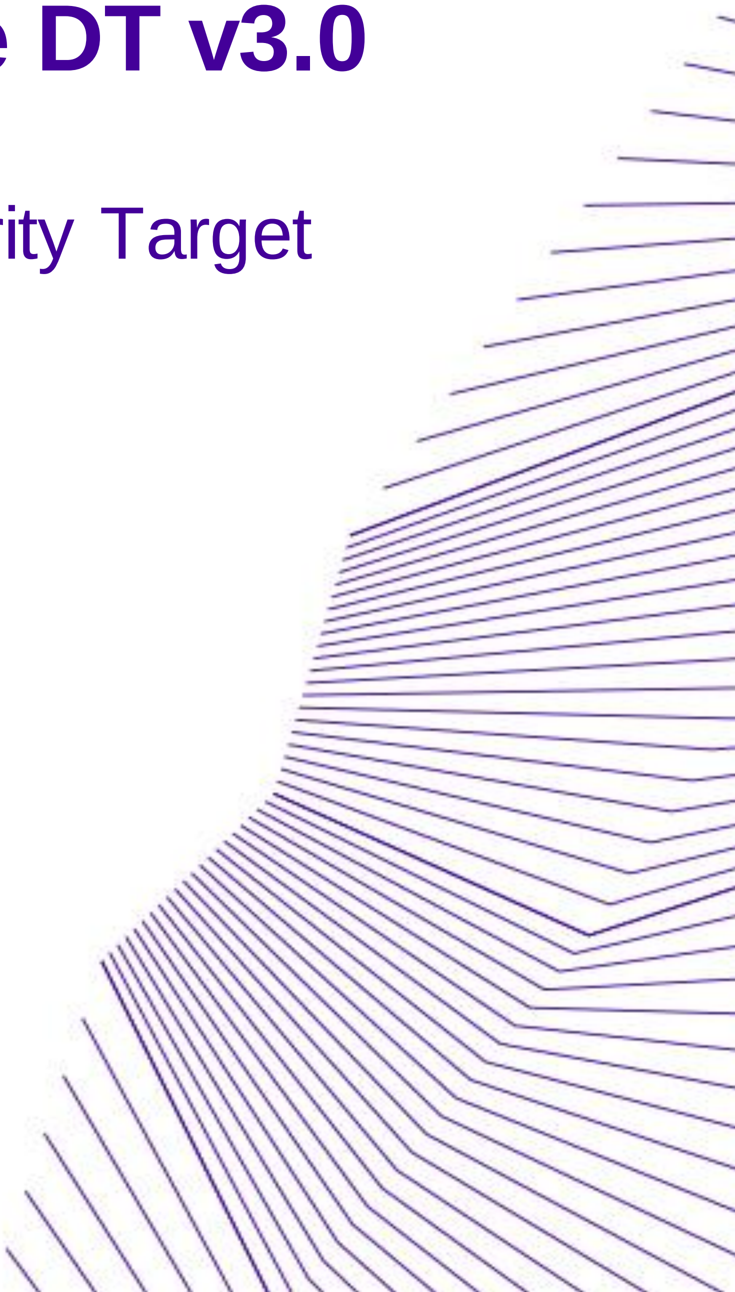
IDeal Drive DT v3.0

Public Security Target



About IDEMIA

OT-Morpho is now IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to empower citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). This new company counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.

| For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

Specif ications and inf ormation are subject to change without notice.

The products described in this document are subject to continuous dev elopment and improv ement.

All trademarks and serv ice marks ref erred to herein, whether registered or not in specif ic countries, are the properties of their respectiv e owners.

- Printed versions of this document are uncontrolled -

DOCUMENT MANAGEMENT

Business Unit – Department	CI – R&D
Document type	FQR
Document Title	IDeal Drive DT v3.0 – Public Security Target
FQR No	550 0046
FQR Issue	1

DOCUMENT REVISION

Date	Revision	Modification
2019/11/14	1	Creation of the document

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 Security Target Introduction

1.1 ST Identification

Title	IDeal Drive DT v3.0 – Public Security Target
ST Identification	FQR 550 0046 Ed 1
CC Version	3.1 Revision 5
Assurance Level	EAL4+ (augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2)
ITSEF	Brightsight
Certification Body	TÜV Rheinland Nederland B.V.
Compliant To Protection Profiles	**[PP-TACHOGRAPH_GEN1], [PP-TACHOGRAPH_GEN2]**
PP References	BSI-CC-PP-0070 BSI-CC-PP-0091
PP Versions	V1.02 for BSI-CC-PP-0070 V1.0 for BSI-CC-PP-0091

1.2 TOE Reference

TOE Commercial Name	IDeal Drive DT V3.0
Applet Code Version (SAAAAR Code)	416304
Guidance Documents	**AGD_OPE [Applet], AGD_PRE [Applet], AGD_PRE [JOP], AGD_OPE [JOP], [SEC_ACCPT], [SEC_REC], [LOAD_GUIDE], [PLT_API]**
Platform Name	ID-ONE COSMO V9 ESSENTIAL
Platform Certificate	CC-18-200833
IC Identifier	CC Identifier: IFX_CCI_000005, IFX_CCI_000008 and IFX_CCI_000014
IC Certificate	BSI-DSZ-CC-0945-V2-2018

2 Technical Terms, Abbreviations and Associated References

2.1 Technical Terms

Term	Definition
Application note	*Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.*
Administrator	*user who performs TOE initialization, TOE personalization, or other TOE administrative functions*
Authentication data	*information used to verify the claimed identity of a user*
Authentication	*Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.*
ECC	*(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.*
Integrity	*The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.*
Java Card	*A smart card with a Java Card operation system.*
MAC	*Message Authentication Code. Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy requires its protection in a suitable way.*
Non repudiation	*One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.*
Public Key	*Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.*

Term	Definition
Random numbers	*Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for software), so called pseudo random numbers are used instead.*
Reference authentication data (RAD)	*Data persistently stored by the TOE for authentication of a user as uthorized for a particular role.*
Secure messaging	*Secure messaging using encryption and message authentication code ac-cording to ISO/IEC 7816-4.*
Signature creation data (SCD)	*private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature*
Signature verification data (SVD)	*public cryptographic key that can be used to verify an electronic signature*
Smart card	*A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (FLASH) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). There-fore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.*
User	*entity (human user or external IT entity) outside the TOE that interacts with the TOE*
Verification authentication data (VAD)	*data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics*
Activity data	*Activity data include cardholder activities data, events and faults data and control activity data*
Card identification data	*User data related to card identification as defined by requirements 190, 191, 192, 194, 215, 231 and 235*
Cardholder activities data	*User data related to the activities carried by the cardholder as defined by requirements 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 and 237*
Cardholder identification data	*User data related to cardholder identification as defined by requirements 195, 196, 216, 232 and 236*
Control activity data	*User data related to law enforcement controls as defined by requirements 210 and 225*

Term	**Definition**
Digital Tachograph	*Recording equipment*
Events and faults data	*User data related to events or faults as defined by requirements 204, 205, 207, 208 and 223*
Identification data	*Identification data include card identification data and cardholder identification data*
JOP	*Java Card Open Platform, certified in accordance with a Java Card protection profile*

2.2 Abbreviations

Acronym	Definition
ST	*Security Target*
PP	*Protection Profile*
TOE	*Target Of Evaluation*
EAL	*Evaluation Assurance Level*
TSF	*TOE security functionality*
VU	*Vehicle Unit*
IC	*Integrated Circuit*
OS	*Operating System*
OSP	*Organizational Security Policy*
SCD	*Signature creation data*
SVD	*Signature verification data*
RAD	*Reference authentication data*
VAD	*Verification authentication data*
DTBS	*Data to be signed*
IDD	*Identification data*
ACD	*Activity data*
APP	*Application*
KPD	*Keys to protect data*
EOL	*End Of Life*
SPA	*Simple Power Analysis*
DPA	*Differential Power Analysis*
PIN	*Personal Identification Number*
PUK	*PIN Unblocked Key*
RNG	*Random Number Generation*
SAR	*Security Assurance Requirements*
SF	*Security Function*
SFP	*Security function policy*
CPS	*Common Personalization System*

JOP	*Java Card Open Platform*
IFD	*Interface Device*

2.3 References

Ref.	Document title
[CC1]	Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1 – Revision 5, April 2017
[CC2]	Common Criteria for information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2017-04-002, Version 3.1 – Revision 5, April 2017
[CC3]	Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2017-04-003, Version 3.1 – Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[EU – 2016/799]	Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components
[EU – 2018/502]	Commission Implementing Regulation (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components
[EU – 1360/2002]	Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002, Annex 1B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)
[PP-TACHOGRAPH_GEN1]	Digital Tachograph– Smart card (Tachograph Card) pp0070b, Version 1.02, 15 November 2011
[PP-TACHOGRAPH_GEN2]	Digital Tachograph– Smart card (Tachograph Card) pp0091b, Version 1.0, 9 May 2017
[PP –IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014

Ref.	Document title
[ST-PL]	FQR 110 8959 Ed 3.0 – ID One Cosmo V9 Essential Public ST
[PP-JAVACARD]	Java Card Protection Profile – Open Configuration Version 3.0 May 2012 ANSSI-CC-PP-2010/03_M01
AGD_PRE [Applet]	FQR 401 7997 Ed 7 – AGD_PRE
AGD_OPE [Applet]	FQR 401 7909 Ed 4 – AGD_OPE
AGD_PRE [JOP]	ID-One COSMO V9 Essential Pre-Perso Guide FQR 110 8797 Ed5 – 22/10/2018
AGD_OPE [JOP]	ID-One COSMO V9 Essential Reference Guide FQR 110 8823 Ed5 – 22/10/2018
[SEC_REC]	Applet Security Recommendations FQR 110 8794 Ed4
[JIL-1]	Application of Attack Potential to Smartcards v3.0 – JIL document – April 2019
[JIL -2]	Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[CR-IC]	BSI Certification Report BSI-DSZ-CC-0945-V2-2018
[JCRE]	"Java Card – RE" Runtime Environment Specification, Classic Edition Version 3.0.5, June 2015, Oracle Technology Network.
[JCVM]	"Java Card – VM" Virtual Machine Specification, Classic Edition Version 3.0.5, June 2015, Oracle Technology Network.
[JCAPI]	"Java Card – API" Application Programming Interfaces, Classic Edition Version 3.0.5, June 2015, Oracle Technology Network.
[RNG-NIST]	The NIST SP 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revise) March 2007
[RNG-CLASS]	A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-Systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011
[JIL-3]	JIL-Certification-of-Open-Smart-Card-Products-v1.1-(for_trial_use), Version 1.1, 4 February 2013
[ADV_ARC]	FQR 401 7906 Ed 3 – ADV_ARC
[PGD]	416304 00 PGD AA
[SEC_ACCPT]	FQR 110 8921 Ed1 – 24/09/2018 - Secure acceptance and delivery of sensitive elements
[LOAD_GUIDE]	ID-One COSMO V9 Essential Application Loading Protection Guidance FQR 110 8798 Ed2 – 24/09/2018
[PLT_API]	FQR 110 8827 Ed1- 23/04/2018 - Java Card API on ID-One Cosmo V9 platform

3 Target Of Evaluation Overview

3.1 TOE objective

The TOE, IDeal Drive DT v3.0, is the solution for Digital Tachograph first generation compliant to the Commission regulation [EU – 1360/2002] and second generation compliant to the European Union regulation 2014/165 and its Commision implementation **[EU – 2016/799]** amended by **[EU – 2018/502].**

The TOE can be used in a recording equipment (or Vehicle Unit) of both Generation 1 as well as Generation 2 VUs.

The TOE supports a single Tachograph Applet that provides both Generation 1 and Generation 2 functionalities with two configurations:

1. Configuration 1: Supporting Generation 1 only functionalities (compliant to **[PP-TACHOGRAPH_GEN1]**).

2. Configuration 2: Supporting both Generation 1 and Generation 2 functionalities (compliant to **[PP-TACHOGRAPH_GEN2]**).

The TOE can be one of defined card, i.e. Driver, Company, Workshop and Controller. The Tachograph card type is set during the personalization phase. The TOE is an Integrated Circuit and its embedded software. The TOE can be delivered under different form factor like wafer, micro-module or smartcard. The embedded software is composed of a Tachograph Java Card applet on top of a Java Card Operating system, ID-One Cosmo v9.0 Essential.

The main objectives of this ST are:

- To describe the TOE as a smartcard product for the tachograph system
- To define the TOE's limit
- To describe the assumptions, threats and security objectives for the TOE
- To describe the security requirements for the TOE
- To define the TOE security functions

3.1.1 Logical scope

The TOE is based on Java Card Open Platform.

The tachograph applet fulfils the recommendations indicated in the guidance documentation of the Java Card Open Platform (**AGD_PRE [JOP], AGD_OPE [JOP], [LOAD_GUIDE], [SEC_ACCPT], [PLT_API] and [SEC_REC]**).

The logical scope of the TOE may be depicted as follows:

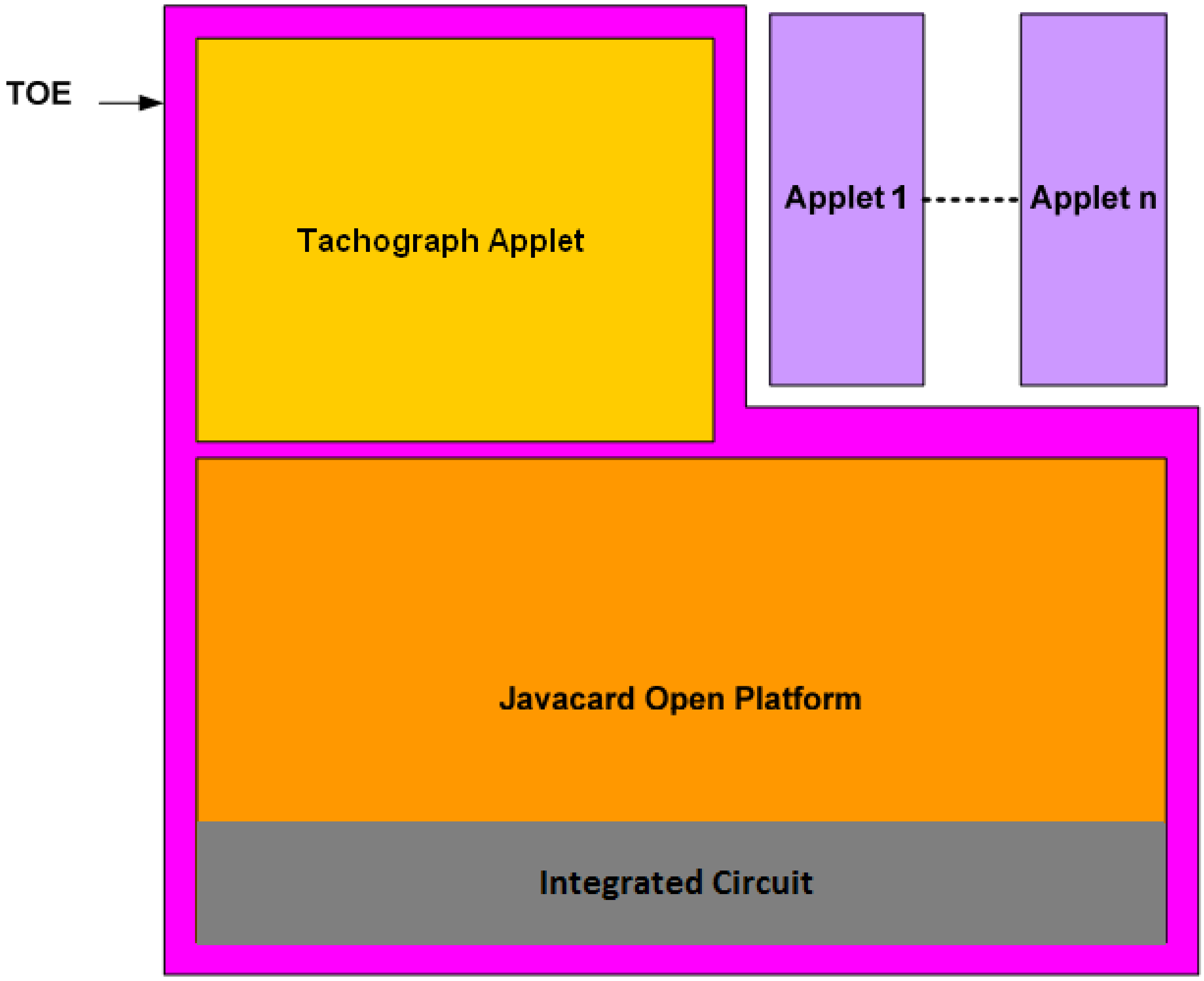


Figure 1: TOE Architecture

3.1.2 Open and isolating Platform

This security target claims conformance to the **[JIL-3]**:

TOE supports "open platform" which can host new applications:

- Before its delivery to the end user (during phases 4, 5 or 6 of the traditional smartcard lifecycle). Such loadings are called "pre-issuance".
- After its delivery to the end user (phase 7). Such loadings are called "post-issuance" and any applet can be loaded at this step.

An "isolating platform" is a platform that maintains the separation of the execution domains of all embedded applications on a platform, as of the platform itself. "Isolation" refers here to domain separation of applications as well as protection of application's data.

3.1.3 Physical scope

The TOE is made of the following part:

- The IC reference is as below:

CC ID
IFX_CCI_000005 IFX_CCI_000008 IFX_CCI_000014

- The Platform is ID-One COSMO V9 Essential
- The Tachograph Applet is IDeal Drive DT V3.0

The following guidance documents will be provided for the TOE:

Description	Audience	Form Factor of Delivery
AGD_PRE [Applet]	Personalising Agent	Electronic Version
AGD_OPE [Applet]	End user of the TOE	
AGD_PRE [JOP]	Prepersonalisation	
AGD_OPE [JOP]	Application Developer	
[LOAD_GUIDE]	Issuer of the platform that aims to load applications	
[SEC_REC]	Developer of Sensitive Applications	
[SEC_ACCPT]	Chip Manufacturer Third party Production sites	
[PLT_API]	Application Developer	

This ST Lite version of the Security Target also serves as a guidance document along with above mentioned documents.

All the above mentioned guidance documents will be delivered via mail in a .pgp encrypted format.

Form factor and Delivery Preparation:
1. As per the Software Development Process of IDEMIA, upon completion of development activities, particular applet will be uploaded into CPS in CAP file format. Before uploading, the applet will be verified through Oracle verifier and IDEMIA verifier.
2. During Release for Sample as project milestone, status of the applet in CPS will be changed into "Pilot version" to be used further for manufacturing samples.
3. During Software Delivery Review as the final R&D project milestone, status of the applet in CPS will be changed into "Industrial release" to be used further for mass production.

Refer Life Cycle chapter of this ST for more details regarding TOE delivery as per different options.

3.1.3.1 Physical overview

Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.

3.1.4 Required non-TOE hardware/software/firmware

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

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

3.1.5 Usage and major security features of the TOE

The main security features of the TOE are as follows:

a) The TOE must preserve card identification data and user identification data stored during the card personalisation process;

b) The TOE must preserve user data stored in the card by Vehicle Units

c) The TOE must allow certain write operations onto the cards to only an authenticated VU.

Specifically the Tachograph Card aims to protect:

a) The data that is stored in such a way as to prevent unauthorised access to and manipulation of the data, and to detect any such attempts;

b) The integrity and authenticity of data exchanged between the recording equipment and the Tachograph Card.

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

a) User identification and authentication;

b) Access control to functions and stored data;

c) Alerting of events and faults;

d) Integrity of stored data;

e) Reliability of services;

f) Data exchange with a Vehicle Unit and export of data to other IT entities;

g) Cryptographic support for VU-card mutual authentication and secure messaging as well as for key generation and key agreement according to **[EU – 2016/799]** Annex 1C, Appendix 11.

Depending on the use case and on the ability of the underlying Java Card open platform, this embedded software may be used

- in contact mode (T=0 and/or T=1 protocol)

4 Life cycle

With respect to the smartcard life-cycle, divided in 7 phases and according to the IC protection profile **[PP -IC]**, the TOE life cycle is divided in seven different phases.

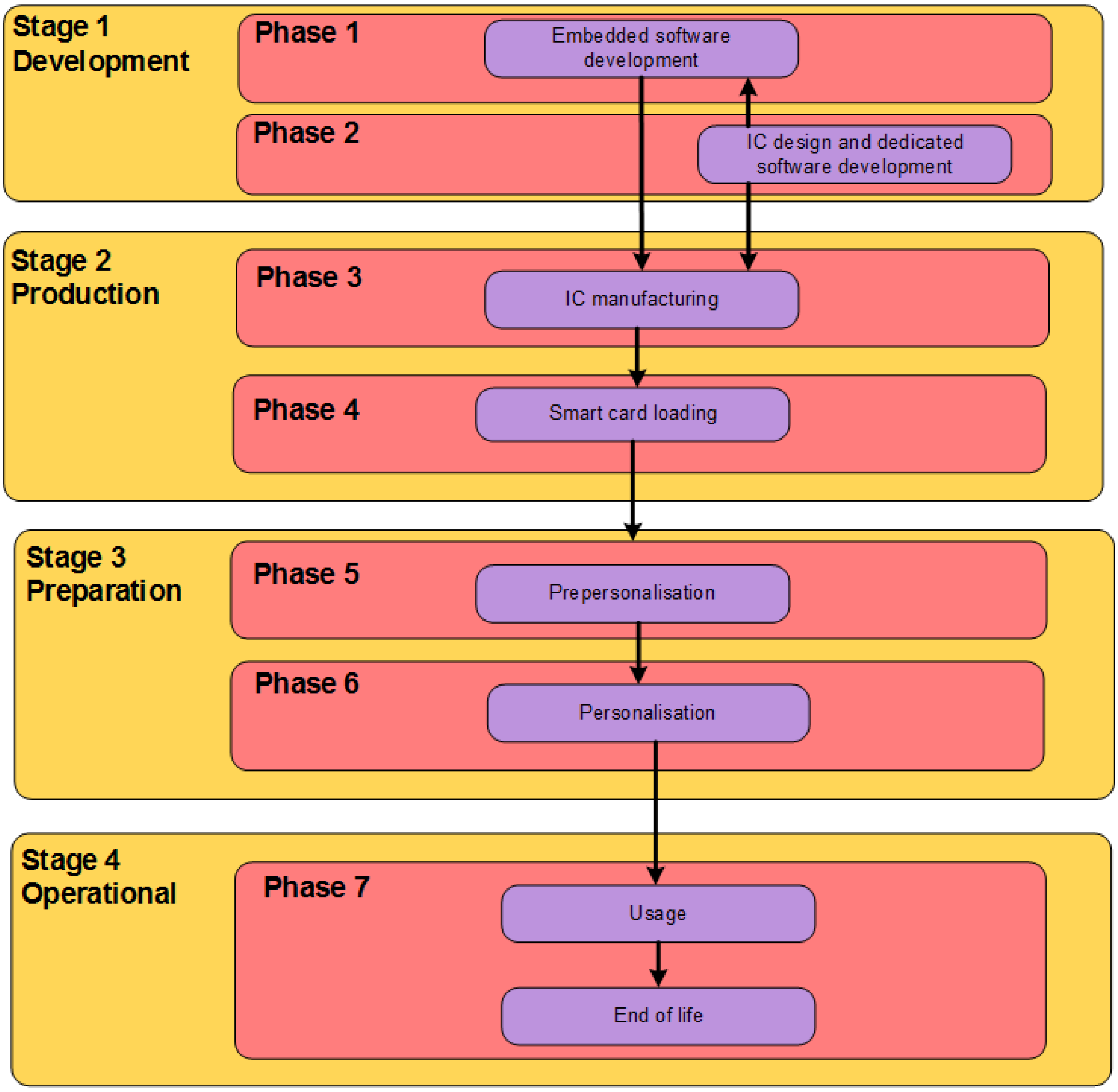


Figure 2 Life cycle Overview

The TOE is an applet embedded on a Java Card Open Platform. The underlying platform is conformant to the **[PP-IC]** smartcard life cycle, and the TOE is also conformant to the **[PP-IC]** smartcard lifecycle.

As described in paragraph 16 of **[PP-TACHOGRAPH_GEN2]**, the TOE environment is separated into the following parts:

- **Development environment:**
  TOE parts are designed, tested and manufactured.

- **Production environment:**
TOE is under construction. The security requirements of the Java Card Open Platform are fulfilled and assurance levels are met.
- **Operational environment:**
TOE is self-protected and can be used as stated (personalized and used). Once personalized according to **AGD_PRE [Applet]**, the TOE is constructed: the security requirements of the TOE are fulfilled and the assurance levels are met.

4.1 Development Environment (Phases 1 & 2 of the IC life cycle [PP-IC])

The development environment encompasses the environment in which the TOE is developed and tested:

- Java Card Open Platform components
- IDeal Drive DT v3.0 Applet

This Environment is composed of three phases:
Phase 1: Embedded Software Development
Phase 2: IC design and dedicated software development

4.1.1 Phase 1: Embedded Software Development

The IC Embedded Software Developer is in charge of:

- Specification, development and validation of the software (Java Card Operating System and Tachograph Applet).

Tachograph Applet and Java Card Open Platform (JOP) development environment is enforced by IDEMIA and its confidentiality and integrity are covered by the evaluation of the development premises of IDEMIA.

To ensure security, access to development tools and products elements (PC, card reader, documentation, source code...) is protected. The protection is based on measures for prevention and detection of unauthorized access.

Role	Actor	Covered by
Embedded Software Developer (Tachograph Applet)	IDEMIA	**ALC**
Embedded Software Developer (Java Card Open Platform)	IDEMIA	**ALC**
Redaction and Review of Documentation	IDEMIA	**ALC**

At the end of phase 1, the Java Card platform code and Tachograph Applet code are protected in integrity and confidentiality by the environment

4.1.2 Phase 2: IC design and dedicated software development

In this phase, the underlying integrated circuit is developed. This phase takes place at the manufacturing site of the IC provider.

The confidentiality and integrity of the Java Card packages and Java Card open platform is covered by the evaluation of the development premises of the IC manufacturer.

Roles, Actors, Sites and coverage for this phase of the product life-cycle are listed in the table below:

Role	Actor	Site	Covered by
IC Developer	Infineon	Infineon development site(s) mentioned in **[CR-IC]**	**ALC [Infineon]**

4.2 Production Environment (Phases 3 & 4 of the IC life cycle)

In this environment, the following two phases take place:

- **Phase 3:** IC manufacturing
- **Phase 4:** Smart card loading

The IC manufacturer is responsible for producing the IC (manufacturing, testing, and initialization). Depending on the intention:

- **(Option 1)** the developer sends the image (containing both the Java Card platform and the Tachograph applet) to be flashed in the IC to the IC manufacturer in the phase 3.

Or

- **(Option 2)** the platform developer sends the image (containing only the Java Card platform) to be flashed in the IC to the IC manufacturer in the phase 3. Once the Java Card platform has been loaded, the package of Tachograph is securely delivered from the applet developer to the smart card loader. The cap file of the applet is then loaded (using GP mechanism) in the Java Card platform by the smart card loader in phase 4 at IDEMIA audited site.

Or

- **(Option 3)** the developer sends the image (containing both the Java Card platform and the Tachograph applet) to be loaded in Flash (using the loader of the IC) to the smart card loader in phase 4.

Several life cycles are available, depending when the Flash Code is loaded. The following tables present roles, actors, sites and coverage for this for this environment of the product life cycle and describe for each of them the TOE delivery point.

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing both platform and applet	Infineon	Infineon production plants Refer to Platform	ALC
Smart card loader	-	-	-	-
TOE Delivery Point				

Table 1 Image containing both platform and applet is loaded at IC manufacturer (Option 1)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing only platform	Infineon	Infineon production plants Refer to Platform	ALC
Smart card loader	Cap file of the applet	IDEMIA	IDEMIA Audited Sites	ALC
	TOE Delivery Point			

Table 2 Cap file of Tachograph applet is loaded through the loader of the IC manufacturer (Option 2)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer send the components containing appropriate key for loading encrypted image	-	-	-	-
TOE Delivery Point				
Smart card loader	Image containing both platform and applet	IDEMIA or another agent	IDEMIA Audited Sites or others sites	AGD

Table 3 Image containing both platform and applet is loaded through the loader of the IC (Option 3)

4.3 Preparation Environment

In this environment, the following two phases take place:

- **Phase 5:** Prepersonalisation
- **Phase 6:** Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the prepersonalisation agent or personalisation agent prior to any operation.

The Tachograph applet is prepersonalised and personalized according to **AGD_PRE [Applet]**.

During personalization, TOE can be configured as any of the following Tachograph Card type:

- Driver card (Configuration 1 or Configuration 2 compliant)
- Workshop card (Configuration 1 or Configuration 2 compliant)

- Control card (Configuration 1 or Configuration 2 compliant)
- Company card (Configuration 1 or Configuration 2 compliant)

This phase is performed by the Personalisation Agent, which controls the TOE, which is in charge of the Java Card applet personalisation and responsible for ensuring a sufficient level of security during this phase.

All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

The Java Card applet is personalized according to guidance document **AGD_PRE [Applet]** and **AGD_OPE [JOP]**, and the following operations are made: creation of applicative data (SVD, RAD, File,…) and the TOE_Administrator Agent key is loaded.

At the end of phase 6, the TOE is personalized and constructed

4.4 Operational Environment

The TOE is under the control of the User (Signatory and/or Administrator).

This phase is covered by **AGD_OPE [Applet]** of the TOE and **AGD_OPE [JOP]** of the underlying Platform.

5 Conformance Claims

5.1 CC Conformance

This Security Target claims conformance to **[CC2], [CC3] and [CEM]**.

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 2	Conformance to the extended part. ▪ FCS.RNG.1: "Random number generation" ▪ FPT_EMS.1: "TOE Emanation"
Part 3	Conformance to EAL 4, augmented with ▪ AVA_VAN.5: "Advanced methodical vulnerability analysis" ▪ ATE_DPT.2: "Testing: security enforcing modules" ▪ ALC_DVS.2: "Sufficiency of security measures"

5.2 Protection Profile Reference

5.2.1 Overview

This security target claims a **strict conformance** to Tachograph Protection Profiles:

1. **[PP-TACHOGRAPH_GEN1]** for Configuration 1
2. **[PP-TACHOGRAPH_GEN2]** for Configuration 2

The underlying integrated circuit is successfully evaluated and certified in accordance with the Security IC Platform Protection Profile **[PP -IC]**.

The underlying Java Card Open Platform of the TOE is evaluated and certified in accordance with the Java Card™ System Protection Profile Open Configuration **[PP-JAVACARD].**

5.2.2 Conformance Rationale

5.2.2.1 Assets

Assets	[PP-Tachograph_GEN1]	[PP-Tachograph_GEN2]	ST
Identification data (IDD)	✓	✓	✓
Activity data (ACD)	✓	✓	✓
Application (APP)		✓	✓
Keys to protect data (KPD)		✓	✓
Signature verification data (SVD)	✓	✓	✓
Verification authentication data (VAD)	✓	✓	✓
Reference authentication data (RAD)	✓	✓	✓
Data to be signed (DTBS)	✓	✓	✓
TOE file system, including specific identification data	✓	✓	✓
Signature creation data (SCD)			Covered by Keys to Protect Data (KPD)
Secret messaging keys (SMK)			Covered by Keys to Protect Data (KPD)

5.2.2.2 Users/Subjects

Users/Subjects	[PP-Tachograph_GEN1]	[PP-Tachograph_GEN2]	ST
Administrator	✓	✓	✓
Vehicle Unit	✓	✓	✓
Other Device	✓	✓	✓
Attacker	✓	✓	✓

5.2.2.3 Threats

Threats	[PP-Tachograph_GEN1]	[PP-Tachograph_GEN2]	ST
T.Identification_Data	✓	✓	✓
T.Application		✓	✓
T.Activity_Data	✓	✓	✓
T.Data_Exchange	✓	✓	✓
T.Clone		✓	✓
T.Personalisation_Data	✓		Covered by A.Personalisation_Phase and OE.Personalisation_Phase

5.2.2.4 Oragnisational Security Policies

Organizational Security Policies	[PP-Tachograph_GEN1]	[PP-Tachograph_GEN2]	ST
P.Crypto		✓	✓
P.EU_Specifications	✓		Covered by the TOE meeting the updated **[EU – 2016/799]**

5.2.2.5 Assumptions

Assumptions	[PP-Tachograph_GEN1]	[PP-Tachograph_GEN2]	ST
A.Personalisation_Phase	✓	✓	✓

5.2.2.6 Security Objectives for the TOE

Security Objectives for the TOE	[PP-Tachograph_GEN1]	[PP-Tachograph_GEN2]	ST
O.Card_Identification_Data	✓	✓	✓
O.Card_Activity_Storage	✓	✓	✓
O.Protect_Secret		✓	✓
O.Data_Access	✓	✓	✓
O.Secure_Communications	✓	✓	✓
O.Crypto_Implement		✓	✓
O.Software_Update		✓	✓

5.2.2.7 Security Objectives for the Operational Enviroment

Security Objectives for the Operational	[PP-Tachograph	[PP-Tachograph	ST

Environment	_GEN1]	_GEN2]	
OE.Personalisation_Phase	✓	✓	✓
OE.Crypto_Admin		✓	✓
OE.EOL		✓	✓
OE.Tachograph_Components	✓		Covered by OE.Crypto_Admin

5.2.2.8 Security Functional Requirements

Security Functional Requirements	[PP-Tachograph _GEN1]	[PP-Tachograph _GEN2]	ST
FAU_ARP.1		✓	✓
FAU_SAA.1	✓	✓	✓
FCO_NRO.1	✓	✓	✓
FDP_ACC.2	✓	✓	✓
FDP_ACF.1	✓	✓	✓
FDP_DAU.1	✓	✓	✓
FDP_ETC.1	✓	✓	✓
FDP_ETC.2	✓	✓	✓
FDP_ITC.1	✓	✓	✓
FDP_ITC.2		✓	✓
FDP_RIP.1	✓	✓	✓
FDP_SDI.2	✓	✓	✓
FIA_AFL.1(1:C)	✓	✓	✓
FIA_AFL.1(2:W)	✓	✓	✓
FIA_ATD.1	✓	✓	✓
FIA_UAU.3	✓	✓	✓
FIA_UAU.4	✓	✓	✓
FIA_UID.2		✓	✓
FIA_USB.1	✓	✓	✓
FPR_UNO.1	✓	✓	✓
FPT_EMS.1	✓	✓	✓
FPT_FLS.1	✓	✓	✓
FPT_PHP.3	✓	✓	✓
FPT_TST.1	✓	✓	✓
FCS_CKM.1(1)		✓	✓
FCS_CKM.2(1)		✓	✓
FCS_CKM.4(1)		✓	✓
FCS_COP.1(1:AES)		✓	✓
FCS_COP.1(2:SHA-2)		✓	✓
FCS_COP.1(3: ECC)		✓	✓
FCS_RNG.1		✓	✓
FIA_UAU.1(1)		✓	✓

FPT_TDC.1(1)		✓	✓
FTP_ITC.1(1)		✓	✓
FCS_CKM.1(2)	✓	✓	✓
FCS_CKM.2(2)	✓	✓	✓
FCS_CKM.4(2)	✓	✓	✓
FCS_COP.1(4:TDES)	✓	✓	✓
FCS_COP.1(5:RSA)	✓	✓	✓
FCS_COP.1(6:SHA-1)		✓	✓
FIA_UAU.1(2)	✓	✓	✓
FPT_TDC.1(2)	✓	✓	✓
FTP_ITC.1(2)	✓	✓	✓
FIA_UID.1	✓		Covered by FIA_UID.2

6 Security Problem Definition

6.1 Assets

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

6.1.1 Primary Assets

D.IDENTIFICATION_DATA

Asset	Definition
Identification data (IDD)	Card identification data, user identification data

D.ACTIVITY_DATA

Asset	Definition
Activity data (ACD)	Activity data

6.1.2 Secondary Assets

D.APPLICATION

Asset	Definition
Application (APP)	Tachograph application.

D.KEYS_TO_PROTECT_DATA

Asset	Definition
Keys to protect data (KPD)	Enduring private keys and session keys used to protect security data and user data held within and transmitted by the TOE, and as a means of authentication.

D.SIGNATURE_VERIFICATION_DATA

Asset	Definition
Signature verification data (SVD)	Public keys certified by Certification Authorities, used to verify electronic signatures.

D.VERIFICATION_AUTHENTICATION_DATA

Asset	Definition
Verification authentication data (VAD)	Authentication data provided as input for authentication attempt as authorised user (i.e. entered PIN on workshop cards).

D.REFERENCE_AUTHENTICATION_DATA

Asset	Definition
Reference authentication data (RAD)	Data persistently stored by the TOE for verification of the authentication attempt as authorised user (i.e. reference PIN on workshop cards).

D.DATA_TO_BE_SIGNED

Asset	Definition
Data to be signed (DTBS)	The complete electronic data to be signed (including both user message and signature attributes).

D.TOE_FILE_SYSTEM

Asset	Definition
TOE file system, including specific identification data	File structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalisation

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

6.2 Subjects and external entities

Following are the subjects, who can interact with the TOE.

S.ADMIN

Role	Definition
Administrator	Usually active only during Initialisation/Personalisation (Phase 6) – listed here for the sake of completeness.

S.VU

Role	Definition
Vehicle Unit	Vehicle Unit (authenticated5), to which the Tachograph Card is connected (S.VU).

S.Other_Device

Role	Definition
Other Device	Other device (not authenticated) to which the Tachograph Card is connected (S.Non-VU).

S.ATTACKER

Role	Definition
Attacker	A human or a process located outside the TOE and trying to undermine the security policy defined by the current ST, 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.

Application note 3: This table defines the subjects in the sense of [CC1] which can be recognised by the TOE independently of their nature (human or process). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entities except the Attacker, who is listed for completeness – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC1]). From this point of view, the TOE itself does not distinguish between "subjects" and "external entities".

6.3 Threats

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

T.IDENTIFICATION_DATA

Label	**Threat**
T.IDENTIFICATION_DATA	Modification of Identification Data - A successful modification of identification data held by the TOE (IDD, see sec. 3.1, e.g. the type of card, or the card expiry date or the user identification data) would allow an attacker to misrepresent driver activity.

T.APPLICATION

Label	Threat

T.APPLICATION	Modification of Tachograph application - A successful modification or replacement of the Tachograph application stored in the TOE (APP, see sec. 3.1), would allow an attacker to misrepresent human user (especially driver) activity.

T.ACTIVITY_DATA

Label	Threat
T.ACTIVITY_DATA	Modification of Activity Data - A successful modification of activity data stored in the TOE (ACD, see sec. 3.1,) would allow an attacker to misrepresent human user (especially driver) activity.

T.DATA_EXCHANGE

Label	Threat
T.DATA_EXCHANGE	Modification of Activity Data during Data Transfer - A successful modification of activity data (ACD deletion, addition or modification, see sec. 3.1) during import or export would allow an attacker to misrepresent human user (especially driver) activity.

T.CLONE

Label	Threat
T.CLONE	Cloning of cards – An attacker could read or copy secret cryptographic keys from a Tachograph card and use it to create a duplicate card, allowing an attacker to misrepresent human user (especially driver) activity.

6.4 Organisational Security Policies

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

P.CRYPTO

Label	Organisational Security Policy
P.Crypto	The cryptographic algorithms and keys described in [EU – 2016/799] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected.

6.5 Assumptions

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

A.PERSONALISATION_PHASE

Personalisation Phase Security - All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation are correct according to [EU – 2016/799] Annex 1C, and are handled correctly so as to preserve the integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE.

7 Security Objectives

7.1 Security Objectives for the TOE

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

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

7.1.1 Security Objectives

O.CARD_IDENTIFICATION_DATA

Label	Security objective for the TOE
O.Card_Identification_Data	Integrity of Identification Data - The TOE must preserve the integrity of card identification data and user identification data stored during the card personalisation process.

O.CARD_ACTIVITY_STORAGE

Label	Security objective for the TOE
O.Card_Activity_Storage	Integrity of Activity Data - The TOE must preserve the integrity of user data stored in the card by Vehicle Units.

O.PROTECT_SECRET

Label	Security objective for the TOE
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

Label	Security objective for the TOE
O.Data_Access	User Data Write Access Limitation - The TOE must limit user data write access to authenticated Vehicle Units.

O.SECURE_COMMUNICATIONS

Label	Security objective for the TOE
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

Label	Security objective for the TOE
O.Crypto_Implement	Cryptographic operation – The cryptographic functions must be implemented as required by [EU – 2016/799] Annex 1C, Appendix 11.

O.SOFTWARE_UPDATE

Label	Security objective for the TOE
O.Software_Update	Software updates - Where updates to TOE software are possible, the TOE must accept only those that are authorised.

7.2 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.

OE.PERSONALISATION_PHASE

Label	Security objective for the operational environment
OE.PERSONALISATION_PHASE	**Secure Handling of Data in Personalisation Phase -** All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation must be correct according to [EU – 2016/799] Annex 1C, and must be handled so as to preserve the integrity and confidentiality of the data. The Personalisation Service Provider must control all materials, equipment and information that are used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalisation process must be appropriately secured with the goal of data integrity and confidentiality.

OE.CRYPTO_ADMIN

Label	Security objective for the operational environment
OE.CRYPTO_ADMIN	Implementation of Tachograph Components – All requirements from [EU – 2016/799] concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.

OE.EOL

Label	Security objective for the operational environment
OE.EOL	End of life - When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, that the confidentiality of symmetric and private cryptographic keys has to be safeguarded.

7.3 Security Objectives Rationale

7.3.1 Threats

T.IDENTIFICATION_DATA 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.APPLICATION 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.ACTIVITY_DATA is addressed by O.CARD_ACTIVITY_STORAGE and O.DATA_ACCESS. The unalterable storage of Activity data as defined in the security objective O.CARD_ACTIVITY_STORAGE counters directly the threat T.ACTIVITY_DATA. In addition, the security objective O.DATA_ACCESS limits the user data write access to authenticated Vehicle Units so that the modification of activity data by regular card commands can be conducted only by authenticated card interface devices.

O.CRYPTO_IMPLEMENT and OE.CRYPTO_ADMIN require the implementation and management of strong cryptography to support this.

T.DATA_EXCHANGE 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 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.

7.3.2 Organisational Security Policies

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

7.3.3 Assumptions

A.PERSONALISATION_PHASE 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.

7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.IDENTIFICATION_DATA	O.CARD_IDENTIFICATION_DATA, O.CRYPTO_IMPLEMENT, OE.CRYPTO_ADMIN	Section 7.3.1
T.APPLICATION	O.PROTECT_SECRET, O.CRYPTO_IMPLEMENT, O.SOFTWARE_UPDATE, OE.EOL	Section 7.3.1
T.ACTIVITY_DATA	O.CARD_ACTIVITY_STORAGE, O.DATA_ACCESS, O.CRYPTO_IMPLEMENT, OE.CRYPTO_ADMIN	Section 7.3.1
T.DATA_EXCHANGE	O.PROTECT_SECRET, O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT, OE.CRYPTO_ADMIN	Section 7.3.1
T.CLONE	O.PROTECT_SECRET, OE.EOL	Section 7.3.1

Table 4 Threats and Security Objectives - Coverage

Security Objectives	Threats
O.CARD_IDENTIFICATION_DATA	T.IDENTIFICATION_DATA
O.CARD_ACTIVITY_STORAGE	T.ACTIVITY_DATA

O.PROTECT_SECRET	T.APPLICATION, T.DATA_EXCHANGE, T.CLONE
O.DATA_ACCESS	T.ACTIVITY_DATA
O.SECURE_COMMUNICATIONS	T.DATA_EXCHANGE
O.CRYPTO_IMPLEMENT	T.IDENTIFICATION_DATA, T.APPLICATION, T.ACTIVITY_DATA, T.DATA_EXCHANGE
O.SOFTWARE_UPDATE	T.APPLICATION
OE.PERSONALISATION_PHASE	
OE.CRYPTO_ADMIN	T.IDENTIFICATION_DATA, T.ACTIVITY_DATA, T.DATA_EXCHANGE
OE.EOL	T.APPLICATION, T.CLONE

Table 5 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.CRYPTO	O.CRYPTO_IMPLEMENT	Section 7.3.2

Table 6 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
O.CARD_IDENTIFICATION_DATA	
O.CARD_ACTIVITY_STORAGE	
O.PROTECT_SECRET	
O.DATA_ACCESS	
O.SECURE_COMMUNICATIONS	
O.CRYPTO_IMPLEMENT	P.CRYPTO
O.SOFTWARE_UPDATE	
OE.PERSONALISATION_PHASE	
OE.CRYPTO_ADMIN	
OE.EOL	

Table 7 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.PERSONALISATION_PHASE	OE.PERSONALISATION_PHASE, OE.CRYPTO_ADMIN	Section 7.3.3

Table 8 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.PERSONALISATION_PHASE	A.PERSONALISATION_PHASE
OE.CRYPTO_ADMIN	A.PERSONALISATION_PHASE
OE.EOL	

Table 9 Security Objectives for the Operational Environment and Assumptions - Coverage

8 Extended Requirements

8.1 Extended Families

8.1.1 Extended Family FPT_EMS - TOE Emanation

8.1.1.1 Description

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret 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, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

8.1.1.2 Extended Components

Extended Component FPT_EMS.1

Description

This family defines requirements to mitigate intelligible emanations.

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Definition

FPT_EMS.1 TOE Emanation

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]

Dependencies: No dependencies.

8.1.2 Extended Family FCS_RNG - Random number generation

8.1.2.1 Description

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

8.1.2.2 Extended Components

Extended Component FCS_RNG.1

Description

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

Definition

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic 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].

Dependencies: No dependencies.

9 Security Requirements

9.1 Security Functional Requirements

Security Function Policy: AC_SFP The Security Function Policy Access Control (AC_SFP) for Tachograph Cards in the end-usage phase based on the [EU – 2016/799] Annex 1C Appendix 2 Chapter 3 and 4 is defined as follows: The 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. Access Rules: The AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access a certain object. The possible commands are described in the Tachograph Card specification [EU – 2016/799] Chapter 3.5. Following Access Conditions are defined in the Tachograph Card specification [EU – 2016/799] Chapter 3.3:

- ALW (Always)- The command can be executed without restrictions.

- NEV (Never)- The command can never be executed.

- PLAIN-C- The command APDU is sent in plain.

- PWD- The command may only be executed if the workshop card PIN has been successfully verified.

- EXT-AUT-G1- The command may only be executed if the External Authenticate command for the generation 1 authentication has been successfully performed.

- SM-MAC-G1- The APDU (command and response) must be applied with generation 1 secure messaging in authentication-only mode.

- SM-C-MAC-G1- The command APDU must be applied with generation 1 secure messaging in authentication only mode.

- SM-R-ENC-G1- The response APDU must be applied with generation 1 secure messaging in encryption mode.

- SM-R-ENC-MAC-G1- The response APDU must be applied with generation 1 secure messaging in encrypt-then-authenticate mode.

- SM-MAC-G2- The APDU (command and response) must be applied with generation 2 secure messaging in authentication-only mode.

- SM-C-MAC-G2- The command APDU must be applied with generation 2 secure messaging in authentication only mode.

- SM-R-ENC-MAC-G2- The response APDU must be applied with generation 2 secure messaging in encrypt-then-authenticate mode

For each type of Tachograph Card the Access Rules (which make use of the Access Conditions described above) for the different objects are implemented according to the requirements in the Tachograph Card Specification [EU – 2016/799] Chapter 4. These access rules cover in particular the rules for the export and import of data.

9.1.1 TOE Security Requirements

FAU_ARP.1 Security alarms

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 [EU – 2016/799] Annex 1C, Appendix 2;

b) For self test errors and stored data integrity errors - respond to any VU command with an 0x64 00 status word indicating the error

upon detection of a potential security violation.

FAU_SAA.1 Potential violation analysis

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

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

a) Accumulation or combination of

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

known to indicate a potential security violation;

b) **None**.

Application Note:

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

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **AC SFP** on

Subjects:

- **S.VU (a vehicle unit in the sense of [EU – 2016/799] Annex 1C)**
- **S.Non-VU (other card interface devices)**

Objects:

User data

- **User Identification data**
- **Activity data**

Security data

- **Cryptographic keys (see Table 16, Table 17, Table 19 and Table 20 of [PP-TACHOGRAPH_GEN2])**
- **PIN (for Workshop card)**

TOE application code

TOE file system

Card identification data

Master file contents and all operations among subjects and objects covered by the SFP.

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

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **AC SFP** to objects based on the following:

Subjects:

- **S.VU (in the sense of [EU – 2016/799] Annex 1C)**
- **S.Non-VU (other card interface devices)**

Objects:

User data

- **User identification data**
- **Activity data**

Security data

- **Cryptographic keys (see Table 16, Table 17, Table 19 and Table 20 of [PP-TACHOGRAPH_GEN2])**
- **PIN (for Workshop card)**

TOE application code

TOE file system (Attribute: access conditions)

Card identification data

Master file contents.

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

GENERAL_READ

- **Driver card, workshop card: user data may be read from the TOE by any user**

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

IDENTIF_WRITE

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

ACTIVITY_WRITE

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

SOFT_UPGRADE

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

FILE_STRUCTURE

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

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

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

SECRET KEYS

- **The TSF shall prevent access to secret cryptographic keys other than for use in the TSF's cryptographic operations, or in case of a workshop card only, for exporting the SensorInstallationSecData to a VU, as specified in [EU – 2016/799] Annex 1C, Appendix 2**.

FDP_DAU.1 Basic Data Authentication

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 the indicated information.

FDP_ETC.1 Export of user data without security attributes

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

FDP_ETC.2 Export of user data with security attributes

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**.

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **AC SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

FDP_ITC.2 Import of user data with security attributes

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:

Software updates are not possible after card is issued to the customer. Updates are only possible before Operational Phase and that too with the help of Platform Security functions.

FDP_RIP.1 Subset residual information protection

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: **session key, SSC, authentication status**.

FDP_SDI.2 Stored data integrity monitoring and action

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: **IntegrityControlledData**.

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

The following data persistently stored by TOE have the user data attribute "IntegrityControlledData":

- **PINs (i.e. objects instance of class OwnerPin orsubclass of interface PIN)**

- **keys (i.e. objects instance of classes implemented the interface Key)**
- **Activity Data and Identification User Data**

If the maximum is reached (15) the Kill card is launched.

FIA_AFL.1(1:C) Authentication failure handling

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

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

FIA_AFL.1(2:WC) Authentication failure handling

FIA_AFL.1.1(2:WC) The TSF shall detect when **5** unsuccessful authentication attempts occur related to **PIN verification of Workshop Card**.

FIA_AFL.1.2(2:WC) [Editorially Refined] When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall

a) warn the entity connected,

b) block the PIN check procedure such that any subsequent PIN check attempt will fail,

c) be able to indicate to subsequent users the reason for the blocking.

FIA_ATD.1 User attribute definition

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

a) User_group (Vehicle_Unit, Non_Vehicle_Unit);

b) User_ID (VRN and registering member state for subject S.VU).

FIA_UAU.3 Unforgeable authentication

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

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

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **key based authentication mechanisms as defined in [EU – 2016/799] Appendix 11, Chapters 4 and 10**.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

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

FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

a) User_group (Vehicle_Unit for S.VU, Non_Vehicle_Unit for S.Non-VU);

b) User_ID (VRN and registering member state for subject S.VU).

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

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**.

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:

IDENTIF_WRITE

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

ACTIVITY_WRITE

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

FPR_UNO.1 Unobservability

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**.

FPT_FLS.1 Failure with preservation of secure state

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

a) Reset;

b) Power supply cut-off;

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

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

FPT_PHP.3 Resistance to physical attack

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

Application Note:

The physical manipulation and physical probing include: changing operational conditions every times: the frequency of the external clock, power supply, and temperature.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self 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 authorised users with the capability to verify the integrity of **TSF data**.

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

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **Side channel emission** in excess of **limits specified by the state-of-the-art attacks on smart card IC** enabling access to **private keys or session keys** and **RAD**

FPT_EMS.1.2 The TSF shall ensure **any users** are unable to use the following interface **smart card circuit contacts** to gain access to **private keys or session keys** and **RAD**

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **deterministic** random number generator that implements **CTR_DRBG as defined in [RNG-NIST]**.

FCS_RNG.1.2 The TSF shall provide random numbers that meet **The average Shannon entropy per internal random bit exceeds 0.999**.

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

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

FCS_CKM.1(1) Cryptographic key generation

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **cryptographic key derivation algorithms specified in [EU – 2016/799] Annex 1C, Appendix 11, Section 10 (for VU authentication and for the secure messaging session key)** and specified cryptographic key sizes **key sizes required by [EU – 2016/799] Annex 1C, Appendix 11, Part B** that meet the following: **Reference [RNG-CLASS] predefined RNG class DRG.3, [EU – 2016/799] Annex 1C, Appendix 11, Section 10**.

FCS_CKM.2(1) Cryptographic key distribution

FCS_CKM.2.1(1) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **secure messaging AES session key agreement as specified in [EU – 2016/799] Annex 1C, Appendix 11, Part B** that meets the following: **[EU – 2016/799] Annex 1C, Appendix 11, Part B**.

Application Note:

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

FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1 [Editorially Refined] 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 [EU – 2016/799] Annex 1C, Appendix 11, sections 6.1 and 14.2..

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

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given **that the digital certificate used in the digital signature for the downloaded data has not expired (see [EU – 2016/799] Appendix 11, sections 6.2 and 14.3]**.

Application Note:

Note that FCO_NRO.1 applies only to driver cards and workshop cards, as those are the only cards capable of creating a signature over downloaded data. See [EU – 2016/799] Appendix 11, sections 6 and 14.

FCS_CKM.4(1) Cryptographic key destruction

FCS_CKM.4.1(1) [Editorially Refined] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key.clearKey() method** that meets the following

- **Requirements in Table 20 of [PP-TACHOGRAPH_GEN2];**
- **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**
- **Java Card API" specification [JCAPI]**.

FCS_COP.1(1:AES) Cryptographic operation

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

a) ensuring authenticity and integrity of data exchanged between a vehicle unit and a tachograph card;

b) where applicable, ensuring confidentiality of data exchanged between a vehicle unit and a tachograph card;

c) decrypting confidential data sent by a vehicle unit to a remote early detection communication reader over a DSRC connection, and verifying the

authenticity of that data; in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **128, 192, 256 bits** that meet the following: **FIPS PUB 197: Advanced Encryption Standard, [EU – 2016/799] Annex 1C, Appendix 11**.

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

FCS_COP.1.1(2:SHA-2) The TSF shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm **SHA-256, SHA-384, SHA-512** and cryptographic key sizes **not applicable** that meet the following: **Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS), [EU – 2016/799] Annex 1C, Appendix 11**.

FCS_COP.1(3:ECC) Cryptographic operation

FCS_COP.1.1(3:ECC) The TSF shall perform **the following cryptographic operations:**

a) digital signature generation;

b) digital signature verification;

c) cryptographic key agreement;

d) mutual authentication between a vehicle unit and a tachograph card;

e) ensuring authenticity, integrity and non-repudiation of data downloaded from a tachograph card in accordance with a specified cryptographic algorithm **[EU – 2016/799] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG** and cryptographic key sizes **in accordance with [EU – 2016/799], Appendix 11, Part B** that meet the following: **[EU – 2016/799] Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-03111 – Elliptic Curve Cryptography – version 2, and the standardized domain parameters in the table below.**

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

Table for Standardised domain parameters.

Application Note:

Where a symmetric algorithm, an asymmetric algorithm and/or a hashing algorithm are used together to form a security protocol, their respective key lengths and hash sizes shall be of (roughly) equal strength. Table for Cipher Suites below shows the allowed cipher suites. ECC keys sizes of 512 bits and 521 bits are considered to be equal in strength.

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

Table for Cipher Suites

FIA_UAU.1(1) Timing of authentication

FIA_UAU.1.1(1) The TSF shall allow **a) Driver card, workshop card – export of user data with security attributes (card data download function) and export of user data without security attributes as allowed by the applicable access rules in [EU – 2016/799] Annex 1C, Appendix 2;**

b) Control card, company card – export of user data without security attributes as allowed by the applicable access rules in [EU – 2016/799] Annex 1C, Appendix 2 on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(1) [Editorially Refined] The TSF shall require each user to be successfully authenticated using the method described in [EU – 2016/799] Annex 1C, Appendix 11, Chapter 10 before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

FIA_UAU.1.1(1) a) allows non secured readers to get signed downloaded data from driver and workshop cards, without any previous authentication. This can be used by company download tools, which are considered as "other devices" in the sense of protection Profile of Digital Tachograph – Tachograph Card, Version 1.0, 9 May 2017. Such download tools, and also vehicle units, are also allowed to read driver and workshop card data in a non secured mode (without any previous authentication). This is allowed by [[EU – 2016/799] Annex 1C, Appendix 2 access rules (see section 4, access rules = 'ALW'). Similarly, FIA_UAU.1.1(1) b) allows "other devices" (without having performed any authentication) to access data from control and company cards, following [EU – 2016/799] Annex 1C, Appendix 2, Section 4 access rules.

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

FPT_TDC.1.1(1) [Editorially Refined] The TSF shall provide the capability to consistently interpret **secure messaging attributes as defined by [EU – 2016/799] Annex 1C, Appendix 11]** when shared between the TSF and a **vehicle unit**.

FPT_TDC.1.2(1) [Editorially Refined] The TSF shall use **the interpretation rules (communication protocols) as defined by [EU – 2016/799] Annex 1C, Appendix 11]** when interpreting the TSF data from a **vehicle unit.**

FTP_ITC.1(1) Inter-TSF trusted channel

FTP_ITC.1.1(1) [Editorially Refined] 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(1) The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3(1) [Editorially Refined] 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].**

Application Note:

The requirements for establishing the trusted channel are given in [EU – 2016/799] Appendix 11, Chapter 10 (for 2nd generation vehicle units).

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

FCS_CKM.1(2) Cryptographic key generation

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **cryptographic key derivation algorithms specified in [EU – 2016/799] Annex 1C, Appendix 11, Section 4 (for the secure messaging session key)** and specified cryptographic key sizes **112 bits** that meet the following: **two-key TDES as specified in [EU – 2016/799] Annex 1C, Appendix 11 Part A, Chapter 3**.

FCS_CKM.2(2) Cryptographic key distribution

FCS_CKM.2.1(2) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **for triple DES session keys as specified in [EU – 2016/799] Annex 1C, Appendix 11 Part A** that meets the following: **[EU – 2016/799] Annex 1C, Appendix 11 Part A, Chapter 3**.

FCS_CKM.4(2) Cryptographic key destruction

FCS_CKM.4.1(2) [Editorially Refined] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key.clearKey() method** that meets the following

- **Requirements in Table 16 and Table 17 of [PP-TACHOGRAPH_GEN2];**
- **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**
- **Java Card API" specification [JCAPI]**.

FCS_COP.1(4:TDES) Cryptographic operation

FCS_COP.1.1(4:TDES) The TSF shall perform **the cryptographic operations (encryption, decryption, Retail-MAC)** in accordance with a specified cryptographic algorithm **Triple DES** and cryptographic key sizes **112 bits** that meet the following: **[EU – 2016/799] Annex 1C, Appendix 11 Part A, Chapter 3**.

FCS_COP.1(5:RSA) Cryptographic operation

FCS_COP.1.1(5:RSA) The TSF shall perform **the cryptographic operations (encryption, decryption, signing, verification)** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bits** that meet the following: **[EU – 2016/799] Annex 1C, Appendix 11 Part A, Chapter 3**.

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

FCS_COP.1.1(6:SHA-1) The TSF shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **not applicable** that meet the following: **Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS)**.

FIA_UAU.1(2) Timing of authentication

FIA_UAU.1.1(2) The TSF shall allow **a) Driver card, workshop card – export of user data with security attributes (digital signature used in card data download function, see [EU – 2016/799] Annex 1C, Appendix 11, Chapters 6 and 14)) and export of user data without security attributes as allowed by the applicable access rules in [EU – 2016/799] Annex 1C, Appendix 2;**

b) Control card, company card – export of user data without security attributes as allowed by the applicable access rules in [EU – 2016/799] Annex 1C, Appendix 2 on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(2) [Editorially Refined] The TSF shall require each user to be successfully authenticated using the method described in [EU – 2016/799] Annex 1C, Appendix 11, Chapter 5 before allowing any other TSF-mediated actions on behalf of that user.

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

FPT_TDC.1.1(2) [Editorially Refined] The TSF shall provide the capability to consistently interpret **secure messaging attributes as defined by [EU – 2016/799] Annex 1C, Appendix 11 Chapter 5** when shared between the TSF and a **vehicle unit.**

FPT_TDC.1.2(2) [Editorially Refined] The TSF shall use **the interpretation rules (communication protocols) as defined by [EU – 2016/799] Annex 1C, Appendix 11 Part A, Chapter 5** when interpreting the TSF data from **vehicle unit.**

FTP_ITC.1(2) Inter-TSF trusted channel

FTP_ITC.1.1(2) [Editorially Refined] 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(2) The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3(2) [Editorially Refined] The TSF shall use the trusted channel for **data import from and export to a vehicle unit in accordance with [EU – 1360/2002] Appendix 2.**

Application Note:

The requirements for establishing the trusted channel are given in [EU – 2016/799] Appendix 11, Chapter 5 (for 1st generation vehicle units).

9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2.

9.2.1 ADV Development

9.2.1.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.1.2 ADV_FSP Functional specification

ADV_FSP.4 Complete functional specification

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

9.2.1.3 ADV_IMP Implementation representation

ADV_IMP.1 Implementation representation of the TSF

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

9.2.1.4 ADV_TDS TOE design

ADV_TDS.3 Basic modular design

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

9.2.2 AGD Guidance documents

9.2.2.1 AGD_OPE Operational user guidance

AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.2.2 AGD_PRE Preparative procedures

AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

9.2.3 ALC Life-cycle support

9.2.3.1 ALC_CMC CM capabilities

ALC_CMC.4 Production support, acceptance procedures and automation

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.2 ALC_CMS CM scope

ALC_CMS.4 Problem tracking CM coverage

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.3 ALC_DEL Delivery

ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.4 ALC_DVS Development security

ALC_DVS.2 Sufficiency of security measures

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

9.2.3.5 ALC_LCD Life-cycle definition

ALC_LCD.1 Developer defined life-cycle model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.6 ALC_TAT Tools and techniques

ALC_TAT.1 Well-defined development tools

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4 ASE Security Target evaluation

9.2.4.1 ASE_CCL Conformance claims

ASE_CCL.1 Conformance claims

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.2 ASE_ECD Extended components definition

ASE_ECD.1 Extended components definition

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

9.2.4.3 ASE_INT ST introduction

ASE_INT.1 ST introduction

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

9.2.4.4 ASE_OBJ Security objectives

ASE_OBJ.2 Security objectives

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.5 ASE_REQ Security requirements

ASE_REQ.2 Derived security requirements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.6 ASE_SPD Security problem definition

ASE_SPD.1 Security problem definition

ASE_APD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.7 ASE_TSS TOE summary specification

ASE_TSS.1 TOE summary specification

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

9.2.5 ATE Tests

9.2.5.1 ATE_COV Coverage

ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.2 ATE_DPT Depth

ATE_DPT.2 Testing: security enforcing modules

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.3 ATE_FUN Functional tests

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.4 ATE_IND Independent testing

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

9.2.6 AVA Vulnerability assessment

9.2.6.1 AVA_VAN Vulnerability analysis

AVA_VAN.5 Advanced methodical vulnerability analysis

AVA_VAN.5.1D The developer shall provide the TOE for testing.

AVA_VAN.5.1C The TOE shall be suitable for testing.

AVA_VAN.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

9.3 Security Requirements Rationale

9.3.1 Objectives

9.3.1.1 Security Objectives for the TOE

Security Objectives

O.CARD_IDENTIFICATION_DATA In the case of a detected integrity error the TOE will indicate the corresponding violation by FAU_ARP.1 and FAU_SAA.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.

Integrity of the stored data within the TOE, specifically the integrity of the identification data, is required by FDP_SDI.2 component.

FPT_EMS.1 requires the TOE to limit emanations, thereby protecting the confidentiality of identification data.

FPT_FLS.1 requires that any failure state should not expose identification data, or compromise its integrity.

FPT_PHP.3 requires the TOE to resist attempts to access identification data through manipulation or physical probing.

FPT_TST.1 requires tests to be carried out to assure that the integrity of the identification data has not been compromised.

O.CARD_ACTIVITY_STORAGE In the case of a detected integrity error the TOE will indicate the corresponding violation by FAU_ARP.1 and FAU_SAA.1.

Access to card activity data is regulated by the security function policy defined in FDP_ACC.2 and FDP_ACF.1 COMPONENETS, which explicitly restricts write access of user data to authorised vehicle units.

Integrity of the stored data within the TOE, specifically the integrity of the card activity data, is required by FDP_SDI.2 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 identification data through manipulation or physical probing.

FPT_TST.1 Requires tests to be carried out to assure that the integrity of card activity data has not been compromised.

O.PROTECT_SECRET FDP_ACC.2 and FDP_ACF.1 requires 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 requirement safeguards the unobservability of secret keys used in cryptographic operations.

FPT_EMS.1 requires the TOE to limit emanations, thereby protecting the confidentiality of the keys.

FPT_PHP.3 requires the TOE to resist attempts to gain access to the keys through manipulation or physical probing.

O.DATA_ACCESS Access to user data is regulated by the security function policy defined in FDP_ACC.2 FDP_ACF.1 components, which explicitly restricts write access of user data to authorised vehicle units.

FIA_AFL.1(1:C), FIA_AFL.1(2:WC) and FIA_UID.2 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.

FIA_ATD.1 and FIA_USB.1 definition of user security attributes supplies a distinction between vehicle units and other card interface devices.

FIA_UAU.1(1) and FIA_UAU.1(2) requirements ensure that write access to user data is not possible without a preceding successful authentication process.

FIA_UAU.3 prevents the use of forged credentials during the authentication process.

FPT_EMS.1 requires the TOE to limit emanations, thereby protecting the authentication process.

FPT_FLS.1 requires that any failure state should not allow unauthorised write access to the card.

FPT_PHP.3 requires the TOE to resist attempts to interfere with authentication through manipulation or physical probing.

FPT_TST.1 requires that tests be carried out to assure that the integrity of the TSF and identification data has not been compromised.

O.SECURE_COMMUNICATIONS During data exchange and upon detection of an integrity error of the imported data FAU_ARP.1 and FAU_SAA.1 will indicate the corresponding violation and will provide a warning to the entity sending the data.

The necessity for the use of a secure communication protocol as well as the access to the relevant card´s keys are defined within FDP_ACC.2 and FDP_ACF.1.

FDP_ETC.1, FDP_ITC.1 and FTP_ITC.1(1) and FTP_ITC.1(2) 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.

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 through FCO_NRO.1, FDP_DAU.1 and FDP_ETC.2.

FDP_RIP.1 requires the secure management of storage resources within the TOE to prevent data leakage.

FIA_UAU.3 and FIA_UAU.4 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 requirement safeguards the unobservability of the establishing process of the trusted channel, and the unobservability of the data exchange itself, both of which contribute to a secure data transfer.

FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM.4(1), FCS_CKM.4(2), FCS_COP.1(1:AES), FCS_COP.1(2:SHA-2), FCS_COP.1(3:ECC), FCS_COP.1(4:TDES), FCS_COP.1(5:RSA), FCS_COP.1(6:SHA-1) and 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(1:AES), FCS_COP.1(2:SHA-2), FCS_COP.1(3:ECC), FCS_COP.1(4:TDES), FCS_COP.1(5:RSA) and FCS_COP.1(6:SHA-1) also realizes the securing of the data exchange itself. Random numbers are generated in support of cryptographic key generation for authentication.

FPT_TDC.1(1) and FPT_TDC.1(2) requires a consistent interpretation of the security related data shared between the TOE and the card interface device.

O.CRYPTO_IMPLEMENT FDP_DAU.1 and FDP_SDI.2 requires approved cryptographic algorithms for digital signatures in support of data authentication.

FIA_UAU.3 and FIA_UAU.4 requires approved cryptographic algorithms are required to prevent the forgery, copying or reuse of authentication data.

FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM.4(1), FCS_CKM.4(2) and 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(1:AES), FCS_COP.1(2:SHA-2), FCS_COP.1(3:ECC), FCS_COP.1(4:TDES), FCS_COP.1(5:RSA) and FCS_COP.1(6:SHA-1) requires aproved cryptographic algorithms for all cryptographic operations.

O.SOFTWARE_UPDATE FDP_ACC.2 and FDP_ACF.1 require that users cannot update TOE software.

FPT_PHP.3 requires the TOE to resist physical attacks that may be aimed at modifying software.

FDP_ITC.2 ensures Import of user data with security attributes.

9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.CARD_IDENTIFICATION_DATA	FAU_ARP.1, FAU_SAA.1, FDP_ACC.2, FDP_ACF.1, FDP_SDI.2, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FPT_EMS.1	Section 9.3.1
O.CARD_ACTIVITY_STORAGE	FAU_ARP.1, FAU_SAA.1, FDP_ACC.2, FDP_ACF.1, FDP_SDI.2, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FPT_EMS.1	Section 9.3.1
O.PROTECT_SECRET	FDP_ACC.2, FDP_ACF.1, FDP_RIP.1, FPR_UNO.1, FPT_PHP.3, FPT_EMS.1	Section 9.3.1
O.DATA_ACCESS	FDP_ACC.2, FDP_ACF.1, FIA_AFL.1(1:C), FIA_AFL.1(2:WC), FIA_ATD.1, FIA_UAU.3, FIA_UID.2, FIA_USB.1, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FIA_UAU.1(1), FIA_UAU.1(2), FPT_EMS.1	Section 9.3.1
O.SECURE_COMMUNICATIONS	FAU_ARP.1, FAU_SAA.1, FCO_NRO.1, FDP_ACC.2, FDP_ACF.1, FDP_DAU.1, FDP_ETC.1, FDP_ETC.2, FDP_ITC.1, FDP_RIP.1, FIA_UAU.3, FIA_UAU.4, FPR_UNO.1, FCS_CKM.1(1), FCS_CKM.2(1), FCS_CKM.4(1), FCS_COP.1(1:AES), FCS_COP.1(2:SHA-2), FCS_COP.1(3:ECC), FPT_TDC.1(1), FCS_CKM.1(2), FCS_CKM.2(2), FCS_CKM.4(2), FCS_COP.1(4:TDES), FCS_COP.1(5:RSA), FCS_COP.1(6:SHA-1), FPT_TDC.1(2), FTP_ITC.1(2), FTP_ITC.1(1), FCS_RNG.1	Section 9.3.1
O.CRYPTO_IMPLEMENT	FDP_DAU.1, FDP_SDI.2, FIA_UAU.3, FIA_UAU.4, FCS_CKM.1(1), FCS_CKM.2(1), FCS_CKM.4(1), FCS_COP.1(1:AES), FCS_COP.1(2:SHA-2), FCS_COP.1(3:ECC), FCS_CKM.1(2), FCS_CKM.2(2), FCS_CKM.4(2), FCS_COP.1(4:TDES),	Section 9.3.1

	FCS_COP.1(5:RSA), FCS_COP.1(6:SHA-1), FCS_RNG.1	
O.SOFTWARE_UPDATE	FDP_ACC.2, FDP_ACF.1, FPT_PHP.3, FDP_ITC.2	Section 9.3.1

Table 10 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives	Rationale
FAU_ARP.1	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.SECURE_COMMUNICATIONS	
FAU_SAA.1	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.SECURE_COMMUNICATIONS	
FDP_ACC.2	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.PROTECT_SECRET, O.DATA_ACCESS, O.SECURE_COMMUNICATIONS, O.SOFTWARE_UPDATE	
FDP_ACF.1	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.PROTECT_SECRET, O.DATA_ACCESS, O.SECURE_COMMUNICATIONS, O.SOFTWARE_UPDATE	
FDP_DAU.1	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FDP_ETC.1	O.SECURE_COMMUNICATIONS	
FDP_ETC.2	O.SECURE_COMMUNICATIONS	
FDP_ITC.1	O.SECURE_COMMUNICATIONS	
FDP_ITC.2	O.SOFTWARE_UPDATE	
FDP_RIP.1	O.PROTECT_SECRET, O.SECURE_COMMUNICATIONS	
FDP_SDI.2	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.CRYPTO_IMPLEMENT	
FIA_AFL.1(1:C)	O.DATA_ACCESS	
FIA_AFL.1(2:WC)	O.DATA_ACCESS	
FIA_ATD.1	O.DATA_ACCESS	
FIA_UAU.3	O.DATA_ACCESS, O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FIA_UAU.4	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FIA_UID.2	O.DATA_ACCESS	
FIA_USB.1	O.DATA_ACCESS	
FPR_UNO.1	O.PROTECT_SECRET, O.SECURE_COMMUNICATIONS	

FPT_FLS.1	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.DATA_ACCESS	
FPT_PHP.3	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.PROTECT_SECRET, O.DATA_ACCESS, O.SOFTWARE_UPDATE	
FPT_TST.1	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.DATA_ACCESS	
FPT_EMS.1	O.CARD_IDENTIFICATION_DATA, O.CARD_ACTIVITY_STORAGE, O.PROTECT_SECRET, O.DATA_ACCESS	
FCS_RNG.1	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_CKM.1(1)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_CKM.2(1)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCO_NRO.1	O.SECURE_COMMUNICATIONS	
FCS_CKM.4(1)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_COP.1(1:AES)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_COP.1(2:SHA-2)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_COP.1(3:ECC)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FIA_UAU.1(1)	O.DATA_ACCESS	
FPT_TDC.1(1)	O.SECURE_COMMUNICATIONS	
FTP_ITC.1(1)	O.SECURE_COMMUNICATIONS	
FCS_CKM.1(2)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_CKM.2(2)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_CKM.4(2)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_COP.1(4:TDES)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_COP.1(5:RSA)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FCS_COP.1(6:SHA-1)	O.SECURE_COMMUNICATIONS, O.CRYPTO_IMPLEMENT	
FIA_UAU.1(2)	O.DATA_ACCESS	
FPT_TDC.1(2)	O.SECURE_COMMUNICATIONS	
FTP_ITC.1(2)	O.SECURE_COMMUNICATIONS	

Table 11 SFRs and Security Objectives

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies

FAU_ARP.1	(FAU_SAA.1)	FAU_SAA.1
FAU_SAA.1	(FAU_GEN.1)	
FDP_ACC.2	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2
FDP_DAU.1	No Dependencies	
FDP_ETC.1	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2
FDP_ETC.2	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2
FDP_ITC.1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.2
FDP_ITC.2	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.2, FPT_TDC.1(1), FTP_ITC.1(1), FPT_TDC.1(2), FTP_ITC.1(2)
FDP_RIP.1	No Dependencies	
FDP_SDI.2	No Dependencies	
FIA_AFL.1(1:C)	(FIA_UAU.1)	FIA_UAU.1(1), FIA_UAU.1(2)
FIA_AFL.1(2:WC)	(FIA_UAU.1)	FIA_UAU.1(1), FIA_UAU.1(2)
FIA_ATD.1	No Dependencies	
FIA_UAU.3	No Dependencies	
FIA_UAU.4	No Dependencies	
FIA_UID.2	No Dependencies	
FIA_USB.1	(FIA_ATD.1)	FIA_ATD.1
FPR_UNO.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FPT_EMS.1	No Dependencies	
FCS_RNG.1	No Dependencies	
FCS_CKM.1(1)	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.2(1), FCS_CKM.4(1), FCS_COP.1(1:AES), FCS_COP.1(3:ECC)
FCS_CKM.2(1)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1), FCS_CKM.4(1)
FCO_NRO.1	(FIA_UID.1)	FIA_UID.2
FCS_CKM.4(1)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1)

FCS_COP.1(1:AES)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1), FCS_CKM.4(1)
FCS_COP.1(2:SHA-2)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1(3:ECC)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2, FCS_CKM.4(1)
FIA_UAU.1(1)	(FIA_UID.1)	FIA_UID.2
FPT_TDC.1(1)	No Dependencies	
FTP_ITC.1(1)	No Dependencies	
FCS_CKM.1(2)	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.2(2), FCS_CKM.4(2), FCS_COP.1(4:TDES), FCS_COP.1(5:RSA)
FCS_CKM.2(2)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2), FCS_CKM.4(2)
FCS_CKM.4(2)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2)
FCS_COP.1(4:TDES)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1), FCS_CKM.4(1), FCS_CKM.1(2), FCS_CKM.4(2)
FCS_COP.1(5:RSA)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1), FCS_CKM.4(1), FCS_CKM.1(2), FCS_CKM.4(2)
FCS_COP.1(6:SHA-1)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FIA_UAU.1(2)	(FIA_UID.1)	FIA_UID.2
FPT_TDC.1(2)	No Dependencies	
FTP_ITC.1(2)	No Dependencies	

Table 12 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FAU_GEN.1 of FAU_SAA.1 is discarded. The dependency FAU_GEN.1 (Audit Data Generation) is not applicable to the TOE. Tachograph cards do not generate audit records but react with an error response. The detection of failure events implicitly covered in FAU_SAA.1 is clarified by a related refinement of the SFR.

The dependency FMT_MSA.3 of FDP_ACF.1 is discarded. The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Personalisation Phase, and are fixed over the whole lifetime of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, either during personalization, or within the usage phase of the TOE.

The dependency FMT_MSA.3 of FDP_ITC.1 is discarded. The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Personalisation Phase, and are fixed over the whole lifetime of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, either during personalization, or within the usage phase of the TOE.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1(2:SHA-2) is discarded. Not applicable as no keys are used for SHA-2.

The dependency FCS_CKM.4 of FCS_COP.1(2:SHA-2) is discarded. Not applicable as no keys are used for SHA-2.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1(6:SHA-1) is discarded. Not applicable as no keys are used for SHA-1.

The dependency FCS_CKM.4 of FCS_COP.1(6:SHA-1) is discarded. Not applicable as no keys are used for SHA-1.

9.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	

ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.2	(ADV_ARC.1) and (ADV_TDS.3) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2

Table 13 SARs Dependencies

9.3.4 Rationale for the Security Assurance Requirements

EAL4 augmented with ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5

9.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

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.

9.3.6 ATE_DPT.2 Testing: security enforcing modules

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

9.3.7 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the nature of the TOE and embedding product, ALC_DVS.2 is the most adequate for a manufacturing process in which several actors (Platform Developer, Operator, Application Developers, IC Manufacturer, etc) exchange and store highly sensitive informations (confidential code, cryptographic keys, personalisation data, etc).

10 TOE Summary Specification

10.1 TOE Summary Specification

The TOE inherits all the security functions provided by the underlying Java Card Open Platform (refer Security Target **[ST-PL]**). On top of these, it adds some supplemental security functions that are described hereafter.

SF.ACCESS_CONTROL_IN_READING

This function controls read access to files and enforces the security policy for data retrieval. This security function applies in phase 7. Prior to any file reading, it ensures the correct access conditions are met:

- The needed subject is authenticated (when needed)
- Expected secure messaging level is applied (when needed)

The function ensures that, for Driver card and workshop card, user data may be read from the TOE by any user, and for Control card and company card: Read Access conditions are provided to all users of TOE. User identification data stored in the 1st generation tachograph application, can be read by S.VU only.

It ensures the key stored in the filesystem of the workshop (KWC) can only be returned protected in confidentiality.

This function also ensures the readilibity of the card by card interface device of a Vehicle Unit or any card reader, in accordance with associated access rights.

SF.ACCESS_CONTROL_IN_WRITING

This function controls write access to files and enforces the security policy for data writing. This security function applies in phase 7. Prior to any file writing, it ensures the correct access conditions are met:

- If the Subject is identified as S.VU, it has access to write activity data to the card.
- Expected secure messaging level is applied (when needed).

The function ensures that for all card types: Card identification data and User identification data may only be written once and before the end of Personalisation and activity data may be written to the card by S.VU only.

Modification of identification data during the end-usage phase of the card life-cycle is not permitted.

It ensures that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

SF.AUTHENTICATION_DURING_PHASE7

This security function is in charge of the mutual authentication, during phase 7 of Tachograph life cycle between the TOE and the IFD. This security function identifies a Vehicle Unit by verifying that it has a valid public key certificate signed by the MSCA. It ensures that the vehicle unit is in possession of the corresponding private key. This is done by sending a random number that the vehicle unit in turn signs with the private key. The TOE then verifies the signature using the copy of public key stored in the TOE during personalization. After a successful verification of a vehicle unite its VRN and Registering Member State is stored in the card.

This security function enables to create a trusted channel by generating a shared ephemeral secret key and a secret dynamic non replay counter (SSC). This trusted channel enables to fulfill access conditions mandated to get access rights to files (Read/Update). The authentication protocol prevents the use of forged data authentication by using randomness. This security function is supported by SF.CRYPTOGRAPHIC_OPERATIONS.

This security function supports export of user data with/without security attributes by the applicable access rules on behalf of the user before the user authentication is actually performed.

Specific to workshop cards there is another functionality implemented for PIN Verification. In case of unsuccesful attempts while PIN Verification, the card will respond with Error messages handled through SF.ERROR_MESSAGES_AND_EXCEPTIONS.

SF.CLEARING_OF_SENSITIVE_INFORMATION

This security function ensures the clearing of sensitive information.

In phase 7

- o Session key, SSC, and authentication state are securely erased when a new authentication is started, or when the TOE is powered off/on
- o Session key and SSC are securely erased in case an error is detected in the incoming command (wrong MAC) or when more than 240 commands under secure messaging have been received
- o Authentication state is securely erased in case an error occurs in the authentication protocols.

SF.CRYPTOGRAPHIC_OPERATIONS

This security function ensures the usage of the secure cryptographic functionalities (including random numbers generation) that are resistant against attacks with high potential (AVA_VAN.5). These functionalities are provided by the underlying platform. This security functionality supports the others one by providing them Cryptographic operations.

SF.CRYPTOGRAPHIC_OPERATIONS performes the following cryptographic operations:

Key Generation:

- o SF.CRYPTOGRAPHIC_OPERATIONS generates AES keys of size 128, 192 and 256 bits.
- o SF.CRYPTOGRAPHIC_OPERATIONS generates T-DES keys of size 112 bits (2 individual keys of 64 bits each out of which 16 are parity bits all set to 0).
- o SF.CRYPTOGRAPHIC_OPERATIONS generates RSA keys of size 1024 bits.
- o SF.CRYPTOGRAPHIC_OPERATIONS generates ECC keys with domain parameters as described in Table for Standardised domain parameters.

Digital Signature Generation and Verification:

- o SF.CRYPTOGRAPHIC_OPERATIONS generates and verifies digital signatures using RSA algorithm with cryptographic key size of 1024 bits.

- SF.CRYPTOGRAPHIC_OPERATIONS generates and verifies digital signatures using ECC algorithm with the domain parameters as mentioned in Standardised domain parameters.

Cryptographic Hashing:

- SF.CRYPTOGRAPHIC_OPERATIONS performs cryptographic hashing in accordance with SHA-1, SHA-256, SHA-384 and SHA-512.

Encryption and Decryption:

- SF.CRYPTOGRAPHIC_OPERATIONS performs Encyption, Decryption and Retail MAC using T-DES.
- SF.CRYPTOGRAPHIC_OPERATIONS performs Encyption, Decryption and CMAC using AES.
- SF.CRYPTOGRAPHIC_OPERATIONS performs Encyption and Decryption using RSA.

Cryptographic Key Agreement:

- SF.CRYPTOGRAPHIC_OPERATIONS performs Cryptographic Key Agreement using ECC.

Mutual Authentication:

- SF.CRYPTOGRAPHIC_OPERATIONS performs Mutual Authentication between the card and vehicle unit using ECC.

Random Number Generation:

- SF.CRYPTOGRAPHIC_OPERATIONS performs Random Number Generation that meets the class DRG.3

Application Note:

More details related to key sizes of the cryptographic operations can be found in SFRs

- FCS_COP.1(1:AES)
- FCS_COP.1(2:SHA-2)
- FCS_COP.1(3:ECC)
- FCS_COP.1(4:TDES)
- FCS_COP.1(5:RSA)
- FCS_COP.1(6:SHA-1)

SF.ERROR_MESSAGES_AND_EXCEPTIONS

This security function is in charge of Handling Authentication failure Messages by:

- Warning the connected entity and assume the user to be a S.Non-VU.
- Block the PIN check procedure such that any subsequent PIN check attempt will fail for Workshop cards and be able to indicate to subsequent users the reason for the blocking.

The Security Function also caters to cardholder authentication failures, self test errors, stored data integrity errors, and activity data input integrity errors also.

SF.PHYSICAL_PROTECTION

This security function protects the TOE against physical attacks. It ensures their detection and provides counteractions.

SF.RAD_MANAGEMENT

This security function is in charge of the management of RAD in phase 7. In particular it is in charge of:

- Verification of VAD in phase 7

SF.SAFE_STATE_MANAGEMENT

This security function ensures that the TOE gets back to a secure state when

- An error is detected by the SF_SELF_TEST
- A tearing occurs (during a copy of data in EEPROM) This security function ensures that when such a case occurs, the TOE is either switched in the state "kill card" or becomes mute and gets back in the idle state (all ephemeral states are reset)

SF.SECURE_MESSAGING

This security function ensures the authenticity and integrity of the communication between the TOE and the IFD (namely a Vehicle Unit). A trusted channel is established after a successful mutual authentication based on a key transport protocol. This security functions relies on a checksum computed over the incoming command, and the outgoing data using Triple DES(for 1st Generation) and AES(for 2nd Generation) algorithm with the secure messaging session key. Moreover, this security function ensures the confidentiality of the content of some file when being read. In such cases, the data are encrypted with the secure messaging session key using Triple DES(for 1st Generation) and AES(for 2nd Generation)algorithms.

In order to protect the TOE against deletion, insertion or replay of protected commands, this security function manages as well a dynamic counter (SSC). This counter is increased each time a protected incoming command/outgoing data is processed. This security function is supported by SF.CRYPTOGRAPHIC_OPERATIONS.

SF.SELF_TESTS

The TOE performs self tests on the TSF data it stores to protect the TOE. In particular, this security function is in charge of:

- Detecting DFA
- Performing self tests of the random generator and cryptographic routines (DES, RSA)
- Monitoring of the integrity of keys, RAD, files, files attributes and TSF data
- Monitoring the integrity of the executable code
- Protecting the cryptographic operation
- Monitoring the correct operation of the executable code

The integrity checking of all the data is checked each time they are accessed. The self tests of the random generator and of the cryptographic routines are made at start up, as well as the integrity checks of the executable code. The protection of the cryptographic operation,of the executable code operation, and against DFA is made during TOE operation. This security function is supported by SF.CRYPTOGRAPHIC_OPERATIONS.

SF.SIGNATURE

This secure function ensures the signature generation of the TOE's file and its verification. For signature generation, it performs the hash computation of the currently selected, using SHA-1 algorithm and its signature with the TOE's private key. The signature verification is performed by unwrapping it with the public key imported on the TOE (using SF.KEY_MANAGEMENT) and the reference hash provided by the outside. This security function is supported by SF.CRYPTOGRAPHIC_OPERATIONS.

10.2 SFRs and TSS

10.2.1 SFRs and TSS - Rationale

TOE Security Requirements

FAU_ARP.1 The FAU_ARP.1 SFR is enforced by the SF.ERROR_MESSAGES_AND_EXCEPTIONS functionality.

The security function reports all the defined errors via SW1 SW2.

FAU_SAA.1 The FAU_SAA.1 SFR is enforced by the SF.ERROR_MESSAGES_AND_EXCEPTIONS functionality.

This security function detects all the mentioned errors and failures and ensures that the SFR is enforced.

FDP_ACC.2 The FDP_ACC.2 SFR is enforced by the SF.ACCESS_CONTROL_IN_READING, SF.ACCESS_CONTROL_IN_WRITING and SF.AUTHENTICATION_DURING_PHASE7 functionality.

The SF.ACCESS_CONTROL_IN_READING and SF.ACCESS_CONTROL_IN_WRITING in combination with SF.AUTHENTICATION_DURING_PHASE7 help identify S.VU and enforce the AC SFP.

FDP_ACF.1 The FDP_ACF.2 SFR is enforced by the SF.ACCESS_CONTROL_IN_READING, SF.ACCESS_CONTROL_IN_WRITING and SF.AUTHENTICATION_DURING_PHASE7 functionality.

The SF.ACCESS_CONTROL_IN_READING and SF.ACCESS_CONTROL_IN_WRITING in combination with SF.AUTHENTICATION_DURING_PHASE7 help identify S.VU and enforce the AC SFP.

FDP_DAU.1 The FDP_DAU.1 SFR is enforced by SF.SIGNATURE functionality.

The operations listed in the FDP_DAU.1 SFR can only be performed by the SF.SIGNATURE functionality and thus the SFR cannot be bypassed.

FDP_ETC.1 The FDP_ETC.1 SFR is enforced by SF.ACCESS_CONTROL_IN_READING and SF.ERROR_MESSAGES_AND_EXCEPTIONS functionalities.

SF.ACCESS_CONTROL_IN_READING ensures proper access conditions with regards to AC SFP are met and SF.ERROR_MESSAGES_AND_EXCEPTIONS handles any data integrity errors.

FDP_ETC.2 The FDP_ETC.2 SFR is enforced by SF.ACCESS_CONTROL_IN_READING and SF.ERROR_MESSAGES_AND_EXCEPTIONS functionalities.

SF.ACCESS_CONTROL_IN_READING ensures proper access conditions with regards to AC SFP are met and SF.ERROR_MESSAGES_AND_EXCEPTIONS handles any data integrity errors.

FDP_ITC.1 The FDP_ITC.1 SFR is enforced by SF.ACCESS_CONTROL_IN_WRITING and SF.ERROR_MESSAGES_AND_EXCEPTIONS functionalities.

SF.ACCESS_CONTROL_IN_WRITING ensures proper access conditions with regards to AC SFP are met and SF.ERROR_MESSAGES_AND_EXCEPTIONS handles any data integrity errors.

FDP_ITC.2 The FDP_ITC.2 SFR is enforced by SF.ACCESS_CONTROL_IN_WRITING and SF.ERROR_MESSAGES_AND_EXCEPTIONS functionalities.

SF.ACCESS_CONTROL_IN_WRITING ensures proper access conditions with regards to AC SFP are met and SF.ERROR_MESSAGES_AND_EXCEPTIONS handles any data integrity errors.

FDP_RIP.1 The FDP_RIP.1 SFR is enforced by the SF.CLEARING_OF_SENSITIVE_INFORMATION functionality.

The previous information content of a resource is made unavailable by SF.CLEARING_OF_SENSITIVE_INFORMATION functionality and thus the SFR cannot be bypassed.

FDP_SDI.2 The FDP_SDI.2 SFR is enforced by the SF.SELF_TESTS and SF_ERROR_MESSAGES_AND_EXCEPTIONS functionalities.

SF.SELF_TESTS along with SF.ERROR_MESSAGES_AND_EXCEPTIONS are able to detect, via self tests, if there are any integrity errors in the stored data thus making sure FDP_SDI.2 is not bypassed.

FIA_AFL.1(1:C) The FIA_AFL.1(1:C) SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7 and SF.ERROR_MESSAGES_AND_EXCEPTIONS functionalities.

SF.AUTHENTICATION_DURING_PHASE7 is able to identify the when the a failed authentication attempt happens and the error is reported though SF.ERROR_MESSAGES_AND_EXCEPTIONS.

FIA_AFL.1(2:WC) The FIA_AFL.1(2:WC) SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7, SF.ERROR_MESSAGES_AND_EXCEPTIONS and SF.RAD_MANAGEMENT functionalities.

SF.RAD_MANAGEMENT and SF.AUTHENTICATION_DURING_PHASE7 are able to identify if the number of failed authentication attempts has crossed the maximum allowed number and block the PIN beyond that. The error is reported by SF.ERROR_MESSAGES_AND_EXCEPTIONS thus ensuring that the SFR is not bypassed.

FIA_ATD.1 The FIA_ATD.1 SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7 functionality.

SF.AUTHENTICATION_DURING_PHASE7 can authenticate and identify users as S.VU and S.NON-VU and stores the attributes related to S.VU upon succesful authentication.

FIA_UAU.3 The FIA_UAU.3 SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7 functionality.

SF.AUTHENTICATION_DURING_PHASE7 ensures that only a VU in possession of the correct private key corresponding to the public key certificates signed by MSCA gets identified as S.VU and forged data cannot be used.

FIA_UAU.4 The FIA_UAU.4 SFR is enforced by the SF.CLEARING_OF_SENSITIVE_INFORMATION and SF.AUTHENTICATION_DURING_PHASE7 functionality.

SF.CLEARING_OF_SENSITIVE_INFORMATION and SF.AUTHENTICATION_DURING_PHASE7 ensures that keys after usage are destroyed and cannot be reused.

FIA_UID.2 The FIA_UID.2 SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7 functionality.

The user (i.e. applet) identification can only be performed by the SF.AUTHENTICATION_DURING_PHASE7 functionality and thus the FIA_UID.2 SFR cannot be bypassed.

FIA_USB.1 The FIA_USB.1 SFR is enforced by the SF.ACCESS_CONTROL_IN_READING and SF.ACCESS_CONTROL_IN_WRITING functionalities.

The user - Package AID association can only be performed by the SF.ACCESS_CONTROL_IN_READING and SF.ACCESS_CONTROL_IN_WRITING functionalities and thus the FIA_USB.1 SFR cannot be bypassed.

FPR_UNO.1 The FPR_UNO.1 SFR is enforced by SF.CRYPTOGRAPHIC_OPERATIONS, SF.AUTHENTICATION_DURING_PHASE7 and SF.PHYSICAL_PROTECTION functionalities.

The sensitive operations listed in the FPR_UNO.1 SFR can only be performed by SF.CRYPTOGRAPHIC_OPERATIONS, SF.AUTHENTICATION_DURING_PHASE7 and SF.PHYSICAL_PROTECTION functionalities listed above and thus the SFR cannot be bypassed.

FPT_FLS.1 The FPT_FLS.1 SFR is enforced by the SF.SAFE_STATE_MANAGEMENT functionality.

SF.SAFE_STATE_MANAGEMENT helps ensure that in case of any errors mentioned in the functional requirement the TOE preserves a safe state.

FPT_PHP.3 The FPT_PHP.3 SFR is enforced by the SF.PHYSICAL_PROTECTION functionality.

The physical manipulation and physical probing detection and management can only be performed by the SF.PHYSICAL_PROTECTION functionality.

FPT_TST.1 The FPT_TST.1 SFR is enforced by the SF.SELF_TESTS functionality.

SF.SELF_TESTS is responsible for running self tests on the TOE thus implementing the FPT_TST.1 Fucntional Requirement.

FPT_EMS.1 The FPR_EMS.1 SFR is enforced by the SF.PHYSICAL_PROTECTION functionality.

SF.PHYSICAL_PROTECTION is responsible for maintaining physical security and ensuring there are no emanations during secret operations in the TOE.

FCS_RNG.1 The FCS_RNG.1 SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality. SF.CRYPTOGRAPHIC_OPERATIONS ensures that a random number compliant with the requirement is generated when needed.

Security functional requirements for external communications (2nd Generation)

FCS_CKM.1(1) The FCS_CKM.1(1) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

The cryptographic key generation operation is performed by the SF.CRYPTOGRAPHIC_OPERATIONS functionality that ensures that cryptographic keys that meet the requirement are generated thus making sure the sfr is implemented.

FCS_CKM.2(1) The FCS_CKM.2(1) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

THe security function generates session keys based on key agreement thus enforcing the SFR

FCO_NRO.1 The FCO_NRO.1 SFR is enforced by the SF.SIGNATURE functionality.

SF.SGINATURE ensures functionality for signature generation and verification thus making sure the SFR is implemented.

FCS_CKM.4(1) The FCS_CKM.4(1) SFR is enforced by the SF.CLEARING_OF_SENSITIVE_INFORMATION functionality.

SF.CLEARING_OF_SENSITIVE_INFORMATION ensure that all the session keys are destroyed on power of or when a new authentication is attempted or upon expiry of the keys.

FCS_COP.1(1:AES) The FCS_COP.1(1:AES) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

SF.CRYPTOGRAPHIC_OPERATIONS is capable of performing the cyrptographic operations defined in the SFR.

FCS_COP.1(2:SHA-2) The FCS_COP.1(2:SHA-2) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

SF.CRYPTOGRAPHIC_OPERATIONS is capable of performing the cyrptographic operations defined in the SFR.

FCS_COP.1(3:ECC) The FCS_COP.1(3:ECC) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS and SF.AUTHENTICATION_DURING_PHASE7 functionalities.

SF.CRYPTOGRAPHIC_OPERATIONS is capable of performing the cyrptographic operations defined in the SFR for the authentication defined in SF.AUTHENTICATION_DURING_PHASE7.

FIA_UAU.1(1) The FIA_UAU.1(1) SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7 and SF.ACCESS_CONTROL_IN_READING functionality.

SF.AUTHENTICATION_DURING_PHASE7 and SF.ACCESS_CONTROL_IN_READING together are responsible for ensuring proper access conditions are met before exporting data and users are authenticated for export of data as defined in [EU – 2016/799] Annex 1C, Appendix 2

FPT_TDC.1(1) The FPT_TDC.1(1) SFR is enforced by the SF.SECURE_MESSAGING functionality.

The security function is responsible for maintaining the secure communication channel between the TOE and any connected entity.

FTP_ITC.1(1) The FTP_ITC.1(1) SFR is enforced by the SF.SECURE_MESSAGING and SF.CRYPTOGRAPHIC_OPERATIONS functionality.

SF.SECURE_MESSAGING and SF.CRYPTOGRAPHIC_OPERATIONS together ensure that all commands and responses are sent using Secure Messaging(using AES) to ensure confidentiality.

Security functional requirements for external communications (1st generation)

FCS_CKM.1(2) The FCS_CKM.1(2) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

The cryptographic key generation operation is performed by the SF.CRYPTOGRAPHIC_OPERATIONS functionality that ensures that cryptographic keys that meet the requirement are generated thus making sure the sfr is implemented.

FCS_CKM.2(2) The FCS_CKM.2(2) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

THe security function generates session keys based on key agreement thus enforcing the SFR

FCS_CKM.4(2) The FCS_CKM.4(2) SFR is enforced by the SF.CLEARING_OF_SENSITIVE_INFORMATION functionality.

SF.CLEARING_OF_SENSITIVE_INFORMATION ensure that all the session keys are destroyed on power of or when a new authentication is attempted or upon expiry of the keys.

FCS_COP.1(4:TDES) The FCS_COP.1(4:TDES) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

SF.CRYPTOGRAPHIC_OPERATIONS is capable of performing the cyrptographic operations defined in the SFR.

FCS_COP.1(5:RSA) The FCS_COP.1(5:RSA) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS and SF.AUTHENTICATION_DURING_PHASE7 functionalities.

SF.CRYPTOGRAPHIC_OPERATIONS is capable of performing the cyrptographic operations defined in the SFR.

FCS_COP.1(6:SHA-1) The FCS_COP.1(6:SHA-1) SFR is enforced by the SF.CRYPTOGRAPHIC_OPERATIONS functionality.

SF.CRYPTOGRAPHIC_OPERATIONS is capable of performing the cyrptographic operations defined in the SFR.

FIA_UAU.1(2) The FIA_UAU.1(2) SFR is enforced by the SF.AUTHENTICATION_DURING_PHASE7 and SF.ACCESS_CONTROL_IN_READING functionality.

SF.AUTHENTICATION_DURING_PHASE7 and SF.ACCESS_CONTROL_IN_READING together are responsible for ensuring proper access conditions are met before exporting data and users are authenticated for export of data as defined in [EU – 2016/799] Annex 1C, Appendix 2

FPT_TDC.1(2) The FPT_TDC.1(2) SFR is enforced by the SF.SECURE_MESSAGING functionality.

The security function is responsible for maintaining the secure communication channel between the TOE and any connected entity.

FTP_ITC.1(2) The FTP_ITC.1(2) SFR is enforced by the SF.SECURE_MESSAGING and SF.CRYPTOGRAPHIC_OPERATIONS functionality.

SF.SECURE_MESSAGING and SF.CRYPTOGRAPHIC_OPERATIONS together ensure that all commands and responses are sent using Secure Messaging(using TDES) to ensure confidentiality.

10.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_ARP.1	SF.ERROR_MESSAGES_AND_EXCEPTIONS
FAU_SAA.1	SF.ERROR_MESSAGES_AND_EXCEPTIONS
FDP_ACC.2	SF.ACCESS_CONTROL_IN_READING, SF.ACCESS_CONTROL_IN_WRITING, SF.AUTHENTICATION_DURING_PHASE7
FDP_ACF.1	SF.ACCESS_CONTROL_IN_READING,

	SF.ACCESS_CONTROL_IN_WRITING, SF.AUTHENTICATION_DURING_PHASE7
FDP_DAU.1	SF.SIGNATURE
FDP_ETC.1	SF.ACCESS_CONTROL_IN_READING, SF.ERROR_MESSAGES_AND_EXCEPTIONS
FDP_ETC.2	SF.ACCESS_CONTROL_IN_READING, SF.ERROR_MESSAGES_AND_EXCEPTIONS
FDP_ITC.1	SF.ACCESS_CONTROL_IN_WRITING, SF.ERROR_MESSAGES_AND_EXCEPTIONS
FDP_ITC.2	SF.ACCESS_CONTROL_IN_WRITING, SF.ERROR_MESSAGES_AND_EXCEPTIONS
FDP_RIP.1	SF.CLEARING_OF_SENSITIVE_INFORMATION
FDP_SDI.2	SF.SELF_TESTS, SF.ERROR_MESSAGES_AND_EXCEPTIONS
FIA_AFL.1(1:C)	SF.AUTHENTICATION_DURING_PHASE7, SF.ERROR_MESSAGES_AND_EXCEPTIONS
FIA_AFL.1(2:WC)	SF.AUTHENTICATION_DURING_PHASE7, SF.ERROR_MESSAGES_AND_EXCEPTIONS, SF.RAD_MANAGEMENT
FIA_ATD.1	SF.AUTHENTICATION_DURING_PHASE7
FIA_UAU.3	SF.AUTHENTICATION_DURING_PHASE7
FIA_UAU.4	SF.CLEARING_OF_SENSITIVE_INFORMATION, SF.AUTHENTICATION_DURING_PHASE7
FIA_UID.2	SF.AUTHENTICATION_DURING_PHASE7
FIA_USB.1	SF.ACCESS_CONTROL_IN_READING, SF.ACCESS_CONTROL_IN_WRITING
FPR_UNO.1	SF.PHYSICAL_PROTECTION, SF.AUTHENTICATION_DURING_PHASE7, SF.CRYPTOGRAPHIC_OPERATIONS
FPT_FLS.1	SF.SAFE_STATE_MANAGEMENT
FPT_PHP.3	SF.PHYSICAL_PROTECTION
FPT_TST.1	SF.SELF_TESTS
FPT_EMS.1	SF.PHYSICAL_PROTECTION
FCS_RNG.1	SF.CRYPTOGRAPHIC_OPERATIONS
FCS_CKM.1(1)	SF.CRYPTOGRAPHIC_OPERATIONS
FCS_CKM.2(1)	SF.CRYPTOGRAPHIC_OPERATIONS
FCO_NRO.1	SF.SIGNATURE
FCS_CKM.4(1)	SF.CLEARING_OF_SENSITIVE_INFORMATION
FCS_COP.1(1:AES)	SF.CRYPTOGRAPHIC_OPERATIONS

FCS_COP.1(2:SHA-2)	SF.CRYPTOGRAPHIC_OPERATIONS
FCS_COP.1(3:ECC)	SF.CRYPTOGRAPHIC_OPERATIONS, SF.AUTHENTICATION_DURING_PHASE7
FIA_UAU.1(1)	SF.AUTHENTICATION_DURING_PHASE7, SF.ACCESS_CONTROL_IN_READING
FPT_TDC.1(1)	SF.SECURE_MESSAGING
FTP_ITC.1(1)	SF.SECURE_MESSAGING, SF.CRYPTOGRAPHIC_OPERATIONS
FCS_CKM.1(2)	SF.CRYPTOGRAPHIC_OPERATIONS
FCS_CKM.2(2)	SF.CRYPTOGRAPHIC_OPERATIONS
FCS_CKM.4(2)	SF.CLEARING_OF_SENSITIVE_INFORMATION
FCS_COP.1(4:TDES)	SF.CRYPTOGRAPHIC_OPERATIONS
FCS_COP.1(5:RSA)	SF.CRYPTOGRAPHIC_OPERATIONS, SF.AUTHENTICATION_DURING_PHASE7
FCS_COP.1(6:SHA-1)	SF.CRYPTOGRAPHIC_OPERATIONS
FIA_UAU.1(2)	SF.AUTHENTICATION_DURING_PHASE7, SF.ACCESS_CONTROL_IN_READING
FPT_TDC.1(2)	SF.SECURE_MESSAGING
FTP_ITC.1(2)	SF.SECURE_MESSAGING, SF.CRYPTOGRAPHIC_OPERATIONS

Table 14 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.ACCESS_CONTROL_IN_READING	FDP_ACC.2, FDP_ACF.1, FDP_ETC.1, FDP_ETC.2, FIA_USB.1, FIA_UAU.1(1), FIA_UAU.1(2)
SF.ACCESS_CONTROL_IN_WRITING	FDP_ACC.2, FDP_ACF.1, FDP_ITC.1, FDP_ITC.2, FIA_USB.1
SF.AUTHENTICATION_DURING_PHASE7	FDP_ACC.2, FDP_ACF.1, FIA_AFL.1(1:C), FIA_AFL.1(2:WC), FIA_ATD.1, FIA_UAU.3, FIA_UAU.4, FIA_UID.2, FPR_UNO.1, FCS_COP.1(3:ECC), FIA_UAU.1(1), FCS_COP.1(5:RSA), FIA_UAU.1(2)
SF.CLEARING_OF_SENSITIVE_INFORMATION	FDP_RIP.1, FIA_UAU.4, FCS_CKM.4(1), FCS_CKM.4(2)
SF.CRYPTOGRAPHIC_OPERATIONS	FPR_UNO.1, FCS_RNG.1, FCS_CKM.1(1), FCS_CKM.2(1), FCS_COP.1(1:AES), FCS_COP.1(2:SHA-2), FCS_COP.1(3:ECC), FTP_ITC.1(1), FCS_CKM.1(2), FCS_CKM.2(2), FCS_COP.1(4:TDES), FCS_COP.1(5:RSA),

	FCS_COP.1(6:SHA-1), FTP_ITC.1(2)
SF.ERROR_MESSAGES_AND_EXCEPTIONS	FAU_ARP.1, FAU_SAA.1, FDP_ETC.1, FDP_ETC.2, FDP_ITC.1, FDP_ITC.2, FDP_SDI.2, FIA_AFL.1(1:C), FIA_AFL.1(2:WC)
SF.PHYSICAL_PROTECTION	FPR_UNO.1, FPT_PHP.3, FPT_EMS.1
SF.RAD_MANAGEMENT	FIA_AFL.1(2:WC)
SF.SAFE_STATE_MANAGEMENT	FPT_FLS.1
SF.SECURE_MESSAGING	FPT_TDC.1(1), FTP_ITC.1(1), FPT_TDC.1(2), FTP_ITC.1(2)
SF.SELF_TESTS	FDP_SDI.2, FPT_TST.1
SF.SIGNATURE	FDP_DAU.1, FCO_NRO.1

Table 15 TSS and SFRs - Coverage

.

11 Security Assurance Requirements

This chapter defines the list of the assurance measures required for the TOE security assurance requirements. The EAL4 + is claimed.

11.1 Evaluation Assurance Level rationale

The following assurance packages are required:

Measures	**Name**
ADV	Development
AGD	Guidance
ALC	Life Cycle
ASE	Security target
ATE	Tests
AVA	Vulnerability

11.1.1 ADV: Development

The following components are included:

Measures	**Level**
ADV_ARC	1
ADV_FSP	4
ADV_IMP	1
ADV_TDS	3

11.1.2 AGD: Guidance

The following components are included:

Measures	**Level**
AGD_OPE	1
AGD_PRE	1

11.1.3 ALC: Life cycle

The following components are included:

Measures	**Level**
ALC_CMC	4
ALC_CMS	4
ALC_DEL	1
ALC_DVS	2 - augmented
ALC_FLR	N/A
ALC_LCD	1
ALC_TAT	1

11.1.4 ASE: Security target

The following components are included:

Measures	Level
ASE_CCL	1
ASE_ECD	1
ASE_INT	1
ASE_OBJ	2
ASE_REQ	2
ASE_SPD	1
ASE_TSS	1

11.1.5 ATE: Tests

The following components are included:

Measures	Level
ATE_COV	2
ATE_DPT	2 - augmented
ATE_FUN	1
ATE_IND	2

11.1.6 AVA : Vulnerability

The following components are included:

Measures	Level
AVA_VAN	5 - augmented

11.2 Rationale for augmentation

11.2.1 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

All the dependencies of AVA_VAN.5, listed below are fulfilled:

- ADV_ARC.1
- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- AGD_OPE.1
- AGD_PRE.1

- ATE_DPT.2

11.2.2 ATE_DPT.2 Testing: security enforcing modules

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

All the dependencies of ATE_DPT.2, listed below are fulfilled:

- ADV_ARC.1
- ADV_TDS.3
- ATE_FUN.1

11.2.3 ALC_DVS.2 Sufficiency of security measures

In order to protect the TOE on development Phase, the component ALC_DVS.2 was added. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2 does not have any dependencies.