SECURITY TARGET
PUBLIC VERSION

TACHOGRAPH G1, G2V1, G2V2 ON IFX_CCI_000039H
EAL 4+

Contents

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	**Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h** **Public Security Target**
Version :	1.7p
ST Reference :	D1551037
Origin :	Thales DIS
IT Security Evaluation Facility :	LETI
IT Security Certification scheme :	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

Product Name :	Tachograph G1 / Tachograph G1 v1.6 Tachograph G2V1 Tachograph G2V2
Product Technical Name :	Tachograph G2V2
Security Controllers :	Infineon IFX_CCI_000039
TOE Name :	Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h
TOE Version :	2.2.1.N
TOE documentation :	Guidance [AGD]
Composition elements:	
Composite TOE identifier:	IFX_CCI_000039h
Composite TOE Version:	T11 (design step) **firmware** BOS & POWS 80.306.16.0 and 80.306.16.1 (Non-ISO ATR: firmware identifier) Flash-loader 09.12.0005 (Flash-loader function) **Software** NRG™ SW(optional) 05.03.4097 (NRG™ SWfunction) HSL (optional) v3.52.9708 (HSL function) UMSLC v01.30.0564 (UMSLC function) SCL (optional) v2.15.000 and v2.11.003 (SCL function)

	ACL (optional) v3.33.003 and v3.02.000 (ACL function)

1.3 TOE IDENTIFICATION

The TOE identification is described in [TRACEABILITY].

1.4 SECURITY TARGET OVERVIEW

The Target of Evaluation (TOE) is the micro-module made of the Integrated Circuit (IC) and its embedded software (ES). The ES encompasses the Smart Tachograph Application and some MultiApp V5.0 javacard platform functionalities.

It includes the associated embedded data of the smart card working on the micro-controller unit in accordance with the functional specifications.

The Security Target defines the security objectives and requirements for the Smart Tachograph Card.

The Security Target is based on the Protection Profiles [PP-TACHOCARD1] and [PP-TACHOCARD2]. As demonstrated in Conformance rationale most of the security elements, security objectives and SFR from [PP-TACHOCARD1] are included in [PP-TACHOCARD2]. Any specificity to [PP-TACHOCARD1] will be clearly visible.

The main objectives of this ST are:

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

1.5 REFERENCES, GLOSSARY AND ABBREVIATIONS

1.5.1 EXTERNAL REFERENCES

Reference	Title - Reference
[CC]	**Common Criteria references**
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2017-04-001, version 3.1 rev 5, April 2017
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2017-04-002, version 3.1 rev 5, April 2017
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2017-04-003, version 3.1 rev 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2017-04-004, version 3.1 rev 5, April 2017
[JIL_CPE]	Joint Interpretation Library: Composite product evaluation for Smart Cards and similar devices, Version 1.5.1 May 2018
[ISO]	**ISO references**
[ISO9797-2]	ISO/IEC 9797: Information security - Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function, 2002
[PP]	**Protection Profiles**
[PP-TACHOCARD1]	Digital Tachograph –Tachograph Card (TC PP) Protection Profile BSI-CC-PP-0070-2011 Version 1.02
[PP-TACHOCARD2]	Digital Tachograph –Tachograph Card (TC PP) Protection Profile BSI-CC-PP-0091-2017 Version 1.0
[PP-IC-0084]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014
[TACHO]	**Tachograph references**
[5](Annex 1C)	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
[5 Amd]	Commission Implementing Regulation (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components
[6] (Annex 1B)	Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’, 05.08.2002, Annex I B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)

[7]	A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-Systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011
[8]	Commission Implementing Regulation (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components
[IFX]	**Chip references**
[ST-IC]	IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite – revision v6.5 – 2024-08-20
[CR-IC]	Certification Report, 4th September 2024, BSI-DSZ-CC-1107-V5-2024 IFX_CCI_00002Dh, 000039h, 00003Ah, 000044h, 000045h, 000046h, 000047h, 000048h, 000049h, 00004Ah, 00004Bh, 00004Ch, 00004Dh, 00004Eh design step T11 with firmware 80.306.16.0, 80.306.16.1 or 80.312.02.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 or v2.11.003, optional ACL v3.35.001, v3.34.000, v3.33.003 or v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance
[JCS]	**Javacard references**
[JCRE3]	Java Card 3.1 Runtime Environment (JCRE) Specification – November 2019 – Published by Oracle
[JCVM3]	Java Card 3.1 Virtual Machine (JCVM) Specification – November 2019 – Published by Oracle
[JCAPI3]	Java Card 3.1 Application Programming Interface (API) Specification, Classic Edition - November 2019 – Published by Oracle
[GP]	**Global Platform references**
[GP23]	Card Technology Secure Channel Protocol '03' Card Specification v2.3 – Amendment D Version 1.1.2 - March 2019 Reference: GPC_SPE_014
[MISC]	**Miscellaneous**
[AES]	FIPS PUB 197 Advanced Encryption Standard
[SP800-67]	SP800-67 Triple Data Encryption Algorithm (TDEA)
[SP800-38 A]	NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of operation
[TR03110-2]	Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.21, 21/12/2016

1.5.2 INTERNAL REFERENCES

Reference	Title - Reference
[ST-TACHOCARD]	TACHOGRAPH G1, G2V1, G2V2 ON IFX_CCI_000039H SECURITY TARGET Ref D1551037
[AGD]	Guidance Documentation including [AGD-OPE], [AGD-PRE], [TRACEABILITY]
[AGD-OPE]	Operational user Guidance Ref: D1551042 Rev 1.2
[AGD-PRE]	Preparative procedures Ref: D1551041 Rev 1.3
[TRACEABILITY]	Traceability document Ref: D1559331 Rev H

1.6 ACRONYMS AND GLOSSARY

1.6.1 ACRONYMS

AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher)
CC	Common Criteria version 3.1
DES	Data Encryption Standard (see FIPS PUB 46-3)
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
ES	Embedded Software
GNSS	Global Navigation Satellite System
IC	Integrated Circuit
ICC	Integrated Circuit Card
IT	Information Technology
MAC	Message Authentication Code
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
OSP	Organisational Security Policy

OS	Operating System
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
SF	Security function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
TSF	TOE Security functions
TSFI	TSF Interface
TSP	TOE Security Policy
VIN	Vehicle Identification Number
VRN	Vehicle Registration Number
VU	Vehicle Unit

1.6.2 GLOSSARY

Glossary Term	Definition
Activity data	Activity data include events data and faults data for all card types and specific data depending on card type, such as control activity data for control cards, driver activity, vehicles used and places for driver cards and company activity data for company cards. For a full definition, see [5] Annex 1C, Appendix 2 Activity data are part of User Data.
Application note	Informative part of the PP containing supporting information that is relevant or useful for the construction, evaluation or use of the TOE.
Attacker	A person or a process trying to undermine the security policy defined by the current PP, especially to change properties of the assets that have to be maintained.
Authentication	A function intended to establish and verify a claimed identity.

Glossary Term	Definition
Authentication data	Data used to support verification of the identity of an entity.
Authenticity	The property that information is coming from a party whose identity can be verified.
Calibration	Updating or confirming vehicle parameters to be held in the data memory. Vehicle parameters include vehicle identification (VIN, VRN and registering Member State) and vehicle characteristics (w, k, l, tyre size, speed limiting device setting (if applicable), current UTC time, current odometer value); during the calibration of a recording equipment, the types and identifiers of all type approval relevant seals in place shall also be stored in the data memory. Any update or confirmation of UTC time only, shall be considered as a time adjustment and not as a calibration. Calibration of a recording equipment requires the use of a workshop card.
Card identification data	The following elements stored on the TOE, as defined in [5] Annex 1C, Appendix 1 and Appendix 2: typeOfTachographCardId, cardIssuingMemberState, cardNumber, cardIssuingAuthorityName, cardIssueDate, cardValidityBegin, cardExpiryDate
Company card	A tachograph card issued by the authorities of a Member State to a transport undertaking needing to operate vehicles fitted with a tachograph, which identifies the transport undertaking, and allows for the displaying, downloading and printing of the data, stored in the tachograph, which have been locked by that transport undertaking.
Control card	A tachograph card issued by the authorities of a Member State to a national competent control authority that identifies the control body and, optionally, the control officer. It allows access to the data stored in the data memory or in the driver cards and, optionally, in the workshop cards for reading, printing and/or downloading. It also gives access to the roadside calibration checking function, and to data on the remote early detection communication reader.
Data memory	An electronic data storage device built into the tachograph card.
Digital Signature	Data appended to, or a cryptographic transformation of, a block of data that allows the recipient of the block of data to prove the authenticity and integrity of the block of data.
Downloading	The copying, together with the digital signature, of a part, or of a complete set, of data files recorded in the data memory of the vehicle unit or in the memory of a tachograph card, provided that this process does not alter or delete any stored data.

Glossary Term	Definition
Driver card	A tachograph card, issued by the authorities of a Member State to a particular driver that identifies the driver and allows for the storage of driver activity data.
European Root Certification Authority (ERCA)	An organisation responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment (TP.360) Via E. Fermi, 1 I-21020 Ispra (VA)
Event	An abnormal operation detected by the smart tachograph that may result from a fraud attempt.
External GNSS Facility	A facility that contains the GNSS receiver when the vehicle unit is not a single unit as well as other components needed to protect the communication of position data to the rest of the vehicle unit.
Fault	An abnormal operation detected by the smart tachograph that may arise from an equipment malfunction or failure.
Human user	A legitimate user of the TOE, being a driver, controller, workshop or company. A user is in possession of a valid tachograph card.
Integrity	The property of accuracy and completeness of information.
Intelligent Dedicated Equipment	Equipment used to download data from a Tachograph card to external storage media.
Interface	A facility between systems that provides the media through which they can connect and interact.
Interoperability	The capacity of systems and the underlying business processes to exchange data and to share information.
Manufacturer	The generic term for a manufacturer producing and completing the Tachograph Card as the TOE.

Glossary Term	Definition
Member State Authority (MSA)	Each Member State of the European Union establishes its own national Member State Authority (MSA) usually represented by a state authority, e.g. Ministry of Transport. The national MSA runs some services, among others the Member State Certification Authority (MSCA). The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy. MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself. Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
Member State Certification Authority (MSCA)	An organisation established by a Member State Authority, responsible for implementation of the MSA policy and for signing certificates for public keys to be inserted into tachograph cards.
Motion Sensor	A part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled.
Personal Identification Number (PIN)	A secret password necessary for using a workshop card and only known to the approved workshop to which that card is issued.
Personalisation	The process by which the equipment-individual data are stored in and unambiguously, inseparably associated with the related equipment.
Registering member state	The Member State of the European Union in which the vehicle is registered. This is represented by a numeric code (see [5] Annex 1C, Appendix 1, Chapter 2.101).
Remote Early Detection Communication	Communication between the remote early detection communication facility and the remote early detection communication reader during targeted roadside checks with the aim of remotely detecting possible manipulation or misuse of recording equipment.
Remote Communication Facility	The equipment of the vehicle unit that is used to perform targeted roadside checks.
Remote Early Detection Communication Reader	A system used by control officers for targeted roadside checks of vehicle units, using a DSRC connection.
Secret key	A symmetric or private asymmetric key.

Glossary Term	Definition
Security Certification	Process to certify, by a Common Criteria certification body, that the tachograph card fulfils the security requirements defined in the relevant Protection Profile.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys and certificates). Security data includes the Sensor Installation Data on a workshop card, see [5] Annex 1C, Appendix 2.
Self Test	Tests run cyclically and automatically by the recording equipment to detect faults.
Smart Tachograph System	The recording equipment, tachograph cards and the set of all directly or indirectly interacting equipment during their construction, installation, use, testing and control, such as cards, remote early detection communication reader and any other equipment for data downloading, data analysis, calibration, generating, managing or introducing security elements, etc.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]). In the context of this PP, the term security data is also used.
User	A human user or connected IT entity.
User identification data	The following data elements stored on the TOE, as defined in Annex IC [5] Appendix 2 and Appendix 1: For driver cards: holderSurname, holderFirstNames, cardHolderBirthDate, cardHolderPreferredLanguage, drivingLicenceIssuingAuthority, drivingLicenceIssuingNation, drivingLicenceNumber. For workshop cards: workshopName, workshopAddress, holderSurname, holderFirstNames, cardHolderPreferredLanguage. For control cards: controlBodyName, controlBodyAddress, holderSurname, holderFirstNames, cardHolderPreferredLanguage. For company cards: companyName, companyAddress, cardHolderPreferredLanguage
User Data	Any data, other than security data, recorded or stored by the Tachograph Card. User data include card identification data, user identification data and activity data. The CC gives the following generic definitions for user data: • Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [1]). • Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).

Glossary Term	Definition
Vehicle Unit	The tachograph excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may be a single unit or several units distributed in the vehicle, provided that it complies with the security requirements of this Regulation; the vehicle unit includes, among other things, a processing unit, a data memory, a time measurement function, two smart card interface devices for driver and co-driver, a printer, a display, connectors and facilities for entering the user's inputs.
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.
Workshop Card	A tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a fitter, a vehicle manufacturer or a workshop, approved by that Member State, which identifies the user and allows for the testing, calibration and activation of tachographs, and/or downloading from them.

1.7 TOE OVERVIEW

1.7.1 TOE TYPE

1st generation VU (compliant with Annex I B [6]) will not have to be replaced, following the application of the new [5] Annex 1C. They will continue to be used in the field, until their end of life. 2nd generation VU (compliant with [5] Annex 1C) will then be gradually introduced in the field.

The TOE need to be interoperable with 1st generation and 2nd generation Digital Tachograph Systems. So Tachograph Cards will be able to be used in both 1st and 2nd generation VUs depending on personalization profile. Tacho Gen1 profile compliant with 1st generation VU and Tacho Gen2 profile compliant with both 1st generation VU and 2nd generation VU.

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

- The Infineon IC
- The MultiApp 5.0 platform (including Thales Crypto library and the operating system).
- The Smart Tachograph application
- The Tachograph Personalization Tool (GDP) used only during the personalization of the product. GDP is deleted before shipping to the final user.
- The OS update application used for software update during operational phase. Only available for Tacho Gen2 profile
- The associated guidance documentation [AGD]

1.7.2 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE

The functional requirements for a Smart Tachograph card are specified in [6] for Tacho Gen1 profile and in in [5] for Tacho Gen2profile.

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

The TOE can be configured and implemented as a driver card, workshop card, control card or company card.

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

In its operational phase only the Smart Tachograph can be selected.

The main security features of the TOE are as follows:

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

Specifically the Tachograph Card aims to protect:

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

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

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

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

The product is compliant with two major industry standards:

- Sun’s Java Card 3.1[JCVM3] [JCRE3]
- The Global Platform Card Specification version 2.3 [GP23],

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

- Hardware Tamper Resistance is managed by the chip security layer that meets the Security IC Platform Protection Profile [PP/BSI-0084].
- Secure operation of the MultiApp 5.0 platform managed inside platform component.

1.7.3 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

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

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

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

1.7.4 TOE DELIVERY

As a summary description of how the parts of the TOE are delivered to the final customer, the Tachograph G2V2 embedded software is delivered mainly in form of a smart card, module or wafer. The form factor is packaged on Thales manufacturing facilities and sent to customer premises or via the wafer init process from the IC Manufacturer premises.

The product is sent to the customer by standard transportation respecting Thales Transport Security Policies.

The different guides accompanying the TOE and parts of the TOE are the ones specified in [AGD] section. They are delivered in form of electronic documents (*.pdf) by Thales’s Technical representative via a secure file sharing platform download action.

Item type	Item	Reference/Version	Form of delivery
Software and Hardware	Tachograph G2V2	Refer to paragraph §1.3	Smart card, module or wafer
Document	Tachograph G2V2: AGD_OPE document - Javacard Platform	Refer to paragraph §1.5.2	Electronic document via secure file download
Document	Tachograph G2V2: AGD_PRE document - Javacard Platform	Refer to paragraph §1.5.2	Electronic document via secure file download

1.8 TOE DESCRIPTION

1.8.1 SMART TACHOGRAPH APPLICATION DESCRIPTION

A Tachograph card is a smart card carrying an application intended for its use with the recording equipment (VU). Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage.

Due to interoperability with VU, the Tachograph cards can be personalized to be compliant with 1st generation VU (refer to [6]) or with 2nd generation VU both version 1 and version 2 (refer to [5] and [5 Amd]) and version 2 (refer to [8])

The functional requirements for a Tachograph card are specified in [6] for Tacho Gen1 profile and [5] Tacho Gen2 profile.

The basic functions of the Smart Tachograph card are:

- to support mutual authentication protocol regarding Tacho Gen1 profile or Tacho Gen2 profile specification,
- to store card identification and card holder identification data. These data are used by the vehicle unit to identify the cardholder, provide accordingly functions and data access rights, and ensure cardholder accountability for his activities,
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder. The card manages two different file structures (DF) : one for Tacho Gen1 profile and another one for Tacho Gen2 profile (version2 only)
- to verify and generate signature for Tacho Gen1 profile and for Tacho Gen2 profile
- to process DSRC Message

A Tachograph card may also be used by any card reader (e.g. of a personal computer) who shall have full read access right on any user data.

A Tachograph card may be of the following types:

- driver card: A tachograph card, issued by the authorities of a Member State to a particular driver that identifies the driver and allows for the storage of driver activity data.
- control card: A tachograph card issued by the authorities of a Member State to a national competent control authority that identifies the control body and, optionally, the control officer. It allows access to the data stored in the data memory or in the driver cards and, optionally, in the workshop cards for reading, printing and/or downloading. It also gives access to the

roadside calibration checking function, and to data on the remote early detection communication reader.

- workshop card: A Tachograph card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Member State. The workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the recording equipment; the workshop card is able to process a DSRC message
- company card: A tachograph card issued by the authorities of a Member State to a transport undertaking needing to operate vehicles fitted with a tachograph, which identifies the transport undertaking, and allows for the displaying, downloading and printing of the data, stored in the tachograph, which have been locked by that transport undertaking.

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

1.8.2 PLATFORM DESCRIPTION

Tachograph G2V2 is using some MultiApp V5.0 platform functionalities.

The MultiApp V5.0 platform is an operating system that complies with two major industry standards:

- Sun's Java Card 3.1, which consists of the Java Card 3.1 Virtual Machine [JCVM3], the Java Card 3.1 Runtime Environment [JCRE3] and the Java Card 3.1 Application Programming Interface [JCAPI3].
- The Global Platform Card Specification version 2.3 [GP23]
- File System APIs: these new APIs are required for the [TR03110-2] based applications.
- GDP: Global Dispatcher Perso application to centralize application personalization (at first for smart Tachograph).
- Support of Flash Modularity: possibility during product construction to embed only features required for a given customer item.

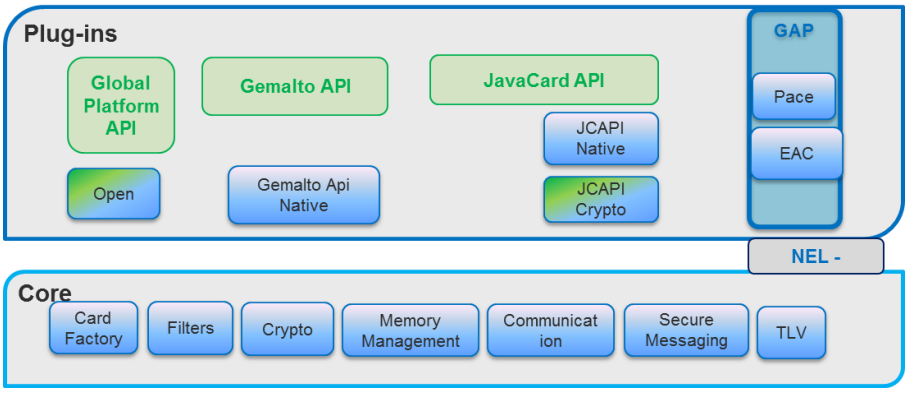


Figure 1: MultiApp V5.0 Java Card platform architecture

As described in Figure 1, the MultiApp V5.0 platform contains the following components:

- **The Core layer**

  It provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the underlying IC. The cryptographic

features implemented in the native layer and which support the Smart Tachograph functionality encompass the following algorithms:

- 3DES (ECB, CBC)
- RSA 1024 (CRT method & public Std method)
- DH 1024
- AES 128, 192, 256
- SHA1, SHA 2 (256, 384, 512)
- HMAC
- ECC (ECDSA et ECDH) up to 521
- Pseudo-Random Number Generation (PRNG)

- **The Plug-ins layer**
  - The **Javacard Runtime Environment**

  It conforms to [JCRE3] and provides a secure framework for the execution of the Java Card programs and data access management (firewall).

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

  - The **Javacard Virtual Machine**

  It conforms to [JCVM3] and provides the secure interpretation of bytecodes.

  - The **API**

  It includes the standard Java Card API [JCAPI3] and the Thales proprietary API.

  - The **Global Platform Issuer Security Domain**

  It conforms to [GP23] and provides card, key and applet management functions (contents and life- cycle) and security control.

The MultiApp V5.0 platform provides the following services:

- Initialization of the Card Manager and management of the card life cycle
- Secure loading and installation of the applets under Security Domain control
- Deletion of applications under Security Domain control
- Secure operation of the applications through the API
- Management and control of the communication between the card and the off-card entity.
- Application life cycle management
- Card basic security services as follows:
  - Checking environmental operating conditions using information provided by the IC
  - Checking life cycle consistency
  - Ensuring the security of the PIN and cryptographic key objects
  - Generating random numbers
  - Handling secure data object and backup mechanisms
  - Managing memory content
  - Ensuring Java Card firewall mechanism

1.8.3 AGILITY CONCEPT

The Smart Tachograph product embeds an optional functionality to update the operating system when the card is already on the field. This functionality is named OS-agility.

The mechanism will allow to correct product issues and security issues when the product is already deployed. The updates are done through a dedicated application and are a list of instructions to update the memory.

The update instructions are packaged into a block protected in confidentiality and integrity by keys known only by Thales DIS. The block can be transmitted and executed by the card only after a successful authentication done with keys only known by the customer. Like this Thales DIS is unable to load some contents into the card without the consent of the customer and the customer also cannot load a content without the consent of Thales DIS.

Prior the execution of the instructions of the patch, some prerequisites are verified, the code ensures that the current product configuration allows the correct execution of the instructions. Some updates can be conditionally be executed following the availability of a dedicated feature. At the end of the execution, the traceability elements are also updated to allow a complete identification of the product (platform version and current patch version). The patch loading mechanism ensures also the atomicity of the updates.

1.8.4 TOE BOUNDARIES AND OUT OF TOE

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

- **Tachograph G2V2** application
- **IFX_CCI_000039** IC which has been certified separately according to [ST-IC] claiming [PP/BSI-0084]
- **MultiApp 5.0** platform (only TACHOGRAPH G2V2 used functionalities)
- **GDP** personalization application
- **OS agility** application

The **TSFs** are composed of:

1. The Tachograph related functions of the Smart Tachograph application: Mutual Authentication Gen1 and Gen2, Verify PIN, Verify Certificate Gen1 and Gen2, Select/read/Update files, Manage Security Environment, Hash file generation, Generation/Verification Signature, Perform DSRC Message check
2. Tachograph Personalization commands through GPD. (Other functions are out of the TOE)
3. The OS agility application
4. The IFX_CCI_000039 IC that supports the MultiApp 5.0 Platform.

Figure 2 represents the product. The TOE is bordered with bold and un-continuous line.
The architecture of MultiApp inside the TOE is presented in platform description chapter.
Note that Tachograph Personalisation Tool (GDP) is deleted after personalisation.
In usage phase only the **Tachograph G2V2** application and OS agility are present in the Applet Layer.
The platform will be in a closed configuration. No possibility to select the Card Manager.
Tachograph G2V2 application is selected by default.

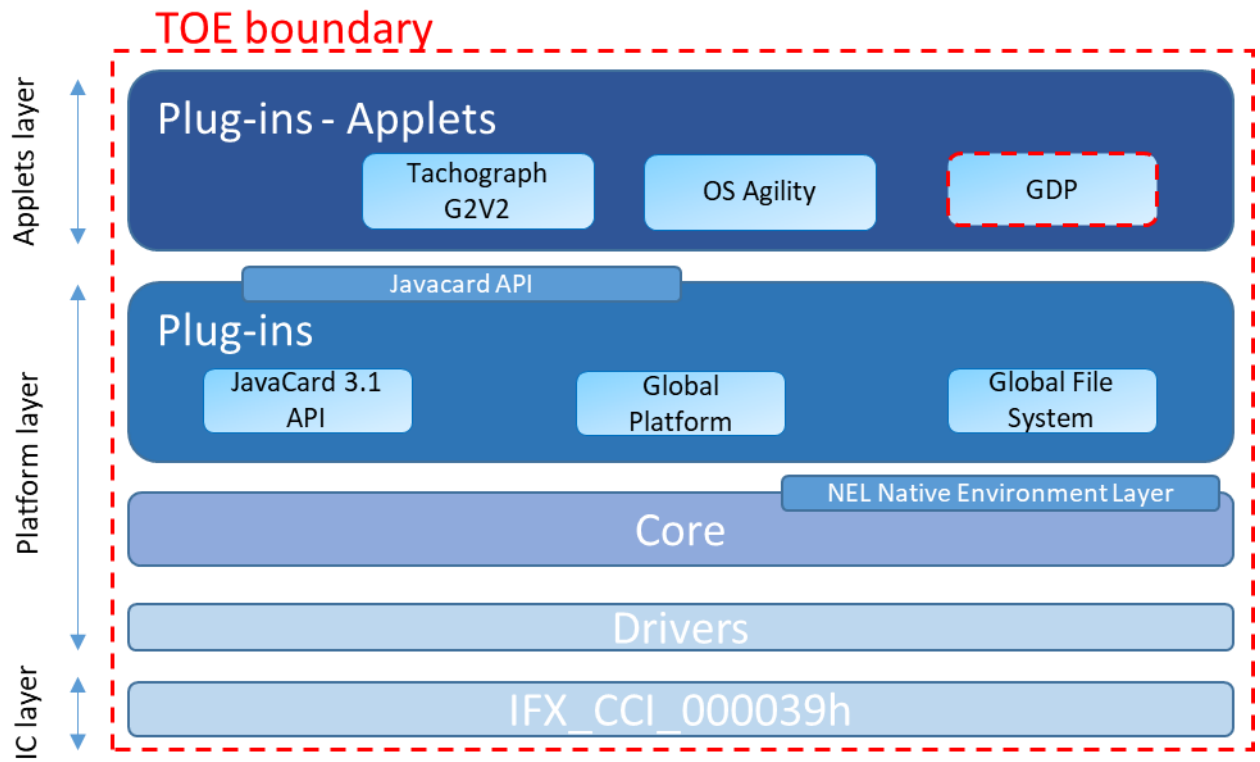


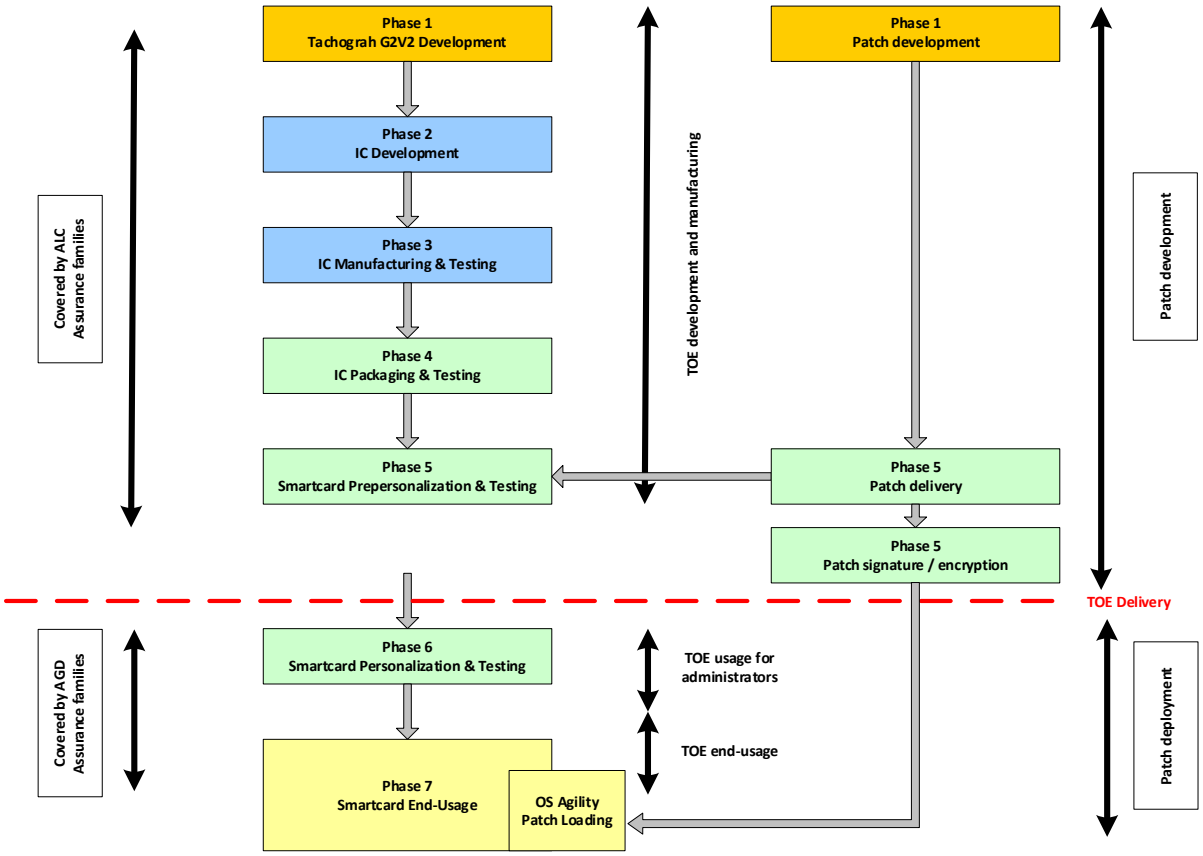
Figure 2 – Smart Tachograph Card

1.8.5 TOE LIFE-CYCLE

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP-IC-0084], the TOE life-cycle is additionally subdivided into 7 steps.)

Note related to patch development

No patch is present within the TOE for the present evaluation. Indeed, should a patch be needed in the future, it would require at least a maintenance of the CC certificate, as required by the CC scheme rules. However, the patch mechanism is part of the TOE and as such its security is assessed within the present evaluation.



Phase	Description / comments		Who	Where
1	MAV5.0 platform development	Platform development & tests (1.a)	**Thales** GP R&D team SL Crypto team - secure environment -	**Thales Development site (see §1.8.6)**
	Thales applets (IAS, eTravel…) development	- Applet Development (1.d) - Applet tests	**Thales** GP R&D team - secure environment -	**Thales Development site (see §1.8.6)**
	Patch development	- Patch Development (1.e) - Patch tests	**Thales** GP R&D team - secure environment -	**Thales Development site (see §1.8.6)**
	PSE team	- Platform configuration (1.c) - Script development	**Thales PSE team**	**Thales manufacturing site (see §1.8.6)**
2	IC development	IFX_CCI_000039 development	**Infineon** - Secure environment -	Infineon development site(s)
3a	IC manufacturing	Manufacturing of virgin IFX_CCI_000039 integrated circuits embedding the Infineon flash loader, and protected by a dedicated transport key.	**Infineon** - Secure environment -	Infineon development site(s)
3b (optional)	Initialization / Pre-personalization	Loading of the Thales software (platform and applets on top based on script generated) – For WAFER init process only		
4	SC manufacturing: IC packaging & Embedding, also called “assembly”	- IC packaging & testing	**4.a) Infineon** - Secure environment – **OR** **4.b) Thales** Production teams - Secure environment -	**Thales manufacturing site (see §1.8.6)**
5.a	Embedding	Put the module on a dedicated form factor (Card, inlay MFF2, other…)	**Thales** Production teams - Secure environment -	**Thales manufacturing site (see §1.8.6)**
5.b	Initialization / Pre-personalization (Not Applicable for wafer-init process)	Loading of the Thales software (platform and applets on top based on script generated)		
6	SC Personalization	Creation of files and loading of end-user data	**SC Personalizer** Thales or another accredited company - Secure environment -	SC Personalizer site
7	End-usage	End-usage for SC issuer	**SC Issuer**	Field
		Application Loading (7.a)	**SC Issuer**	Field
		End-usage for cardholder	**Cardholder**	Field
		Patch update (7.b)	**Thales**	Field

Figure 3: Life cycle description

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

Remark2: For initialization/pre-personalization IC flash loader will be used based the IC manufacturer recommendation. The flash loader is deactivated definitively after the loading of the flashmask. No possibility to go back the flash loader after this phase.

Remark3: Embedding (module put on a dedicated form factor) will be done on an audited site.

1.8.6 INVOLVED THALES-DIS SITES

- **Development and Project Management**
  - La Ciotat (France)
    - CC project management
  - Gémenos
    - project management
  - Singapore
    - Platform & Application development
  - Meudon (France)
    - Platform development
  - Vantaa
    - Platform & Application development support

- **Manufacturing**
  - Gémenos, Singapore, Vantaa, Tczew, Curitiba, Chanhassen, Pont-Audemer, Montgomery

- **IT activities**
  - Gémenos, Calamba, Chennai, Noida, Paris (TELEHOUSE)

2 CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This security target claims conformance to the Common Criteria (CC) version 3.1 revision 5.
The conformance to the CC is claimed as follows:

CC	Conformance Claim
Part 1 [CC-1]	Strict conformance
Part 2 [CC-2]	Conformance with extensions : FCS_RNG.1 Quality metric for random numbers FPT_EMS.1 TOE Emanation
Part 3 [CC-3]	Conformance

The [CEM] has to be taken into account.

2.2 PP CLAIM

This ST claims strict conformance to the Protection Profile [PP-TACHOCARD1] for Tacho Gen1 profile and [PP-TACHOCARD2] for Tacho Gen2 profile.

This security target is a composite security target, including the IC security target [ST-IC]. However the security problem definition, the objectives, and the SFR of the IC are not described in this document.

There are extra Threats, OSP, Assumptions, TOE objectives and SFR dedicated to OS update, written in dedicated paragraphs and without conflict with [PP-TACHOCARD1] and [PP-TACHOCARD2].

As no other modification was done, we can conclude that the conformance is demonstrated.

2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2, ATE_DPT2 and AVA_VAN.5 as defined in CC part 3 [CC-3].

2.4 CONFORMANCE RATIONALE

2.4.1 ASSETS

Assets	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
Identification data (IDD)	Yes	Yes	Included in this Security Target
Activity data (ACD)	Yes	Yes	Included in this Security Target

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

- All assets from [PP-TACHOCARD1] are included in [PP-TACHOCARD2] .

2.4.2 SECONDARY ASSETS

Assets	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
Signature creation data (SCD)	Yes	No	Included in Keys to protect data (KPD)
Secret messaging keys (SMK)	Yes	No	Included in Keys to protect data (KPD)
Application (APP)	No	Yes	Included in this Security Target
Keys to protect data (KPD)	No	Yes	Included in this Security Target
Signature verification data (SVD)	Yes	Yes	Included in this Security Target
Verification authentication data (VAD)	Yes	Yes	Included in this Security Target
Reference authentication data (RAD)	Yes	Yes	Included in this Security Target
Data to be signed (DTBS)	Yes	Yes	Included in this Security Target
TOE file system, including specific identification data	Yes	Yes	Included in this Security Target

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

- Most of assets from [PP-TACHOCARD1] are included in [PP-TACHOCARD2] . Others are covered by [PP-TACHOCARD2] secondary assets.

2.4.3 SUBJECTS AND EXTERNAL ENTITIES

Subjects and external entities	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
Administrator	Yes	Yes	Included in this Security Target
Vehicle Unit	Yes	Yes	Included in this Security Target
Other devices	Yes	Yes	Included in this Security Target
Attacker	Yes	Yes	Included in this Security Target

Table 3 Subjects and external entities

- All subjects from [PP-TACHOCARD1] are included in [PP-TACHOCARD2] .

2.4.4 THREATS

Threats	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
T.Identification_Data	Yes	Yes	Included in this Security Target
T.Activity_Data	Yes	Yes	Included in this Security Target
T.Data_Exchange	Yes	Yes	Included in this Security Target
T.Personalisation_Data	Yes	No	Covered by A.Personalisation_Phase and OE.Personalisation_Phase
T.Application	No	Yes	Included in this Security Target
T.Clone	No	Yes	Included in this Security Target

Table 4 Threats addressed by the TOE

- Most of Threats from [PP-TACHOCARD2] are included in [PP-TACHOCARD2] . Others are covered by [PP-TACHOCARD2].

2.4.5 ASSUMPTIONS

OSP	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
A.Personalisation_Phase	Yes	Yes	Included in this Security Target

Table 5 Assumptions

- Assumptions are shared between [PP-TACHOCARD1] and [PP-TACHOCARD2].

2.4.6 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
P.EU_Specifications	Yes	No	Included in this Security Target
P.Crypto	Yes	Yes	Included in this Security Target

Table 6 Organisational security policies

- Organizational Security Policies are not shared between [PP-TACHOCARD1] and [PP-TACHOCARD2] and differences will be clearly highlighted in dedicated chapter.

2.4.7 SECURITY OBJECTIVES FOR THE TOE

Security Objectives	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
OT.Card_Identification_Data	Yes	Yes	Included in this Security Target
OT.Card_Activity_Storage	Yes	Yes	Included in this Security Target
OT.Data_Access	Yes	Yes	Included in this Security Target
OT.Secure_Communications	Yes	Yes	Included in this Security Target
O.Protect_Secret	No	Yes	Included in this Security Target
O.Crypto_Implement	No	Yes	Included in this Security Target
O.Software_Update	No	Yes	Included in this Security Target

Table 7 – Security objectives for the TOE

- All Security objectives from [PP-TACHOCARD1] are included in **[PP-TACHOCARD2]** .

2.4.8 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Security Objectives for the Operational Environment	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
OE.Personalisation_Phase	Yes	Yes	Included in this Security Target
OE.Tachograph_Components	Yes	Included in OE.Crypto_Admin	Included in this Security Target
OE.Crypto_Admin	No	Yes	Included in this Security Target
OE.EOL	No	Yes	Included in this Security Target

Table 8 – Security objectives for the Operational Environment

- Most of Security objectives for the Operational Environment from [PP-TACHOCARD1] are included in [PP-TACHOCARD2] . Others are covered by [PP-TACHOCARD2].

2.4.9 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

Security functional requirements for the TOE	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
FAU_SAA.1.1	Yes	Yes	Included in this Security Target
FAU_SAA.1.2	Yes	Yes	Included in this Security Target
FCO_NRO.1.1	Yes	Yes	Included in this Security Target
FCO_NRO.1.2	Yes	Yes	Included in this Security Target
FCO_NRO.1.3	Yes	Yes	Included in this Security Target
FCS_CKM.1.1	Yes	FCS_CKM.1.1(2)	Included in this Security Target

Security functional requirements for the TOE	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
FCS_CKM.2.1	Yes	FCS_CKM.2.1(2)	Included in this Security Target
FCS_CKM.4.1	Yes	FCS_CKM.4.1(2)	Included in this Security Target
FCS_COP.1.1/RSA	Yes	FCS_COP.1.1(5:RSA)	Included in this Security Target
FCS_COP.1.1/TDES	Yes	FCS_COP.1.1(4:TDES)	Included in this Security Target
FDP_ACC.2.1	Yes	Yes	Included in this Security Target
FDP_ACC.2.2	Yes	Yes	Included in this Security Target
FDP_ACF.1.1	Yes	Yes	Partially identical – Will be split between TachoGen1 profile and TachoGen2 profile
FDP_ACF.1.2	Yes	Yes	Partially identical – Will be split between TachoGen1 profile and TachoGen2 profile
FDP_ACF.1.3	Yes	Yes	Included in this Security Target
FDP_ACF.1.4	Yes	Yes	Included in this Security Target
FDP_DAU.1.1	Yes	Yes	Included in this Security Target
FDP_DAU.1.2	Yes	Yes	Included in this Security Target
FDP_ETC.1.1	Yes	Yes	Included in this Security Target
FDP_ETC.1.2	Yes	Yes	Included in this Security Target
FDP_ETC.2.1	Yes	Yes	Included in this Security Target

Security functional requirements for the TOE	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
FDP_ETC.2.2	Yes	Yes	Included in this Security Target
FDP_ETC.2.3	Yes	Yes	Included in this Security Target
FDP_ETC.2.4	Yes	Yes	Included in this Security Target
FDP_ITC.1.1	Yes	Yes	Included in this Security Target
FDP_ITC.1.2	Yes	Yes	Included in this Security Target
FDP_ITC.1.3	Yes	Yes	Included in this Security Target
FDP_RIP.1.1	Yes	Yes	Included in this Security Target
FDP_SDI.2.1	Yes	Yes	Included in this Security Target
FDP_SDI.2.2	Yes	Yes	Included in this Security Target
FIA_AFL.1.1/C	Yes	FIA_AFL.1.1(1:C)	Included in this Security Target
FIA_AFL.1.2/C	Yes	FIA_AFL.1.2(1:C)	Included in this Security Target
FIA_AFL.1.1/WSC	Yes	FIA_AFL.1.1(2:WC)	Included in this Security Target
FIA_AFL.1.2/WSC	Yes	FIA_AFL.1.2(2:WC)	Included in this Security Target
FIA_ATD.1.1	Yes	Yes	Included in this Security Target
FIA_UAU.1.1	Yes	FIA_UAU.1.1(2)	Included in this Security Target
FIA_UAU.1.2	Yes	FIA_UAU.1.2(2)	Included in this Security Target

Security functional requirements for the TOE	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
FIA_UAU.3.1	Yes	Yes	Included in this Security Target
FIA_UAU.3.2	Yes	Yes	Included in this Security Target
FIA_UAU.4.1	Yes	Yes	Included in this Security Target
FIA_UID.1.1	Yes	No	Covered by FIA_UID.2
FIA_UID.1.2	Yes	No	Covered by FIA_UID.2
FIA_USB.1.1	Yes	Yes	Included in this Security Target
FIA_USB.1.2	Yes	Yes	Included in this Security Target
FIA_USB.1.3	Yes	Yes	Included in this Security Target
FPR_UNO.1.1	Yes	Yes	Included in this Security Target
FPT_EMS.1.1	Yes	Yes	Included in this Security Target
FPT_EMS.1.2	Yes	Yes	Included in this Security Target
FPT_FLS.1.1	Yes	Yes	Included in this Security Target
FPT_PHP.3.1	Yes	Yes	Included in this Security Target
FPT_TDC.1.1	Yes	Yes	identical since only VU can authenticate
FPT_TDC.1.2	Yes	Yes	identical since only VU can authenticate
FPT_TST.1.1	Yes	Yes	Included in this Security Target
FPT_TST.1.2	Yes	Yes	Included in this Security Target

Security functional requirements for the TOE	Included in [PP-TACHOCARD1]	Included in [PP-TACHOCARD2]	Comments
FPT_TST.1.3	Yes	Yes	Included in this Security Target
FTP_ITC.1.1	Yes	Yes	identical since only VU can authenticate
FTP_ITC.1.2	Yes	Yes	Included in this Security Target
FTP_ITC.1.3	Yes	Yes	identical since only VU can authenticate

Table 9 Security functional requirements for the TOE

- Most of Security functional requirements for the TOE from [PP-TACHOCARD1] are included in [PP-TACHOCARD2] . Others are either covered by [PP-TACHOCARD2] or differences will be clearly highlighted in dedicated chapter.

3 SECURITY PROBLEM DEFINITION

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

3.1 ASSETS

3.1.1 ASSETS FOR THE TOE FROM PROTECTION PROFILES

Asset	Definition
Identification data (IDD)	Card identification data, user identification data (see Glossary for more details).
Activity data (ACD)	Activity data (see Glossary for more details).

Table 10 Assets

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

Asset	Definition
Verification authentication data (VAD)	Authentication data provided as input for authentication attempt as authorised user (i.e. entered PIN on workshop cards).
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).
Data to be signed (DTBS)	The complete electronic data to be signed (including both user message and signature attributes).
TOE file system, including specific identification data	File structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalisation

Table 11 – Secondary assets to be protected by the TOE and its environment

3.1.2 SUPPLEMENTARY ASSETS

The following assets are related to patch management in post-issuance phase (phase 7). As mentioned in section 1.8.5, there is no patch associated to the present TOE, however the patch mechanisms are within the evaluation scope.

Asset	Definition
D.OS-UPDATE_DEC-KEY	Refinement of D.APP_KEYS. It is a Thales DIS cryptographic key (K_{ENC}), owned by the OS Developer, and used by the TOE to decrypt the additional code to be loaded. Note: no assumption is made on the type of this decryption key, i.e. it can be either a symmetric key or the secret component of an asymmetric key pair. To be protected from unauthorized disclosure and modification.
D.OS-UPDATE_SGNVER-KEY	Thales DIS keys used for the signature It is a Thales DIS cryptographic key (K_{MAC}), owned by the OS Developer, and used by the TOE to verify the signature of the additional code to be loaded. Note: no assumption is made on the type of this signature verification key, i.e. it can be either a symmetric key or the public component of an asymmetric key pair. Case of a symmetric key: to be protected from unauthorized disclosure and modification. Case of an asymmetric public key: to be protected from unauthorized modification.

Asset	Definition
D.OS-UPDATE_ADDITIONALCODE	Code to be added to the OS after TOE issuance. The additional code has to be signed by the OS Developer. After successful verification of the signature by the Initial TOE, the additional code is loaded and installed/activated through an atomic activation (to create an Updated TOE). To be protected from unauthorized disclosure and modification.
D.OS-UPDATE-CODE-ID	Identification data associated to the additional code. It is loaded and/or updated in the same atomic operation as additional code loading. To be protected from unauthorized modification. Application Note: The identification data (D.OS-UPDATE-CODE-ID) may be also protected from unauthorized disclosure (confidentiality requirement) to not permitting an attacker to determine if a given TOE has been updated or not (even if it is not possible to distinguish between functional and security updates). However, confidentiality is not mandatory since in most cases the identification data must be readily available on the field through technical commands, even in the TERMINATED state.

3.2 SUBJECTS AND EXTERNAL ENTITIES

Role	Definition
Administrator	Usually active only during Initialisation/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 PP, especially to change properties of the maintained assets. For example, a driver could be an attacker if he misuses the driver card. An attacker is assumed to possess at most a *high* attack potential.

Table 12 - Subjects and external entities

3.3 THREATS

3.3.1 THREAT FOR THE TOE FROM [PP-TACHOCARD1]

Label	Threat
T.Personalisation_Data	**DataDisclosure or Modification of Personalisation Data** - A successful modification of personalisation data (such as TOE file system, cryptographic keys, RAD) to be stored in the TOE or disclosure of cryptographic material during the personalisation would be a threat to the security of the TOE. The threat addresses the execution of the TOE's personalisation process and its security. The threat agent for T.Personalisation_Data is Attacker.

3.3.2 OTHER HREATS FOR THE TOE FROM PROTECTION PROFILES

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

Table 13 - Threats addressed by the TOE

3.3.3 SUPPLEMENTARY THREATS

The following threats are related to patch loading in post-issuance.

Label	Threat

T.UNAUTHORIZED_TOE_CODE_UPDATE	An attacker attempts to update the TOE code with a malicious update that may compromise the security features of the TOE. Targeted asset(s): D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA .
T.FAKE-SGNVER-KEY	An attacker modifies the signature verification key used by the TOE to verify the signature of the additional code. Hence, he is able to sign and successfully load malicious additional code inside the TOE. Targeted assets: D.OS-UPDATE_SGNVER-KEY, D.OS-UPDATE_ADDITIONALCODE.
T.WRONG-UPDATE-STATE	An attacker prevents the OS Update operation to be performed atomically, resulting in an inconsistency between the resulting TOE code and the identification data: • The additional code is not loaded within the TOE, but the identification data is updated to mention that the additional code is present; • The additional code is loaded within the TOE, but the identification data is not updated to indicate the change. Targeted asset: D.OS-UPDATE-CODE-ID.
T.INTEG-OS-UPDATE_LOAD	The attacker modifies (part of) the additional code when it is transmitted to the TOE for installation. Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.
T.CONFID-OS-UPDATE_LOAD	The attacker discloses (part of) the additional code when it is transmitted to the TOE for installation. Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.

3.4 ASSUMPTIONS

3.4.1 ASSUMPTIONS FOR THE TOE FROM PROTECTION PROFILES

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

Table 14 – Assumptions

3.4.2 Supplementary assumptions

Assumptions related to patch loading.

Label	Assumption
A.OS-UPDATE-EVIDENCE	For additional code loaded pre-issuance, it is assumed that: • Evaluated technical and/or audited organizational measures have been implemented to ensure that the additional code: (1) has been issued by the genuine OS Developer (2) has not been altered since it was issued by the genuine OS Developer. For additional code loaded post-issuance, it is assumed that the OS Developer provides digital evidence to the TOE in order to prove the following: (1) he is the genuine developer of the additional code and (2) the additional code has not been modified since it was issued by the genuine OS Developer.
A.SECURE_ACODE_MANAGEMENT	It is assumed that: • The Key management process related to the OS Update capability takes place in a secure and audited environment. • The cryptographic keys used by the cryptographic operations are of strong quality and appropriately secured to ensure confidentiality, authenticity and integrity of those keys.

3.5 ORGANIZATIONAL SECURITY POLICIES

3.5.1 Organizational security policies for the TOE from protection profiles

3.5.1.1 For Tacho Gen1

Label	Organisational Security Policy
P.EU_Specifications	All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents [6]. To ensure the interoperability between the components all Tachograph Card and Vehicle Unit requirements concerning handling, construction and functionality inclusive the specified cryptographic algorithms and key length have to be fulfilled.

Table 15 – Organisational Security Policy for Tachogen1

3.5.1.2 For Tacho Gen2

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

Table 16 – Organisational Security Policy for Tachogen2

3.5.2 SUPPLEMENTARY OSP

OSP related to patch loading.

Label	Organisational Security Policy
OSP.ATOMIC_ACTIVATION	Additional code has to be loaded and installed on the Initial TOE through an atomic activation to create the Updated TOE. Each additional code shall be identified with unique Identification Data. During such atomic activation, identification Data of the Initial TOE have to be updated to clearly identify the Updated TOE. In case of interruption or incident during activation, the TOE shall remain in its initial state or fail secure.
OSP.TOE_IDENTIFICATION	Identification Data of the resulting Updated TOE shall identify the Initial TOE and the activated additional code. Identification Data shall be protected in integrity.
OSP.ADDITIONAL_CODE_SIGNING	The additional code has to be signed with a cryptographic key according to relevant standard and

	the generated signature is associated to the additional code. The additional code signature must be checked during loading to assure its authenticity and integrity and to assure that loading is authorized on the TOE. The cryptographic key used to sign the additional code shall be of sufficient quality and its generation shall be appropriately secured to ensure the authenticity, integrity and confidentiality of the key.
OSP.ADDITIONAL_CODE_ENCRYPTION	The additional code has to be encrypted according to relevant standard in order to ensure its confidentiality when it is transmitted to the TOE for loading and installation. The encryption key shall be of sufficient quality and its generation shall be appropriately secured to ensure the confidentiality, authenticity and integrity of the key.

4 SECURITY OBJECTIVES

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

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

- Integrity and confidentiality of assets,
- Protection of the TOE and associated documentation and environment during development and production phases.

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 SECURITY OBJECTIVES FOR THE TOE FROM PROTECTION PROFILES

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.

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

Table 17 – Security objectives for the TOE

4.1.2 SUPPLEMENTARY SECURITY OBJECTIVES

Related to patch loading.

Label	Security objective for the TOE
O.SECURE_LOAD_ACODE	Security Target of a TOE embedding a Loader shall include the following Security Objectives. The TOE shall check an evidence of authenticity and integrity of the additional code to be loaded. The TOE enforces that only an allowed version of the additional code can be loaded. The TOE shall forbid the loading of an additional code not intended to be assembled with the TOE. During the loading of the additional code, the TOE shall remain secure.
O.SECURE_AC_ACTIVATION	Activation of the additional code and update of the Identification Data shall be performed at the same time in an atomic way. All the operations needed for the code to be able to operate as in the Updated TOE shall be completed before activation. If the atomic activation is successful, then the resulting product is the Updated TOE, otherwise (in case of interruption or incident which prevents the forming of the Updated TOE), the TOE shall preserve a secure state.
O.TOE_IDENTIFICATION	The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.

Label	Security objective for the TOE
	After atomic activation of the additional code, the Identification Data of the Updated TOE allows identifications of both the Initial TOE and additional code. The user must be able to uniquely identify Initial TOE and additional code(s) which are embedded in the Updated TOE.
O.CONFID-OS-UPDATE.LOAD	The TOE shall decrypt the additional code prior installation.

Table 18 – Supplementary security objectives for the TOE

Application Note: Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION). Confidentiality protection can be achieved either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

4.2.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT FOR THE TOE FROM PROTECTION PROFILES

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

Table 19 – Security objectives for the environment

4.2.2 SUPPLEMENTARY SECURITY OBJECTIVES FOR THE ENVIRONMENT

Related to patch loading.

Label	Security objective for the environment
OE.OS-UPDATE-EVIDENCE	For additional code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that the additional code (1) has been issued by the genuine OS Developer (2) has not been altered since it was issued by the genuine OS Developer. For additional code loaded post-issuance, the OS Developer shall provide digital evidence to the TOE that (1) he is the genuine developer of the additional code and (2) the additional code has not been modified since it was issued by the genuine OS Developer.
OE.OS-UPDATE-ENCRYPTION	For additional code loaded post-issuance, the OS Developer shall encrypt the additional code so that its confidentiality is ensured when it is transmitted to the TOE for loading and installation.

Label	Security objective for the environment
OE.SECURE_ACODE_MANAGEMENT	Key management processes related to the OS Update capability shall take place in a secure and audited environment. The key generation processes shall guarantee that cryptographic keys are of sufficient quality and appropriately secured to ensure confidentiality, authenticity and integrity of the keys.

Table 20 – Supplementary security objectives for the environment

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 RATIONALE BETWEEN OBJECTIVES AND THREATS, ASSUMPTIONS, OSP

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

	Security objectives of the TOE	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update	Objectives for operational environment	OE.Personalisation_Phase	OE.Crypto_Admin	OE.EOL
Threats												
T.Personalisation_Data*										X		
T.Identification_Data		X					X				X	
T.Activity_Data			X		X		X				X	
T.Application				X			X	X				X
T.Data_Exchange				X		X	X				X	

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

Table 21 – Security Objective for Tachograph G2V2 Application Rationale

*** only for TachoGen1 profile**

T.Personalisation_Data is addressed by the security objective of the operational environment OE.Personalisation_Phase which requires correct and secure handling of the personalisation data regarding integrity and confidentiality. It prevents the modification and disclosure of the personalisation data as well as the disclosure of cryptographic material during the execution of the personalisation process.

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

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

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

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

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

The OSP **P.EU_Specifications** is covered by all objectives of the TOE and the objective for the environment OE.Tachograph_Components. The security objectives of the TOE OT.Card_Identification_Data, OT.Card_Activity_Storage, OT.Data_Access and OT.Secure_Communications require that the corresponding measures are implemented by the Tachograph Cards as specified by the EU documents. The objective for the environment OE.Tachograph_Components requires this for the Vehicle Unit.

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

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

The following table provides an overview for security objectives coverage for OS Update feature.

	O.SECURE_LOAD_ACODE	O.SECURE_ACTIVATION_ACODE	O.TOE_IDENTIFICATION	O.CONFID-OS-UPDATE.LOAD	OE.OS-UPDATE-EVIDENCE	OE.OS-UPDATE-ENCRYPTION	OE.SECURE_ACODE_MANAGEMENT
T.UNAUTHORIZED_TOE_CODE_UPDATE	X						
T.FAKE-SGNVER-KEY	X						
T.WRONG-UPDATE-STATE		X	X				
T.INTEG-OS-UPDATE_LOAD	X						
T.CONFID-OS-UPDATE_LOAD				X			
OSP.ATOMIC_ACTIVATION		X					
OSP.TOE_IDENTIFICATION			X				
OSP.ADDITIONAL_CODE_SIGNING	X						
OSP.ADDITIONAL_CODE_ENCRYPTION				X		X	
A.OS-UPDATE-EVIDENCE					X		
A.SECURE_ACODE_MANAGEMENT							X

Table 22 – Security Objective for OS update Rationale

T.UNAUTHORIZED_TOE_CODE_UPDATE This threat is covered by the O.SECURE_LOAD_ACODE security objective that ensures the authenticity and the integrity of the additional code. It ensure also that that only the allowed code will be load in a secure process.

T.FAKE-SGNVER-KEY This threat is covered by the O.SECURE_LOAD_ACODE security objective which ensures the authenticity and the integrity of the additional code to avoid loading malicious additional code.

T.WRONG-UPDATE-STATE This threat is covered by the O.SECURE_AC_ACTIVATION and O.TOE_IDENTIFICATION security objective that ensures that the update state stay secure during all the loading process

T.INTEG-OS-UPDATE_LOAD This threat is covered by the O.SECURE_LOAD_ACODE security objective that ensures the authenticity and the integrity of the additional code.

T.CONFID-OS-UPDATE_LOAD This threat is covered by the O.CONFID-OS-UPDATE.LOAD security objective that ensures the confidentiality of the additional code when transmitted until installation.

OSP.ADDITIONAL_CODE_ENCRYPTION is enforced by the TOE security objective of the environment OE.OS-UPDATE-ENCRYPTION which ensure the confidentiality of the additional code and by O.CONFID-OS-UPDATE.LOAD which performs the decryption of the additional code prior installation.

OSP.ADDITIONAL_CODE_SIGNING is enforced by the TOE security objective O.SECURE_LOAD_ACODE which ensure the integrity of the additional code

OSP.ATOMIC_ACTIVATION is enforced by the TOE security objective O.SECURE_AC_ACTIVATION which ensure the atomicity of the activation of the additional code

OSP.TOE_IDENTIFICATION is enforced by the TOE security objective O.TOE_IDENTIFICATION which ensure the identification of the additional code

A.OS-UPDATE-EVIDENCE This assumption is upheld by the security objective on the operational environment OE.OS-UPDATE-EVIDENCE that guarantees that the additional code has been issued by the genuine OS Developer, has not been altered since it was issued by the genuine OS Developer.

A.SECURE_ACODE_MANAGEMENT This assumption is upheld by the security objective on the operational environment OE.SECURE_ACODE_MANAGEMENT that guarantees that cryptographic keys are of sufficient quality and appropriately secured to ensure confidentiality, authenticity and integrity of the keys.

4.3.2 COMPATIBILITY BETWEEN OBJECTIVES OF [ST-TACHOCARD] AND [ST-IC]

4.3.2.1 Compatibility between objectives for the TOE

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

Label of the chip TOE security objective	Title of the chip TOE security objective	Linked Composite-product TOE security objectives
O.Phys-Manipulation	Protection against Physical Manipulation	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Phys-Probing	Protection against Physical Probing	O.Card_Activity_Data O.Card_Identification_Data O.Data_Protect_Secret
O.Malfunction	Protection against Malfunction	OTCard_Activity_Data O.Protect_Secret

Label of the chip TOE security objective	Title of the chip TOE security objective	Linked Composite-product TOE security objectives
O.Leak-Inherent	Protection against Inherent Information Leakage	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Leak-Forced	Protection against Forced Information Leakage	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Abuse-Func	Protection against Abuse of Functionality	O.Card_Activity_Data O.Card_Identification_Data O.Protect_Secret
O.Identification	TOE Identification	No direct link to the composite-product TOE objectives, however chip traceability information stored in NVM is used by the TOE to answer identification CC assurance requirements.
O.RND	Random Numbers	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0
O.TDES	Cryptographic service Triple-DES	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0
O.AES	Cryptographic service AES	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0
O.Mem-Access	Area based Memory Access Control	O.Data_Access
O.Prot_TSF_Confidentiality	Protection of confidentiality of TSF	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0
O.RSA	Cryptographic service RSA	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0
O.ECC	Cryptographic service ECC	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0

Label of the chip TOE security objective	Title of the chip TOE security objective	Linked Composite-product TOE security objectives
O.AES-TDES-MAC	Cryptographic service AES-Triple-DES-MAC	No direct link to the composite-product TOE objectives;This objective is ensure by the platform MultiApp 5.0

Table 23 – Compatibility between objectives for the TOE

O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION and O.CONFID-OS-UPDATE.LOAD are objectives added to this platform it does no conflict with the objectives of [ST-IC].

We can therefore conclude that the objectives for the TOE and the objectives for [ST-IC] are consistent.

4.3.2.2 Compatibility between objectives for the environment

Label of the chip TOE security objective	Title of the chip TOE security objective	Linked Composite-product TOE security objectives
OE.Resp-Appl	Treatment of User Data	Covered by TOE Security Objectives: O.Card_Activity_Data ,O.Card_Identification_Data , O.Protect_Secret, O.Secure_Communications,
OE.Process-Sec-IC	Protection during composite product manufacturing	Fulfilled by ALC.DVS.2 and ALC_DEL.1 during phases 4 and 5. After phase 5, covered by O.Protect_Secret, O.Secure_Communications, OE.Personalisation_Phase and O.EOL
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	Fulfilled through the transport key verification at the beginning of phases 4 and 5, as stated in ALC_DEL.1

Table 24 – Compatibility between objectives for the environment for the TOE

OE.SECURE_ACODE_MANAGEMENT is partially covered by OE.Resp-Appl.

OE.OS-UPDATE-EVIDENCE, OE.OS-UPDATE-ENCRYPTION are specific to [ST_TACHOCARD] and they do no conflict with the objectives of [ST-IC].

We can therefore conclude that the objectives for the environment for the TOE and the objectives for the environment for [ST-IC] are consistent.

5 EXTENDED COMPONENTS DEFINITION

Family FPT_EMS (TOE Emanation) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation.

Family FCS_RNG (Random number generation) is defined and justified in [7] Section 3.

5.1 FCS_RNG (GENERATION OF RANDOM NUMBERS)

Rationale

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

Family behaviour

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

Component levelling:

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

Management

There are no management activities foreseen.

Audit

There are no auditable activities foreseen

FCS_RNG.1 Generation of random numbers

Hierarchical to: -

Dependencies: -

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

5.2 FPT_EMS (TOE EMANATION)

Rationale

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

Family behaviour

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

Component levelling:

FPT_EMS TOE emanation	1

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

Management

There are no management activities foreseen.

Audit

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_EMS.1.1	The TOE shall not emit [assignment*: types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment*: list of types of user data*].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 SECURITY REQUIREMENTS

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

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP-TACHOCARD1] and [PP-TACHOCARD2] .

6.1.1 SECURITY FUNCTION POLICY

The Security Function Policy Access Control (AC_SFP) for Tachograph Cards in the end-usage phase based on:

- the Tachograph Cards Specification [6] Annex 1B, Appendix 2 sec. 3 and 4 for Tacho Gen1 profile
- the Tachograph Cards Specification [5] Annex 1C, Appendix 2 Chapter 3 and 4 for Tacho Gen2 profile

is defined as follows:

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

The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access a certain object.

Following Access Conditions are defined in the Tachograph Card specification [6], sec. 3.3 for Tacho Gen1 profile:

- NEV (Never) - The command can never be executed.
- ALW (Always) - The command can be executed without restrictions.
- AUT (Key based authentication) - The command can be executed only if the preceding external authentication (done by the command External Authenticate) has been conducted successfully.
- PRO SM (Secure Messaging providing data integrity and authenticity for command resp. response) - The command can be executed and the corresponding response can be accepted only if the command/response is secured with a cryptographic checksum using Secure Messaging as defined in the Tachograph Card Specification [6], sec. 3.
- AUT and PRO SM (combined, see description above)

Following Access Conditions are defined in the Tachograph Card specification [5], sec. 3.3 for Tacho Gen2 profile:

- ALW - The action is always possible and can be executed without any restriction. Command and response APDU are sent in plain text, i.e. without secure messaging.
- NEV - The action is never possible.
- PLAIN-C - The command APDU is sent in plain, i.e. without secure messaging.

- PWD - The action may only be executed if the workshop card PIN has been successfully verified, i.e. if the card internal security status 'PIN_Verified' is set. The command must be sent without secure messaging.
- EXT-AUT-G1- The action may only be executed if the External Authenticate command for the generation 1 authentication has been successfully performed.
- SM-MAC-G1 - The APDU (command and response) must be applied with generation 1 secure messaging in authentication-only mode.
- SM-C-MAC-G1 - The command APDU must be applied with generation 1 secure messaging in authentication only mode.
- SM-R-ENC-G1 - The response APDU must be applied with generation 1 secure messaging in encryption mode, i.e. no message authentication code is returned.
- SM-R-ENC-MAC-G1 - The response APDU must be applied with generation 1 secure messaging in encrypt-then-authenticate mode.
- SM-MAC-G2 - The APDU (command and response) must be applied with generation 2 secure messaging in authentication-only mode.
- SM-C-MAC-G2 - The command APDU must be applied with generation 2 secure messaging in authentication only mode.
- SM-R-ENC-MAC-G2 - The response APDU must be applied with generation 2 secure messaging in encrypt-then-authenticate mode.

For each type of Tachograph Card the Access Rules (which make use of the Access Conditions described above) for the different objects are implemented according to the requirements in [6], sec. 4 for TachoGen1 profile and in [5] sec. 4 for Tacho Gen2 profile. These access rules cover in particular the rules for the export and import of data.

For the Tachograph Card type Workshop Card an additional AC is necessary. A mutual authentication process between the card and the external world is only possible if a successful preceding verification process with the PIN of the card has been taken place.

6.1.1 SECURITY FUNCTIONAL REQUIREMENTS FROM PROTECTION PROFILES

6.1.1.1 Security functional requirements for Security functional requirements for the Smart Tachograph

6.1.1.1.1 Class FAU Security Audit

6.1.1.1.1.1 FAU_ARP.1 Security alarms

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

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

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

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

Application integrity error : SW1 SW2:6FCD

Store data integrity error : SW1 SW2:6400

upon detection of a potential security violation.

6.1.1.1.1.2 FAU_SAA.1 Potential violation analysis

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

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

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

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

known to indicate a potential security violation;

b) [assignment: **No other rules**[1]].

6.1.1.1.2 Class FCO Communication

6.1.1.1.2.1 FCO_NRO.1 Selective proof of origin

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

[1] [assignment: any other rules]

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

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

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

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

6.1.1.1.3 Class FDP User data protection

6.1.1.1.3.1 FDP_ACC.2 Complete access control

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

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

Objects

- User data
  - User Identification data
  - Activity data
- Security data
  - Cryptographic keys
  - PIN (for Workshop card)
- TOE application code
- TOE file system
- Card identification data
- Master file contents]

and all operations among subjects and objects covered by the SFP.

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

6.1.1.1.3.2 FDP_ACF.1 Security attribute based access control (1:TachoGen1)

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

FDP_ACF.1.1(1:TachoGen1) The TSF shall enforce the [AC SFP] to objects based on the following: [Subjects:
- S.VU (in the sense of the Tachograph Card specification)
- S.Non-VU (other card interface devices)

Objects

- User data
  - User identification data
  - Activity data
- Security data
  - cards´s private signature key
  - public keys
  - session keys
  - PIN (for workshop card)
- TOE software code
- TOE file system
- identification data of the TOE
- identification data of the TOE`s personalisation
- security attributes for subjects:
  - USER_GROUP
  - USER_ID
- security attributes for objects:
  - Access Rules

FDP_ACF.1.2(1:TachoGen1) 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 cardholder identification data which may be read by S.VU only;

IDENTIF_WRITE
- all card types: identification data may only be written once and before the end of Personalisation; no user may write or modify identification data during end-usage phase of card's life-cycle;

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

SOFT_UPGRADE
- all card types: no user may upgrade TOE's software;

FILE_STRUCTURE
- All card types: files structure and access conditions shall be created before the Personalisation is completed and then locked from any future modification or deletion by any user

- IDENTIF_TOE_READ:
- all card types: identification data of the TOE and identification data of the TOE's personalisation may be read from the TOE by any user;

- IDENTIF_TOE_WRITE:
- all card types: identification data of the TOE may only be written once and before the Personalisation; no user may write or modify these identification data during the Personalisation;

- IDENTIF_TOE_PERS_WRITE:

- all card types: identification data of the TOE's personalisation may only be written once and within the Personalisation ; no user may write or modify these identification data during end-usage phase of card's life-cycle.

FDP_ACF.1.3(1:TachoGen1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4(1:TachoGen1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

6.1.1.1.3.3 FDP_ACF.1 Security attribute based access control (2:TachoGen2)

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

FDP_ACF.1.1(2:TachoGen2) The TSF shall enforce the AC_SFP to objects based on the following:
subjects:
- S.VU (in the sense of [5] Annex 1C)
- S.Non-VU (other card interface devices)

objects:

- user data:
  - identification data
  - activity data

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

FDP_ACF.1.2(2:TachoGen2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

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

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

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

SOFT_UPGRADE

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

FILE_STRUCTURE

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

FDP_ACF.1.3(2:TachoGen2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4(2:TachoGen2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [
SECRET KEYS

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

6.1.1.1.3.4 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.

6.1.1.1.3.5 FDP_ETC.1 Export of user data without security attributes

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

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

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

6.1.1.1.3.6 FDP_ETC.2 Export of user data with security attributes

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

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

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

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

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

6.1.1.1.3.7 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].

6.1.1.1.3.8 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.2.4The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

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

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

Note: The application is loaded during initialization/pre-perso step.
Tacho Gen1 profile will be delivered with no possibility to update the application software.
Tacho Gen2 profile will be delivered with possibility to update the application software. Therefore security attributes signature verification status and decryption status should be verified.

6.1.1.1.3.9 FDP_RIP.1 Subset residual information protection

Hierarchical to: -

Dependencies: -

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

6.1.1.1.3.10 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: -
Dependencies: -

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

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

6.1.1.1.4 Class FIA Identification and authentication

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

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

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

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

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

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

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

FIA_AFL.1.2(2:WC) When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [
a) warn the entity connected,
b) block the PIN check procedure such that any subsequent PIN check attempt will fail,
c) be able to indicate to subsequent users the reason for the blocking].

6.1.1.1.4.3 FIA_ATD.1 User attribute definition

Hierarchical to: -
Dependencies: -

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

6.1.1.1.4.4 FIA_UAU.3 Unforgeable authentication

Hierarchical to: -
Dependencies: -

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

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

6.1.1.1.4.5 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: -
Dependencies: -

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

6.1.1.1.4.6 FIA_UID.2 User authentication before any action

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

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

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

6.1.1.1.4.7 FIA_USB.1 User-subject binding

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

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [
a) User_group (Vehicle_Unit for S.VU, Non_Vehicle_Unit for S.Non-VU);
b) User_ID (VRN and registering member state for subject S.VU)].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of the user security attributes with subjects acting on the behalf of users: [assignment: **none**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: **none**].

6.1.1.1.5 Class FPR Privacy

6.1.1.1.5.1 FPR_UNO.1 Unobservability

Hierarchical to: -
Dependencies: -

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

6.1.1.1.6 Class FPT Protection of the TSF

6.1.1.1.6.1 FPT_EMS.1 TOE emanation

Hierarchical to: -
Dependencies: -

FPT_EMS.1.1 The TOE shall not emit [assignment: **Side channel current**] in excess of [assignment: **State of the art limits**] enabling access to [private keys and session keys] and [assignment: security and **activity data**].

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

6.1.1.1.6.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -
Dependencies: -

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

6.1.1.1.6.3 FPT_PHP.3 Resistance to physical attack

Hierarchical to: -
Dependencies: -

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

6.1.1.1.6.4 FPT_TST.1 TSF testing

Hierarchical to: -
Dependencies: -

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

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

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

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

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

6.1.1.2.1 Class FCS Cryptographic support

6.1.1.2.1.1 FCS_CKM.1 Cryptographic key generation (1)

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1(1)	The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [5] Annex 1C, Appendix 11, Section 10 (for VU authentication and for the secure messaging session key)] and specified cryptographic key sizes [key sizes required by [5] Annex 1C, Appendix 11, Part B] that meet the following: [Reference [6] predefined RNG class [selection: *PTG.2, PTG.3, DRG.2, DRG.3, DRG.4, NTG.1*], [5] Annex 1C, Appendix 11, Section 10].

6.1.1.2.1.2 FCS_CKM.2 Cryptographic key distribution (1)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1(1)	The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [secure messaging AES session key agreement as specified in [5] Annex 1C, Appendix 11, Part B] that meets the following [5] Annex 1C, Appendix 11, Part B].

6.1.1.2.1.3 FCS_CKM.4 Cryptographic key destruction (1)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1(1)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: **physical irreversible destruction of the stored key value**] that meets the following [- Requirements defined in [PP-TACHOCARD2] 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 - [assignment: **no standard**]].

6.1.1.2.1.4 FCS_COP.1 Cryptographic operation (1: AES)

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1:AES) The TSF shall perform [the following:
a) ensuring authenticity and integrity of data exchanged between a vehicle unit and a tachograph card;
b) where applicable, ensuring confidentiality of data exchanged between a vehicle unit and a tachograph card;
c) decrypting confidential data sent by a vehicle unit to a remote early detection communication reader over a DSRC connection, and verifying the authenticity of that data;]

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

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

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

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

6.1.1.2.1.6 FCS_COP.1 Cryptographic operation (3: ECC)

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

FCS_COP.1.1(3:ECC) The TSF shall perform [the following cryptographic operations:
a) digital signature generation;
b) digital signature verification;
c) cryptographic key agreement;
d) mutual authentication between a vehicle unit and a tachograph card;
e) ensuring authenticity, integrity and non-repudation of data downloaded from a tachograph card]

in accordance with a specified cryptographic algorithm [[5] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [5], Appendix 11, Part B] that meet the following: [[5] Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR- 03111 – Elliptic Curve Cryptography – version 2, and the standardized domain parameters in Table 25:

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 25 Standardised domain parameters

6.1.1.2.1.7 FCS_RNG.1 Random number generation

Hierarchical to: -
Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: ***hybrid deterministic***] random number generator that implements: [assignment:
- (DRG.4.1) The internal state of the RNG shall [***use PTRNG of class PTG.2 as random source***].
- (DRG.4.2) The RNG provides forward secrecy.
- (DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.
- (DRG.4.4) The RNG provides enhanced forward secrecy [***after [calling the re-seed function that acts as a refreshing done at each random generation]***].
- (DRG.4.5) The internal state of the RNG is seeded by an [***internal entropy source, PTRNG of class PTG.2***].

].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment:
- (DRG.4.6) The RNG generates output for which **[*2^35*]** strings of bit length 128 are mutually different with probability [***equal to (1 – 1/2^58)***].
- (DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [***None***].

].

6.1.1.2.2 Class FIA Identification and authentication

6.1.1.2.2.1 FIA_UAU.1 Timing of authentication (1)

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

FIA_UAU.1.1(1) The TSF shall allow [
a) Driver card, workshop card – export of user data with security attributes (card data download function) and export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2;

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

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

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

6.1.1.2.3 Class FPT Protection of the TSF

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

Hierarchical to: -
Dependencies: -

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

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

6.1.1.2.4 Class FTP Trusted path/channels

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

Hierarchical to: -
Dependencies: -

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

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

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

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

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

6.1.1.3.1 Class FCS Cryptographic support

6.1.1.3.1.1 FCS_CKM.1 Cryptographic key generation (2)

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

6.1.1.3.1.2 FCS_CKM.2 Cryptographic key distribution (2)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1(2)	The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [for triple DES session keys as specified in [5] Annex 1C, Appendix 11 Part A] that meets the following [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

6.1.1.3.1.3 FCS_CKM.4 Cryptographic key destruction (2)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1(2)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following [- Requirements defined in [PP-TACHOCARD1] Table 16 and Table 17 ; - Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means - [assignment: ***no standards***]].

6.1.1.3.1.4 FCS_COP.1 Cryptographic operation (4:TDES)

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

FCS_COP.1.1(4:TDES) The TSF shall perform [the cryptographic operations (encryption, decryption, Retail-MAC)] in accordance with a specified cryptographic algorithm [Triple DES] and cryptographic key sizes [112 bits] that meet the following: [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

6.1.1.3.1.5 FCS_COP.1 Cryptographic operation (5:RSA)

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

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

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

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

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

6.1.1.3.2 Class FIA Identification and authentication

6.1.1.3.2.1 FIA_UAU.1 Timing of authentication (2)

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

FIA_UAU.1.1(2) The TSF shall allow [
a) Driver card, workshop card – export of user data with security attributes (digital signature used in card data download function, see [5] Annex 1C, Appendix 11, Chapters 6 and 14)) and export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2;
b) Control card, company card – export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2]

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

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

6.1.1.3.3 Class FPT Protection of the TSF

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

Hierarchical to: -
Dependencies: -

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

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

6.1.1.3.4 Class FTP Trusted path/channels

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

Hierarchical to: -
Dependencies: -

FTP_ITC.1.1(2) The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **the vehicle unit** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(2) The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.

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

6.1.2 SECURITY FUNCTIONAL REQUIREMENTS FROM PLATFORM

6.1.2.1 Class FCS Cryptographic support

6.1.2.1.1 FCS_CKM.1 Cryptographic key generation (3:GP Session)

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(GP Session) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **GP session keys** and specified cryptographic key sizes **112 bits for SCP01 and SCP02 / 128,192,256 bits for SCP03** that meet the following **SCP01,SCP02,SCP03 cf [GP23]**

6.1.2.1.2 FCS_CKM.1 Cryptographic key generation (4:Card private key)

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 (Card private key) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation or ECC key generation** and specified cryptographic key sizes **1024 bits for RSA/ 160,192,224,256,320,384,512,521 bits for ECC** that meet the following **None**

6.1.2.1.3 FCS_CKM.2 Cryptographic key distribution (3: Public Key)

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(Public Key) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **"Generate Asymmetric key pair" command** that meets the following **None**

6.1.2.1.4 FCS_CKM.2 Cryptographic key distribution (4: Certificate)

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(Certificate) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **"Read Binary" command** that meets the following **None**

6.1.2.1.5 FCS_CKM.4 Cryptographic key destruction (3: GP Session)

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(GP Session) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: **[no standard]**.

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

6.1.2.1.6 FCS_COP.1 Cryptographic operation (7:HMAC)

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

6.1.2.1.7 FCS_COP.1 Cryptographic operation (8: GP MAC)

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

6.1.2.1.8 FCS_COP.1 Cryptographic operation (9: GP ENC)

FCS_COP.1.1(9: GP ENC) The TSF shall perform **[Encryption and decryption in GP session]** in accordance with a specified cryptographic algorithm **[TDES-ECB]** and cryptographic key sizes **[112 bits]** that meet the following**: [SP800-67] and [SP800-38 A]** .

6.1.2.2 Class FIA Identification and authentication

6.1.2.2.1 FIA_AFL.1 Authentication failure handling (3: Card interface GP)

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

FIA_AFL.1.1(3: Card interface GP) The TSF shall detect when **[*3*]** unsuccessful authentication attempts occur related to **[authentication of a card interface device in personalization]**.

FIA_AFL.1.2(3: Card interface GP) When the defined number of unsuccessful authentication attempts has been **met** , the TSF shall **:**

- **block GP authentication**

6.1.3 SECURITY FUNCTIONAL REQUIREMENTS FOR PATCH MANAGEMENT

6.1.3.1 Class FMT Security Management

6.1.3.1.1 FMT_SMR.1/OS-UPDATE Security roles

FMT_SMR.1.1/OS-UPDATE The TSF shall maintain the roles **OS Developer, OS Patch Loader, Issuer**.

FMT_SMR.1.2/OS-UPDATE The TSF shall be able to associate users with roles.

6.1.3.1.2 FMT_SMF.1/OS-UPDATE Specification of Management Functions

FMT_SMF.1.1/OS-UPDATE The TSF shall be capable of performing the following management functions: **activation of additional code.**

Application Note:

Once verified and installed, additional code is become immediately effective.

6.1.3.1.3 FMT_MSA.3/OS-UPDATE Security attribute initialisation

FMT_MSA.3.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/OS-UPDATE The TSF shall allow the **OS Developer** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

The additional code signature verification status must be set to “Fail” by default, therefore preventing any additional code from being installed until the additional code signature is actually successfully verified by the TOE.

6.1.3.2 Class FIA Identification and authentication

6.1.3.2.1 FIA_ATD.1/OS-UPDATE User attribute definition

FIA_ATD.1.1/OS-UPDATE The TSF shall maintain the following list of security attributes belonging to individual users: **additional code ID for each activated additional code**.

Refinement: "Individual users" stands for additional code.

6.1.3.3 Class FDP User data protection

6.1.3.3.1 FDP_ACC.1/OS-UPDATE Subset access control

FDP_ACC.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** on **the following list of subjects, objects and operations:**

- **Subjects: S.OS-Developer is the representative of the OS Developer within the TOE, who responsible for verifying the signature and decrypting the**

additional code before authorizing its loading, installation and activation, [None]

- **Objects: additional code and associated cryptographic signature**
- **Operations: loading, installation and activation of additional code**

6.1.3.3.2 FDP_ACF.1/OS-UPDATE Security attribute based access control

FDP_ACF.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to objects based on the following:

- **Security Attributes:**
  - **The additional code cryptographic signature verification status**
  - **The Identification Data verification status (between the Initial TOE and the additional code)**

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

- **The verification of the additional code cryptographic signature (using D.OS-UPDATE_SGNVER-KEY) by S.OS-Developer is successful.**
- **The decryption of the additional code prior installation (using D.OS-UPDATE_DEC-KEY) by S.OS-Developer is successful.**
- **The comparison between the identification data of both the Initial TOE and the additional code demonstrates that the OS Update operation can be performed.**
- **[None]**

FDP_ACF.1.3/OS-UPDATE The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[None]**.

FDP_ACF.1.4/OS-UPDATE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[None].**

Application Note:

Identification data verification is necessary to ensure that the received additional code is actually targeting the TOE and that its version is compatible with the TOE version.

Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION). Confidentiality protection can be achieved either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

6.1.3.4 Class FTP Trusted path/channels

6.1.3.4.1 FTP_TRP.1/OS-UPDATE Trusted Path

FTP_TRP.1.1/OS-UPDATE The TSF shall provide a communication path between itself and **remote** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[none]**.

FTP_TRP.1.2/OS-UPDATE The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/OS-UPDATE The TSF shall require the use of the trusted path for **the transfer of the additional code to the TOE.**

Application Note:

During the transmission of the additional code to the TOE for loading the confidentiality shall be ensured either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

In case that the additional code is encrypted independently of the trusted path the ST writer can select 'none' in FTP_TRP.1.1/OS-UPDATE.

Otherwise, the trusted path shall ensure the confidentiality of the transmitted additional code. In this case the ST writer shall select 'disclosure' in FTP_TRP.1.1/OS-UPDATE.

6.1.3.5 Class FCS Cryptographic support

6.1.3.5.1 FCS_COP.1/OS-UPDATE-DEC Cryptographic operation

FCS_COP.1.1/OS-UPDATE-DEC The TSF shall perform **Decryption of the additional code prior installation** in accordance with a specified cryptographic algorithm **[AES-CBC]** and cryptographic key sizes **[AES-256]** that meet the following: **[assignment:** AES-CBC ISO9797-M2 NIST SP800-38A**]**.

6.1.3.5.2 FCS_COP.1/OS-UPDATE-VER Cryptographic operation

FCS_COP.1.1/OS-UPDATE-VER The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm **[AES-CMAC]** and cryptographic key sizes **[AES-256]** that meet the following: **[assignment:** NIST SP800-38B**]**.

6.1.3.6 Class FPT Protection of the TSF

6.1.3.6.1 FPT_FLS.1/OS-UPDATE Failure with preservation of secure state

FPT_FLS.1.1/OS-UPDATE The TSF shall preserve a secure state when the following types of failures occur: **interruption or incident which prevents the forming of the Updated TOE**.

Application Note:

The OS Update operation must be either successful, or fail securely. The TOE code and identification data must be updated in an atomic way in order to always be consistent. In case of interruption or incident during the OS Update operation, the OS Developer may choose to implement any technical behavior, provided that the TOE remains in a secure state, for example by canceling the operation (the TOE remains the Initial TOE) or entering an error state, and consistency is maintained between the TOE code and the ID data.

6.2 SECURITY ASSURANCE REQUIREMENTS

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

The assurance level is EAL4 augmented on:

- ALC_DVS.2: Sufficiency of security measures.
- ATE_DPT.2: Testing: Security enforcing modules
- AVA_VAN.5: Advanced methodical vulnerability analysis

6.3 SECURITY REQUIREMENTS RATIONALE

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

6.3.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE FOR THE TOE FROM PROTECTION PROFILES

The following table shows, which SFRs for the TOE support which security objectives of the TOE. The table shows, that every objective is supported by at least one SFR and that every SFR supports at least one objective.

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FAU_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 (1:TachoGen1)	X	X	X	X	X		X
FDP_ACF.1	Security attribute based access control (2:TachoGen2)	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

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FDP_RIP.1	Subset residual information protection			X		X		
FDP_SDI.2	Stored data integrity monitoring and action	X	X				X	
FIA_AFL.1	Authentication failure handling (1:C)				X			
FIA_AFL.1	Authentication failure handling (2:WC)				X			
FIA_ATD.1	User attribute definition				X			
FIA_UAU.3	Unforgeable authentication				X	X	X	
FIA_UAU.4	Single-use authentication mechanism					X	X	
FIA_UID.2	User authentication before any action				X			
FIA_USB.1	User-subject binding				X			
FPR_UNO.1	Unobservability			X		X		
FPT_EMS.1	TOE emanation	X	X	X	X			
FPT_FLS.1	Failure with preservation of secure state	X	X		X			
FPT_PHP.3	Resistance to physical attack	X	X	X	X	X		X
FPT_TST.1	TSF testing	X	X		X			
FCS_CKM.1	Cryptographic key generation (1)					X	X	

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FCS_CKM.2	Cryptographic key distribution (1)					X	X	
FCS_CKM.4	Cryptographic key destruction (1)					X	X	
FCS_COP.1	Cryptographic operation (1:AES)					X	X	
FCS_COP.1	Cryptographic operation (2:SHA-2)					X	X	
FCS_COP.1	Cryptographic operation (3:ECC)					X	X	
FCS_RNG.1	Random number generation					X	X	
FIA_UAU.1	Timing of authentication (1)				X			
FPT_TDC.1	Inter-TSF basic TSF data consistency (1)					X		
FTP_ITC.1	Inter-TSF trusted channel (1)					X		
FCS_CKM.1	Cryptographic key generation (2)					X	X	
FCS_CKM.2	Cryptographic key distribution (2)					X	X	
FCS_CKM.4	Cryptographic key destruction (2)					X	X	
FCS_COP.1	Cryptographic operation (4:TDES)					X	X	
FCS_COP.1	Cryptographic operation (5:RSA)					X	X	

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FCS_COP.1	Cryptographic operation (6:SHA-1)					X	X	
FIA_UAU.1	Timing of authentication (2)				X			
FPT_TDC.1	Inter-TSF basic TSF data consistency (2)					X		
FTP_ITC.1	Inter-TSF trusted channel (2)					X		

Table 26 – Coverage of security objectives for the TOE by SFRs

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

Security Objective	SFR	Rationale
O.Card_Identification_Data	FAU_ARP.1 FAU_SAA.1	In the case of a detected integrity error the TOE will indicate the corresponding violation.
	FDP_ACC.2 FDP_ACF.1(all)	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.

Security Objective	SFR	Rationale
	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(all)	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(all)	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(all)	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.

Security Objective	SFR	Rationale
	FIA_AFL.1(1:C) FIA_AFL.1(1:WC)	These components require that if authentication fails the TOE reacts with a warning to the connected entity, and the user is assumed not to be an authorised vehicle unit.
	FIA_ATD.1 FIA_USB.1	The definition of user security attributes supplies a distinction between vehicle units and other card interface devices.
	FIA_UAU.1(1&2) FIA_UID.2	These requirements ensure that write access to user data is not possible without a preceding successful authentication process.
	FIA.UAU.3	Prevents the use of forged credentials during the authentication process.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the authentication process.
	FPT_FLS.1	Requires that any failure state should not allow unauthorised write access to the card.
	FPT_PHP.3	Requires the TOE to resist attempts to interfere with authentication through manipulation or physical probing.
	FPT_TST.1	Requires that tests be carried out to assure that the integrity of the TSF and identification data has not been compromised.
O.Secure_Communications	FAU_ARP.1 FAU_SAA.1	During data exchange, upon detection of an integrity error of the imported data, the TOE will indicate the corresponding violation and will provide a warning to the entity sending the data.
	FDP_ACC.2 FDP_ACF.1(all)	The necessity for the use of a secure communication protocol as well as the access to the relevant card´s keys are defined within these requirements.
	FDP_ETC.1 FDP_ITC.1 FTP_ITC.1(1&2)	These requirements provide for a secure data exchange (i.e. the data import and export) between the TOE and the card interface device by using a trusted channel. This includes assured identification of its end points and protection of the data transfer from modification and disclosure. By this means, both parties are capable of verifying the integrity and authenticity of received data. The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device.

Security Objective	SFR	Rationale
	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(1&2) FCS_CKM.2(1&2) FCS_CKM.4(1&2) FCS_COP.1(all) FCS_RNG.1	The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device with agreement of session keys. FCS_COP.1 also realizes the securing of the data exchange itself. Random numbers are generated in support of cryptographic key generation for authentication.
	FPT_TDC.1(1&2)	Requires a consistent interpretation of the security related data shared between the TOE and the card interface device.
O.Crypto_Implement	FDP_DAU.1 FDP_SDI.2	Approved cryptographic algorithms are required for digital signatures in support of data authentication.
	FIA_UAU.3 FIA_UAU.4	Approved cryptographic algorithms are required to prevent the forgery, copying or reuse of authentication data.
	FCS_CKM.1(1&2) FCS_CKM.2(1&2) FCS_CKM.4(1&2) FCS_RNG.1	Key generation, distribution and destruction must be done using approved methods. Random numbers are generated in support of cryptographic key generation for authentication.
	FCS_COP.1(all)	Approved cryptographic algorithms are required for all cryptographic operations.

Security Objective	SFR	Rationale
O.Software_Update	FDP_ACC.2 FDP_ACF.1(all)	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 27 – Suitability of the SFRs

6.3.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE FOR PLATFORM

		O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FCS_CKM.1	Cryptographic key destruction (3: GP session)					X	X	
FCS_CKM.1	Cryptographic key destruction (4: card private key)					X	X	
FCS_CKM.2	Cryptographic key distribution (3: Public key)					X	X	
FCS_CKM.2	Cryptographic key distribution (4: Certificate)					X	X	
FCS_CKM.4	Cryptographic key destruction (3: GP Session)					X	X	
FCS_COP.1	Cryptographic operation (7:HMAC)					X	X	
FCS_COP.1	Cryptographic operation (8:GP MAC)					X	X	
FCS_COP.1	Cryptographic operation (9:GP ENC)					X	X	
FIA_AFL.1	Authentication failure handling (3: Card interface GP)				X			

Table 28 – Coverage of security objectives for the TOE by SFRs

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

Security Objective	SFR	Rationale
O.Data_Access	FIA_AFL.1.1(all)	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.
O.Secure_Communications	FCS_CKM.1(1&2) FCS_CKM.2(1&2) FCS_CKM.4(1&2) FCS_COP.1(all)	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.
O.Crypto_Implement	FCS_CKM.1(all) FCS_CKM.2(all) FCS_CKM.4(all)	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.

Table 29 – Suitability of the SFRs

6.3.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE FOR PATCH MANAGEMENT

	O.SECURE_LOAD_ACODE	O.SECURE_AC_ACTIVATION	O.TOE_IDENTIFICATION	O.CONFID-OS-UPDATE.LOAD
FDP_ACC.1/OS-UPDATE	X	X	X	X
FDP_ACF.1/OS-UPDATE	X	X	X	X
FIA_ATD.1/OS-UPDATE			X	
FMT_MSA.3/OS-UPDATE	X	X	X	X
FMT_SMR.1/OS-UPDATE	X	X	X	X
FMT_SMF.1/OS-UPDATE	X	X	X	X
FTP_TRP.1/OS-UPDATE				X
FCS_COP.1/OS-UPDATE-DEC				X
FCS_COP.1/OS-UPDATE-VER	X			
FPT_FLS.1/OS-UPDATE	X	X	X	

Table 30: Security Functional Requirement Rationale for Patch Management

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

Security Objective	SFR	Rationale
O.SECURE_LOAD_ACODE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, SFR FCS_COP.1/OS-UPDATE-VER	This security objective specifies that the TOE shall check the authenticity and the integrity of the additional code to be loaded.
	FPT_FLS.1/OS-UPDATE	Any interruption or incident will prevent the forming and activation of the additional code.
O.SECURE_AC_ACTIVATION	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE	This security objective specifies that the activation of the additional code and update of the Identification Data shall be performed at the same time in an atomic way.
	FPT_FLS.1/OS-UPDATE	Any interruption or incident will prevent the forming and activation of the additional code.
O.TOE_IDENTIFICATION	FDP_ACC.1/OS-UPDATE , FDP_ACF.1/OS-UPDATE, FIA_ATD.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE	This security objective specifies the identifications of both the Initial TOE and additional code.
	FPT_FLS.1/OS-UPDATE	Any interruption or incident will prevent any change of the identification data.
O.CONFID-OS-UPDATE.LOAD	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC	This security objective specifies that The TOE shall decrypt the additional code prior installation.

Table 31 – Suitability of the SFRs

6.3.4 DEPENDENCY RATIONALE FROM PROTECTION PROFILES

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

SFR	Dependencies	Rationale
TC Core		
FAU_ARP.1	FAU_SAA.1	Satisfied by FAU_SAA.1
FAU_SAA.1	FAU_GEN.1	*See note 1 below*
FCO_NRO.1	FIA_UID.1	Satisfied by FIA_UID.2
FDP_ACC.2	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2 *See note 2 below*
FDP_DAU.1	-	-
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2 *See note 2 below*
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1, FTP_ITC.1 or FTP_TRP.1, FPT_TDC.1	Satisfied by FDP_ACC.2, FTP_ITC.1(1 & 2) and FPT_TDC.1(1 & 2)
FDP_RIP.1	-	-
FDP_SDI.2	-	-
FIA_AFL.1(1:C)	FIA_UAU.1	Satisfied by FIA_UAU.1(1 & 2)
FIA_AFL.1(2:WC)	FIA_UAU.1	Satisfied by FIA_UAU.1(1 & 2)
FIA_ATD.1	-	-
FIA_UAU.3	-	-
FIA_UAU.4	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1	Satisfied by FIA_ATD.1
FPR_UNO.1	-	-
FPT_EMS.1	-	-
FPT_FLS.1	-	-
FPT_PHP.3	-	-
FPT_TST.1	-	-

SFR	Dependencies	Rationale
2nd generation specific		
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2(1), FCS_COP.1(1:AES & 3:ECC) and FCS_CKM.4(1)
FCS_CKM.2(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1) and FCS_CKM.4(1)
FCS_CKM.4(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1(1)
FCS_COP.1(1:AES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1) and FCS_CKM.4(1)
FCS_COP.1(2:SHA-2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-2
FCS_COP.1(3:ECC)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4(1)
FCS_RNG.114	-	-
FIA_UAU.1(1)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(1)	-	-
FTP_ITC.1(1)	-	-
1st generation specific		
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2(2), FCS_COP.1(4:TDES &
5:RSA) and FCS_CKM.4(2)	-	-
FCS_CKM.2(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_CKM.4(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1(2)
FCS_COP.1(4:TDES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_COP.1(5:RSA)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4(2)
FCS_COP.1(6:SHA-1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-1

SFR	Dependencies	Rationale
FIA_UAU.1(2)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(2)	-	-
FTP_ITC.1(2)	-	-

Table 32 – Dependency rationale

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.

6.3.5 DEPENDENCY RATIONALE FOR PLATFORM

SFR	Dependencies	Rationale
FCS_CKM.1 (3:GP session)	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4	FCS_COP1, FCS_CKM.4
FCS_CKM.1 (4: card private key)	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4	FCS_COP1, FCS_CKM.4
FCS_CKM.2 (3: Public key)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_CKM.2 (4: Certificate)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_CKM.4 (3 : GP session)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2	FCS_CKM.1
FCS_COP.1 (7 :HMAC)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FDP_ITC.1, FCS_CKM.4
FCS_COP.1 (8 :GP MAC)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FDP_ITC.1, FCS_CKM.4
FCS_COP.1 (9 :GP ENC)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FDP_ITC.1, FCS_CKM.4
FIA_AFL.1 (3 : Card interface GP)	FIA_UAU.1	FIA_UAU.1

Table 33 – Dependency rationale

6.3.6 DEPENDENCY RATIONALE FOR PATCH MANAGEMENT

SFR	Dependencies	Rationale
FDP_ACC.1/OS-UPDATE	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/OS-UPDATE
FDP_ACF.1/OS-UPDATE	FDP_ACC.1 Subset access control FMT_MSA.3Security attribute initialisation	FDP_ACC.1/OS-UPDATE FMT_MSA.3/OS-UPDATE
FIA_ATD.1/OS-UPDATE	No Dependencies	
FMT_MSA.3/OS-UPDATE	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Note 1: justification 1 for non-satisfied dependencies FMT_SMR.1/OS-UPDATE

SFR	Dependencies	Rationale
FMT_SMR.1/OS-UPDATE	FIA_UID.1 Timing of identification	FIA_UID.2
FMT_SMF.1/OS-UPDATE	No Dependencies	
FTP_TRP.1/OS-UPDATE	No Dependencies	
FCS_COP.1/OS-UPDATE-DEC	[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	Note 2: justification 2 for non-satisfied dependencies
FCS_COP.1/OS-UPDATE-VER	[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	Note 2: justification 2 for non-satisfied dependencies
FPT_FLS.1.1/OS-UPDATE	No Dependencies	

Note 1: FMT_MSA.1 is not necessary here as there is no management of these security attributes.

Note 2: FDP_ITC.1 or FDP_ITC.2 concerns import of user data and there is no user data (only TSF code) imported by such operation. There is no key generation FCS_CKM.1 or deletion FCS_CKM.4 for ES update. Keys are imported in Pre-Personalisation and are never erased.

6.3.7 SECURITY ASSURANCE REQUIREMENTS RATIONALE

EAL4 was chosen for this application as specified in [PP-TACHOCARD1] and [PP-TACHOCARD2].

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

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

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

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

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

6.3.8 COMPATIBILITY BETWEEN SFR OF [ST-TACHOCARD] AND [ST-IC]

The following table lists the SFRs that are declared on the [ST-IC] Integrated Circuit Security Target and separates them in:

IP_SFR: Irrelevant Platform-SFRs not being used by the Composite-ST.
RP_SFR-SERV: Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.
MRP_SFR-MECH: Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE, as specified in [JIL_CPE].

These definitions are according to the [JIL_CPE]. on which the Platform TOE on our case is the relaying IC, the [ST-IC] Integrated Circuit.

The first column lists the [ST-IC] and the next columns indicate their classification according to the paragraph above. The SFR's on the cells of the classification belong the Smart Tachograph TOE described in this document. If there is no SFR on each cell is because not all CC class families have a corresponding match on both sides, but all SFRs from the [ST-IC] have been classified. Moreover, no contradictions have been found between the Platform-SFRs set and the SFRs related to the composite product

IFX_CCI_000039 SFR's	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
Security functional requirements of the TOE defined in [PP-IC-0084]			
FRU_FLT.2			X FDP_SDI.2 FPT_PHP.3.1
FPT_FLS.1			X FPT_FLS.1 FPT_FLS.1/OS-UPDATE
FMT_LIM.1			X No direct link to SFRs but not in conflict with [ST-IC]
FMT_LIM.2			X No direct link to SFRs but not in conflict with [ST-IC]
FAU_SAS.1	X		
FDP_SDC.1			X FPT_EMS.1
FDP_SDI.2			X FDP_SDI.2
FPT_PHP.3			X FPT_PHP.3
FDP_ITT.1			X No direct link to SFRs but not in conflict with [ST-IC]
FPT_ITT.1			X No direct link to SFRs but not in conflict with [ST-IC]
FDP_IFC.1			X No direct link to SFRs but not in conflict with [ST-IC]

IFX_CCI_000039 SFR's	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FCS_RNG.1/TRNG	X		
FCS_RNG.1/DRNG	X		
FCS_RNG.1/DRNG4			X FCS_RNG.1
FCS_RNG.1/HPRG	X		
FCS_COP.1/SCP/TDES		X FCS_COP.1.1(4:TDES) FCS_COP.1.1(9: GP ENC)	
FCS_CKM.4/SCP/TDES		X FCS_CKM.4	
FCS_COP.1/SCP/AES		X FCS_COP.1.1(7: HMAC) FCS_COP.1.1(1:AES) FCS_COP.1/OS-UPDATE-DEC FCS_COP.1/OS-UPDATE-VER	
FCS_CKM.4/SCP/AES		X FCS_CKM.4	
FCS_COP.1/SCL/TDES	X		
FCS_CKM.4/SCL/TDES	X		
FCS_COP.1/SCL/AES	X		
FCS_CKM.4/SCL/AES	X		
FMT_LIM.1/Loader		X No direct link to SFRs but not in conflict with [ST-IC]	
FMT_LIM.2/Loader		X No direct link to SFRs but not in conflict with [ST-IC]	
FTP_ITC.1		X FTP_ITC.1	
FDP_UCT.1		X FDP_ACC.2	

IFX_CCI_000039 SFR's	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FDP_UIT.1			X FDP_DAU.1 FDP_ACF.1
FDP_ACC.1/Loader		X FDP_ACC.2	
FDP_ACF.1/Loader		X FDP_ACF.1	
FIA_API.1			X FIA_UAU.1
Additional security functional requirements of the [ST-IC]			
FPT_TST.2			X No direct link to SFRs but not in conflict with [ST-IC]
FDP_ACC.1		X FDP_ACC.2	
FDP_ACF.1		X FDP_ACF.1	
FMT_MSA.1		X No direct link to SFRs but not in conflict with [ST-IC]	
FMT_MSA.3		X FMT_MSA.3/OS-UPDATE	
FMT_SMF.1		X FMT_SMF.1/OS-UPDATE	
FMT_SMR.1		X FMT_SMR.1/OS-UPDATE	
FCS_COP.1/SCP/TDES-MAC		X FCS_COP.1.1(4:TDES)	
FCS_COP.1/SCP/AES-MAC		X FCS_COP.1/OS-UPDATE-DEC	
FCS_COP.1/RSA/<iteration>		X FCS_COP.15(5 :RSA)	
FCS_CKM.1/RSA/<iteration>		X FCS_CKM.1	
FCS_CKM.4/RSA		X FCS_CKM.4	

IFX_CCI_000039 SFR's	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FCS_COP.1/ECC/<iteration>		X FCS_ COP.1(3:ECC)	
FCS_CKM.1/ECC	X		
FCS_CKM.4/ECC	X		
FMT_MTD.1/Loader	X		
FMT_SMR.1/Loader	X		
FMT_SMF.1/Loader	X		
FIA_UID.2/Loader	X		

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

6.3.9 COMPATIBILITY BETWEEN SAR OF [ST_TACHOCARD] AND [ST-IC]

The assurance level for [ST_ TACHOCARD] is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 when the assurance level for the Integrated Circuit Security Target [ST-IC] is EAL6 augmented with ALC_FLR.1.

Therefore SAR for [ST_ TACHOCARD] and [ST-IC] are compatible as all components of [ST_ TACHOCARD] are covered by equivalent or higher in [ST-IC].

We can therefore conclude that the SAR of [ST_ TACHOCARD] and [ST-IC] are consistent.

7 TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the TOE embedded software and by the chip.

7.1.1 TSFS PROVIDED BY THE TOE FOR THE SMART TACHOGRAPH APPLICATION

SF	Description	SFRs
SF.TEST: Self-test	The TSF performs the following tests: • When starting a work session, • working condition of the work memory (RAM), • integrity of code in EEPROM,	FAU_SAA.1 FAU_ARP.1 FDP_ACC.2 FDP_ACF.1 FPT_TST.1
SF.EXCEPTION: Error Messages and exceptions	The TOE reports the following errors: • Message format errors, • Integrity errors, • Life cycle status errors, • Errors in authentication attempt. The card becomes mute (secure Fail State) when one of the following errors occurs: • Error on integrity of keys or PINs, • Out of range in frequency or voltage,	FDP_SDI.2 FIA_AFL.1 FPT_PHP.3

SF	Description	SFRs
	• Life cycle status errors,	
SF.ERASE: Data erasure	The whole RAM is erased after reset. When a new mutual authentication is performed, the former session key set is destroyed without any possibility of even partial recovery.	FCS_CKM.4
SF.INTEGRITY: Data Integrity	The function provides the ability to check the integrity of the following data elements stored in the card: • Cryptographic keys including card private key, public key and corresponding attributes, • Authentication data including PIN and corresponding attributes, • Data contained in the File System, including Identification data, Activity data.	FAU_SAA.1 FAU_ARP.1 FDP_DAU.1 FDP_SDI.2 FPT_TST.1
SF.HIDE: Data and operation hiding	The TOE hides sensitive data transfers and operations from outside observations. The TOE is protected against SPA, DPA, DFA & timing attacks	FDP_RIP.1 FPR_UNO.1 FPT_EMS.1
SF.CARD_MGR: Card manager (CM)	This function controls the execution of the card internal process when command messages are sent to the card. The messages handled are defined as specified in ISO 7816. Controls include: CM Format verification • Identification: the instruction code of the message is supported, • Format analysis: the class is consistent with the instruction code, P1/P2/P3 parameter values are supported by the identified command. CM Access checking • Life cycle analysis: the identified command shall be enabled in the current TOE life cycle phase of the TOE. • Check that the command sequence is respected, • Check that the authenticated user is allowed to send the command. CM Execution • Execution: activation of the executable code corresponding to the card internal process for the command message. CM Response • Control the build-up of the response.	FDP_ACC.2 FDP_ACF.1 FDP_ETC.1 FDP_ETC.2 FDP_ITC.1 FDP_ITC.2 FIA_UAU.1 FIA_UID.2

SF	Description	SFRs
SF.KEY_GEN: Key generation	The TOE can generate the Card private/public key pair in personalization phase: • RSA 1024 bits for Tacho Gen1 application • ECC for Tacho Gen2 application For Tacho Gen1 the TOE generates Session keys, using TDES with 2 keys, in usage phase. The generation process includes the distribution to the remote IT. For Tacho Gen2 the TOE generates Session keys based on AES symmetric cryptography, in usage phase. The generation process includes the distribution to the remote IT.	FCS_CKM.1 FCS_CKM.2
SF.SIG: Signature creation and verification	The TOE can sign a message digest, which is the result of a hash operation performed on a Tachograph data file, stored in the TOE. This hashing is performed by SF.HASH and the result is stored in the card. The TOE can verify the signature of a message imported into the card. For Tacho Gen1,the TOE uses a RSA PKCS#1 signature scheme with a 1024 bit modulus, as defined in [RSA-PKCS#1]. For Tacho Gen2, the TOE uses the signature scheme algorithm ECDSA as specified in [DSS].	FCO_NRO.1 FCS_COP.1 FDP_DAU.1 FDP_ITC.2
SF.ENC: Encryption and decryption	The TOE encrypts and decrypts messages. For Tacho Gen1, the encryption uses TDES with 2 keys, in CBC mode according to [SP800-67] and [SP800-38 A]. For Tacho Gen2, the encryption uses AES algorithm according to [AES].	FCS_COP.1 FPT_TDC.1 FTP_ITC.1
SF.HASH : Message hashing	The TOE can generate a hash of a file stored in the card. For Tacho Gen1, hashing is done using SHA-1 algorithm as specified in [FIPS180-4]. For Tacho Gen2, hashing is done using SHA-2 algorithm as specified in [FIPS180-4]	FCS_COP.1 FDP_DAU.1
SF.MAC: MAC generation and verification	The TOE generates and verifies the MAC of messages. For Tacho Gen1, MAC computation uses TDES with 2 keys, in CBC mode according to [SP800-67] and [SP800-38 A] . For Tacho Gen2, MAC computation uses AES algorithm according to [AES].	FCS_COP.1 FTP_ITC.1

SF	Description	SFRs
SF.TRUSTED : Trusted Path	This function establishes a secure channel, using a mutual authentication mechanism. The secure channel is GP in Personalization phase. In usage phase the secure channel is done with TDES session keys with Tacho Gen1 or AES session keys with Tacho Gen2. In GP, a ratification counter limits the number of failed consecutive authentication attempts. The counter initial value is 3. When the authentication fails, the counter is decremented. When the authentication succeeds, the counter is set to its initial value. The authentication mechanism is blocked and cannot be used any longer if the counter reaches zero. When the secure channel is established, the messages may be MACed and Encrypted, depending on the function performed. The imported keys are encrypted.	FAU_SAA.1 FAU_ARP.1 FIA_UAU.1 FIA_UAU.3 FIA_UAU.4 FTP_ITC.1 FIA_UID.2
SF.PIN : PIN management	This SF controls all the operation relative to the PIN management, including the Cardholder authentication: • PIN creation: the PIN is stored and is associated to a maximum presentation number. • PIN verification: the PIN can be accessed only if its format and integrity are correct. After 5 consecutive unsuccessful verification of the PIN, it is blocked. When the PIN is blocked, then it cannot be used anymore.	FAU_SAA.1 FAU_ARP.1 FIA_AFL.1
SF.ACC : Access Authorization	The function controls the access conditions of a file. This SF puts the access conditions on a file when it is created. It checks that the AC are met before accessing a file in the card. This SF maintains the roles of the user. This SF also maintains the security attributes USER_GROUP and USER_ID.	FDP_ACC.2 FDP_ETC.1 FDP_ETC.2 FDP_ITC.1 FDP_ITC.2 FIA_ATD.1 FIA_USB.1
SF.DOMAIN : Domain Separation	This SF maintains the Security Domains. It ensures that the Tachograph application has its own security environment, separate from the security environment of the OS. RSA/ECC keys have their own RAM space.	FDP_RIP.1

SF	Description	SFRs
SF.DRIVER : Chip driver	This function ensures the management of the chip security features: • Enforce shield protection, • physical integrity of the IC, • physical environment parameters,	FPT_PHP.3
SF.ROLLBACK: Safe fail state recovery	The function shall ensure that the TOE returns to its previous secure state when following events occur. • power cut-off or variations, • unexpected reset	FPT_FLS.1
SF.RND: RNG	Provide a random value	FCS_RNG.1

7.1.2 TSFS PROVIDED BY THE TOE FOR OS UPDATE

SF	Description	SFRs
SF.OSAGILITY: OS Agility Management	Provides the role management as defined in	FMT_SMR.1/OS-UPDATE
	Provides Patch management functions linked to the states of the TOE as defined in	FMT_SMF.1/OS-UPDATE
	The TSF maintains the following list of security attributes belonging to individual users: **additional code ID for each activated additional code**	FIA_ATD.1/OS-UPDATE
	The OS Update module load, install and activate the additional code	FDP_ACC.1/OS-UPDATE FDP_ACF.1/OS-UPDATE
	The default values for security attributes are defined by the OS Update Access Control Policy	FMT_MSA.3/OS-UPDATE
	Provides a communication path between itself and remote	FTP_TRP.1/OS-UPDATE
	It provides the secure transfer of data through SM as defined in	FCS_COP.1/OS-UPDATE-VER FCS_COP.1/OS-UPDATE-DEC
	Provides physical protection of the TOE and preservation of TOE secure state as defined in	FPT_FLS.1/OS-UPDATE

7.1.3 TSFS PROVIDED BY THE IC

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IC]. The IC and its primary embedded software have been evaluated at level EAL 6+. These SF are the same for the IC considered in this ST;

SF	Description
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

Table 34: Security Functions provided by the Infineon IFX_CCI_000039 chips

These SF are described in [ST-IC].

7.2 TOE SUMMARY SPECIFICATION RATIONALE

Security functions/ Security requirements	SF.TEST	SF.EXCEPTION	SF.ERASE	SF.INTEGRITY	SF.HIDE	SF.CARD_MGR	SF.KEY_GEN	SF.SIG	SF.ENC	SF.HASH	SF.MAC	SF.TRUSTED	SF.PIN	SF.ACC	SF.DOMAIN	SF.DRIVER	SF.ROLLBACK	SF.RND	SF.OSAGILITY
FAU_ARP.1	X			X								X	X						
FAU_SAA.1	X			X								X	X						
FCO_NRO.1								X											
FDP_ACC.2	X					X								X					
FDP_ACF.1(1:TachoGen1)						X													
FDP_ACF.1(2:TachoGen2)						X													
FDP_DAU.1				X				X		X									
FDP_ETC.1						X								X					
FDP_ETC.2						X								X					
FDP_ITC.1						X					X			X					
FDP_ITC.2						X		X						X					
FDP_RIP.1					X										X				
FDP_SDI.2		X		X															
FIA_AFL.1(1 :C)		X																	
FIA_AFL.1(1 :WC)		X											X						
FIA_ATD.1														X					
FIA_UAU.3												X							
FIA_UAU.4												X							
FIA_UID.2						X						X							
FIA_USB.1														X					
FPR_UNO.1					X														
FPT_EMS.1					X														

Security functions/ Security requirements	SF.TEST	SF.EXCEPTION	SF.ERASE	SF.INTEGRITY	SF.HIDE	SF.CARD_MGR	SF.KEY_GEN	SF.SIG	SF.ENC	SF.HASH	SF.MAC	SF.TRUSTED	SF.PIN	SF.ACC	SF.DOMAIN	SF.DRIVER	SF.ROLLBACK	SF.RND	SF.OSAGILITY
FPT_FLS.1																	X		
FPT_PHP.3		X														X			
FPT_TST.1	X			X															
FCS_CKM.1(1)							X												
FCS_CKM.2(1)							X												
FCS_CKM.4(1)			X																
FCS_COP.1(1 :AES)									X		X								
FCS_COP.1(2:SHA-2)										X									
FCS_COP.1(3:ECC)								X											
FCS_RNG.1																		X	
FIA_UAU.1(1)						X						X							
FPT_TDC.1(1)									X										
FTP_ITC.1(1)									X			X							
FCS_CKM.1(2)							X												
FCS_CKM.2(2)							X												
FCS_CKM.4(2)			X																
FCS_COP.1(4:TDES)									X		X								
FCS_COP.1(5:RSA)								X											
FCS_COP.1(6:SHA-1)										X									
FIA_UAU.1(2)						X						X							
FPT_TDC.1(2)									X										
FTP_ITC.1(2)									X			X							
FCS_CKM.1 (GP Session)							X												

Security functions/ Security requirements	SF.TEST	SF.EXCEPTION	SF.ERASE	SF.INTEGRITY	SF.HIDE	SF.CARD_MGR	SF.KEY_GEN	SF.SIG	SF.ENC	SF.HASH	SF.MAC	SF.TRUSTED	SF.PIN	SF.ACC	SF.DOMAIN	SF.DRIVER	SF.ROLLBACK	SF.RND	SF.OSAGILITY
FCS_CKM.1 (Card private key)							X												
FCS_CKM.2(Public Key)							X												
FCS_CKM.4(GP Session)			X																
FCS_COP.1(7: HMAC)								X		X									
FCS_COP.1(8: GP MAC)											X								
FCS_COP.1(9: GP ENC)									X										
FIA_AFL.1(3: Card interface GP)		X																	
FDP_ACC.1/OS-UPDATE																			X
FDP_ACF.1/OS-UPDATE																			X
FIA_ATD.1/OS-UPDATE																			X
FMT_MSA.3/OS-UPDATE																			X
FMT_SMR.1/OS-UPDATE																			X
FMT_SMF.1/OS-UPDATE																			X
FTP_TRP.1/OS-UPDATE																			X
FCS_COP.1/OS-UPDATE-DEC																			X
FCS_COP.1/OS-UPDATE-VER																			X
PT_FLS.1/OS-UPDATE																			X

END OF DOCUMENT