Ref: D1432174 Rev 1.2
[AGD-PRE]	**Preparative procedures** Ref: D1432175 Rev 1.5
[AGD-USR]	**Personalisation Manual** Ref: D1427389 Rev 1.c

1.5 GLOSSARY

Activity data	Activity data include events data and faults data for all card types and specific data depending on card type, such as control activity data for control cards, driver activity, vehicles used and places for driver cards and company activity data for company cards. For a full definition, see [5] Annex 1C, Appendix 2 Activity data are part of User Data.
Card identification data	The following elements stored on the TOE, as defined in [5] Annex 1C, Appendix 1 and Appendix 2: typeOfTachographCardId, cardIssuingMemberState, cardNumber, cardIssuingAuthorityName, cardIssueDate, cardValidityBegin, cardExpiryDate
Cardholder activities data	User data related to the activities carried by the cardholder:
User identification data	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
Control activity data	User data related to law enforcement controls
Digital tachograph	Recording equipment
Events and faults data	User data related to events or faults
Identification data	Identification data include card identification data and user identification data.
Sensitive data	Data stored by the tachograph card that need to be protected for integrity, unauthorized modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data
Security data	The specific data needed to support security enforcing functions (e.g. crypto keys)
System	Equipment, people or organisations involved in any way with the recording equipment
User	A legitimate user of the TOE, being a driver, controller, workshop or company. A user is in possession of a valid tachograph card.
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.

1.5.1 Abbreviations

CC	Common Criteria version 3.1
CSP	Certification-Service Provider
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level
ES	Embedded Software
HI	Human Interface
HW	Hardware
IC	Integrated Circuit
ICC	Integrated Circuit Card
IT	Information Technology
NVM	Non Volatile Memory
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
SF	Security function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security functions
TSFI	TSF Interface
TSP	TOE Security Policy
VIN	Vehicle Identification Number
VRN	Vehicle Registration Number
VU	Vehicle Unit

2 TOE OVERVIEW

2.1 TOE DESCRIPTION

The Target of Evaluation (TOE) is the tachograph micro-module defined by:

- The Infineon IC
- The MultiApp 4.0.1 platform (including Gemalto Crypto library and the operating system).
- The Tachograph Generation V2 application
- The Tachograph Personalization Tool (GDP) used only during the personalization of the product. GDP is deleted before shipping to the final user.

In the personalization and usage phases, the micro-module will be inserted in a plastic card. Therefore when the TOE is in personalization and usage phases, the expression “Tachograph card” will often be used instead of “Tachograph micro-module”.

The plastic card is outside the scope of this Security Target.

The TOE is a “contact-only” smartcard compliant with [ISO7816], and supporting T=0 and T=1 communication protocols.

TOE Components	Identification	Constructor
IC	M7892	INFINEON
Platform	MultiApp version 4.01	Gemalto
Tachograph Generation V2 Application (	Tacho Gen V2	Gemalto
Tachograph Personalisation Tool	GDP	Gemalto

Table 1. Tachograph Generation V2 Card components

The TOE defined in this Security Target is the Javacard Tachograph Generation V2 application supported by the MultiApp 4.0.1 Java Card platform.

In its operational phase only the Tachograph Generation V2 can be selected.

The TOE will be designed and produced in a secure environment and used by each user in a hostile environment.

The functional requirements for a Tachograph Generation V2 card are specified in Regulation (EU) No 165/2014 Appendix 2, 10 and 11.

The product provides the following services:

Enforce Mutual authentication Gen1 or Gen2

Storing of card identification and card holder identification data

Storing of Activity data (events, control activities data, faults data)

Perform the verification of certificate Gen1 and Gen2.

Generate signature on internal data to export

Perform the verification (integrity, authenticity) of a DSRC message

Downloading of User Data

Personalization of the product f

The product is compliant with two major industry standards:

- Sun's Java Card 3.0.4 [JCVM304] [JCRE304]
- The Global Platform Card Specification version 2.2.1 [GP221],

The Tachograph security functions take advantage of the platform security functions:

- Hardware Tamper Resistance is managed by the chip security layer that meets the Security IC Platform Protection Profile [PP/BSI-0084].
- Secure operation of the MultiApp 4.0.1 platform managed inside platform component.

2.1.1 TOE boundaries and out of TOE

The TOE is composed of the IC, the software platform and the Tachograph Generation V2 application:

M7892 IC which has been certified separately according to [ST-IC] claiming [PP/BSI-0084]
MultiApp 4.0.1 platform
TACHO Gen2 application
GDP application

The **TSFs** are composed of:

1. The Tachograph related functions of the **TACHO Gen2** application: Mutual Authentication Gen1 and Gen2, Verify PIN, Verify Certificate Gen1 and Gen2, Select/read/Update files, Manage Security Environment, Hash file generation, Generation/Verification Signature, Perform DSRC Message check
2. Tacho Personalization commands through GPD. (Other functions are out of the TOE)
3. **The M7892 IC** that supports the MultiApp 4.01.Platform.

Figure 1 represents the product. The TOE is bordered with bold and un-continuous line.

The architecture of MultiApp inside the TOE is presented in platform description chapter below.

Note that Tachograph Personalisation Tool (GDP) is deleted after personalisation.

In usage phase only The Tacho Gen2 application is present in the Applet Layer.

The platform will be in a closed configuration. No possibility to select the Card Manager.

Tacho Gen2 is selected by default.

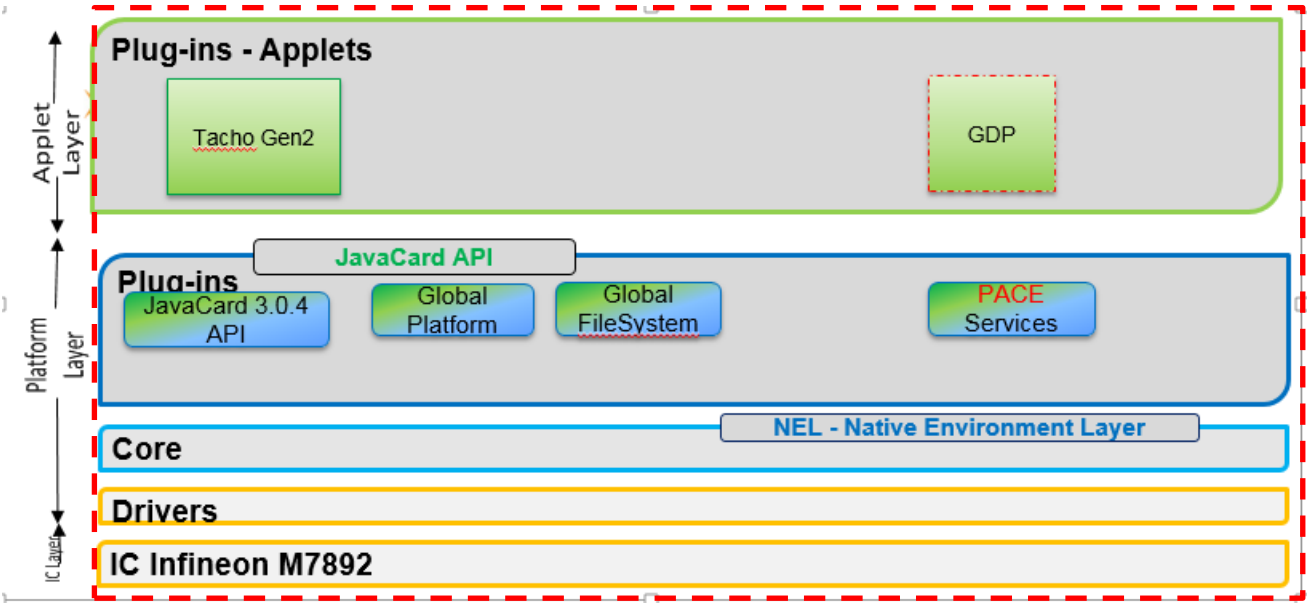


Figure 1 – TACHOGRAPH Generation V2 Card

2.2 TOE DESCRIPTION

2.2.1 Platform description

MultiApp ID V4.0.1 platform is a Java Open Platform that complies with two major industry standards:

- Sun's Java Card 3.0.4, which consists of the Java Card 3.0.4 Virtual Machine [JVCM304], Java Card 3.0.4 Runtime Environment [JCRE304] and the Java Card 3.0.4 Application Programming Interface [JCAPI304].
- The GlobalPlatform Card Specification version 2.2.1[GP221]

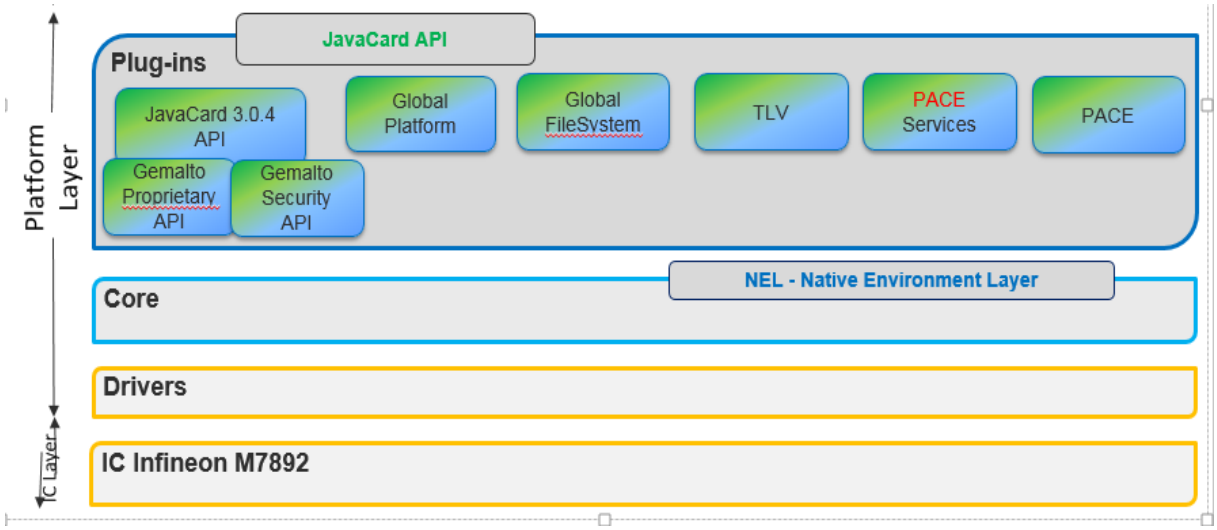


Figure 2: MultiApp ID V4.0.1 javacard platform architecture

As described in figure 2, the MultiApp ID V4.0.1 platform contains the following components:

The *Native Layer* provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the dedicated IC.

The cryptographic features implemented in the native layer, and which support the Tachograph generation V2 functionality, are:

- DES, 3DES (ECB, CBC)
- RSA up to 4096 (CRT method & public Std method), 2048 (Std private method)
- DH up to 2048
- AES 128, 192, 256
- SHA1, SHA 2 (224, 256, 384, 512)
- HMAC
- ECC (ECDSA et ECDH) up to 521
- Pseudo-Random Number Generation (PRNG) & Software random.

The *Java Card Runtime Environment*,

It conforms to [JCRE304] and provides a secure framework for the execution of the Java Card programs and data access management (firewall).

Among other features, multiple logical channels are supported, as well as extradition, DAP, Delegated management, SCP01 and SCP02 and SCP03.

The *Java Card Virtual Machine*,
It conforms to [JCVM304] and provides the secure interpretation of bytecodes.

The *API*
It includes the standard Java Card API [JCAPI304] and Gemalto proprietary API.

The *Open Platform Card Manager*
It conforms to [GP221] and provides card, key and applet management functions (contents and life-cycle) and security control.

The MultiApp V4.0.1 platform provides the following services:

Initialization of the Card Manager and management of the card life cycle[1].

Secure channel according to GP [GG221] protocol[2].

Secure operation of the applications through the API

Management and control of the communication between the card and the CAD

Card basic security services as follows:

Checking environmental operating conditions using information provided by the IC

Checking life cycle consistency

Ensuring the security of the PIN and cryptographic key objects

Generating random numbers

Handling secure data object and backup mechanisms

Managing memory content

Ensuring Java Card firewall mechanism

[1] Available only during personalization. No more usable in user phase
[2] Available only during personalization. No more usable in user phase

2.2.2 TACHO V2 Application description

A Tachograph card is a smart card carrying an application intended for its use with the recording equipment (VU).

The basic functions of the Tachograph Gen V2 card are:

to support mutual authentication protocol regarding Tacho Gen1 or Tacho Gen2 specification,

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

to store cardholder activities data, events and faults data and control activities data, related to the cardholder. The card manages two different file structures (DF) : one for Tacho Gen1 and another onefor Tach Gen2

to verify and generate signature for Tacho Gen1 and for Tacho Gen2

to process DSRC Message

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

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

The functional requirements for a Tachograph card are specified in [5] and [7].

“Tachograph card” means:

smart card intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage.

A Tachograph card may be of the following types:

driver card,

control card,

workshop card,

company card;

“company card” means:

A Tachograph card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment;

The company card identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company;

“control card” means:

A Tachograph card issued by the authorities of a Member State to a national competent control authority;

the control card identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading; the control card is able to process a DSRC message

“driver card” means:

A Tachograph card issued by the authorities of a Member State to a particular driver;

the driver card identifies the driver and allows for storage of driver activity data;

“workshop card” means:

A Tachograph card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Member State.

The workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the recording equipment; the workshop card is able to process a DSRC message

Further description can be found in [5]

The TOE is designed for the four types of cards. The personalization process differentiates these types of cards.

2.2.3 TOE life-cycle

2.2.4 Actors

Actors	Identification
Integrated Circuit (IC) Developer	IFX
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	IFX
Module manufacturer	Gemalto
Initializer/Pre-personalizer	Gemalto
Administrator or Personalization Agent	The agent who personalizes the Tachograph application.
End User	The rightful user of the TOE for whom the Administrator personalizes the card.

Table 2: Identification of the actors

The Smart card product life cycle, as defined in [PP-IC-0084], is split up into 7 phases where the following authorities are involved:

2.2.5 Life cycle description

Phase (name)	Phase (card)	Actor	Comment
Development	1. OS & Tacho Gen2 applet& script Development	Developer (Gemalto)	- Development of Java Card Platform and Tachp application -Generation of principal HEX, mapping description - Script generation for initialization and pre-personalization
	2 HW Development	IC manufacturer (Infineon)	- Development of IC
Manufacturing	3 Mask manufacturing	IC manufacturer (Infineon)	Manufacturing of virgin chip integrated circuits embedding the Infineon flash loader and protected by a dedicated transport key.
	4 Module manufacturing	Module creation (Gemalto or Infineon)	IC packaging & testing
	5.a Embedding (Optional) *This operation can be done before or after 5.b*	*Form Factor manufacturer (Gemalto)*	*Put the module on a dedicated form factor (Card,other)*
	5.b Initialization / Pre-personalization	Pre-personalizer (Gemalto)	Loading of the Gemalto software (platform and Tacho application and initialized the platform and Tacho application
Personalization	6 Personalization	Personalizer	- Personalization
Usage	7 Usage	Holder	- The Issuer is responsible of card delivery to the end-user

Remark1: Initialization & pre-personalization operation could be done on module or on other form factor. The form factor does not affect the TOE security.

Remark3: For initialization/pre-personalization IC flash loader will be used based the IC manufacturer recommendation. The flash loader is deactivated definitively after the loading of the flashmask. No possibility to go back the flash loader after this phase.

Remark4: Embedding (module put on a dedicated form factor) will be done on an audited site.

3 CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

This Security Target is built with CC V.3.1 Revision 5

This ST is [CC-2] extended with FPT_EMS TOE emanation and FCS_RNG.1 .

This ST is [CC-3] conformant.

Evaluation type

This is a composite evaluation, which relies on the M7892 Infineon chip certificate and evaluation results.

M7892 **chip certificate**:

Certification done under the BSI scheme
Certification reports [CR-IC]
Security Target [ST-IC] strictly conformant to IC Protection Profile [PP/0084]
Common criteria version: 3.1
Assurance level: EAL6 augmented by ALC_FLR.1

Consequently, the composite product evaluation (i.e. the present evaluation) includes the additional composition tasks defined in the CC supporting document “Composite product evaluation for smart cards and similar devices” [CCDB].

3.2 PP CLAIM, PACKAGE CLAIM

This ST claims strict conformance to the Protection Profile [PP-TACHOCARD]

[ST-IC] refines the assets, threats, objectives and SFR of [PP-IC-0084].

This TOE claims conformance to Package EAL4 augmented (+) with:

ALC_DVS.2: Sufficiency of security measures.

ATE_DPT.2: Testing Enforcing modules

AVA_VAN.5: Advanced methodical vulnerability analysis

3.3 CONFORMANCE RATIONALE

The ST security objectives and requirements are identical to those of the claimed PP [PP-TACHOCARD] in the ST.

4 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the TOE environment and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions.

4.1 ASSETS

Asset name	Description	Generic security property to be maintained by the TOE
Identification data (IDD)	Primary asset: card identification data, user identification data (see Glossary for more details)	Integrity
Activity data (ACD)	Primary asset: cardholder activities data, events and faults data and control activity data (see Glossary for more details)	Integrity, Authenticity, for parts of the activity data also Confidentiality
Keys to protect (KPD)	Secondary asset: 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.	Confidentiality, Integrity
Application (APP)	Secondary asset: Tachograph application	Integrity
Signature verification data (SVD)	Secondary asset: public keys certified by Certification Authorities, used to verify electronic signatures	Integrity, Authenticity
Verification authentication data (VAD)	Secondary asset: authentication data provided as input for authentication messaging attempt as authorised user (PIN)	Integrity
Reference authentication data (RAD)	Secondary asset: data persistently stored by the TOE for verification of the authentication attempt as authorised user	Confidentiality, Integrity
Data to be signed (DTBS)	Secondary asset: the complete electronic data to be signed (including both user message and signature attributes)	Integrity, Authenticity

Asset name	Description	Generic security property to be maintained by the TOE
TOE File system incl. specific identification data	Secondary asset: file structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalisation	Integrity

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. The GST [8] defines “sensitive data” which include security data and user data as data stored by the Tachograph Card, which integrity, confidentiality and protection against unauthorized modification need to be enforced. User data include 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.

4.2 SUBJECTS AND EXTERNAL ENTITIES

Role	Definition
Administrator	S.Administrator: the subject is usually active only during Initialisation/Personalisation (Phase 6) – listed here for the sake of completeness..
Vehicle Unit	S.VU: Vehicle Unit (with a UserID), which the Tachograph Card is connected to.
Other devices	S.Non-VU: Other device (without UserID) which the Tachograph Card is connected to.
Attacker	A human or a process located outside the TOE and trying to undermine the security policy defined by the current PP, especially to change properties of the maintained assets. For example, a driver could be an attacker if he misuses the driver card. An attacker is assumed to possess at most a high attack potential..

4.3 THREATS

Threat name	Description
T.Identification_Data	A successful modification of identification data held by the TOE (e.g. the type of card, or the card expiry date or the cardholder identification data) would allow 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 , would allow an attacker to misrepresent human user (especially driver) activity.
T.Activity_Data	A successful modification of activity data stored in the TOE, would allow an attacker to misrepresent human user (especially driver) activity.

Threat name	Description
T.Data_Exchange	A successful modification of activity data (addition, deletion, modification) during import or export would allow an attacker to misrepresent human user (especially driver) activity.
T.Clone	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.

4.4 ASSUMPTIONS

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

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

4.5 ORGANIZATIONAL SECURITY POLICIES

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

4.6 COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART

4.6.1 Statement of Compatibility – Threats part

The following table lists the relevant threats of the M7892 security target [ST-IC], and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.

IC relevant threat label	IC relevant threat title	IC relevant threat content	Link to the composite-product threats
T.Leak-Inherent	Inherent Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets. No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.	T.Data_Exchange T.Personalisation_Data
T.Phys-Probing	Physical Probing	An attacker may perform physical probing of the TOE in order (i) to disclose User Data (ii) to disclose/reconstruct the Security IC Embedded Software or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.	T.Data_Exchange T.Personalisation_Data
T.Malfunction	Malfunction due to Environmental Stress	An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or	T.Identification_Data T.Activity_Data T.Data_Exchange

		(ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions.	T.Personalisation_Data
T.Phys-Manipulation	Physical Manipulation	An attacker may physically modify the Security IC in order to (i) modify User Data (ii) modify the Security IC Embedded Software (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.	T.Identification_Data T.Activity_Data T.Clone T.Application
T.Leak-Forced	Forced Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets even if the information leakage is not inherent but caused by the attacker.	T.Identification_Data T.Activity_Data T.Data_Exchange T.Clone
T.Abuse-Func	Abuse of Functionality	An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate User Data (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the User Data or the Security IC Embedded Software.	T.Identification_Data T.Activity_Data T.Clone

T.RND	Deficiency of Random Numbers	An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.	T.Identification_Data T.Activity_Data T.Data_Exchange T.Clone

4.6.2 Statement of Compatibility – OSPs part

The following table lists the relevant OSPs of the M7892 security target [ST-IC], and provides the link to the OSPs related to the composite-product, showing that there is no contradiction between the two.

IC OSP label	IC OSP content	Link to the composite product
P.Process-TOE	Identification during TOE Development and Production: An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.	No contradiction with the present evaluation; the chip traceability information is used to identify the composite TOE.
P.Add-Functions	Additional Specific Security Functionality: The TOE shall provide the following specific security functionality to the Smartcard Embedded Software: Triple Data Encryption Standard (TDES) Advanced Encryption Standard (AES) Elliptic Curve Cryptography (EC) River-Shamir Adleman cryptography (RSA)	. The TOE doesn't use these Additional Specific Security Functionality. The TOE use is own crypto library for TDES, AES, EC and RSA.
P.Crypto-Service	The TOE provides secure hardware based cryptographic services for the IC Embedded Software: • Triple Data Encryption Standard (TDES) • Advanced Encryption Standard (AES) • Hash function SHA	The TOE uses TDES, AES and SHA hardware based cryptographic services.
P.Lim_Block_Loader	**Limiting and Blocking the Loader Functionality** The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation	The loader is locked after initialisation step.

4.6.3 Statement of Compatibility – Assumptions part

The following table lists the relevant assumptions of the M7892 security target [ST-IC] and provides the link to the assumptions related to the composite-product, showing that there is no contradiction between the two.

IC assumption label	IC assumption title	IC assumption content	IrPA	CfPA	SgPA	Link to the composite product
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).		X	X	Fulfilled by the composite ALC_DVS.2 and ALC_DEL.1 SARs until the end of phase 5 (TOE delivery point). Covered by the assumption A.USE_PROD after the TOE delivery point.
A.Key-Function	Usage of Key-dependent Functions	Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).		X		OT.Secure_Communications
A.Resp-Appl	Treatment of User Data of the Composie TOE	All User data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.		X		OT.Data_Access,OT.Card_Activity_Storage,OT.Card_Identification_Data, OT.Secure_Communications

5 SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment

The security objectives of the TOE cover principally the following aspects:

- Integrity and confidentiality of assets,

- Protection of the TOE and associated documentation and environment during development and production phases.

5.1 SECURITY OBJECTIVES FOR THE TOE

This section describes the security objectives for the TOE, which address the aspects of identified threats to be countered by the TOE independently of the TOE environment and organizational security policies to be met by the TOE independently of the TOE environment.

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

5.2 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.

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

5.3 SECURITY OBJECTIVES RATIONALE

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

	Security objectives of the TOE	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update	Objectives for operational environment	OE.Personalisation_Phase	OE.Crypto_Admin	OE.EOL
Threats												
T.Identification_Data		X					X				X	
T.Activity_Data			X		X		X				X	
T.Application				X			X	X				X
T.Data_Exchange				X		X	X				X	
T.Clone				X								X
OSPs												
P.Crypto							X					
Assumptions												
A.Personalisation_Phase										X	X	

Table 3: Security Objective Rationale

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

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

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**.**

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

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

5.4 COMPOSITION TASKS – OBJECTIVES PART

5.4.1 Statement of compatibility – TOE objectives part

The following table lists the relevant TOE security objectives of the M7892 chip and provides the link to the composite-product TOE security objectives, showing that there is no contradiction between the two sets of objectives.

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
O.Leak-Inherent	Protection against Inherent Information Leakage	The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC - by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and - by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines). This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Phys-Probing	Protection against Physical Probing	The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Security IC Embedded Software or against the disclosure of other critical information about the operation of the TOE. This includes protection against - measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or	O.Card_Activity_Data O.Card_Identification_Data O.Data_Protect_Secret

		- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis) with a prior reverse-engineering to understand the design and its properties and functions.	
O.Malfunction	Protection against Malfunctions	The TOE must ensure its correct operation. The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.	OTCard_Activity_Data O.Protect_Secret
O.Phys-Manipulation	Protection against Physical Manipulation	The TOE must provide protection against manipulation of the TOE (including its software and Data), the Security IC Embedded Software and the User Data. This includes protection against - reverse-engineering (understanding the design and its properties and functions), - manipulation of the hardware and any data, as well as - controlled manipulation of memory contents (Application Data).	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Leak-Forced	Protection against Forced Information Leakage	The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker - by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or - by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”. If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Abuse-Func	Protection against Abuse of Functionality	The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical User Data, (ii) manipulate critical User Data of the Security IC Embedded Software, (iii) manipulate Soft-coded Security IC Embedded Software or (iv) bypass, deactivate, change or explore security	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret

		features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.	
O.Identification	TOE Identification	The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.	No direct link to the composite-product TOE objectives, however chip traceability information stored in NVM is used by the TOE to answer identification CC assurance requirements.
O.RND	Random Numbers	The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 4.0.1

5.4.2 Statement of compatibility – TOE ENV objectives part

The following table lists the relevant ENV security objectives related to the M7892 chip, and provides the link to the composite-product, showing that they have been taken into account and that no contradiction has been introduced.

IC ENV security objective label	IC ENV security objective title	IC ENV security objective content	Link to the composite-product
OE.Resp-Appl	Treatment of User Data	Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant User Data to unauthorized users or processes when communicating with a terminal.	Covered by TOE Security Objectives: O.Card_Activity_Data ,O.Card_Identification_Data ,O.Protect_Secret, O.Secure_Communications,
OE.Process-Sec-IC	Protection during composite product manufacturing	Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.3) must be protected appropriately.	Fulfilled by ALC.DVS.2 and ALC_DEL.1 during phases 4 and 5. After phase 5, covered by O.Protect_Secret, O.Secure_Communications, OE.Personalisation_Phase and O.EOL
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.	Fulfilled through the transport key verification at the beginning of phases 4 and 5, as stated in ALC_DEL.1

6 EXTENDED COMPONENTS DEFINITION

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 defined and justified in [7] Section 3.

6.1 FCS_RNG (GENERATION OF RANDOM NUMBERS)

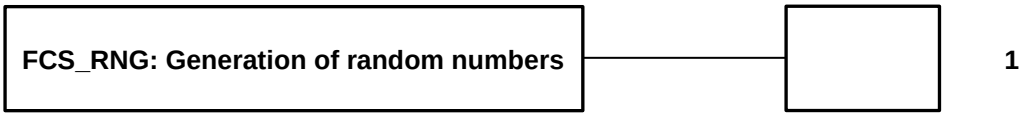
Rationale

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

Family behaviour

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

Component levelling:



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

There are no management activities foreseen.

Audit

There are no auditable activities foreseen

FCS_RNG.1 Generation of random numbers

Hierarchical to:-

Dependencies:-

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

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

6.2 FPT_EMS (TOE EMANATION)

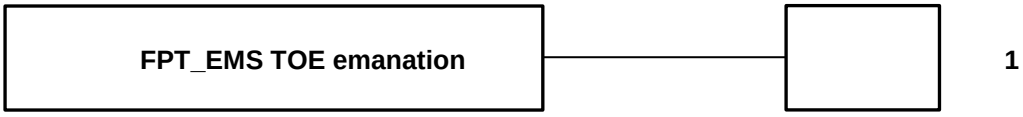
Rationale

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 byCC Part 2 [CC-2]

Family behaviour

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 levelling:



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

Management

There are no management activities foreseen.

Audit

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No 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*].

7 SECURITY REQUIREMENTS

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

7.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP-TACHOCARD]

[ST-IC] deals with the security functional requirements of [PP/BSI-0084].

7.1.1 Security Function Policy

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

Subjects:

·S.VU (in the sense of the Tachograph Card specification)

·S.Non-VU (other card interface devices)

Security attributes for subjects:

·USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)

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

Objects:

-·user data:

- •identification data (card identification data, cardholder identification data)
- •activity data (cardholder activities data, events and faults data, control activity data)

-·security data:

- •cards´s private signature key
- •public keys (in particular card´s public signature key; keys stored permanently on the card or imported into the card using certificates)
- •session keys
- •PIN (for workshop card only)

-·TOE software code

-·TOE file system (incl. file structure, additional internal structures, access conditions)

-·identification data of the TOE concerning the IC and the Smartcard Embedded Software (indicated as identification data of the TOE in the following text)

- identification data of the TOE`s personalisation concerning the date and time of the personalisation (indicated as identification data of the TOE`s personalisation in the following text)

Security attributes for objects:

·Access Rules based on defined Access Conditions (see below) for:

•user data

•security data

•identification data of the TOE

•identification data of the TOE's personalisation

·Digital signature for each data to be signed

Operations:

user data:

•identification data: selecting (command Select), reading (command Read Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)

•activity data: selecting (command Select), reading (command Read Binary), writing / modification (command Update Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)

·security data:

•card´s private signature key: generation of a digital signature (command PSO Compute Digital Signature), internal authentication (command Internal Authenticate), external authentication (command External Authenticate)

•public keys (in particular card´s public signature key): referencing over a MSE-command (for further usage within cryptographic operations as authentication, verification of a digital signature etc.)

•session keys: securing of commands with Secure Messaging

•PIN (only relevant for Workshop Card): verification (command Verify PIN)

·TOE software code: No Operations

TOE file system (incl. file structure, additional internal structures, access conditions): No Operations

·identification data of the TOE: selecting and reading

·identification data of the TOE's personalisation (date and time of personalisation): selecting and reading.

Access Rules:

The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access a certain object. The possible commands and Access conditions are described in the Tachograph Card specification [5], ANNEX 1C Appendix 2.

7.1.2 Security functional requirements list

Identification	Description
FAU	Security Audit
FAU_SAA.1	Security Audit Analysis
FAU_ARP.1	Security alarms
FCO	Communication
FCO_NRO.1	Non-repudiation of origin
FCS	Cryptographic support
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FCS_RNG.1	Random number generation
FDP	User data protection
FDP_ACC.2	Complete Access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic Data Authentication
FDP_ETC.1	Export of user data without security attributes
FDP_ETC.2	Export of user data with security attributes
FDP_ITC.1	Import of User Data without security attributes
FDP_ITC.2	Import of User Data with security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FIA	Identification and Authentication
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.3	Unforgeable authentication

FIA_UAU.4	Single use authentication mechanisms
FIA_UID.2	User authentication before any action
FIA_USB.1	User subject binding
FPR	Privacy
FPR_UNO.1	Unobservability
FPT	Protection of the TOE Security Function
FPT_EMS.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_TDC.1	Inter-TSF TSF data consistency
FPT_TST.1	TSF testing
FTP	Trusted path/Channel
FTP_ITC.1	Inter-TSF trusted channel

Table 3 Tacho Generation V2 security functional requirements list

Some SFR iterations have a different name from the Protection Profile [PP-TACHOCARD]

Some SFR iterations are specific to this Security Target.

The table below will help the reader of this Security Target to match which SFR is from the PP, which one is an addition.

Requirement in this ST	SFR in [PP-TACHOCARD]	Additions
FAU_SAA.1	FAU_SAA.1	
FAU_ARP.1	FAU_ARP.1	
FCO_NRO.1	FCO_NRO.1	
FCS_CKM.1 / Session GP		YES
FCS_CKM.1 / Session Tacho Gen1	**FCS_CKM.1 (2)**	
FCS_CKM.1 / Session Tacho Gen2	**FCS_CKM.1 (1)**	
FCS_CKM.1 / Card Private Key		YES
FCS_CKM.2/ Session Tacho Gen1	**FCS_CKM.2 (2)**	
FCS_CKM.2/ Session Tacho Gen2	**FCS_CKM.2 (1)**	
FCS_CKM.2/ Public Key		YES
FCS_CKM.2/ Certificate		YES
FCS_CKM.4/ Session GP		YES
FCS_CKM.4/ Session Tacho Gen1	**FCS_CKM.4 (2)**	

Requirement in this ST	SFR in [PP-TACHOCARD]	Additions
FCS_CKM.4/ Session Tacho Gen2	**FCS_CKM.2 (1)**	
FCS_COP.1/RSA	**FCS_COP.1 (5:RSA)**	
FCS_COP.1/TDES	**FCS_COP.1 (4:TDES)**	
FCS_COP.1 / HASH	**FCS_COP.1 (6:SHA-1)**	
FCS_COP.1 / HMAC		YES
FCS_COP.1 / AES	**FCS_COP.1 (1:AES)**	
FCS_COP.1 / SHA-2	**FCS_COP.1 (2:SHA-2)**	
FCS_COP.1 / ECC	**FCS_COP.1 (3:ECC)**	
FCS_COP.1/GP MAC		YES
FCS_COP.1/GP ENC		YES
FCS_RNG.1	**FCS_RNG.1**	
FDP_ACC.2 / AC_SFP SFP	FDP_ACC.2	
FDP_ACF.1 / AC_SFP SFP	FDP_ACF.1	
FDP_DAU.1	FDP_DAU.1	
FDP_ETC.1	FDP_ETC.1	
FDP_ETC.2	FDP_ETC.2	
FDP_ITC.1	FDP_ITC.1	
FDP_ITC.2	FDP_ITC.2	
FDP_RIP.1	FDP_RIP.1	
FDP_SDI.2	FDP_SDI.2	
FIA_AFL.1 /C	FIA_AFL.1 (1:C)	
FIA_AFL.1 /WC	FIA_AFL.1 (2:WC)	
FIA_AFL.1 Card Interface GP		YES
FIA_ATD.1	FIA_ATD.1	
FIA_UAU.1 / Gen1	**FIA_UAU.1 (2)**	
FIA_UAU.1 / Gen2	**FIA_UAU.1 (1)**	
FIA_UAU.3	FIA_UAU.3	
FIA_UAU.4	FIA_UAU.4	
FIA_UID.2	FIA_UID.2	
FIA_USB.1	FIA_USB.1	
FPR_UNO.1	FPR_UNO.1	
FPT_EMS.1	FPT_EMS.1	
FPT_FLS.1	FPT_FLS.1	
FPT_PHP.3	FPT_PHP.3	

Requirement in this ST	SFR in [PP-TACHOCARD]	Additions
FPT_TDC.1 /Gen1	**FPT_TDC.1 (2)**	
FPT_TDC.1 /Gen2	**FPT_TDC.1 (1)**	
FPT_TST.1	FPT_TST.1	
FTP_ITC.1 /Gen1	**FPT_ITC.1 (2)**	
FTP_ITC.1 /Gen2	**FPT_ITC.1 (1)**	

7.1.3 Class FAU Security Audit

7.1.3.1 FAU_ARP.1 Security alarms

Hierarchical to: No Other component

FAU_ARP.1.1 The TSF shall take **the following actions:**

a)For user authentication failures and activity data input integrity errors – respond to the VU through SW1 SW2 status words, as defined in [5] Annex 1C, Appendix 2;

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

Application integrity error : SW1 SW2:6F10

Store data integrity error : SW1 SW2:6400

upon detection of a potential security violation.

7.1.3.2 FAU_SAA.1 Security Audit Analysis

Hierarchical to: No Other component

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 (5 consecutive unsuccessful PIN checks)
- Self test error
- Stored data integrity error
- Activity data input integrity error

known to indicate a potential security violation;

b) No other rules[3]

Dependencies: FAU.GEN.1 Audit Data Generation Not applicable for a smart card

[3] [assignment: any other rules]

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

7.1.4 Class FCO Communication

7.1.4.1 FCO_ NRO.1 Selective proof of origin

Hierarchical to: No other component

FCO_NRO.1.1	The TSF shall be able to generate evidence of origin for transmitted **data to be downloaded to external media** at the request of the **recipient in accordance with [5] Annex 1C, Appendix 11, sections 6.1 and 14.2.**
FCO_NRO.1.2	The TSF shall be able to relate the **user identity by means of digital signature** of the originator of the information, and **the hash value over the data to be downloaded to external media** of the information to which the evidence applies.
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given **that the digital certificate used in the digital signature for the downloaded data has not expired (see [5] Appendix 11, sections 6.2 and 14.3)**.

Dependencies: FIA_UID.1 Timing of identification

Application note: Note that FCO_NRO.1 applies only to driver cards and workshop control cards, As those are the only cards capable of creating a signature over downloaded data See [5] Appendix11.

7.1.5 Class FCS Cryptographic support

7.1.5.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other component

generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that

FCS_CKM.1.1 The TSF shall meet the following: **[assignment: list of standards]**.

FCS_CKM.1.1 / Session GP	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **GP session keys** and specified cryptographic key sizes **112 bits for SCP01 and SCP02 / 128,192,256 bits for SCP03** that meet the following **SCP01,SCP02,SCP03 cf [GP221]**
FCS_CKM.1.1 / Session Tacho Gen1	The TSF shall generate keys in accordance with a specified key generation algorithm **cryptographic key derivation algorithms specified in [5] Annex 1C, Appendix 11, Section 4 (for the secure messaging session key)**and specified cryptographic key sizes **112 bits** that meet the following **two-key TDES as specified in [5] Annex 1C,Appendix 11 Part A, Section 3.**
FCS_CKM.1.1 / Session Tacho Gen2	The TSF shall generate keys in accordance with a specified key generation algorithm **cryptographic key derivation algorithms specified in [5] Annex 1C, Appendix 11, Section 10 (for VU authentication and for the secure messaging session key)** and specified cryptographic key sizes **key sizes required by [5] Annex 1C, Appendix 11, Part B** that meet the following: **Reference [7] predefined RNG class [DRG.4], [5] Annex 1C, Appendix 11, Section 10.**
FCS_CKM.1.1 / Card private key	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation or ECC key generation** and specified cryptographic key sizes **1024 bits for RSA/ 160,192,224,256,320,384 bits for ECC** that meet the following **None**

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

FCS_COP.1 Cryptographic operations]

FCS_CKM.4 Cryptographic key destruction

7.1.5.2 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other component

FCS_CKM.2.1 / Session Tacho Gen 1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **for triple DES session keys as specified in**

	[5] Annex 1C, Appendix 11 Part A that meets the following **[5] Annex 1C, Appendix 11 Part A, Section 3**.
FCS_CKM.2.1 / Session Tacho Gen 2	The TSF shall distribute cryptographic keys in accordance with a specified key distribution method **secure messaging AES session key agreement as specified in [5] Annex 1C, Appendix 11, Part B** that meets the following **[5] Annex 1C, Appendix 11, Part B.**
FCS_CKM.2.1 / Public Key	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **"Generate Asymmetric key pair" command** that meets the following **None**
FCS_CKM.2.1 / Certificate	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **"Read Binary" command** that meets the following **None**

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

7.1.5.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other component

FCS_CKM.4.1 / Session GP	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: **[no standard]**.
FCS_CKM.4.1 / Session Tacho Gen1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: - Requirements defined in [PP-TACHOCARD] Table 16 and Table 17 - Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means - **[no standard]**
FCS_CKM.4.1 / Session Tacho Gen2	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: - Requirements defined in [PP-TACHOCARD] Table 20 - Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means - **[no standard]**

Note:

There is no iteration for the Card private key. Disabling the signature function is performed by invalidating the Card certificate. So there is no need to delete the card private key.

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]

7.1.5.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other component

For 1st generation

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: **[5] Annex 1C, Appendix 11 Part A, Chapter 3.**
FCS_COP.1.1/HASH	The TSF shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **not applicabl]** that meet the following**: Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS).**
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: **[5] Annex 1C, Appendix 11 Part A, Chapter 3.**

For 2nd generation

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 PUB 197: Advanced Encryption Standard**.

FCS_COP.1.1/SHA-2 The TSF shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm **SHA-256, SHA-384, SHA-512** and cryptographic key sizes **not applicable** that meet the following: **Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS), [5] Annex 1C, Appendix 11.**

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-repudation of data downloaded from a tachograph card]
in accordance with a specified cryptographic algorithm **[5] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG** and cryptographic key sizes **in accordance with [5], Appendix 11, Part B** that meet the following**: [5] Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-03111 – Elliptic Curve Cryptography – version 2, and the standardized domain parameters :**

Name	Size (bits)	Object identifier
NIST P-256	256	secp256r1
BrainpoolP256r1	256	brainpoolP256r1
NIST P-384	384	secp384r1
BrainpoolP384r1	384	brainpoolP384r1
NIST P-521	512	brainpoolP512r1
BrainpoolP521r1	521	secp521r1

FCS_COP.1.1/HMAC The TSF shall perform **[HMAC signature verification]** in accordance with a specified cryptographic algorithm **[AES]** and cryptographic key sizes **[SHA-1, SHA-224, SHA-256, SHA-384, SHA-512]** that meet the following**: [ISO9797-2]**.

FCS_COP.1.1/GP MAC The TSF shall perform **[MAC computation in GP session]** in accordance with a specified cryptographic algorithm **[TDES-CBC]** and cryptographic key sizes **[112 bits]** that meet the following**: [SP800-67] and [SP800-38 A]**.

FCS_COP.1.1/GP ENC The TSF shall perform **[Encryption and decryption in GP session]** in accordance with a specified cryptographic algorithm **[TDES-ECB]** and cryptographic key sizes **[112 bits]** that meet the following**: [SP800-67] and [SP800-38 A]**.

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

7.1.5.5 FCS_RNG.1 Generation of random numbers

Hierarchical to: No other components

Dependencies: No dependencies

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

(DRG.4.1) The internal state of the RNG shall [***use PTRNG of class PTG.2 as random source***].
(DRG.4.2) The RNG provides forward secrecy.
(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.
(DRG.4.4) The RNG provides enhanced forward secrecy [***after [calling the re-seed function that acts as a refreshing done at each random generation]***].
(DRG.4.5) The internal state of the RNG is seeded by an [***internal entropy source, PTRNG of class PTG.2***].

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

(DRG.4.6) The RNG generates output for which **[*2^35*]** strings of bit length 128 are mutually different with probability [***equal to (1 – 1/2^58)*]**.

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [***None***].

7.1.6 Class FDP User data protection

7.1.6.1 FDP_ACC.2 Complete access control

Hierarchical to: No other component

FDP_ACC.2.1/ SFP AC_SFP The TSF shall enforce the **AC_SFP** on

Subjects:
- **S.VU (a vehicle unit in the sense of [5] Annex 1C)**
- **S.Non-VU (other card interface devices)**

Objects:
- **User data:**
  - **User identification data**
  - **Activity data**
- **Security data:**
  - **Cryptographic keys**
  - **Session keys**
  - **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/ SFP	AC_SFP	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.

Dependencies: FDP_ACF.1 Security attribute based access control

7.1.6.2 FDP_ACF.1 Security attributes based access control

Hierarchical to: No other component

The only security attribute related to Access Control is **USER_GROUP**. It is an attribute of the User. It can have the following values: VEHICLE_UNIt, NON_VEHICLE_UNIT.

FDP_ACF.1.1/ AC_SFP SFP

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

Subjects:
- **S.VU (in the sense of [5] Annex 1C)**
- **S.Non-VU (other card interface devices)**

Objects:
- **User data:**
  - **User identification data**
  - **Activity data**
- **Security data:**
  - **Cryptographic keys**
  - **Session keys**
  - **PIN (for workshop card)**
- **TOE application code**
- **TOE file system (Attribute : access conditions)**
- **Card identification data**
- **Master file contents**

FDP_ACF.1.2/ AC_SFP SFP

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

- GENERAL_READ:
Driver card, workshop card: user data may be read from the TOE by any user
Control card, company card: user data may be read from the TOE by any user, except user identification data stored in the 1st generation tachograph application which may be read by S.VU only

- IDENTIF_WRITE:

All card types: card identification data and user identification data may only be written once and before the end of Personalisation

No user may write or modify identification data during end-usage phase of card life-cycle

- ACTIVITY_WRITE:

All card types: activity data may be written to the TOE 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 the Personalisation is completed and then locked from any future modification or deletion by any user without successful authentication by the party responsible for card initialisation

FDP_ACF.1.3/ AC_SFP SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules **none**.
FDP_ACF.1.4/ AC_SFP SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **SECRET KEYS** **-The TSF shall prevent access to secret cryptographic keys other than for use in the TSF's cryptographic operations, or in case of a workshop card only, for exporting the SensorInstallationSecData to a VU, as specified in [5] Annex 1C, Appendix 2.**

Dependencies: FDP_ACC.1 Subset access control
FDP_MSA.3 Static attribute initialization

7.1.6.3 FDP_DAU.1 Basic Data Authentication

Hierarchical to: No Other component

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

Dependencies: No dependency

7.1.6.4 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other component

FDP_ETC.1.1	The TSF shall enforce the **AC_SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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

Refinement: The certificate is exported without security attribute.

7.1.6.5 FDP_ETC.2: Export of user data with security attributes

Hierarchical to: No other component

FDP_ETC.2.1	The TSF shall enforce the **AC_SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: **none**.

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

Refinement: The User data are exported with a security attribute, which is the signature of the file.

7.1.6.6 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other component

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**.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control],
FMT_MSA.3 Static attribute initialization.

7.1.6.7 FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other component

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 the TOE:

- unauthenticated inputs from external sources shall not be accepted as executable code;
- if application software updates are permitted they shall be verified using cryptographic security attributes before being implemented.

Application note: The TOE will be delivered with no possibility to update the application software. The application is loaded during initialization/pre-perso step.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control],
[FPT_ITC.1 Inter-TSF trusted channel, or
FP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency.

7.1.6.8 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other component

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[deallocation of the resource from]** the following objects: **[Card Private Key].**

Dependencies: No dependency

7.1.6.9 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:

The following data persistently stored by TOE have the user data attribute "**integrity checked stored data**":
Identification data, Activity data, Card private key, Euro public key

FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for **[integrity errors]** on all objects, based on the following attributes: **[integrity checked stored data]**.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall **warn the entity connected.**

Dependencies: No dependency

7.1.7 Class FIA Identification and authentication

7.1.7.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other component

FIA_AFL.1.1 / Card interface GP	The TSF shall detect when **[*3*]** unsuccessful authentication attempts occur related to **[authentication of a card interface device in personalization]**.
FIA_AFL.1.2 / Card interface GP	When the defined number of unsuccessful authentication attempts has been **met** , the TSF shall **:** **warn the entity connected** **block the authentication mechanism** **be able to indicate to subsequent users the reason of the blocking**
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 warn **the entity connected and assume the user as S.Non-VU**
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 **warn the entity connected, block the PIN check procedure such that any subsequent PIN check attempt will fail and be able to indicate to subsequent users the reason of the blocking.**

Dependencies: FIA_UAU.1 Timing of authentication

.

7.1.7.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other component

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users **[** - USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)

- USER_ID (VRN and registering member state for subject S.VU).

Dependencies: No dependency

7.1.7.3 FIA_UAU.1 Timing of authentication

Hierarchical to: No other component

Driver & Workshop Cards

FIA_UAU.1.1 /Gen1	The TSF shall allow **Driver card, workshop card: export of user data with security attributes (digital signature used in card data download function, see in [5] Annex 1C, Appendix 11,Chapter 6 and 14) and export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2** **Control card, company card: export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/Gen1	The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11,Chapter 5** before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.1.1 /Gen2	The TSF shall allow **Driver card, workshop card: export of user data with security attributes (card data download function) and export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2** **Control card, company card: export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/Gen2	The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11,Chapter 10** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification.

7.1.7.4 FIA_UAU.3 Unforgeable authentication

Hierarchical to: No other component

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 user of the TSF.

Dependencies: No dependency

7.1.7.5 FIA_UAU.4 Single-use authentication

Hierarchical to: No other component

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

Dependencies: No dependency

*7.1.7.6 FIA_UID.2 User **authentication before any action***

Hierarchical to: FIA_UID.1Timing of identification

.

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.

Dependencies: No dependency

Note: In the smart card, Identification and authentication are a single process.

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

7.1.7.7 FIA_USB.1 User-subject binding

Hierarchical to: No Other component

FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: - **USER_GROUP (VEHICLE_UNIT for S.VU, NON_VEHICLE_UNIT for S.Non-VU)** **USER_ID (VRN and Registering member state for subject S.VU)**
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**none].**
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[none].**

Dependencies: FIA_ATD.1 User attribute definition

7.1.8 Class FPR Privacy

7.1.8.1 FPR_UNO.1 Unobservability

Hierarchical to: No other component

FPR_UNO.1.1	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**.

Dependencies: no dependency

7.1.9 Class FPT Protection of the TSF

7.1.9.1 FPT_EMS.1 TOE Emanation

Hierarchical to: No other component

FPT_EMS.1.1	The TOE shall not emit [**Side channel current**] in excess of [**State of the art limits**] enabling access to **privates key(s) and session keys** and [**activity data**].
FPT_EMS.1.2	The TOE shall ensure **any users** are unable to use the following interface **smart card circuit contacts** to gain access to **private key(s) and session keys and [activity data]**

Dependencies: No dependency

7.1.9.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other component

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **- Reset** **- power supply cut-off** **- Deviation from the specified values of the power supply** **- Unexpected abortion of the TSF execution due to external or internal events (especially interruption of a transaction before completion)**

Dependencies: No dependency

7.1.9.3 FPT_PHP TSF.3 Resistance to physical attack

Hierarchical to: No other component

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.

Dependencies: No dependency

7.1.9.4 FPT_TDC.1 Inter-TSF TSF basic data consistency

Hierarchical to: No Other component

FPT_ TDC.1.1/Gen1	The TSF shall provide the capability to consistently interpret **secure messaging attributes as defined by [5] Annex 1C, Appendix 11 , Chapter 5** when shared between the TSF and **a vehicle unit**.
FPT_ TDC.1.2/Gen1	The TSF shall **use the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11 Part A, Chapter 5**] when interpreting the TSF data from **a vehicle unit**.

Application note: “Trusted IT product” in FPT_TDC.1/Gen1 refers to generation 1 vehicle units.

FPT_ TDC.1.1/Gen2	The TSF shall provide the capability to consistently interpret **secure messaging attributes as defined by [5] Annex 1C, Appendix 11** when shared between the TSF and a vehicle unit.

FPT_ TDC.1.2/Gen2	The TSF shall use **the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11** when interpreting the TSF data from a vehicle unit.

Dependencies: No dependency

Application note: “Trusted IT product” in FPT_TDC.1/Gen2 refers to generation 2 vehicle units.

7.1.9.5 FPT_TST.1 TSF testing

Hierarchical to: No other component

FPT_TST.1.1	The TSF shall run a suite of self-tests tests **during initial start-up 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**.

Dependencies: No dependency

7.1.10 Class FTP Trusted Path / Channel

7.1.10.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other component

FTP_ITC.1.1/Gen1	The TSF shall provide a communication channel between itself and **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/Gen1	The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3/Gen1	The TSF shall **use** the trusted channel **data import from and export to a vehicle unit in accordance with [6] Appendix 2.**
FTP_ITC.1.1/Gen2	The TSF shall provide a communication channel between itself and 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/Gen2	The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/Gen2	The TSF shall 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.**

.

Dependencies: No dependency

7.2 SECURITY ASSURANCE REQUIREMENTS

The TOE security assurance requirements define the assurance requirements for the TOE using only assurance components drawn from [CCPART3].

The assurance level is **EAL4** augmented on:

ALC_DVS.2: Sufficiency of security measures.

ATE_DPT.2: Testing: Security enforcing modules

AVA_VAN.5: Advanced methodical vulnerability analysis

7.3 SECURITY REQUIREMENTS RATIONALE

The aim of this section is to demonstrate that the combination of the security functional requirements and assurance measures is suitable to satisfy the identified security objectives.

7.3.1 Security Functional Requirements Rationale

The following table shows, which SFRs for the TOE support which security objectives of the TOE. The table shows, that every objective is supported by at least one SFR and that every SFR supports at least one 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_SAA.1	X	X			X		
FAU_ARP.1	X	X			X		
FCO_NRO.1					X		
FCS_CKM.1 / Session GP					X		
FCS_CKM.1 / Session Tacho Gen1					X	X	
FCS_CKM.1 / Session Tacho Gen2					X	X	
FCS_CKM.1 / Card Private Key					X	X	
FCS_CKM.2/ Session Tacho Gen1					X	X	
FCS_CKM.2/ Session Tacho Gen2					X	X	
FCS_CKM.2/ Public Key					X	X	
FCS_CKM.2/ Certificate					X	X	
FCS_CKM.4/ Session GP					X	X	
FCS_CKM.4/ Session Tacho Gen1					X	X	

	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FCS_CKM.4/ Session Tacho Gen2					X	X	
FCS_COP.1/RSA					X	X	
FCS_COP.1/TDES					X	X	
FCS_COP.1 / HASH					X	X	
FCS_COP.1 / HMAC					X	X	
FCS_COP.1 / AES					X	X	
FCS_COP.1 / SHA-2					X	X	
FCS_COP.1 / ECC					X	X	
FCS_COP.1/GP MAC					X	X	
FCS_COP.1/GP ENC					X	X	
FCS_RNG.1					X	X	
FDP_ACC.2 / AC_SFP SFP	X	X	X	X	X		X
FDP_ACF.1 / AC_SFP SFP	X	X	X	X	X		X
FDP_DAU.1					X	X	
FDP_ETC.1					X		
FDP_ETC.2					X		
FDP_ITC.1					X		
FDP_ITC.2							X
FDP_RIP.1			X		X		
FDP_SDI.2	X	X				X	
FIA_AFL.1 /C				X			
FIA_AFL.1 /WC				X			
FIA_AFL.1 /Card Interface GP				X			

	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FIA_ATD.1				X			
FIA_UAU.1 / Gen1				X			
FIA_UAU.1 / Gen2				X			
FIA_UAU.3				X	X	X	
FIA_UAU.4					X	X	
FIA_UID.2				X			
FIA_USB.1				X			
FPR_UNO.1			X		X		
FPT_EMS.1	X	X	X	X			
FPT_FLS.1	X	X		X			
FPT_PHP.3	X	X	X	X			X
FPT_TDC.1 /Gen1					X		
FPT_TDC.1 /Gen2					X		
FPT_TST.1	X	X		X	X		
FTP_ITC.1 /Gen1					X		
FTP_ITC.1 /Gen2					X		

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

Security Objective	SFR	Rationale
O.Card_Identification_Data	FAU_ARP.1 FAU_SAA.1	In the case of a detected integrity error the TOE will indicate the corresponding violation.
	FDP_ACC.2 FDP_ACF.1	Access to TSF data, especially to the identification data, is regulated by the security function policy defined in the components FDP_ACC.2 and FDP_ACF.1, which explicitly denies write access to personalised identification data.
	FDP_SDI.2	Integrity of the stored data within the TOE, specifically the integrity of the identification data, is required by this component.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of identification data.
	FPT_FLS.1	Requires that any failure state should not expose identification data, or compromise its integrity.
	FPT_PHP.3	Requires the TOE to resist attempts to access identification data through manipulation or physical probing.
	FPT_TST.1	Requires tests to be carried out to assure that the integrity of the identification data has not been compromised.

Security Objective	SFR	Rationale
O.Card_Activity_Storage	FAU_ARP.1 FAU_SAA.1	In the case of a detected integrity error the TOE will indicate the corresponding violation.
	FDP_ACC.2 FDP_ACF.1	Access to card activity data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorised vehicle units.
	FDP_SDI.2	Integrity of the stored data within the TOE, specifically the integrity of the identification data, is required by this component.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of card activity data.
	FPT_FLS.1	Requires that any failure state should not expose card activity data, or compromise its integrity.
	FPT_PHP.3	Requires the TOE to resist attempts to access card activity data through manipulation or physical probing.
	FPT_TST.1	Requires tests to be carried out to assure that the integrity of the card activity data has not been compromised.

Security Objective	SFR	Rationale
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.

Security Objective	SFR	Rationale
O.Data_Access	FDP_ACC.2 FDP_ACF.1	Access to user data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorised vehicle units.
	FIA_AFL.1/C FIA_AFL.1/WC FIA_AFL.1/Card Interface GP	These components require that if authentication fails the TOE reacts with a warning to the connected entity, and the user is assumed not to be an authorised vehicle unit or the administrator during personalization operation.
	FIA_ATD.1 FIA_USB.1	The definition of user security attributes supplies a distinction between vehicle units and other card interface devices.
	FIA_UAU.1 Gen1 FIA_UAU.1 /Gen2 FIA_UID.2	These requirements ensure that write access to user data is not possible without a preceding successful authentication process.
	FIA.UAU.3	Prevents the use of forged credentials during the authentication process.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the authentication process.
	FPT_FLS.1	Requires that any failure state should not allow unauthorised write access to the card.
	FPT_PHP.3	Requires the TOE to resist attempts to interfere with authentication through manipulation or physical probing.
	FPT_TST.1	Requires that tests be carried out to assure that the integrity of the TSF and identification data has not been compromised.

Security Objective	SFR	Rationale
O.Secure_Communications	FAU_ARP.1 FAU_SAA.1	During data exchange, upon detection of an integrity error of the imported data, the TOE will indicate the corresponding violation and will provide a warning to the entity sending the data.
	FDP_ACC.2 FDP_ACF.1	The necessity for the use of a secure communication protocol as well as the access to the relevant card´s keys are defined within these requirements.
	FDP_ETC.1 FDP_ITC.1 FTP_ITC.1 /Gen1 FTP_ITC.1 /Gen2	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.
	FCS_CKM.1(all) FCS_CKM.2(all) FCS_CKM.4(all) 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 /Gen1 FPT_TDC.1 /Gen2	Requires a consistent interpretation of the security related data shared between the TOE and the card interface device.

Security Objective	SFR	Rationale
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(all) FCS_CKM.2(all) FCS_CKM.4(all) 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.

Security Objective	SFR	Rationale
O.Software_Update	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.

7.3.2 Dependencies

7.3.2.1 SFRs dependencies

Requirements	CC dependencies	Satisfied dependencies
FAU_SAA.1	FAU_GEN.1	justification 1 for non-satisfied dependencies
FAU_ARP.1	None	
FCO_NRO.1	FIA_UID.1	Card reset
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4	FCS_COP1, FCS_CKM.4
FCS_CKM.2	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2	FCS_CKM.1
FCS_COP.1/RSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	justification 2 for non-satisfied dependencies
FCS_COP.1/HASH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FDP_ITC.1, FCS_CKM.4
FCS_COP.1/TDES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/AES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/SHA-2	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/ECC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	justification 2 for non-satisfied dependencies
FCS_COP.1/HMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/GP MAC	(FCS_CKM.1 or FDP_ITC.1 or	FCS_CKM.1, FCS_CKM.4

Requirements	CC dependencies	Satisfied dependencies
	FDP_ITC.2), FCS_CKM.4	
FCS_COP.1/GP ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_RNG.1	None	
FDP_ACC.2/AC_SFP SFP	FDP_ACF.1	FDP_ACF.1/AC_SFP SFP
FDP_ACF.1/AC_SFP SFP	FDP_ACC.1. FMT_MSA.3	FDP_ACC.1/AC_SFP SFP, justification 3 for non-satisfied dependencies
FDP_DAU.1	none	
FDP_ETC.1	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/AC_SFP SFP
FDP_ETC.2	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/AC_SFP SFP
FDP_ITC.1	(FDP_ACC.1 or FDP_IFC.1), FMT_MSA.3	FDP_ACC.2/AC_SFP SFP, justification 3 for non-satisfied dependencies
FDP_ITC.2	(FDP_ACC.1 or FDP_IFC.1), (FPT_ITC.1 or FTP_TRP.1) FPT_TDC.1	FDP_ACC.2/AC_SFP SFP, FDP_ITC.1, FPT_TDC.1
FDP_RIP.1	none	
FDP_SDI.2	none	
FIA_AFL.1 / Card interface GP	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1 / C	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1 / WC	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	none	
FIA_UAU.1 /Gen1 FIA_UAU.1 /Gen2	FIA_UID.1	FIA_UID.1
FIA_UAU.3	none	
FIA_UAU.4	none	
FIA_UID.2	none	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FPR_UNO.1	none	
FPT_EMS.1	none	
FPT_FLS.1	none	
FPT_PHP.3	none	
FPT_TDC.1	none	
FPT_TST.1	none	

Requirements	CC dependencies	Satisfied dependencies
FTP_ITC.1 /Gen1 FTP_ITC.1 /Gen2	none	

Justification for non-satisfied dependencies:

No.1: The dependency FAU_GEN.1 (Audit Data Generation) is not applicable to the TOE. Tachograph cards do not generate an audit record but reacts with an error response. The detection of failure events implicitly covered in FAU_SAA.1 is clarified by a related refinement of the SFR.

No.2: The SFR FCS_COP.1/RSA and FCS_COP.1/ECC uses keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1/RSA and FCS_COP.1/ECC.

No.3: The access control TSF according to FDP_ACC

uses security attributes which are defined during the Personalisation Phase and are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, neither during the personalisation nor within the usage phase of the TOE. This argument holds for FDP_ACF.1 as well as for FDP_ITC.1.

7.3.2.2 Assurance measures rationale

EAL4 was chosen for this application as specified in [5] Appendix 10.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the Tachograph's development and manufacturing especially for the secure handling of the Tachograph material.

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

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives O.Protect_Secret and O.Card_Activity_Storage.

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

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL4)		
ALC_DVS.2	no dependencies	
ATE_DPT.2	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1	ADV_ARC.1 ADV_TDS.4 ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.4
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.3

7.4 COMPATIBILITY BETWEEN SFR OF [ST] AND [ST-IC]

FAU_SAA.1, FAU_ARP.1, FCO_NRO.1, FCS_CKM.2/ Session Tacho Gen1, FCS_CKM.2/ Session Tacho Gen2, FCS_CKM.2/ Public Key, FCS_CKM.2/ Certificate, FCS_CKM.4/ Session GP, FCS_CKM.4/ Session Tacho Gen1, FCS_CKM.4/ Session Tacho Gen2, FDP_ACC.2 / AC_SFP SFP,FDP_ACF.1 / AC_SFP SFP,FDP_DAU.1, FDP_ETC.1, FDP_ETC.2, FDP_ITC.1, FDP_ITC.2, FDP_RIP.1, FIA_AFL.1 /C, FIA_AFL.1 /WC, FIA_AFL.1 Card Interface GP, FIA_ATD.1, FIA_UAU.1 / Gen1, FIA_UAU.1 / Gen2, FIA_UAU.3, FIA_UAU.4, FIA_UID.2, FIA_USB.1, FPR_UNO.1, FPT_FLS.1 , FPT_TDC.1 /Gen1, FPT_TDC.1 /Gen2, FTP_ITC.1 /Gen1, FTP_ITC.1 /Gen2 are SFR specific to this security target and they do no conflict with the SFR of [ST-IC].

FCS_CKM.1, FCS_COP.1 and FCS_RNG.1 of this Security Target are supported by FCS_CKM.1, FCS_COP.1 and FCS_RNG.1 of [ST-IC].

FDP_SDI.2 of this Security Target is supported by FDP_SDI.1 and FDP_SDI.2 of [ST-IC].

FPT_PHP.3 of this Security Target is supported by FPT_PHP.3 of [ST-IC].

FPT_TST.1 of this Security Target is supported by FPT_TST.1 of [ST-IC].

We can therefore conclude that the SFR of [ST-JCS] and [ST-IC] are consistent.

8 TOE SUMMARY SPECIFICATION

The security functionalities provided by the IC are described in [ST-IC]. The TOE Security Functionalities are described below.

8.1 TOE SECURITY FUNCTIONALITIES : BASIC

SF.TEST Self-test

The TSF performs the following tests:

When starting a work session,

working condition of the work memory (RAM),

integrity of code in EEPROM,

Dependencies: SF.INTEGRITY

SF.EXCEPTION Error Messages and exceptions

The TOE reports the following errors:

- Message format errors,
- Integrity errors,
- Life cycle status errors,
- Errors in authentication attempt.

The card becomes mute (secure Fail State) when one of the following errors occurs:

- Error on integrity of keys or PINs,
- Out of range in frequency or voltage,
- Life cycle status errors,

Dependencies: SF.DRIVER

SF.ERASE Data erasure

The whole RAM is erased after reset.

When a new mutual authentication is performed, the former session key set is destroyed without any possibility of even partial recovery.

Dependencies: No dependency

SF.INTEGRITY Data Integrity

The function provides the ability to check the integrity of the following data elements stored in the card:

Cryptographic keys including card private key, Euro public key and corresponding attributes,

Authentication data including PIN and corresponding attributes,

Data contained in the File System, including Identification data, Activity data.

Dependencies: No dependency

SF.HIDE Data and operation hiding

The TOE hides sensitive data transfers and operations from outside observations.

The TOE is protected against SPA, DPA, DFA & timing attacks

Dependencies: No dependency

SF.CARD_MGR Card manager (CM)

This function controls the execution of the card internal process when command messages are sent to the card. The messages handled are defined as specified in ISO 7816. Controls include:

CM Format verification

- Identification: the instruction code of the message is supported,
- Format analysis: the class is consistent with the instruction code, P1/P2/P3 parameter values are supported by the identified command.

CM Access checking

- Life cycle analysis: the identified command shall be enabled in the current TOE life cycle phase of the TOE.
- Check that the command sequence is respected,
- Check that the authenticated user is allowed to send the command.

CM Execution

- Execution: activation of the executable code corresponding to the card internal process for the command message.

CM Response

- Control the build-up of the response.

Dependencies: SF.ACC

8.2 TOE SECURITY FUNCTIONALITIES : CRYPTOGRAPHIC

SF.KEY_GEN Key generation

- The TOE can generate the Card private/public key pair in personalization phase:
  - , RSA 1024 bits for Tacho Gen1 application
  - ECC for Tacho Gen2 application
- For Tacho Gen1 the TOE generates Session keys, using TDES with 2 keys, in usage phase. The generation process includes the distribution to the remote IT.
- For Tacho Gen2 the TOE generates Session keys based on AES symmetric cryptography, in usage phase. The generation process includes the distribution to the remote IT.

Dependencies: No dependency

SF.SIG Signature creation and verification

- The TOE can sign a message digest, which is the result of a hash operation performed on a Tachograph data file, stored in the TOE. This hashing is performed by SF.HASH and the result is stored in the card.
- The TOE can verify the signature of a message imported into the card.
- For Tacho Gen1,the TOE uses a RSA PKCS#1 signature scheme with a 1024 bit modulus, as defined in [RSA-PKCS#1].
- For Tacho Gen2, the TOE uses the signature scheme algorithm ECDSA as specified in [DSS].

Dependencies: SF.KEY_GEN, SF.HASH

SF.ENC Encryption and decryption

- The TOE encrypts and decrypts messages.
- For Tacho Gen1, the encryption uses TDES with 2 keys, in CBC mode according to [SP800-67] and [SP800-38 A].
- For Tacho Gen2, the encryption uses AES algorithm according to [AES].

Dependencies: SF.KEY_GEN

SF.HASH Message hashing

- The TOE can generate a hash of a file stored in the card.
- For Tacho Gen1, hashing is done using SHA-1 algorithm as specified in [FIPS180-4].
- For Tacho Gen2, hashing is done using SHA-2 algorithm as specified in [FIPS180-4]

Dependencies: No dependency

SF.MAC MAC generation and verification

- The TOE generates and verifies the MAC of messages.
- For Tacho Gen1, MAC computation uses TDES with 2 keys, in CBC mode according to [SP800-67] and [SP800-38 A].
- For Tacho Gen2, MAC computation uses AES algorithm according to [AES].

Dependencies: SF.KEY_GEN

SF.TRUSTED Trusted Path

This function establishes a secure channel, using a mutual authentication mechanism.

The secure channel is GP in Personalization phase.

In usage phase the secure channel is done with TDES session keys with Tacho Gen1 or AES session keys with Tacho Gen2.

In GP, a ratification counter limits the number of failed consecutive authentication attempts. The counter initial value is 3. When the authentication fails, the counter is decremented. When the authentication succeeds, the counter is set to its initial value. The authentication mechanism is blocked and cannot be used any longer if the counter reaches zero.

When the secure channel is established, the messages may be MACed and Encrypted, depending on the function performed. The imported keys are encrypted.

Dependencies: SF.HASH, SF.MAC, SF.ENC

SF.PIN PIN management

This SF controls all the operation relative to the PIN management, including the Cardholder authentication:

- PIN creation: the PIN is stored and is associated to a maximum presentation number.
- PIN verification: the PIN can be accessed only if its format and integrity are correct. After 5 consecutive unsuccessful verification of the PIN, it is blocked. When the PIN is blocked, then it cannot be used anymore.

Dependencies: No dependency

8.3 TOE SECURITY FUNCTIONALITIES: CARD MANAGEMENT

SF.ACC Access Authorization

The function controls the access conditions of a file.

This SF puts the access conditions on a file when it is created. It checks that the AC are met before accessing a file in the card.

This SF maintains the roles of the user.

This SF also maintains the security attributes USER_GROUP and USER_ID.

Dependencies: No dependency

SF.DOMAIN Domain Separation

This SF maintains the Security Domains.

It ensures that the Tachograph application has its own security environment, separate from the security environment of the OS.

RSA/ECC keys have their own RAM space.

Dependencies: No dependency

8.4 TOE SECURITY FUNCTIONALITIES: PHYSICAL MONITORING

SF.DRIVER Chip driver

This function ensures the management of the chip security features:

- Enforce shield protection,
- physical integrity of the IC,
- physical environment parameters,

Dependencies: No dependency

SF.ROLLBACK Safe fail state recovery

The function shall ensure that the TOE returns to its previous secure state when following events occur.

- power cut-off or variations,
- unexpected reset

Dependencies: SF.DRIVER

8.5 TOE SUMMARY SPECIFICATION RATIONALE

This section demonstrates that TOE security functions are suitable to meet the functional requirements. Table below shows that each TOE functional requirement is mapped to at least one TOE security function.

Security functions/ Security requirements	SF.TEST	SF.EXCEPTION	SF.ERASE	SF.INTEGRITY	SF.HIDE	SF.CARD_MGR	SF.KEY_GEN	SF.SIG	SF.ENC	SF.HASH	SF.MAC	SF.TRUSTED	SF.PIN	SF.ACC	SF.DOMAIN	SF.DRIVER	SF.ROLLBACK	SF.RND
FAU_SAA.1	X			X								X	X					
FAU_ARP.1	X			X								X	X					
FCO_NRO.1								X			X							
FCS_CKM.1 / Session GP							X											
FCS_CKM.1 / Session Tacho Gen1							X											
FCS_CKM.1 / Session Tacho Gen2							X											
FCS_CKM.1 / Card private key							X											
FCS_CKM.2 / Session Tacho Gen1							X											
FCS_CKM.2 / Session Tacho Gen2							X											
FCS_CKM.2 / Public key							X											
FCS_CKM.2 / Certificate						X												
FCS_CKM.4 / Session GP			X															
FCS_CKM.4 / Session Tacho Gen1			X															
FCS_CKM.4 / Session Tacho Gen2			X															
FCS_COP.1 / RSA								X										
FCS_COP.1 / HASH										X								
FCS_COP.1 / HMAC								X										
FCS_COP.1 / TDES									X		X							
FCS_COP.1 / AES									X		X							
FCS_COP.1 / SHA-2										X								
FCS_COP.1 / ECC								X										
FCS_COP.1 / GP MAC											X							
FCS_COP.1 / GP ENC									X									
FCS_RNG.1																		X
FDP_ACC.2 / AC_SFP SFP	X					X								X				
FDP_ACF.1 / AC_SFP SFP	X					X								X				
FDP_DAU.1				X				X		X								
FDP_ETC.1						X					X			X				
FDP_ETC.2						X					X			X				
FDP_ITC.1						X					X			X				
FDP_ITC.2						X		X						X				
FDP_RIP.1					X										X			
FDP_SDI.2		X		X														

Security functions/ Security requirements	SF.TEST	SF.EXCEPTION	SF.ERASE	SF.INTEGRITY	SF.HIDE	SF.CARD_MGR	SF.KEY_GEN	SF.SIG	SF.ENC	SF.HASH	SF.MAC	SF.TRUSTED	SF.PIN	SF.ACC	SF.DOMAIN	SF.DRIVER	SF.ROLLBACK	SF.RND
FIA_AFL.1 / Card interface GP		X																
FIA_AFL.1 / C		X																
FIA_AFL.1 / WC		X											X					
FIA_ATD.1														X				
FIA_UAU.1 / Gen1						X						X						
FIA_UAU.1 / Gen2						X						X						
FIA_UAU.3												X						
FIA_UAU.4												X						
FIA_UID.2						X						X						
FIA_USB.1														X				
FPR_UNO.1					X													
FPT_EMS.1					X													
FPT_FLS.1																	X	
FPT_PHP.3		X														X		
FPT_TDC.1/Gen1									X									
FPT_TDC.1/Gen2									X									
FPT_TST.1	X																	
FTP_ITC. 1/Gen1						X			X		X	X						
FTP_ITC. 1/Gen2						X			X		X	X						

Table 4- Security functionalities versus security requirements

8.6 COMPOSITION RATIONALE

This section shows the compatibility between the elements defined in the security target of the IC [ST-IC] and that of the under-evaluation TOE (platform and tachograph application).

There is no inconsistency between the threats defined in the security target of the IC [ST-IC] and the threats defined for the platform.

There is no inconsistency between the OSP defined in [ST-IC] and the OSP defined for the platform.

There is no inconsistency between the security objectives (for the TOE) defined in [ST-IC] and that defined for the platform.

There is no inconsistency between the TOE security requirements for the IC and that for the platform.

The dependencies between the IC security functions and the TOE security functions has described below.

SF [ST-IC] / SF TACHO	SF.PS	SF.PMA	SF.PLA	SF_CS	SF.DPM
SF.TEST	X	X			X
SF.EXCEPTION			X		
SF.ERASE					
SF.INTEGRITY					
SF.HIDE	X		X		
SF.CARD_MGR					
SF.KEY_GEN				X	
SF.SIG				X	
SF.ENC				X	
SF.HASH				X	
SF.MAC				X	
SF.RND				X	
SF.TRUSTED				X	
SF.PIN					
SF.ACC					
SF.DOMAIN					
SF.DRIVER		X			
SF.ROLLBACK					

Table 5. TOE Security Functionalities /IC Security function dependencies