STMicroelectronics

J-Tacho Security Target Public Version

Common Criteria for IT security evaluation

J-TACHO_SecurityTarget_Lite Rev. B
05 April 2019

BLANK

J-TACHO
Security Target Public Version

Common Criteria for IT Evaluation

1. INTRODUCTION

1.1 Document Reference

Document identification: **J-TACHO Security Target - Public Version**
Revision: **B**
Registration: **J-TACHO_SecurityTarget_Lite**

1.2 Security Target Reference

Document identification: **J-TACHO Security Target**
Revision: **F**
Registration: **J-TACHO Security Target**

1.3 TOE Reference

- TOE Name and Version: **J-Tacho v.1.2.6**

2. SCOPE

This document is a sanitized version of the Security Target used for the evaluation. It is classified as public information.

INDEX

List of tables

List of figures

3. REFERENCE DOCUMENTS

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CEM-2017-04-004.

[PP_TACHO] Digital Tachograph – Tachograph Card (TC PP) – BSI-CC-PP-0091-2017, Version 1.0

[EU_2016_165] 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.

[EC1360_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).

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

[JCVM3] Java Card Platform, versions 3.0 (March 2008), 3.0.1 (April 2009) and 3.0.4 (September 2011), Classic Edition, Virtual Machine (Java Card VM) Specification. Published by Sun Microsystems, Inc.

[JCAPI3] Java Card Platform, versions 3.0 (March 2008), 3.0.1 (April 2009) and 3.0.4 (September 2011), Classic Edition, Application Programming Interface, March 2008. Published by Sun Microsystems, Inc.

[JCRE3] Java Card Platform, versions 3.0 (March 2008), 3.0.1 (April 2009) and 3.0.4 (September 2011), Classic Edition, Runtime Environment (Java Card RE) Specification. March 2008. Published by Sun Microsystems, Inc.

[GP221] GlobalPlatform Card Specification, Version 2.2.1, January 2011.

[PP_JC_Closed] Java Card System – Closed Configuration Protection Profile, Version 3.0, December 2012 [ANSSI-CC-PP-2010/07-M01]

[PP_0035] Security IC Platform Protection Profile, Version 1.0, 15 July 2007.

[BSI_ PP_0084] BSI-CC-PP-0084-2014 – Eurosmart – Security IC Platform Protection Profile with Augmentation Packages.

[STLite_ST31G480] ST31G480 D01 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFIRE EV1 and MIFARE PLUS X Security Target for composition, Rev D01.3, October 2018.

[BSI_AIS20] Functionality classes and evaluation methodology for deterministic random number generators, BSI, Version 1, 02-12-1999

[BSI_AIS20/AIS31] A proposal for: Functionality classes for random number generators, W. Killmann & W. Schindler, BSI, Version 2.0, 18 September 2011

[NIST_800-22] National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Special Publication 800-22 Rev.1a April 2010

[Tacho_AGD_OPE] J-TACHO Operational User Guidance v1

[Tacho_AGD_PRE] J-TACHO Preparative Procedure v1

4. DEFINITIONS

Term	Meaning
0x	C-fashion hexadecimal prefix
A.XXX	Assumption
AID	Application identifier, an ISO-7816 data format used for unique identification of Java Card applets (and certain kinds of files in card file systems). The Java Card platform uses the AID data format to identify applets and packages. AIDs are administered by the International Opens Organization (ISO), so they can be used as unique identifiers. AIDs are also used in the security policies (see "Context" below): applets' AIDs are related to the selection mechanisms, packages' AIDs are used in the enforcement of the firewall. Note: although they serve different purposes, they share the same namespace.
APDU	Application Protocol Data Unit, an ISO 7816-4 defined communication format between the card and the off-card applications. Cards receive requests for service from the CAD in the form of APDUs. These are encapsulated in Java Card System by the javacard.framework.APDU class ([JCAPI3]). APDUs manage both the selection-cycle of the applets (through Java Card RE mediation) and the communication with the Currently selected applet.
APDU buffer	The APDU buffer is the buffer where the messages sent (received) by the card depart from (arrive to). The Java Card RE owns an APDU object (which is a Java Card RE Entry Point and an instance if the javacard.framework.APDU class) that encapsulates APDU messages in an internal byte array, called the APDU buffer. This object is made accessible to the currently selected applet when needed, but any permanent access (out-of selection-scope) is strictly prohibited for security reasons.
Applet	The name given to any Java Card technology-based application. An applet is the basic piece of code that can be selected for execution from outside the card. Each applet on the card is uniquely identified by its AID.
CAD	Card Acceptance Device or card reader. The device where the card is inserted, and which is used to communicate with the card. Unless explicitly said otherwise, in this document, CAD covers PCD.
CAP file	A file in the Converted applet format. A CAP file contains a binary representation of a package of classes that can be installed on a device and used to execute the package's classes on a Java Card virtual machine. A CAP file can contain a user library, or the code of one or more applets.
CC	Common Criteria
Class	In object-oriented programming languages, a class is a prototype for an object. A class may also be considered as a set of objects that share a common structure and behavior. Each class declares a collection of fields and methods associated to its instances. The contents of the fields determine the internal state of a class instance, and the methods the operations that can be applied to it. Classes are ordered within a class hierarchy. A class declared as a specialization (a subclass) of another class (its super class) inherits all the fields and methods of the latter. Java platform classes should not be confused with the classes

	of the functional requirements (FIA) defined in the CC.
CM	Card Manager
Context	A context is an object-space partition associated to a package. Applets within the same Java technology-based package belong to the same context. The firewall is the boundary between contexts (see “Current context”).
Current Context	The Java Card RE keeps track of the current Java Card System context (also called “the active context”). When a virtual method is invoked on an object, and a context switch is required and permitted, the current context is changed to correspond to the context of the applet that owns the object. When that method returns, the previous context is restored. Invocations of static methods have no effect on the current context. The current context and sharing status of an object together determine if access to an object is permissible.
Currently Selected Applet	The applet has been selected for execution in the current session. The Java Card RE keeps track of the currently selected Java Card applet. Upon receiving a SELECT command from the CAD or PCD with this applet’s AID, the Java Card RE makes this applet the currently selected applet over the I/O interface that received the command. The Java Card RE sends all further APDU commands received over each interface to the currently selected applet on this interface ([JCRE3], Glossary).
Default Applet	The applet that is selected after a card reset or upon completion of the PICC activation sequence on the contactless interface ([JCRE3], §4.1)
DPA	Differential Power Analysis is a form of side channel attack in which an attacker studies the power consumption of a cryptographic hardware device such as a smart card.
EAL	Evaluation Assurance Level
Embedded Software	Pre-issuance loaded software.
ES	Embedded Software
Firewall	The mechanism in the Java Card technology for ensuring applet isolation and object sharing. The firewall prevents an applet in one context from unauthorized access to objects owned by the Java Card RE or by an applet in another context.
HAL	Hardware Abstraction Layer
IC	Integrated Circuit
Installer	The installer is the on-card application responsible for the installation of applets on the card. It may perform (or delegate) mandatory security checks according to the card issuer policy (for bytecode-verification, for instance), loads and link packages (CAP file(s)) on the card to a suitable form for the Java Card VM to execute the code they contain. It is a subsystem of what is usually called “card manager”; as such, it can be seen as the portion of the card manager that belongs to the TOE. The installer has an AID that uniquely identifies him, and may be implemented as a Java Card applet. However, it is granted specific privileges on an implementation-specific manner ([JCRE3],§10). The installer is the on-card application responsible for the installation of applets on the card. It may perform (or delegate) mandatory security checks according to the card issuer policy (for bytecode-verification, for instance), loads and link packages (CAP file(s)) on the card to a suitable form for the Java Card VM to execute the code they contain. It is a subsystem of what is usually called “card manager”; as such, it can be seen as the portion of the card manager that belongs to the TOE.

	The installer has an AID that uniquely identifies him, and may be implemented as a Java Card applet. However, it is granted specific privileges on an implementation-specific manner ([JCRE3],§10).
Interface	A special kind of Java programming language class, which declares methods, but provides no implementation for them. A class may be declared as being the implementation of an interface, and in this case must contain an implementation for each of the methods declared by the interface (See also shareable interface).
Java Card RE	The runtime environment under which Java programs in a smart card are executed. It is in charge of all the management features such as applet lifetime, applet isolation, object sharing, applet loading, applet initializing, transient objects, the transaction mechanism and so on.
Java Card RE Entry Point	An object owned by the Java Card RE context but accessible by any application. These methods are the gateways through which applets request privileged Java Card RE services: the instance methods associated to those objects may be invoked from any context, and when that occurs, a context switch to the Java Card RE context is performed. There are two categories of Java Card RE Entry Point Objects: Temporary ones and Permanent ones. As part of the firewall functionality, the Java Card RE detects and restricts attempts to store references to these objects.
Java Card RMI	Java Card Remote Method Invocation is the Java Card System version 2.2 and 3 Classic Edition mechanism enabling a client application running on the CAD platform to invoke a method on a remote object on the card. Notice that in Java Card System, version 2.1.1, the only method that may be invoked from the CAD is the process method of the applet class.
Java Card System	Java Card System includes the Java Card RE, the Java Card VM, the Java Card API and the installer.
Java Card VM	The embedded interpreter of bytecodes. The Java Card VM is the component that enforces separation between applications (firewall) and enables secure data sharing.
Logical Channel	A logical link to an application on the card. A new feature of the Java Card System, version 2.2 and 3 Classic Edition, that enables the opening of simultaneous sessions with the card, one per logical channel. Commands issued to a specific logical channel are forwarded to the active applet on that logical channel. Java Card platform, version 2.2.2 and 3 Classic Edition, enables opening up to twenty logical channels over each I/O interface (contacted or contactless).
NVRAM	Non-Volatile Random Access Memory, a type of memory that retains its contents when power is turned off.
O.xxx	Security objectives for the TOE.
Object Deletion	The Java Card System version 2.2 and 3 Classic Edition mechanism ensures that any unreferenced persistent (transient) object owned by the current context is deleted. The associated memory space is recovered for reuse prior to the next card reset.
OE.xxx	Security objectives for the environment.
OSP.xxx	Organizational security policies.
Package	A package is a namespace within the Java programming language that may contain classes and interfaces. A package defines either a user library, or one or more applet definitions. A package is divided in two sets of files: export files (which exclusively contain the public interface information for an entire

	package of classes, for external linking purposes; export files are not used directly in a Java Card virtual machine) and CAP files.
PCD	Proximity Coupling Device. The PCD is a contactless card reader device.
PICC	Proximity Card. The PICC is a card with contactless capabilities.
PP	Protection Profile.
RAM	Random Access Memory, is a type of computer memory that can be accessed randomly.
ROM	Read Only Memory.
SC	Smart Card
SCP	Smart Card Platform.It is comprised of the integrated circuit, the operating system and the dedicated software of the smart card.
SF.xxx	Security Functionality
Shareable Interface	An interface declaring a collection of methods that an applet accepts to share with other applets. These interface methods can be invoked from an applet in a context different from the context of the object implementing the methods, thus “traversing” the firewall.
SIO	An object of a class implementing a shareable interface.
ST	Security Target
Subject	An active entity within the TOE that causes information to flow among objects or change the system’s status. It usually acts on behalf of a user. Objects can be active and thus are also subjects of the TOE.
TOE	Target Of Evaluation
Transient Object	An object whose contents are not preserved across CAD sessions. The contents of these objects are cleared at the end of the current CAD session or when a card reset is performed. Writes to the fields of a transient object are not affected by transactions.
User	Any application interpretable by the Java Card RE. That also covers the packages. The associated subject(s), if applicable, is (are) an object(s) belonging to the javacard.framework.applet class.
VM	Virtual Machine

5. J-TACHO Security Target

5.1 ST Introduction

5.1.1 Security Target Reference

Document identification: **J-Tacho** Security Target
Revision: F
Date: 03 April 2019
Registration: **J-Tacho Security Target**

5.1.2 TOE Reference

TOE Name and Version: **J-Tacho v.1.2.6**
TOE short Name: **J-Tacho**
The TOE comprises the following items:

- The Tachograph Application - package version 1.13
- J-SAFE3 Java Card Platform (including the native Operating System) v1.2.6
- Hardware: ST31G480 D01 (available formats are listed in 5.1.6).
- J-TACHO – Operational User Guidance [Tacho_AGD_OPE]
- J-TACHO – Preparative Procedure [Tacho_AGD_PRE]

5.1.3 Purpose

This document details the **Security Target** of **J-TACHO**: **STMicroelectronics Tachograph application:** a EAL4+ certified a Digital Tachograph Card based on the requirements and recommendations of the EU regulation 165/2014, on top of J-SAFE3 Java Card Platform and designed on certified IC ST31G480 **platform (**ST31G480 D01 including optional cryptographic library NESLIB, V.6.2.1) (see [STLite_ST31G480].
The precise description of the Target of Evaluation (TOE) and the related features are given in next sections.
A glossary of terms and abbreviations used in this document is given in chapter 4.
The Security Target conforms to the Protection Profile: Digital Tachograph – Tachograph Card [PP_TACHO].

5.1.4 TOE overview

The TOE is the micro-module made of the Integrated Circuit (IC) and its embedded software. Embedded Software includes J-SAFE3 Java Card platform and the Tachograph Application (both First and Second Generation). It includes the associated embedded data of the smart card working on the micro-controller unit in accordance with the functional specifications.
This Security Target defines security objectives and security requirements for the Digital Tachograph Card based on the requirements and recommendations of the EU Regulation 165/2014. The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the Tachograph application and data during its life cycle.
Detailed description of the TOE, of its security functionalities, its security features, its security environment, assets to be protected and threats to be countered, of its security objectives and security requirements can be found in next sections (see §5.1.5 and §5.1.8).

5.1.5 TOE TYPE

The Target of Evaluation detailed in this Security Target is STM Tachograph Application **J-Tacho** (from now on also referenced as the TOE).

The TOE is constituted by the following blocks:

- The Tachograph Application - (including 1st and 2nd generation application functionalities)
- J-SAFE3 Java Card Platform (including the native Operating System, providing to the Java Card System a low-level support of hardware functionalities and implementing I/O communication);
- The hardware IC and its associated crypto library (already certified as ST31G480 D01 including optional crypto library NESLIB V.6.2.1) (see [STLite_ST31G480]).

The TOE is compliant with Global Platform 2.2.1 standard [GP221] which provides a set of APIs and technologies to perform in a secure way the operations involved in the management of the applications hosted by the card.

Being J-TACHO a closed product, card content management interface is permanently disabled before card delivery.
After TOE delivery GP functionality is available for TOE Identification.
Besides, only the API subset related to life-cycle management of card and J-TACHO application are considered as part of the TOE, while all other GP API and the Card Manager application belongs to the TOE environment and are not in the scope of current evaluation.

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

The TOE is a smart card, the Tachograph Card, which is configured and implemented as a **driver card, workshop card, control card or company card** in accordance with [EU_2016_165] Annex 1C, Appendix 2, Appendix 10 and Appendix 11. In particular, this implies the compliance with the following standards: ISO/IEC 7810 Identification cards – Physical characteristics and ISO/IEC 7816 Identification cards - Integrated circuit cards part 1,2,3,4,8.

5.1.6 TOE Boundaries

Physical Boundaries

The TOE is constituted by hardware and software parts and is available in several formats depending on the product end usage:

- Contact-only card (IC packaged as micro-module and embedded in a plastic card body)
- IC packaged in several module formats for integration on PCBs or plastic cards)
- Wafers or sawn wafers (e.g.: to be embedded by third parties)

Logical Boundaries

The Target of Evaluation (TOE) is composed of the Java Card J-TACHO, a Digital Tachograph Application, the Java Card smart card platform and the IC.

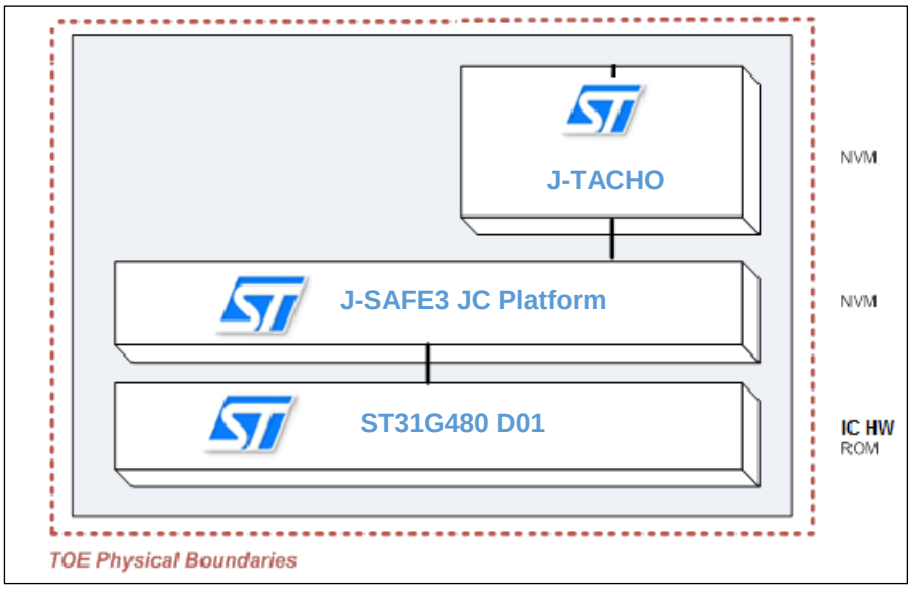


Figure 1 – J-TACHO Digital Tachograph

5.1.7 Hardware IC and dedicated crypto library

The basis of this composite evaluation is the STMicroelectronics' **ST31G480** certified Secured Microcontroller plus the NesLib v.6.2.1 crypto-library.

The ST31G480 Secure Microcontroller with Cryptographic Library has been certified by ANSSI (cert. report ANSSI-CC-2019/12) with assurance level EAL5+: its associated Security Target Lite is [STLite_ST31G480].

NOTE: Even though the TOE includes the IC and the crypto-library, not all the functionalities of the IC and crypto-library are used.
NOTE: the TOE does not need any other hardware or software outside of the TOE to operate as claimed.

5.1.8 TOE FUNCTIONALITIES

The TOE provides the following basic functionalities:

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

The TOE provides the following main security functionalities:

- Preservation of card identification data and user identification data stored during the card personalization process;
- Safe storage of user data stored in the card by Vehicle Units (VU)
- Allowance of certain write operations onto the cards to only an authenticated VU.

Specifically the Tachograph Card aims to protect:

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

- 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:

- User identification and authentication;
- Access control to functions and stored data;
- Alerting of events and faults;
- Integrity of stored data;
- Reliability of services;
- Data exchange with a Vehicle Unit and export of data to other IT entities;
- Cryptographic support for VU-card mutual authentication and secure messaging as well as for key generation and key agreement according to [EU_2016_165] Annex 1C, Appendix 11.

All cryptographic mechanisms, including algorithms and the length of corresponding keys, have to be implemented exactly as required and defined in [EU_2016_165] Annex 1C, Appendix 11, Part B for second generation mechanisms, and in [EU_2016_165] Annex 1C, Appendix 11, Part A for first generation mechanisms.
Cryptographic mechanisms supported by all cards include mutual authentication towards VUs. Additional cryptographic mechanisms, as applied within the different types of card are:

1. **Driver cards** – creation of signatures over data downloads
2. **Workshop cards** – PIN verification, verification of MACs over Remote Tachograph Monitoring data and decryption of such data, creation of signatures over data downloads from workshop cards
3. **Control cards** - verification of MACs over Remote Tachograph Monitoring data and decryption of such data, verification of signatures over data downloaded from VUs, driver cards or workshop cards.

As stated the TOE implements the Tachograph Application - (1st and 2nd generation). The main differences between the 2nd generation Digital Tachograph System and the 1st generation are reported in [PP_TACHO].

Below a short list of functionalities provided by the underlying java card platform J-SAFE3.

- communication protocols:
  - ISO 7816 T=0 (direct and inverse convention)
  - ISO 7816 T=1 (direct and inverse convention)
  - Extended Length APDUs (Only T=1)
- Cryptographic functionalities:
  - 3-DES (112 and 168 bit keys) for encryption/decryption in ECB and CBC mode, MAC generation and verification (CBC-MAC, Retail-MAC)
  - AES (key length 128, 192, 256) for encryption/decryption in ECB and CBC mode, MAC generation and verification (CBC-MAC, CMAC)
  - RSA (with keys up to 2048 bits) for encryption/decryption, signature verification, key generation in both Standard and CRT mode.
  - Message Digest with SHA-1, SHA-224, SHA-256, SHA384, SHA-512 algorithms
  - Elliptic Curve cryptography over GF(p) for key length between 112 and 521 bits
  - Diffie-Hellman and EC Diffie-Hellman key agreement algorithms
  - Secure random number generation mechanisms compliant to PTG.2 Class and DRG.3 Class defined in [BSI_AIS20/AIS31].
- JC functionalities compliant with [PP_JC_Closed]:
  - Logical Channel awareness (only Basic Logical Channel is supported)
  - Object Deletion (garbage collection) with memory reclamation
  - Application loading, linking and installation operations limited to pre-delivery phase in a controlled environment
- Proprietary functionalities:
  - Key Agreement based on Discrete Logarithm (Diffie-Hellmann)

- Stateless (one-shot) ECDSA, RSA and Digest operations
- Optimized handling of EC Curve parameters among EC Keys
- Secure Storage API (integrity-protected arrays)
- Secure comparison of byte arrays
- Generation of random primes

5.1.9 TOE Life-Cycle

The TOE life cycle, i.e. the OS, the Java Card platform and the J-TACHO application, spans from product development phase to its operational phase/usage by the final user. The TOE life cycle is fully conform to the claimed PP. The TOE life cycle phases are those detailed in Figure 2. We refer to IC Protection Profile [PP_0035] and [BSI_ PP_0084] for a thorough description of

Phases 1 to 7:

- Phases 1 Embedded Software (Native OS, Java Card System, other platform components such as Card Manager, J-TACHO Applets).
- Phases 2 IC development (IC with Dedicated Software and NesLib v.6.2.1 Cryptographic Library)
- Phase 3 and 4 IC manufacturing, packaging and testing. Some IC pre-personalization steps may occur in Phase 3.
- Phase 5 TOE Product Finishing Process concerns with the embedding of software components within the IC.
- Phase 6 is dedicated to the TOE personalization prior final use.
- Phase 7 is the TOE operational phase.

The TOE life cycle is composed of four stages:

- Development,
- Storage, pre-personalization and testing
- Personalization
- Usage.

The following entities and roles are identified:
TOE Developer: STMicroelectronics srl, Marcianise (CE) Italy
IC Manufacturer: STMicroelectronics SAS, Rousset France
TOE Personalization Agent: Public administration or National accredited TOE personalization center enabled to issue personalized Tachograph card.

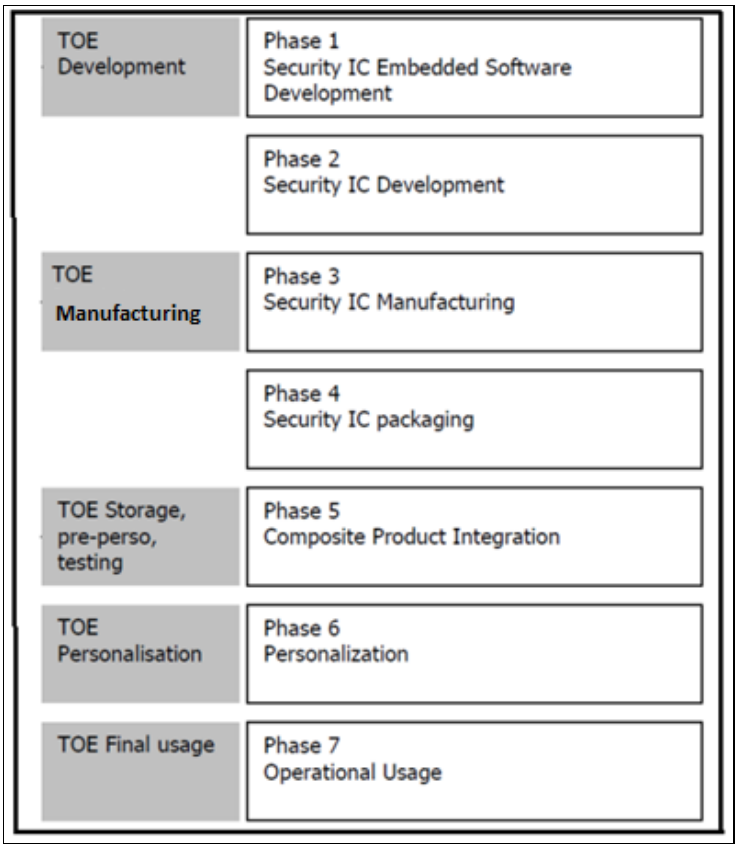


Figure 2 - TOE life cycle

Phase 1:
TOE development is performed during Phase 1. This includes OS, Java card system platform (JCS) and **J-Tacho** application, design, implementation, testing and documentation. The TOE development fulfils requirements of the final product, including conformance to product specifications (e.g. Java Card, GlobalPlatform, [EU_2016_165], etc…), and recommendations of the guidelines of IC, crypto-library and J-SAFE3. The TOE development occurs in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements.
TOE Development is performed by **STMicroelectronics S.r.l** in the site of **MARCIANISE (ITALY)**.

Phase2, Phase 3 and Phase 4:
In Phase 3, the Security IC Manufacturer may store, pre-personalize the TOE and potentially conduct tests on behalf of the TOE developer. This support is specifically used when the TOE delivery shall be done by IC Manufacturer at the end of phase 5: in this case the TOE Developer may deliver in a secure way to IC Manufacturer a NVM image of final product configuration. On its turn, the IC Manufacturer can perform complete TOE pre-personalization on behalf of TOE Developer using the NVM image in order to obtain a fully operational TOE. The IC Manufacturing environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites.
The IC Development is performed by **STMicroelectronics SAS Rousset (FRANCE).**

Phase 5:
The Phase 5 composite product integration is identical to the Phase 5 Smart Card Product Finishing Process in [PP_TACHO].
TOE Developer and/or the IC Manufacturer act as Composite Product Integrator.
The Composite Product Integrator shall initialize and pre-personalize the TOE by configuring it according to product needs, then it shall download the **J-Tacho** application on top of the JCS and finally it shall permanently disable card content management features (e.g. OS

lock, disable card manager), thus making the TOE fully operational and ready for the delivery.
The delivery of the TOE occurs at the end of Phase 5 Composite Product Integration. Delivery and acceptance procedures shall guarantee the authenticity, the confidentiality and integrity of the TOE.
Being the Composite Product Integrator's environment the same as the TOE Developer/IC Manufacturer, integrity and confidentiality of the TOE and of any related material are also guaranteed.
The TOE Composite Product Integration is performed by **STMicroelectronics S.r.l** in the site of **MARCIANISE (ITALY)** and/or **STMicroelectronics SAS Rousset (FRANCE).**

Phase 6:
In Phase 6, the applet J-TACHO of the final product, which have been installed on the TOE in Phase 5, can be further personalized with the creation of the application file structure defined in [EU_2016_165] and with end user data.
The TOE can be used as a Tachograph Card (driver card, workshop card, control card or company card) only after its personalisation, in which application data including Tachograph Card specific cryptographic keys are stored.
The TOE Personalization agent has to follow the procedure as described in Tacho_AGD_PRE to authenticate the role and for TOE personalization.
The TOE Personalization agent is a Public administration or National accredited TOE personalization center enabled to issue personalized Tachograph card.

Phase 7:
The TOE final usage environment coincides with the environment of the product where the TOE is embedded in. It covers a wide spectrum of situations that cannot be covered by evaluations and, therefore, the TOE and the product shall provide the full set of security functionalities to avoid abuse of the product by un-trusted entities.

Notes on current evaluation:

- Current evaluation process covers phases from 1 to 5,
- The TOE delivery is done by the below entities at the end of phase 5 before TOE personalization:
  - on behalf of **STMicroelectronics S.r.l., MARCIANISE** by qualified ST production sites (see [STLite_ST31G480] **STMicroelectronics SAS Rousset**)
  - by **STMicroelectronics S.r.l., MARCIANISE**
- TOE delivery comprises the following items:
  - Hardware: **ST31G480 D01** (available formats are listed in 5.1.6).
  - J-SAFE3 Java Card Platform v2.1.6 (including the native Operating System)
  - The Tachograph Application - (1st and 2nd generation) – applet **J-TACHO**
  - J-TACHO Operational User Guidance v1 [Tacho_AGD_OPE]
  - J-TACHO Preparative Procedure v1 [Tacho_AGD_PRE]

The delivery is protected by secured transport and tracking measures. TOE identification procedures are described in the guidance documents Tacho_AGD_PRE.

Product Phase	TOE Life Cycle Phase	Responsible
Development	Phase 1	TOE Developer **STMicroelectronics S.r.l., MARCIANISE**
Manufacturing	Phase 2, Phase 3, Phase 4,	IC Manufacturer **STMicroelectronics SAS Rousset**
Storage, pre-personalization and testing	Phase 5	TOE Developer or IC Manufacturer **STMicroelectronics S.r.l., MARCIANISE** **STMicroelectronics SAS Rousset**
Personalization	Phase 6	Personalizer **Public administration or National accredited TOE personalization center**.
Usage	Phase 7	End User

Table 1: TOE life cycle, entities and roles

6. Conformance Claims (ASE_CCL)

6.1 CC Conformance Claim

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5. April 2017 ,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5. April 2017,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5. April 2017

as follows:

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

6.2 Protection Profile Claim

This ST claims strict conformance to the PP:

- Digital Tachograph – Tachograph Card (TC PP) – BSI-CC-PP-0091-2017, Version 1.0 [PP_TACHO] and extends the TOE security functionality to address the authentication of the Personalization Agent after delivery, as allowed by the PP. The impacted SFRs are the following: FDP_ACC.2.1, FDP_ACF.1.1, FDP_ACF.1.2 and FDP_UID.2.1.

6.3 Package Claim

This protection profile claims conformance to the assurance package defined in [EU_2016_165] Annex 1C, Appendix 10, as follows:
“SEC_006 The assurance level for each Protection Profile shall be EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5”.

6.4 Conformance Claim Rationale

This Security Target claims strict conformance to the protection profiles Digital Tachograph – Tachograph Card (TC PP) – BSI-CC-PP-0091-2017, Version 1.0 [PP_TACHO].

7. Security Problem Definition (ASE_SPD)

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

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

7.1 Assets

This section introduces the assets to be protected.
For each asset it is specified the kind of dangers that weigh on it.

Asset	**Definition**	**Property to be protected by the TOE**
Identification data (IDD)	Card identification data, user identification data (see Glossary for more details)	Integrity
Activity data (ACD)	Activity data (see Glossary for more details).	Integrity, Authenticity, Confidentiality

Table 2: Primary assets to be protected by the TOE and its environment

Asset	**Definition**	**Property to be protected by the TOE**
Application (APP)	Tachograph application.	Integrity
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.	Confidentiality, Integrity
Signature verification data (SVD)	Public keys certified by Certification Authorities, used to verify electronic signatures.	Integrity, Authenticity
Verification authentication data (VAD)	Authentication data provided as input for authentication attempt as authorised user (i.e. entered PIN on workshop cards).	Integrity
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).	Confidentiality, Integrity
Data to be signed (DTBS)	The complete electronic data to be signed (including both user message and signature attributes).	Integrity, Authenticity
TOE file system, including specific	File structure, access conditions, identification data concerning the IC	Integrity

identification data	and the Smartcard Embedded Software as well as the date and time of the personalisation	

Table 3: Secondary assets to be protected by the TOE and its environment

IDD and ACD are primary assets while all the others are secondary assets to be protected by the TOE and its environment
All primary assets represent User Data in the sense of the CC. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets. The secondary assets represent TSF and TSF-data in the sense of the CC. Security data and user data, stored by the Tachograph Card, need to be protected against 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.

7.2 Subjects and external entities

This Security Target considers the following subjects, who can interact with the TOE.

Role	Definition
Administrator/Personalization Agent	Usually active only during Personalisation (Phase 6) – listed here for the sake of completeness.
Vehicle Unit	Vehicle Unit (authenticated), to which the Tachograph Card is connected (S.VU).
Other Device	Other device (not authenticated) to which the Tachograph Card is connected (S.Non-VU).
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.

Table 4: Subjects and external entities

Application note: 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”.

Application note: The subject Administrator/Personalization Agent is included only in few security functional requirements related to role authentication before the TOE Personalisation (Phase 6) is allowed this because the ST describes the TOE functionalities only for the end-usage/operational usage (Phase 7) - after personalisation.

7.3 Threats

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

The threats are defined in the following table.

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

Table 5: Threats addressed by the TOE

7.4 Organizational 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.

Label	Organisational Security Policy
P.Crypto	The cryptographic algorithms and keys described in [EU_2016_165] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected.

Table 6: Organisational security policies

7.5 Assumptions

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

Label	Assumption
A.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_165] Annex 1C, and are handled correctly so as to preserve the integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE.

Table 7: Assumptions

7.6 Security objectives (ASE_OBJ)

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.

7.6.1 Security objectives for the TOE

The TOE security objectives address the protection to be provided by the TOE, independent of the TOE environment, and are listed in the table below. All security objectives are expressed in the context of the requirements of [EU_2016_165] and [EC1360_2002].

Label	Security objective for the TOE
O.Card_Identification_Data	Integrity of Identification Data - The TOE must preserve the integrity of card identification data and user identification data stored during the card personalisation process.
O.Card_Activity_Storage	Integrity of Activity Data - The TOE must preserve the integrity of user data stored in the card by Vehicle Units.
O.Protect_Secret	Protection of secret keys – The TOE must preserve the confidentiality of its secret cryptographic keys, and must prevent them from being copied.

O.Data_Access	User Data Write Access Limitation - The TOE must limit user data write access to authenticated Vehicle Units.
O.Secure_Communications	Secure Communications - The TOE must support secure communication protocols and procedures between the card and the Vehicle Unit when required.
O.Crypto_Implement	Cryptographic operation – The cryptographic functions must be implemented as required by [EU_2016_165] Annex 1C, Appendix 11.
O.Software_Update	Software updates - Where updates to TOE software are possible, the TOE must accept only those that are authorised.

Table 8: Security objectives for the TOE

7.6.2 Security objectives for the operational environment

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

Label	Security objective for the environment
OE.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_165] Annex 1C, and must be handled so as to preserve the integrity and confidentiality of the data. The Personalisation Service Provider must control all materials, equipment and information that are used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalisation process must be appropriately secured with the goal of data integrity and confidentiality.
OE.Crypto_Admin	Implementation of Tachograph Components – All requirements from [EU_2016_165] concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.
OE.EOL	End of life - When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, that the confidentiality of symmetric and private cryptographic keys has to be safeguarded.

Table 9: Threats addressed by the operational environment

7.6.3 Security objectives rationale

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

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

Table 10: Security Objectives Rationale

7.6.4 SPD and Security Objectives Relation

T.Identification_Data
This threat is countered by the security objective that ensures the integrity of Identification Data (O.Card_Identification_Data) that preserves integrity of card identification data and user identification data stored during the card personalisation process. Objectives O.Crypto_Implement and OE.Crypto_Admin contribute to cover this threat by requiring implementation and management of strong cryptography.

T.Application
Objective O.Software_Update covers this threat by requiring that any update to the tachograph application is authorized. O.Crypto_Implement and O.Protect_Secret support the covering of the threat by preserving the confidentiality of TOE's secret cryptographic keys, preventing their copy and misuse. OE.EOL ensures that at the end of card's life it is properly disposed in order to prevent misuse.

T.Activity_Data
This threat is covered by integrity of Activity Data security objectives according to which the TOE must preserve the integrity of user data stored in the card by VU (O.Card_Activity_Storage), O.Data_Access security objective supports the coverage by ensuring that only authenticated VU access user data stores in the TOE. O.Crypto_Implement and OE.Crypto_Admin contribute to cover this threat by requiring implementation and management of strong cryptography.

T.Data_Exchange
The threat is covered by O.Secure_Communications that requires usage of Secure Communications for the TOE. Beisdes, O.Crypto_Implement and OE.Crypto_Admin give the necessary strong crypto support to manage the communication security while O.Protect_Secret support the covering of the threat by preserving the confidentiality of TOE's secret cryptographic keys, preventing their copy and misuse.

T.Clone

This threat is covered by security objective O.Protect_Secret that prevent an attacker from extracting cryptographic material from the TOE. It is also covered by OE.EOL security objective that ensures proper disposal of the card at the end of card's life.

P.Crypto requires usage of specific cryptographic algorithms and keys when data confidentiality, integrity, authenticity and/or non-repudiation need to be protected, this is addressed by corresponding security objective O.Crypto_Implement.

A.Personalization_Phase requires that all data structures and data (including cryptographic keys) on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation are handled correctly so as to preserve the integrity and confidentiality of these data. This is ensured by the corresponding objectives for the environment OE.Personalization_Phase and OE.Crypto_Admin.

7.7 Statement of Compatibility concerning Composite Security Target (ASE_COMP)

This is a Statement of Compatibility between this Composite ST and the Platform ST of the hardware and associated crypto-library ST31G480 D01 [STLite_ST31G480].

The following mappings regarding SFRs, threats, assumptions, organizational security policies and objectives demonstrate the compatibility between the Composite Security Target and the Platform ST.

SFRs, Policies, Objectives and Assumptions related to MFPlus and DESFire are not relevant since they are not in the scope of this TOE.

The table below shows the mapping between the Platform SFRs and the Composite ST SFRs. Both the relevant and the irrelevant SFRs are listed.

Platform SFRs	Composite ST SFRs
FRU_FLT.2	IP_SFR: Not relevant / Not used
FPT_FLS.1	RP_SRF: FPT_FLS.1
FMT_LIM.1/Test	IP_SFR: Not relevant / Not used
FMT_LIM.2/Test	IP_SFR: Not relevant / Not used
FMT_LIM.1/Loader	IP_SFR: Not relevant / Not used
FMT_LIM.2/Loader	IP_SFR: Not relevant / Not used
FAU_SAS.1	IP_SFR: Not relevant / Not used
FDP_SDC.1	IP_SFR: Not relevant / Not used
FDP_SDI.2	IP_SFR: Not relevant / Not used
FPT_PHP.3	RP_SRF: FPT_PHP.3
FDP_ITT.1	IP_SFR: Not relevant / Not used
FPT_ITT.1	IP_SFR: Not relevant / Not used
FDP_IFC.1	IP_SFR: Not relevant / Not used
FCS_RNG.1	RP_SRF: FCS_RNG.1
FCS_COP.1/DRBG	RP_SRF: Contributes to implementation of: FCS_RNG.1
FCS_COP.1	RP_SRF: Contributes to implementation of FCS_COP.1: FCS_COP.1/AES_2nd FCS_COP.1/SHA-2_2nd FCS_COP.1/ECC_2nd FCS_COP.1/1st_TDES FCS_COP.1/1st_RSA FCS_COP.1/1st_SHA-1
FCS_CKM.1	RP_SRF: Contributes to implementation of FCS_CKM.1: FCS_CKM.1/2nd FCS_CKM.1/1st
FDP_ACC.2/Memories	IP_SFR: Not relevant / Not used
FDP_ACF.1/Memories	IP_SFR: Not relevant / Not used

FMT_MSA.3/Memories	IP_SFR: Not relevant / Not used
FMT_MSA.1/Memories	IP_SFR: Not relevant / Not used
FMT_SMF.1/Memories	IP_SFR: Not relevant / Not used
FDP_ITC.1/Loader	IP_SFR: Not relevant / Not used
FDP_ACC.1/Loader	IP_SFR: Not relevant / Not used
FDP_ACF.1/Loader	IP_SFR: Not relevant / Not used
FMT_MSA.3/Loader	IP_SFR: Not relevant / Not used
FMT_MSA.1/Loader	IP_SFR: Not relevant / Not used
FMT_SMR.1/Loader	IP_SFR: Not relevant / Not used
FIA_UID.1/Loader	IP_SFR: Not relevant / Not used
FMT_SMF.1/Loader	IP_SFR: Not relevant / Not used
All MFPlus SFRs	IP_SFR: Not relevant / Not used
All DESFire SFRs	IP_SFR: Not relevant / Not used

Table 11 - Platform SFRs VS Composite TOE SFRs

There is no conflict between security objectives of the Composite ST and the Platform ST:

Platform Objectives	Composite ST Objectives	Remarks
BSI.O.Identification	Not relevant	Not direct link to the composite product. Nevertheless, chip traceability data is used by the TOE to fulfill identification CC assurance requirements
BSI.O.Leak-Inherent **BSI.O.Leak-Forced** **BSI.O.Phys-Probing** **BSI.O.Phys-Manipulation**	O.Card_Identification_Data O.Card_Activity_Data O.Data_Protect_Secret	
BSI.O.Malfunction	O.Card_Activity_Data O.Data_Protect_Secret	
BSI.O.Abuse-Func	O.Card_Identification_Data O.Card_Activity_Data O.Data_Protect_Secret	
BSI.O.RND	Not relevant	Not direct link to the composite product. This is ensured by J-SAFE3 Platform.
BSI.O.Cap-Avail-Loader	Not relevant	
AUG1.O.Add-Functions	Not relevant	
AUG4.O.Mem Access	Not relevant	
O.Controlled-ES-Loading	Not relevant	
MFPlus and DESFire are not embedded, objectives related to them are not valid and not listed here	Not relevant	
	Additional Objectives	
	O.Data_Access	
	O.Secure_Communications	
	O.Crypto_Implement	
	O.Software_Update	

Table 12 - Platform Objectives VS Composite TOE Objectives

There is no conflict between security objectives for the environment of the Composite ST and the Platform ST:

Platform OE	Composite ST Objectives for the Environment
BSI.OE.Lim-Block-Loader	Fulfilled by Transport Key Verification as described in ALC_DEL.1
BSI.OE.Resp-Appl	Covered by TOE Security Objectives O.Card_Identification_Data O.Card_Activity_Data O.Data_Protect_Secret O.Secure_Communications
BSI.OE.Process-Sec-IC	Fulfilled by ALC_DVS.2 and ALC_DEL.1 during phases 4 and 5. After phase 5, covered by O.Protect_Secret, O.Secure_communications, OE.EOL and OE.Personalisation_Phase
	Additional Objectives for the Environment
	OE.Crypto_Admin

Table 13 - Platform OEs VS Composite TOE OEs

There is no conflict regarding the security assurance requirements: composite evaluation security assurance requirements represent a subset of the security assurance requirements of the underlying platform:

Platform SARs (EAL5 augmented by ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, AVA_VAN.5)	Composite SARs (EAL4 augmented by ATE_DPT.2 and AVA_VAN.5)
ADV_ARC.1	ADV_ARC.1
ADV_FSP.5	ADV_FSP.4
ADV_IMP.2	ADV_IMP.1
ADV.INT.2	-
ADV_TDS.5	ADV_TDS.3
AGD_OPE.1	AGD_OPE.1
AGD_PRE.1	AGD_PRE.1
ALC_CMC.5	ALC_CMC.4
ALC_CMS.5	ALC_CMS.4
ALC_DEL.1	ALC_DEL.1
ALC_DVS.2	ALC_DVS.1
ALC_FLR.1	-
ALC_LCD.1	ALC_LCD.1
ALC_TAT.3	ALC_TAT.1
ASE_CCL.1	ASE_CCL.1
ASE_ECD.1	ASE_ECD.1
ASE_INT.1	ASE_INT.1
ASE_OBJ.2	ASE_OBJ.2
ASE_REQ.2	ASE_REQ.2
ASE_SPD.1	ASE_SPD.1
ASE_TSS.2	ASE_TSS.1
ATE_COV.2	ATE_COV.2
ATE_DPT.3	ATE_DPT.2
ATE_FUN.1	ATE_FUN.1
ATE_IND.2	ATE_IND.2
AVA_VAN.5	AVA_VAN.5

Table 14 - Platform SARs VS Composite TOE SARs

8. Extended Components Definition (ASE_ECD)

For this ST the security functional requirements in [CC2] have been extended to cover part of the TOE functionality that cannot otherwise clearly be expressed with the following SFRs: FCS_RNG (Random number generation) and FPT_EMS (TOE Emanation)

8.1 Definition of Family FCS_RNG

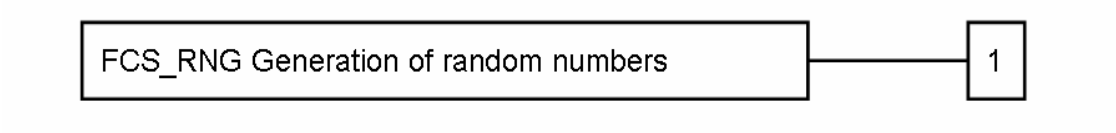
Section extracted from Eurosmart – Security IC Platform Protection Profile with Augmentation Packages [[BSI_ PP_0084]*].*

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behavior:

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

Component leveling:



FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Application note: 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 an random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid

deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

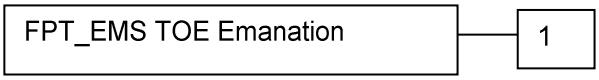
8.2 Definition of Family FPT_EMS

To define the IT security functional requirements of the TOE related to leakage of information based on emanation, an additional family (FPT_EMs) of the Class FPT (protection of the TSF) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behavior:

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

Component leveling:



FPT_EMS.1 Generation of random numbers requires that the TOE does not produce intelligible emissions that enable access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 Random number generation.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

9. Security requirements (ASE_REQ)

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

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

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

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

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

Some additions have been made to the ST with respect to the PP SFRs, to incorporate in the ST the authentication of the personalization agent. The added words are written ***bold, underlined and italicised***.

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

Security functional requirements for the TOE

This section is subdivided to show security functional requirements that relate to the TOE itself, and those that relate to external communications.
Section 9.1 addresses requirements for the tachograph card.
Section 9.2 addresses the communication requirements for 2nd generation vehicle units to be used with the TOE.
Section 9.3 addresses the communication requirements for 1st generation vehicle units to be used with the TOE.

SFRs in [PP_TACHO]	SFRs in this ST
FAU_ARP.1	FAU_ARP.1
FAU_SAA.1	FAU_SAA.1
FCO_NRO.1	FCO_NRO.1
FDP_ACC.2	FDP_ACC.2
FDP_ACF.1	FDP_ACF.1
FDP_DAU.1	FDP_DAU.1
FDP_ETC.1	FDP_ETC.1
FDP_ETC.2	FDP_ETC.2
FDP_ITC.1	FDP_ITC.1
FDP_ITC.2	FDP_ITC.2
FDP_RIP.1	FDP_RIP.1
FDP_SDI.2	FDP_SDI.2

FIA_AFL.1(1:C)	FIA_AFL.1/C
FIA_AFL.1(2:WC)	FIA_AFL.1/WC
FIA_ATD.1	FIA_ATD.1
FIA_UAU.3	FIA_UAU.3
FIA_UAU.4	FIA_UAU.4
FIA_UID.2	FIA_UID.2
FIA_USB.1	FIA_USB.1
FPR_UNO.1	FPR_UNO.1
FPT_EMS.1	FPT_EMS.1
FPT_FLS.1	FPT_FLS.1
FPT_PHP.3	FPT_PHP.3
FPT_TST.1	FPT_TST.1
Tachograph card 2nd generation specific	
FCS_CKM.1(1)	FCS_CKM.1/2nd
FCS_CKM.2(1)	FCS_CKM.2/2nd
FCS_CKM.4(1)	FCS_CKM.4/2nd
FCS_COP.1(1:AES)	FCS_COP.1/AES_2nd
FCS_COP.1(2:SHA-2)	FCS_COP.1/SHA-2_2nd
FCS_COP.1(3:ECC)	FCS_COP.1/ECC_2nd
FCS_RNG.1	FCS_RNG.1
FIA_UAU.1(1)	FIA_UAU.1/2nd
FPT_TDC.1(1)	FPT_TDC.1/2nd
FTP_ITC.1(1)	FTP_ITC.1/2nd
Tachograph card 1st generation specific	
FCS_CKM.1(2)	FCS_CKM.1/1st
FCS_CKM.2(2)	FCS_CKM.2/1st
FCS_CKM.4(2)	FCS_CKM.4/1st
FCS_COP.1(4:TDES)	FCS_COP.1/1st_TDES
FCS_COP.1(5:RSA)	FCS_COP.1/1st_RSA
FCS_COP.1(6:SHA-1)	FCS_COP.1/1st_SHA-1
FIA_UAU.1(2)	FIA_UAU.1/1st
FPT_TDC.1(2)	FPT_TDC.1/1st
FTP_ITC.1(2)	FTP_ITC.1/1st

9.1 Security functional requirements for the Tachograph Card

9.1.1 Class FAU Security Audit

FAU_ARP.1 Security alarms

Hierarchical to:-
Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take the following actions:

a. For user authentication failures activity data input integrity errors – respond to the VU through SW1 SW2 status words, as defined in [EU_2016_165] Annex 1C, Appendix 2;

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

For self-test error: SW1SW2=0x6400
For stored data integrity error: SW1SW2=0x6581 or 0x6281

upon detection of a potential security violation.

FAU_SAA.1 Potential violation analysis

Hierarchical to:-
Dependencies: FAU_GEN.1 Audit data generation

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

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

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

known to indicate a potential security violation;

b. *[none]*[1].

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.

9.1.2 Class FCO Communication

FCO_NRO.1 Selective proof of origin

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

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [data to be downloaded to external media] at the request of the [recipient] **in accordance with [EU_2016_165] 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_165] Appendix 11, sections 6.2 and 14.3].

[1] [assignment: *any other rules*]

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_165] Appendix 11, sections 6 and 14.

9.1.3 Class FDP User data protection

FDP_ACC.2 Complete access control

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

FDP_ACC.2.1 The TSF shall enforce the [AC SFP] on [
Subjects**:**

- S.VU (a vehicle unit in the sense of [EU_2016_165] Annex 1C)
- S.Non-VU (other card interface devices)
- ***Personalization Agent***

Objects:

- User data
  - User Identification data
  - Activity data
- Security data
  - Cryptographic keys (KPD in Table 3)
  - 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

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

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_165] Annex 1C)
- S.Non-VU (other card interface devices)
- ***Personalization Agent***

Objects:

- User data
  - User identification data
  - Activity data
- Security data

  - Cryptographic keys (KPD in Table 3)
  - PIN (for Workshop card)
- TOE application code
- TOE file system (Attribute: access conditions)
- Card identification data
- Master file contents].

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

- **GENERAL_READ**
  - Driver card, workshop card: user data may be read from the TOE by any user
  - Control card, company card: user data may be read from the TOE by any user, except user identification data stored in the 1st generation tachograph application, which may be read by S.VU only
- **IDENTIF_WRITE**
  - All card types: card identification data and user identification data may only be written once and before the end of Personalisation
  - No user may write or modify identification data during the end-usage phase of the card life-cycle
- **ACTIVITY_WRITE**
  - All card types: activity data may be written to the card by S.VU only
- **SOFT_UPGRADE**
  - All card types: TOE application 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].

***Application note**: The Personalization Agent Authentication Key(s) are pre-loaded in the TOE at the end of **Phase 5 - TOE composite product integration**.*

***Application note**: The operation "FILE_STRUCTURE" is allowed when the TOE is in the **Phase 6 – TOE Personalization** only after successful "Personalization Agent" authentication.*

***Application note**: When the TOE is in the **Phase 6 – TOE Personalization** or in **Phase 7 – TOE Operational usage** the operation "SOFT_UPGRADE2" isn't allowed.*

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

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

- **SECRET KEYS**

- The TSF shall prevent access to secret cryptographic keys other than for use in the TSF's cryptographic operations, or in case of a workshop card only, for exporting the SensorInstallationSecData to a VU, as specified in [EU_2016_165] Annex 1C, Appendix 2].

FDP_DAU.1 Basic data authentication

Hierarchical to:-

Dependencies:-

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

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

FDP_ETC.1 Export of user data without security attributes

Hierarchical to:-
Dependencies:FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control

FDP_ETC.1.1 The TSF shall enforce the [AC SFP] when exporting user data controlled under the SFP(s), outside the TOE.

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

FDP_ETC.2 Export of user data with security attributes

Hierarchical to:-
Dependencies:FDP_ACC.1 Subset access control,
or FDP_IFC.1 Subset information flow control

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

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

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

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

FDP_ITC.1 Import of user data without security attributes

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

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

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

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

FDP_ITC.2 Import of user data with security attributes

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

FDP_ITC.2.1 The TSF shall enforce the [Input Sources SFP] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside of the TOE: [

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

Application note: requirement for verified software updates not applicable since application software cannot be updated outside of the manufacturing environment.

FDP_RIP.1 Subset residual information protection

Hierarchical to:-
Dependencies:-

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] [2] the following objects: [cryptographic keys, (*KDP in* Table 3: Secondary assets to be protected by the TOE and its environment)*]* [3].

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:-
Dependencies:-

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [integrity errors] [4] on all objects, based on the following attributes [integrity checked stored user data attributes] [5].

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

2 [selection: *allocation of the resource to, deallocation of the resource from*]
3 [assignment: *list of objects*]
4 [assignment: *integrity errors*]
5 [assignment: *user data attributes*]

9.1.4 Class FIA Identification and authentication

FIA_AFL.1/Authentication failure handling (C)

Hierarchical to: -
Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_AFL.1.2/(C) When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [

- warn the entity connected,
- assume the user to be S.Non-VU].

FIA_AFL.1/ Authentication failure handling (WC)

Hierarchical to:-
Dependencies:FIA_UAU.1 Timing of authentication

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

FIA_AFL.1.2/(WC) When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [:

- warn the entity connected,
- block the PIN check procedure such that any subsequent PIN check attempt will fail,
- be able to indicate to subsequent users the reason for the blocking.]

FIA_ATD.1 User attribute definition

Hierarchical to:-
Dependencies:-

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

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

FIA_UAU.3 Unforgeable authentication

Hierarchical to:-
Dependencies:-

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

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to:-
Dependencies:-

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [key based authentication mechanisms as defined in [EU_2016_165] Appendix 11, Chapters 4 and 10].

FIA_UID.2 User authentication before any action

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

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

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

Application note: Only after a successful authentication the "Personalization Agent" can take control of the TOE and execute the steps and operations as described in the life cycle Phase 6 "TOE Personalization".

FIA_USB.1 User-subject binding

Hierarchical to:-
Dependencies:FIA_ATD.1 User attribute definition

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

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of the user security attributes with subjects acting on the behalf of users: [*the TOE in the personalization phase creates all data structure and security attributes as defined in [EU_2016_165] Appendix 2, Chapters 4]*[6].

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: *[TOE in operational usage doesn't allow changing of attributes]*[7].

9.1.5 Class FPR Privacy

FPR_UNO.1 Unobservability

Hierarchical to:-
Dependencies:-

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

6 [assignment: *rules for the initial association of attributes*]
7 [assignment: *rules for the changing of attributes*]

9.1.6 Class FPT Protection of the TSF

FPT_EMS.1 TOE emanation

Hierarchical to:-
Dependencies:-

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations*[8] in excess of *state-of-the-art limits*[9] enabling access to [private keys or session keys] and *none*[10].

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 *none*[11].

Application note: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The TOE chip has to provide a smart card contacts interface according to ISO/IEC 7816-2 (not only used by the terminal but maybe by an attacker). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:-
Dependencies:-

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

Hierarchical to:-
Dependencies:-

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

Application note: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSF security could not be violated at any time. Hence,

8 [assignment: *types of emissions*]
9 [assignment: *specified limits*]
10 [assignment: *list of types of user data*]
11 [assignment: *list of types of user data*]

automatic response means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

FPT_TST.1 TSF testing

Hierarchical to:-
Dependencies:-

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 authorized users with the capability to verify the integrity of [TSF data].

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

9.2 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.

9.2.1 Class FCS Cryptographic support

FCS_CKM.1/2nd Cryptographic key generation

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

FCS_CKM.1.1/2nd The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [EU_2016_165] 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_165] Annex 1C, Appendix 11, Part B] that meet the following: [Reference [RNG_FUNC_CLA] predefined RNG class [DRG.3][12], [EU_2016_165] Annex 1C, Appendix 11, Section 10].

FCS_CKM.2/2nd Cryptographic key distribution

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

FCS_CKM.2.1/2nd The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [secure messaging AES session key agreement as specified in [EU_2016_165]

[12] [selection: *PTG.2, PTG.3, DRG.2, DRG.3, DRG.4, NTG.1*]

Annex 1C, Appendix 11, Part B] that meets the following [EU_2016_165] Annex 1C, Appendix 11, Part B].

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

FCS_CKM.4/2nd Cryptographic key destruction

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

FCS_CKM.4.1/2nd The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*physical deletion by overwriting the memory data]* [13] that meets the following [

- Requirements in [PP_TACHO], Table 20;
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means
- *[*[none]*]*[14].

FCS_COP.1/AES_2nd Cryptographic operation

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

FCS_COP.1.1/AES_2nd 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_165] Annex 1C, Appendix 11].

FCS_COP.1/SHA-2_2nd Cryptographic operation

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

13 [assignment: *cryptographic key destruction method*]
14 [assignment: *list of standard*]

FCS_COP.1.1/SHA-2_2nd 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_165] Annex 1C, Appendix 11].

FCS_COP.1/ECC_2nd Cryptographic operation

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

FCS_COP.1.1/ECC_2nd 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_165] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [EU_2016_165], Appendix 11, Part B] that meet the following: [[EU_2016_165] Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-03111 – Elliptic Curve Cryptography – version 2, and the standardized domain parameters in Table 15].

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 15: Standardised domain parameters

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

Table 16: Cipher suites

Application note: Table 16 shows the allowed cipher suites. ECC keys sizes of 512 bits and 521 bits are considered to be equal in strength for all purposes within this ST.

FCS_RNG.1 Random number generation

Hierarchical to:-
Dependencies:-

FCS_RNG.1.1 The TSF shall provide a [deterministic][15] random number generator that implements:

(DRG.3.1) if initialized with a random seed *[using a PTRNG of class PTG.2 as random source]*[16] the internal state of the RNG shall *[have at least 100 bits of min-entropy]*[17]

(DRG.3.2) The RNG provides forward secrecy

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

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

(DRG.3.4) The RNG initialized with a random seed *[during every startup and after 2^{32} requests]*[18], generates output for which *[more than 2^{34}]*[19] strings of bit length 128 are mutually different with probability *[$w>1-2^{-16}$]*[20].

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A *[and the NIST statistical test suite [NIST_800-22]]*[21]

9.2.2 Class FIA Identification and authentication

FIA_UAU.1/2nd Timing of authentication

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

FIA_UAU.1.1/2nd 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_165] 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_165] Annex 1C, Appendix 2]
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/2nd The TSF shall require each user to be successfully authenticated **using the method described in [EU_2016_165]_Annex 1C, Appendix 11, Chapter 10** before allowing any other TSF-mediated actions on behalf of that user.

Application note: FIA_UAU.1.1/2nd a) allows non secured readers to get signed downloaded data from driver and workshop cards, without any previous authentication. This can be used by company download tools, which are considered as "other devices" in the sense of this ST. Such download

15 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
16 [selection: *using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]*]
17 [selection: *have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*]
18 [assignment: *requirements for seeding*]
19 [assignment: *number of strings*]
20 [assignment: *probability*]
21 [assignment: *additional test suites*]

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_165] Annex 1C, Appendix 2 access rules (see section 4, access rules = 'ALW'). Similarly, FIA_UAU.1.1/2nd b) allows "other devices" (without having performed any authentication) to access data from control and company cards, following [EU_2016_165] Annex 1C, Appendix 2, Section 4 access rules.

9.2.3 Class FPT Protection of the TSF

FPT_TDC.1/2nd Inter-TSF basic TSF data consistency

Hierarchical to:-
Dependencies:-

FPT_TDC.1.1/2nd The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [EU_2016_165] Annex 1C, Appendix 11] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

FPT_TDC.1.2/2nd The TSF shall use [the interpretation rules (communication protocols) as defined by [EU_2016_165] Annex 1C, Appendix 11] when interpreting the TSF data from ~~another trusted IT product~~ **a vehicle unit**.

9.2.4 Class FTP Trusted path/channels

FTP_ITC.1/2nd Inter-TSF trusted channel

Hierarchical to:-
Dependencies:-

FTP_ITC.1.1/2nd The TSF shall provide a communications 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.1.2/2nd The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3/2nd The TSF shall ~~initiate communication via~~ **use** the trusted channel for [all commands and responses exchanged with a vehicle unit after successful chip authentication and until the end of the session].

Application note: The requirements for establishing the trusted channel are given in [EU_2016_165] Appendix 11, Chapter 10 (for 2nd generation vehicle units).

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

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

9.3.1 Class FCS Cryptographic support

FCS_CKM.1/1st Cryptographic key generation

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

FCS_CKM.1.1/1st The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [EU_2016_165] 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_165] Annex 1C, Appendix 11 Part A, Chapter 3].

FCS_CKM.2/1st Cryptographic key distribution

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

FCS_CKM.2.1/1st The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [for triple DES session keys as specified in [EU_2016_165] Annex 1C, Appendix 11 Part A] that meets the following [[EU_2016_165] Annex 1C, Appendix 11 Part A, Chapter 3].

FCS_CKM.4/1st Cryptographic key destruction

Hierarchical to:-
Dependencies:[FDP_ITC.1 Import of user data without security attributes
orFDP_ITC.2 Import of user data with security attributes
orFCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/1st The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*physical deletion by overwriting the memory data]* [22] that meets the following [

- Requirements in [PP_TACHO], Table 16 and Table 17 ;
- Temporary private and secret cryptographic keys are destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means.
- *[*none*]*[23].

FCS_COP.1/1st_TDES Cryptographic operation

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

[22] [assignment: *cryptographic key destruction method*]
[23] [assignment: *list of standard*]

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

FCS_COP.1.1/1st_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_165] Annex 1C, Appendix 11 Part A, Chapter 3].

FCS_COP.1/1st_RSA Cryptographic operation

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

FCS_COP.1.1/1st_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_165] Annex 1C, Appendix 11 Part A, Chapter 3].

FCS_COP.1/1st_SHA-1 Cryptographic operation

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

FCS_COP.1.1/1st_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)].

9.3.2 Class FIA Identification and authentication

FIA_UAU.1/1st Timing of authentication

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

FIA_UAU.1.1/1st 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_165] 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_165] 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_165] Annex 1C, Appendix 2]

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

FIA_UAU.1.2/1st The TSF shall require each user to be successfully authenticated **using the method described in [EU_2016_165] Annex 1C, Appendix 11, Chapter 5** before allowing any other TSF-mediated actions on behalf of that user.

9.3.3 Class FPT Protection of the TSF

FPT_TDC.1/1st Inter-TSF basic TSF data consistency

Hierarchical to:-
Dependencies:-

FPT_TDC.1.1/1st The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [EU_2016_165] Annex 1C, Appendix 11 Chapter 5] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

FPT_TDC.1.2/1st The TSF shall use [the interpretation rules (communication protocols) as defined by [EU_2016_165] Annex 1C, Appendix 11 Part A, Chapter 5] when interpreting the TSF data from ~~another trusted IT product~~ **a vehicle unit**.

9.3.4 Class FTP Trusted path/channels

FTP_ITC.1/1st Inter-TSF trusted channel

Hierarchical to:-
Dependencies:-

FTP_ITC.1.1/1st The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **the vehicle unit** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/1st The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3/1st The TSF shall ~~initiate communication via~~ **use** the trusted channel for [data import from and export to a vehicle unit in accordance with [EC1360_2002] Appendix 2].

Application note: The requirements for establishing the trusted channel are given in [EU_2016_165]Appendix 11, Chapter 5 (for 1st generation vehicle units).

9.4 TOE Security assurance requirements

The assurance level for this protection profile is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [CC3].
These security assurance requirements are derived from [EU_2016_165] Annex 1C, Appendix 10 (SEC_006).

ASSURANCE CLASS	ASSURANCE COMPONENTS
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.2 Testing: security enforcing modules ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample.
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 17: Security Assurance Requirements - EAL 4 extended with ATE_DPT.2 and AVA_VAN.5

9.5 Security assurance requirements rationale

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [EU_2016_165] Annex 1C, Appendix 10.

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

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

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 4: Subjects and external entities, entry 'Attacker'). This decision represents a part of the conscious security policy for the card required by the regulations, and reflected by the current PP [PP_TACHO].

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

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2 and
- AVA_VAN.5.

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

COMPONENT	DEPENDENCIES REQUIRED BY CC PART 3 [CC3]	DEPENDENCY SATISFIED BY
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 18: SARs' dependencies (additional to EAL4 only)

9.6 Security requirements rationale

9.6.1 Rationale for SFRs' dependencies

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

SFR	DEPENDENCIES	RATIONALE

SFRs' for Tachograph Card		
FAU_ARP.1	FAU_SAA.1	Satisfied by FAU_SAA.1
FAU_SAA.1	FAU_GEN.1	See note 1 below
FCO_NRO.1	FIA_UID.1	Satisfied by FIA_UID.2
FDP_ACC.2	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2 See note 2 below
FDP_DAU.1	-	-
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3	Partially satisfied by FDP_ACC.2 See note 2 below
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1, FTP_ITC.1 or FTP_TRP.1, FPT_TDC.1	Satisfied by FDP_ACC.2, FTP_ITC.1(1st & 2nd) and FPT_TDC.1(1st & 2nd)
FDP_RIP.1	-	-
FDP_SDI.2	-	-
FIA_AFL.1(C)	FIA_UAU.1	Satisfied by FIA_UAU.1(1st & 2nd)
FIA_AFL.1(WC)	FIA_UAU.1	Satisfied by FIA_UAU.1(1st & 2nd)
FIA_ATD.1	-	-
FIA_UAU.3	-	-
FIA_UAU.4	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1	Satisfied by FIA_ATD.1
FPR_UNO.1	-	-
FPT_EMS.1	-	-
FPT_FLS.1	-	-
FPT_PHP.3	-	-
FPT_TST.1	-	-
SFRs' specific to 2nd generation Tachograph Card		
FCS_CKM.1/2nd	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2/2nd, FCS_COP.1/AES_2nd FCS_COP.1/ECC_2nd and FCS_CKM.4/2nd
FCS_CKM.2/2nd	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1/2nd and FCS_CKM.4/2nd
FCS_CKM.4/2nd	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1/2nd
FCS_COP.1/AES_2nd	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1/2nd and FCS_CKM.4/2nd

FCS_COP.1/SHA-2_2nd	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-2
FCS_COP.1/ECC_2nd	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4/2nd
FCS_RNG.1	-	-
FIA_UAU.1/2nd	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1/2nd	-	-
FTP_ITC.1/2nd	-	-
SFRs' specific to 1st generation Tachograph Card		
FCS_CKM.1/1st	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2/1st, FCS_COP.1/1st_TDES FCS_COP.1/1st_RSA and FCS_CKM.4/1st
FCS_CKM.2/1st	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1/1st and FCS_CKM.4/1st
FCS_CKM.4/1st	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1/1st and FCS_CKM.4/1st
FCS_COP.1/1st_TDES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1/1st and FCS_CKM.4/1st
FCS_COP.1/1st_RSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4/1st
FCS_COP.1/1st_SHA-1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-1
FIA_UAU.1/1st	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1/1st	-	-
FTP_ITC.1/1st	-	-

Table 19: SFRs' dependencies

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

Note 2: The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Personalisation Phase, and are fixed over the whole lifetime of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, either during personalization, or within the usage phase of the TOE. This argument holds for both FDP_ACF.1 and FDP_ITC.1.

9.6.2 Rationale tables of security objectives and SFRs

The Table 20 provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FAU_ARP.1	Security alarms	x	x			x		
FAU_SAA.1	Potential violation analysis	x	x			x		
FCO_NRO.1	Selective proof of origin					x		
FDP_ACC.2	Complete access control	x	x	x	x	x		x
FDP_ACF.1	Security attribute based access control	x	x	x	x	x		x
FDP_DAU.1	Basic data authentication					x	x	
FDP_ETC.1	Export of user data without security attributes					x		
FDP_ETC.2	Export of user data with security attributes					x		
FDP_ITC.1	Import of user data without security attributes					x		
FDP_ITC.2	Import of user data with security attributes							x
FDP_RIP.1	Subset residual information protection			x		x		
FDP_SDI.2	Stored data integrity monitoring and action	x	x				x	
FIA_AFL.1(C)	Authentication failure handling				x			
FIA_AFL.1(WC)	Authentication failure handling				x			
FIA_ATD.1	User attribute definition				x			
FIA_UAU.3	Unforgeable authentication				x	x	x	
FIA_UAU.4	Single-use authentication mechanism					x	x	
FIA_UID.2	User authentication before any action				x			
FIA_USB.1	User-subject binding				x			
FPR_UNO.1	Unobservability			x		x		
FPT_EMS.1	TOE emanation	x	x	x	x			
FPT_FLS.1	Failure with preservation of secure state	x	x		x			
FPT_PHP.3	Resistance to physical attack	x	x	x	x			x
FPT_TST.1	TSF testing	x	x		x			
SFRs' specific to 2nd generation Tachograph Card								
FCS_CKM.1/2nd	Cryptographic key generation					x	x	
FCS_CKM.2/2nd	Cryptographic key distribution					x	x	
FCS_CKM.4/2nd	Cryptographic key destruction					x	x	
FCS_COP.1/AES_2nd	Cryptographic operation					x	x	
FCS_COP.1/SHA-2_2nd	Cryptographic operation					x	x	
FCS_COP.1/ECC_2nd	Cryptographic operation					x	x	
FCS_RNG.1	Random number generation					x	x	
FIA_UAU.1/2nd	Timing of authentication				x			
FPT_TDC.1/2nd	Inter-TSF basic TSF data consistency					x		

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FTP_ITC.1/2nd	Inter-TSF trusted channel					x		
SFRs' specific to 1st generation Tachograph Card								
FCS_CKM.1/1st	Cryptographic key generation					x	x	
FCS_CKM.2/1st	Cryptographic key distribution					x	x	
FCS_CKM.4/1st	Cryptographic key destruction					x	x	
FCS_COP.1/1st_TDES	Cryptographic operation					x	x	
FCS_COP.1/1st_RSA	Cryptographic operation					x	x	
FCS_COP.1/1st_SHA-1	Cryptographic operation					x	x	
FIA_UAU.1/1st	Timing of authentication				x			
FPT_TDC.1/1st	Inter-TSF basic TSF data consistency					x		
FTP_ITC.1/1st	Inter-TSF trusted channel					x		

Table 20: Coverage of security objectives for the TOE by SFRs

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in Table 21.

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

	FDP_ACC.2 FDP_ACF.1	Access to card activity data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorised vehicle units
	FDP_SDI.2	Integrity of the stored data within the TOE, specifically the integrity of the card activity data, is required by this component.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of card activity data.
	FPT_FLS.1	Requires that any failure state should not expose card activity data, or compromise its integrity.
	FPT_PHP.3	Requires the TOE to resist attempts to access card activity data through manipulation or physical probing.
	FPT_TST.1	Requires tests to be carried out to assure that the integrity of card activity data has not been compromised.
O.Protect_Secret	FDP_ACC.2 FDP_ACF.1	Require that the TOE prevent access to secret keys other than for the TOE's cryptographic operations.
	FDP_RIP.1	Requires the secure management of storage resources within the TOE to prevent data leakage.
	FPR_UNO.1	This requirement safeguards the unobservability of secret keys used in cryptographic operations.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of the keys.
	FPT_PHP.3	Requires the TOE to resist attempts to gain access to the keys through manipulation or physical probing.
O.Data_Access	FDP_ACC.2 FDP_ACF.1	Access to user data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorised vehicle units.
	FIA_AFL.1/(C) FIA_AFL.1/(WC)	These components require that if authentication fails the TOE reacts with a warning to the connected entity, and the user is assumed not to be an authorised vehicle unit.
	FIA_ATD.1 FIA_USB.1	The definition of user security attributes supplies a distinction between vehicle units and other card interface devices.
	FIA_UAU.1/(1st & 2nd) FIA_UID.2	These requirements ensure that write access to user data is not possible without a preceding successful authentication process.
	FIA.UAU.3	Prevents the use of forged credentials during the authentication process.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the authentication process.
	FPT_FLS.1	Requires that any failure state should not allow unauthorised write access to the card.
	FPT_PHP.3	Requires the TOE to resist attempts to interfere with authentication through manipulation or physical probing.
	FPT_TST.1	Requires that tests be carried out to assure that the integrity of the TSF and identification data has not been compromised.
O.Secure_Communications	FAU_ARP.1 FAU_SAA.1	During data exchange, upon detection of an integrity error of the imported data, the TOE will indicate the corresponding violation and will provide a warning to the entity sending the data.

	FDP_ACC.2 FDP_ACF.1	The necessity for the use of a secure communication protocol as well as the access to the relevant card´s keys are defined within these requirements.
	FDP_ETC.1 FDP_ITC.1 FTP_ITC.1/(1st & 2nd)	These requirements provide for a secure data exchange (i.e. the data import and export) between the TOE and the card interface device by using a trusted channel. This includes assured identification of its end points and protection of the data transfer from modification and disclosure. By this means, both parties are capable of verifying the integrity and authenticity of received data. The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device.
	FCO_NRO.1 FDP_DAU.1 FDP_ETC.2	Within the TOE's end-usage phase, the TOE offers a data download functionality with specific properties. The TOE provides the capability to generate an evidence of origin for the data downloaded to the external media, to verify this evidence of origin by the recipient of the data downloaded, and to download the data to external media in such a manner that the data integrity can be verified.
	FDP_RIP.1	Requires the secure management of storage resources within the TOE to prevent data leakage.
	FIA_UAU.3 FIA_UAU.4	These requirements support the security of the trusted channel, as the TOE prevents the use of forged authentication data, and as the TOE's input for the authentication tokens and for the session keys within the preceding authentication process is used only once.
	FPR_UNO.1	This requirement safeguards the unobservability of the establishing process of the trusted channel, and the unobservability of the data exchange itself, both of which contribute to a secure data transfer.
	FCS_CKM.1/(1st & 2nd) FCS_CKM.2/(1st & 2nd) FCS_CKM.4/(1st & 2nd) FCS_COP.1/(all) FCS_RNG.1	The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device with agreement of session keys. FCS_COP.1 also realizes the securing of the data exchange itself. Random numbers are generated in support of cryptographic key generation for authentication.
	FPT_TDC.1/(1st & 2nd)	Requires a consistent interpretation of the security related data shared between the TOE and the card interface device.
O.Crypto_Implement	FDP_DAU.1 FDP_SDI.2	Approved cryptographic algorithms are required for digital signatures in support of data authentication.
	FIA_UAU.3 FIA_UAU.4	Approved cryptographic algorithms are required to prevent the forgery, copying or reuse of authentication data.
	FCS_CKM.1/(1st & 2nd) FCS_CKM.2/(1st & 2nd) FCS_CKM.4/(1st & 2nd) FCS_RNG.1	Key generation, distribution and destruction must be done using approved methods. Random numbers are generated in support of cryptographic key generation for authentication.
	FCS_COP.1/(all)	Approved cryptographic algorithms are required for all cryptographic operations.
O.Software_Update	FDP_ACC.2 FDP_ACF.1	Require that users cannot update TOE software.
	FDP_ITC.2	Provides verification of imported software updates.
	FPT_PHP.3	Requires the TOE to resist physical attacks that may be aimed at modifying software.

Table 21: Suitability of the SFRs

9.7 Security requirements – internal consistency

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

- (SFRs)

The dependency analysis in section 9.6.1 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 9 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. The current PP [PP_TACHO] accurately reflects the requirements of EU Parliament and Council Regulation 165/2014, Annex I C [EU_2016_165], which is assumed to be internally consistent.

- (SARs)

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the assurance components in section 9.5 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 9.6 and 9.5. Furthermore, as also discussed in section 9.5 the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

10. TOE summary specification (ASE_TSS)

The TOE provides the following security functionality :

- Vehicle Unit, other device and Personalization Agent Authentication
- Secure Messaging
- Access Control
- Key Derivation, Cryptographic and Data Signature
- Data Protection
- Java Platform and OS

These Security Functions are implemented by the realization of the Security Functional requirements, according to chap. 9. The details of the implementation of this TOE security functionality are provided in the following sections.

10.1 Statement of the TOE security functionality

10.1.1 SF_Auth Vehicle Unit, other device and Personalization agent Authentication

The TOE implements an authentication mechanism to authenticate external entities and to assign roles right and security attributes (FIA_UID.2, FIA_ATD.1, FIA_USB.1). The external entities are the Vehicle Unit and Other Device see Table 4.

The purpose of the TSF SF_AUTH is to authenticate the user before any action is allowed/performed (FIA_UID.2).

The authentication mechanism implements an authentication failure mechanism according to SFRs (FIA_AFL.1(C) and FIA_AFL.1(WC), FAU_ARP.1, FAU_SAA.1).

The authentication mechanism avoid the use of forged or copied or reuse of authentication data (FIA_UAU.3, FIA_UAU.4).

The authentication mechanism is based on the authentication methods described in [EU_2016_165] Annex 1C, Appendix 11, Chapter 10 (FIA_UAU.1/2nd) and [EU_2016_165] Annex 1C, Appendix 11, Chapter 5 (FIA_UAU.1/1st).

The purpose of the TSF SF_AUTH is also to authenticate the roles of “Personalization Agent” when the TOE is in the life cycle Phase 6 “TOE Personalization”. The Personalization Agent Authentication Key(s) are pre-loaded in the TOE at the end of Phase 5 “TOE composite product integration”. After a successful authentication the “Personalization Agent” takes control of the TOE, safely stores card identification data and user identification data and execute the steps and operations as described in the life cycle Phase 6 “TOE Personalization” (FIA_UID.2). The authentication mechanism is based on challenge-response protocol according to Tacho_AGD_PRE using the AES algorithm and key length of 128, 192 and 256 bits.

Only after its personalization with the specific cryptographic keys the TOE can be used as one of four different types of Tachograph Card (driver card, workshop card, control card or company card).

10.1.2 SF_SM Secure Messaging

The TOE implements the thrusted channel based on secure messaging security function providing confidentiality and integrity of transferred data with authenticated external entities according to the SFRs (FTP.ITC.1/2nd, FTP.ITC.1/1st, FTP.TDC.1/2nd, FTP.TDC.1/1st).

The secure messaging is using AES and 3DES algorithms for encryption/decryption and MAC computation according to SFRs (FCS_COP.1.1/AES_2nd, FCS_COP.1.1/1st_TDES).

The secure messaging is using algorithm AES and cryptographic key sizes 128, 192, 256 bits according to SFRs (FCS_COP.1.1/AES_2nd).

The secure messaging is using algorithm TDES and cryptographic key sizes 112 bits according to SFRs (FCS_COP.1.1/1st_TDES).

10.1.3 SF_AC Access Control

The TOE implements a data access control mechanism to allow/deny the execution of operations on objects to external entities/subjects (FDP_ACC.2, FDP_ACF.1).

The TSF SF_AC checks that for each operation initiated by a subject on objects the security attributes for that roles authorization are satisfied (FDP_ACC.2, FDP_ACF.1).

The TSF SF_AC security function covers the management of subject an object as defined in (FDP_ACC.2, FDP_ACF.1). The operations allowed are defined in (FDP_ACF.1).

The TSF SF_AC satisfy the SFRs (FDP_ETC.1,FDP_ETC.2,FDP_ITC.1,FDP_ITC.2) for what concern the import/export of user data with/without related security attributes.

10.1.4 SF_KCS Key Derivation, Cryptographic and Data Signature

The TOE implements the SF_KCS for the support of key derivation, cryptographic and data signature functionalities.

The TSF SF_KCS implements a cryptographic key generation, distribution and destruction mechanism according to SFRs (FCS_CKM.1/2nd, FCS_CKM.2/2nd, FCS_CKM.4/2nd, FCS_CKM.1/1st, FCS_CKM.2/1st and FCS_CKM.4/1st).

The TSF SF_KCS implements cryptographic functionalities with the support of algorithm AES with cryptographic key sizes 128, 192, 256 bits according to SF (FCS_COP.1/AES_2nd).

The TSF SF_KCS implements cryptographic functionalities with the support of algorithm TDES with cryptographic key sizes 112 bits according to SF (FCS_COP.1/1st_TDES).

The TSF SF_KCS implements encryption/decryption, data signature generation/verification and cryptographic key agreement with the support of algorithm based on ECC (ECDSA, ECKA-EG) with cryptographic key sizes 256, 384, 512, 521 bits according to SFRs (FCS_COP.1/ECC_2nd, FCO_NRO.1).

The TSF SF_KCS implements encryption/decryption and data signature generation/verification with the support of algorithm RSA with cryptographic key sizes 1024 bits according to SFRs (FCS_COP.1/1st_RSA, FCO_NRO.1).

The TSF SF_KCS implements hashing cryptographic functionalities with the support of algorithm SHA-256, SHA-384 and SHA-512 according to SFR (FCS_COP.1/SHA-2_2nd).

The TSF SF_KCS implements hashing cryptographic functionalities with the support of algorithm SHA-1 according to SFR (FCS_COP.1/1st_SHA-1).

The TSF SF_KCS implements a deterministic random number generator according to SFR (FCS_RNG.1).

10.1.5 SF_DProt Data Protection

This TOE Security Function Data Protection is responsible for protection of the TSF data, user data, and TSF functionality.

The TSF SF_DProt Data Protection is composed of software implementations of test and security functionalities to protect data, detect data corruption and preserve a secure TOE status.

Performing self-tests of the TOE at each power-up including a set of tests to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1)

Initializing memory after reset and Initializing memory of de-allocated data and secure destruction of cryptographic key, secrets and private material (FCS_CKM.4, FDP_RIP.1).

Protecting and monitoring the integrity of all stored user data and preventing use of corrupted data by stopping the operation involved and setting an error (FDP_SDI.2, FAU_ARP.1, FAU_SAA.1).

Protecting confidentiality of sensible stored user data, cryptographic keys and residual cryptographic key information, by storing sensible information ciphered and by clearing all the buffers used for computations by randomizing their contents (FPR_UNO.1).

The TSF preserves the secure state after sensitive processing failure (RNG, power loss, memory or functional failure) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)

This TSF enforces protection of cryptographic key data during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMS.1).

10.1.6 SF_OSPlat Java Platform and OS

This TSF is implemented at SW layer JCS and Kernel. Here the TSF is described as a single and cumulative security function representing the following sub-functions which services and characteristics are reported below in the description: **SF.SECURE_MANAGEMENT, SF.CRYPTO_KEY, SF.CRYPTO_OP, SF.TRANSACTION, SF.PIN and SF.OBJECT_DELETION**. The TSF provides optimized services for data integrity, memory management, I/O functions, atomic data transaction, cryptographic support, test and management of HW peripheral of Integrated Circuit ST31G480 D01 including crypto library NESLIB V.6.2.1. The TSF provide and manages the following functionalities:

Secure Management functionalities (SF.SECURE_MANAGEMENT) such as:

- Memory cleaning upon: allocation of class instances, arrays, and APDU buffer, and de-allocation of array object, any transient object, any reference to an object instance created during an aborted transaction (FDP_RIP.1).

- Unobservability: operations on secret keys and PIN codes are not observable by other subjects by observation of variations in power consumption or timing analysis, (supporting fulfilment of FPR_UNO.1, FPT_EMS.1).
- Preservation of a secure state when the following types of failures occur: loss of power or card tearing, NVRAM memory wear-out, failed checksum verification on sensitive data (Supporting fulfilment of FAU_SAA.1, FPT_FLS.1).
- Monitor events related to TOE security and to preserve a TOE secure state, auditable events are: card tearing, power failure, abnormal environmental operating conditions (frequency, voltage, and temperature), physical tampering and NVRAM consistency/integrity check failure (Supporting fulfilment of FAU_SAA.1, FPR_PHP.3).
- Exception handling: This function addresses the TOE exception management. The reasons of these exceptions are: range of operating conditions, integrity errors, life cycle and TOE internal audit failure. Upon detection of exception and depending on exception severity the TOE may end the working session entering a state were the TOE becomes irresponsive or, in case of major severity, may change its life cycle state entering the “end of use” state.
- Testing: This function ensures the tests of TOE functionalities. It includes the test of Integrated Circuit ST31G480 hardware components and its environmental operating conditions such as temperature, voltage and clock frequency. Depending on the typology and on the operation to be performed, the test is executed at power-up or before/after sensitive operation e.g. digital signature or cryptographic computation. Upon detection of an anomaly and depending on anomaly severity the TOE may end the working session entering a state becoming irresponsive or, in case of major severity, may change its life cycle state entering the “end of use” state (Supporting fulfilment of FAU_SAA.1, FPT_TST.1).

Crypto Key management functionalities (SF.CRYPTO_KEY) such as:

- key generation
- key destruction (supporting the fulfilment of SFRs: FDP_RIP.1)
- integrity and the unobservability of the keys (supporting the fulfilment of SFRs: FDP_SDI.2).

Crypto Operation (SF.CRYPTO_OP): functionalities of encryption/decryption and signature creation/verification with the support of the following algorithms:

- DES ECB and CBC
- Triple DES ECB and CBC with 16, 24 bytes of key
- AES ECB and CBC with 128, 256 bits of key
- RSA CRT with key length 512, 768, 1024 and 2048 bits
- ECC (ECDSA, ECKA) with key length up to 521 bits
- Hashing (SHA-1, SHA-256, SHA-384, SHA-512)
- Deterministic Random Number Generation

Supporting the fulfilment of SFRs: FCS_CKM.1/2nd, FCS_CKM.2/2nd, FCS_CKM.4/2nd, FCS_COP.1/AES_2nd, FCS_COP.1/SHA-2_2nd, FCS_COP.1/ECC_2nd, FCS_RNG.1, FPT_TDC.1/2nd, FTP_ITC.1/2nd, FCS_CKM.1/1st, FCS_CKM.2/1st, FCS_CKM.4/1st, FCS_COP.1/1st_TDES, FCS_COP.1/1st_RSA, FCS_COP.1/1st_SHA-1, FPT_TDC.1/1st, FTP_ITC.1/1st.

Data Transaction management (SF.TRANSACTION): functionalities concerning NVRAM changes in order to assures the coherence of the data if a failure or power interruption occurs during their update

PIN management (SF.PIN): This security functionality is related to all the operation related to PIN objects.

In particular SF.PIN:

- provides means to perform PIN Verification;
- automatically decreases the try check counter of PINs in case of PIN verification failure;
- provides the functionality to update PIN value and the try counter.

PIN verification procedure consists in the comparison of the PIN provided by the user application requesting the verification procedure with the PIN stored into a PIN object.

This security functionality also guarantees the integrity of the stored PIN value, try counter and verification status (supporting the fulfilment of SFRs: FDP_SDI.2, FIA_AFL.1/WC).

Secure data deletion (SF.OBJECT_DELETION): de-allocation of memory resources of data no longer accessible. The security functionality also guarantees that the information content of unreachable data cannot be retrieved anymore (supporting the fulfilment of SFRs: FDP_RIP.1).

10.2 TOE summary specification rationale

The following table provides a list of the TOE Security Functionalities (TSF) and the coverage of the SFRs.

SFR \ SF	SF_AUTH	SF_SM	SF_AC	SF_KCS	SF_DProt	SF_OSPlat
FAU_ARP.1	x				x	
FAU_SAA.1	x				x	x
FCO_NRO.1				x		
FDP_ACC.2			x			
FDP_ACF.1			x			
FDP_DAU.1				x		
FDP_ETC.1			x			
FDP_ETC.2			x			
FDP_ITC.1			x			
FDP_ITC.2			x			
FDP_RIP.1					x	x
FDP_SDI.2					x	x
FIA_AFL.1/C	x			x		
FIA_AFL.1/WC	x					x
FIA_ATD.1	x					
FIA_UAU.3	x					
FIA_UAU.4	x					
FIA_UID.2	x					
FIA_USB.1	x					
FPR_UNO.1					x	x
FPT_EMS.1						x
FPT_FLS.1					x	x
FPT_PHP.3					x	x
FPT_TST.1					x	x
FCS_CKM.1/2nd				x		x
FCS_CKM.2/2nd				x		x
FCS_CKM.4/2nd				x	x	x
FCS_COP.1/AES_2nd		x		x		x
FCS_COP.1/SHA-2_2nd				x		x
FCS_COP.1/ECC_2nd				x		x
FCS_RNG.1				x		x
FIA_UAU.1/2nd	x					
FPT_TDC.1/2nd		x		x		x
FTP_ITC.1/2nd		x		x		x
FCS_CKM.1/1st				x		x
FCS_CKM.2/1st				x		x
FCS_CKM.4/1st				x	x	x
FCS_COP.1/1st_TDES		x		x		x
FCS_COP.1/1st_RSA				x		x
FCS_COP.1/1st_SHA-1				x		x
FIA_UAU.1/1st	x					
FPT_TDC.1/1st		x		x		x
FTP_ITC.1/1st		x		x		x

Table 22 - Mapping of Security Functional Requirements (SFRs) on TOE Security Functions (TSFs)

11. QUALITY REQUIREMENTS

12. ENVIRONMENTAL/ECOLOGICAL REQUIREMENTS

STMicroelectronics recommends viewing documents on the screen rather than printing to limit paper consumption.