Document Administration

Recipient

Department	Name

For the attention of

Department	Name

Summary

The following document comprises the Security Target for a TOE evaluated according to Common Criteria Version 2.3. The TOE being subject of the evaluation is the smartcard product

MICARDO V3.6 R1.0 Tachograph V2.0

from Sagem Orga GmbH. The IT product under consideration shall be evaluated according to CC EAL 4 augmented with a minimum strength level for the TOE security functions of SOF-high.

Keywords

Target of Evaluation (TOE), Common Criteria, IC, Dedicated Software, Smartcard Embedded Software, Basic Software, Application Software, Tachograph Application, Security Objectives, Assumptions, Threats, TOE Security Function (TSF), TOE Security Enforcing Function (SEF), Level of Assurance, Strength of Functions (SOF), Security Functional Requirement (SFR), Security Assurance Requirement (SAR), Security Function Policy (SFP)

Responsibility for updating the document

Karsten Klohs karsten.klohs@sagem-orga.com

Sagem ORGA GmbH

MICARDO V3.6 R1.0 Tachograph V2.0

ST-Lite

Document Id:	3TachoEval.CSL.0002
Archive:	3
Product/project/subject:	TachoEval (Evaluierung Tachograph Card gemäß CC EAL4+)
Category of document:	CSL (ST-Lite)
Consecutive number:	0002
Version:	V1.02
Date:	12 May 2011
Author:	Karsten Klohs
Confidentiality:	

Checked report:	not applicable
Authorized (Date/Signature):	not applicable
Accepted (Date/Signature):	not applicable

Document Organisation

i Notation

None of the notations used in this document need extra explanation.

ii Official Documents and Standards

See Bibliography.

iii Revision History

Version	Type of change	Author / team
V1.00	First edition, derived from the security target of the certification baseline product “MICARDO V3.6 R1.0”	Karsten Klohs
V1.01	Minor editorial corrections	Karsten Klohs
V1.02	Key words added into docuement attributes	Karsten Klohs

Table of Contents

1 ST Introduction

1.1 ST and TOE Identification

This Security Target refers to the smartcard product "MICARDO V3.6 R1.0 Tachograph V2.0" (TOE) provided by Sgame Orga GmbH for a Common Criteria evaluation.

Title:	Security Target Lite - MICARDO V3.6 R1.0 Tachograph V2.0
Document Category:	Security Target for a CC Evaluation
Document ID:	Refer to document administration.
Version:	Refer to document administration.
Publisher:	Sagem Orga GmbH
Confidentiality:	Refer to document administration
TOE ID:	"MICARDO V3.6 R1.0 Tachograph V2.0" (Smartcard Product containing IC with Embedded Software dedicated for the Tachograph Application)
Certification ID:	BSI-DSZ-CC-0661
IT Evaluation Scheme:	German CC Evaluation Scheme
Evaluation Body:	SRC Security Research & Consulting GmbH
Certification Body:	Bundesamt für Sicherheit in der Informationstechnik (BSI)

1.2 ST Overview

Target of Evaluation (TOE) and subject of this Security Target (ST) is the smartcard product "MICARDO V3.6 R1.0 Tachograph V2.0" developed by Sagem Orga GmbH.

For the delivery of the TOE two different ways are established:

- The TOE is delivered to the customer in form of a complete initialised smartcard.
- Alternatively, the TOE is delivered to the customer in form of an initialised module. In this case, the smartcard finishing process (embedding of the delivered modules, final card tests) is task of the customer.

As the form of the delivery of the TOE does not concern the security features of the TOE in any way the TOE will be named in the following with "Tachograph Card" for short, independently of its form of delivery.

The TOE will be employed within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment. A Tachograph Card allows for identification of the identity (or identity group) of the cardholder by the recording equipment and allows for data transfer and storage. A Tachograph Card may be of the type Driver Card, Control Card, Workshop Card or Company Card.

The TOE comprises the following components:

- Integrated Circuit (IC) "Philips SmartMX P5CC037V0A Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH
- Smartcard Embedded Software (based on a native implementation) with a specific Tachograph Application provided by Sagem Orga GmbH

The Tachograph Application consists of a configurable software part for the Tachograph Card´s file system. The configuration of the Tachograph Card concerns the following points:

- Choice of the card type: A complete Driver Card, Control Card, Workshop Card or Company Card with complete file system as defined in the Tachograph Card Specification /TachAn1B/, main body, Appendix 2, chap. 4 is produced. Alternatively, a General Tachograph Card set up for the different types Driver Card, Control Card, Workshop Card and Company Card is generated. In this case, after initialisation resp. prior to the personalisation of the card, one of the four prepared card types as desired by the customer has to be blown up by using a specific card command.
- Choice of the personalisation scheme: Securing the transfer of personalisation data can be done on base of a dynamic scheme (Secure Messaging with a session key) or alternatively on base of a static scheme (Secure Messaging with a static key).

The TOE is configured by Sagem Orga GmbH according to the different possibilities for configuration described before. The configuration of the product is defined prior to its delivery and cannot be changed after delivery.

The TOE is developed and constructed in full accordance with the Tachograph Card Specification /TachAn1B/, main body, Appendix 2, Appendix 10 (Tachograph Card Generic Security Target) and Appendix 11. In particular, this implies the conformance of the Tachograph Card with the following standards:

- ISO/IEC 7810 Identification cards – Physical characteristics
- ISO/IEC 7816 Identification cards - Integrated circuits with contacts:
  - Part 1: Physical characteristics
  - Part 2: Dimensions and location of the contacts
  - Part 3: Electronic signals and transmission protocols
  - Part 4: Inter-industry commands for interchange
  - Part 8: Security related inter-industry commands
- ISO/IEC 10373 Identification cards – Test methods

As mentioned, the TOE with all its components complies with the Tachograph Card Specification and its functional and security requirements as specified in /TachAn1B/, main body, Appendix 2, Appendix 10 (Tachograph Card Generic Security Target) and Appendix 11. Particularly, this ST takes into account the “Tachograph Card Generic Security Target” for the Tachograph Card in /TachAn1B/, Appendix 10. In order to achieve the required system security, the Tachograph Card and the corresponding ST meet all the security requirements and evaluation conditions defined in the Tachograph card´s “Generic Security Target” under consideration of the interpretations in /JILDigTacho/.

The CC evaluation and certification of the TOE against the present ST serves for the security certificate in the sense of the Tachograph Card Specification /TachAn1B/, main body, chap. VIII. 2. The CC evaluation and certification of the TOE implies the proof for the compliance of the TOE with the requirements of /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target).

The main objectives of this ST are

- to describe the TOE as a smartcard product for the Tachograph System
- to define the limits of the TOE
- to describe the assumptions, threats and security objectives for the TOE
- to describe the security requirements for the TOE
- to define the TOE security functions

1.3 CC Conformance

The CC evaluation of the TOE is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.3, August 2005 (/CC 2.3 Part1/)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.3, August 2005 (/CC 2.3 Part2/)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.3, August 2005 (/CC 2.3 Part3/)

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, Version 2.3, August 2005 (/CEM 2.3/)

This Security Target is written in accordance with the above mentioned Common Criteria Version 2.3 and claims the following CC conformances:

- Part 2 extended
  (Note: The supplement „extended“ is only relevant for the SFRs of the underlying IC with its IC Dedicated Support Software.)
- Part 3 conformant

Furthermore, the ST is written in view of the requirements of the „Generic Security Target“ for the Tachograph Card within the Tachograph Card Specification /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target) and the JIL interpretations and requirements in /JILDigTacho/. In particular, this ST complies with the Protection Profile PP9911 „Smartcard Integrated Circuit with Embedded Software“ (/PP9911/). The IC evaluation in compliance with the Protection Profile PP9806 (/PP9806/) as required in /TachAn1B/, Appendix 10 is replaced by the comparable IC evaluation according to the Protection Profile BSI-PP-0002 (/BSI-PP-IC/). Refer for this to the report of the BSI concerning the comparability of the Protection Profiles PP9806 and BSI-PP-0002 (/CompPP9806-BSIPP0002/).

The chosen level of assurance for the TOE is **EAL 4 augmented**. The augmentation includes the assurance components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4.

The minimum strength level for the TOE security functions is **SOF-high**.

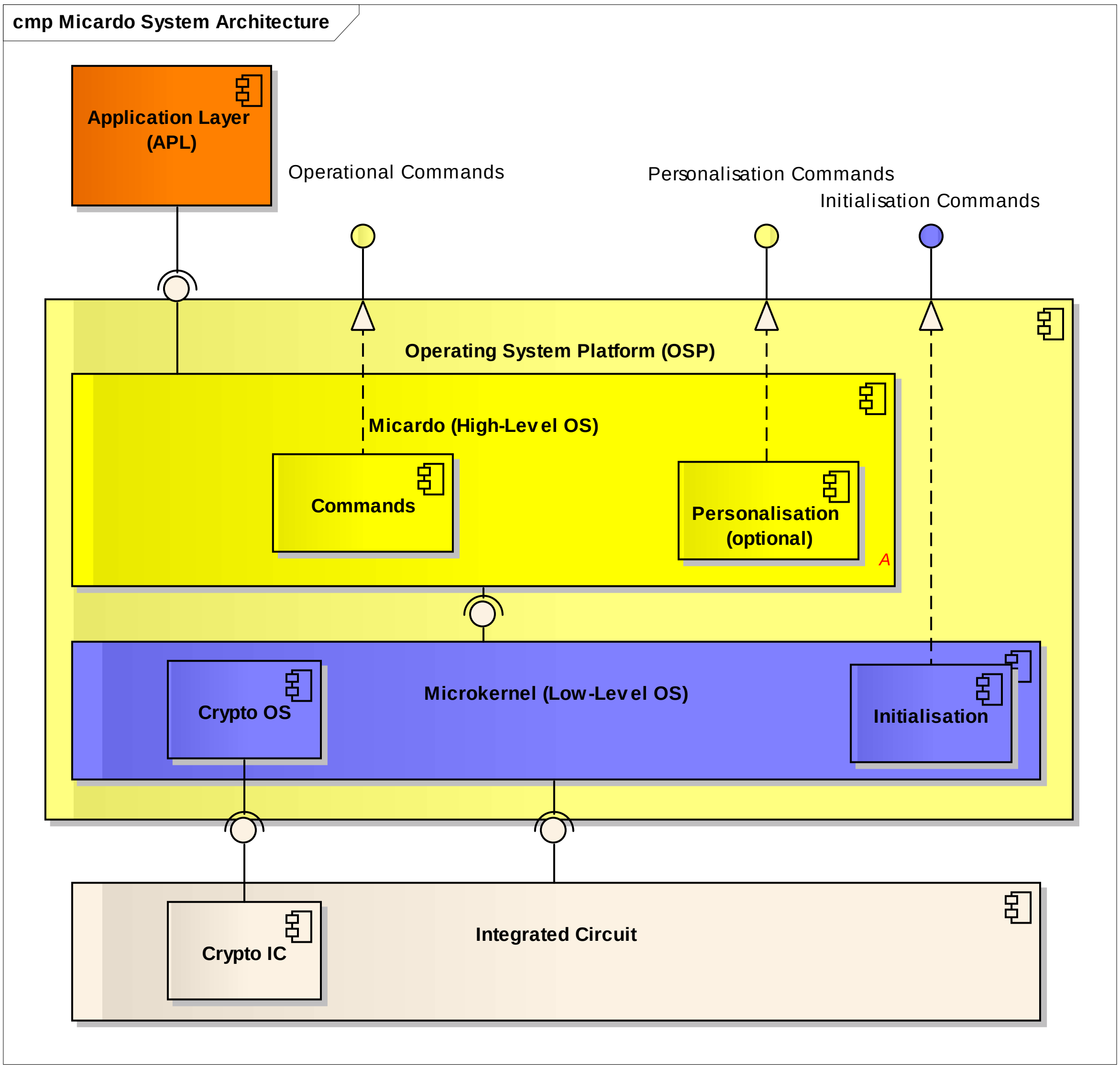
In order to avoid redundancy and to minimize the evaluation efforts, the evaluation of the TOE will be conducted as a composite evaluation and will make use of the evaluation results of the CC evaluation of the underlying semiconductor "NXP SmartMX P5CC037V0A Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH. The IC incl. its IC Dedicated Software is evaluated according to Common Criteria EAL 4 augmented with a minimum strength level for its security functions of SOF-high and is listed under the Certification ID BSI-DSZ-CC-0612. The evaluation of the IC is based on the Protection Profile BSI-PP-0002 (/BSI-PP-IC/). In order to avoid redundancies to the hardware evaluation, the compliance of the TOE to the Protection Profile /BSI-PP-IC/ is primarily shown by appropriate reference to the hardware evaluation.

2 TOE Description

2.1 Architecture Overview

The whole smartcard product is realised as a proprietary operating system platform on which the application layer is set up. The operating system platform is based on a microcontroller which is at least evaluated according to Common Criteria EAL4 augmented with a minimum strength for its security functions of SOF-high. Any cryptographic functionality which is supplied by the microcontroller either in hardware or in terms of cryptographic library is also evaluated according to the same level of assurance.

The operating system platform is decomposed in the high-level operating system MICARDO and the native low-level operating system which is called Microkernel. The following figure shows this general architecture and its components:



The different components will now be described in more detail.

2.1.1 Integrated Circuit (IC) with its Dedicated Software

The basis for the OS platform is a microcontroller in with the code is embedded in terms of a so called “ROM mask”. The microcontroller can also supply dedicated software (e.g. a cryptographic library) which supports the operating system implementation.

Detailed information about the IC hardware and the dedicated software is provided in the security targets, the data sheets, and the guidance documents provided by the IC supplier.

2.1.2 Operating System Platform

The operating system platform is designed as proprietary software consisting of two layers, the high-level operating system MICARDO and the native low-level operating system which is called “Microkernel”. The core responsibilities of these two layers can be summarised as follows:

- MICARDO (High-Level OS) is responsible for
  - the object / file system which supports the application layer
  - the command interface as required by the application layer
  - an optional personalisation module for a more efficient personalisation process
- Microkernel (Low-Level OS) is responsible for
  - the hardware abstraction layer (HAL). Essentially, the Microkernel allows for an exchange of hardware (the IC) without any need to modify the high-level OS.
  - the implementation of the cryptographic core routines. It is the task of the microkernel to implement the collaboration with the cryptographic support supplied by the hardware and its dedicated software. Furthermore, the Microkernel offers a unified interface to cryptographic functions to the high-level OS layer.
  - the implementation of generic support functions for the high-level OS which range from memory management to transaction mechanisms
  - a dedicated initialisation module which provides a command interface for the fast and secure initialisation of the card. In particular, the initialisation is only possible by the use of an initialisation that is encrypted and secured with a cryptographic checksum. Furthermore, the initialisation commands provide testing mechanisms for the NVM area and a way to identify non-initialised smartcards.

2.1.3 Application Layer

The application layer comprises all applications which are supplied by the product in question. Essentially, an application is a part of the file system either in terms of a so called “Dedicated File” (DF) or “Application Dedicated File” (ADF), which are roughly equivalent to directories in a conventional file system. The application is further decomposed into key, elementary files and other kinds of data. In particular, the application uses the access rule mechanism supplied by the operating system to define and enforce access policies. This way, the semantics of the application is defined.

The initialisation phase configures the NVM of the smartcard. In particular, the initialisation writes the file system which corresponds to the loading of the application. However, it is important to observe that the term application in the smartcard context does not refer to executable code. The only part which consists of executable code is the operating system platform, which is already embedded in the IC as a ROM mask during the manufacturing process.

After the application has been stored and configured during initialisation and personalsiation, the following properties hold:

- it is not possible to delete the application
- the access rules as applicable for the end-usage phase of the product are active and cannot be modified
- loading of additional applications is only possible under the conditions specified by the product specification
- the application provides means to identify and to prove the authenticity of the smartcard product.

2.1.4 Tachograph Product Overview

The Target of Evaluation (TOE) is the smartcard product " MICARDO V3.6 R1.0 Tachograph V2.0" (Tachograph Card for short in the following) implemented in accordance with the Tachograph Card Specification /TachAn1B/, main body, Appendix 2, Appendix 10 (Tachograph Card Generic Security Target) and Appendix 11.

The Tachograph Card is based on the microcontroller "NXP SmartMX P5CC037V0A Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH. The IC incl. its Dedicated Software is evaluated according to Common Criteria EAL 4 augmented with a minimum strength level for its security functions of SOF-high (refer to Certification ID BSI-DSZ-CC-0612). Basis for the TOE's Smartcard Embedded Software is the microcontroller "NXP SmartMX P5CC037V0A Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software". The microcontroller and its Dedicated Software are developed and produced by NXP Semiconductors GmbH (within phase 2 and 3 of the smartcard product life-cycle, see chap. 2.2).

Detailed information on the IC Hardware, the IC Dedicated Software (in particular the Crypto Library) and the IC interfaces can be found in /ST_IC/ and /ST_IC_CL/.

Application Layer implements the specific Tachograph Application (file system with dedicated access rules and further security related data).

The Tachograph Application contains in particular the Tachograph Card´s file system. As each type of Tachograph Card has its own file system with own elementary and dedicated files and own access rules, the Tachograph Application depends on the respective card type. The Tachograph Application covers either the complete file system for a Driver Card, Control Card, Workshop Card or Company Card or is alternatively prepared for the four card types. In the latter case, after initialisation resp. prior to the personalisation of the card, one of the four prepared card types has to be blown up by usage of a specific card command. Furthermore, different personalisation schemes for the personalisation of the Tachograph Card may be defined. These two points will be considered as configuration of the TOE. The configuration will be done by Sagem Orga GmbH prior to the delivery of the product and cannot be changed afterwards.

The Tachograph Card offers the capability to check its authenticity. For this purpose, the Tachograph Application contains the private part of a dedicated authentication key pair (RSA 1024 Bit) over which by an internal authentication procedure the authenticity of the Tachograph Card can be proven. The authentication key pair depends on the Tachograph Application and its configuration and may be chosen customer specific. The corresponding public part of the authentication key pair is delivered through a trusted way to the external world.

Furthermore, the Tachograph Application contains a data area for storing identification data of the TOE resp. of the TOE's personalisation. The data area will be filled in the framework of the initialisation resp. the personalisation of the TOE with a specific operating system command and can be read out with a further specific operating system command. Once the identification data have been written, there is afterwards no change possible.

2.1.5 TOE Product Scope

The following table contains an overview of all deliverables associated to the TOE:

TOE component	Description / Additional Information	Type	Transfer Form
TOE-IC	NXP SmartMX P5CC037V0A Secure Smart Card Controller (incl. its IC Dedicated Software, covering in particular the Crypto Library)	HW / SW	---
TOE-OSP	Smartcard Operating System Software (implemented in ROM/EEPROM of the microcontroller)	SW	---
TOE-APL	Smartcard Application Software (depending on the TOE's configuration resp. card type, implemented in the EEPROM of the microcontroller)	SW	---
Note: The TOE itself will be delivered as initialised smartcard or as initialised module.			
User Guide Personaliser	User guidance for the Personaliser of the Tachograph Card	DOC	Document in paper / electronic form
User Guide for the Operation of Tachograph Cards	User guidance for the Operation of Tachograph Cards by Issuer and Vehicle Unit Developer	DOC	Document in paper / electronic form
Identification Data Sheet of the Tachograph Card	Data Sheet with information on the actual identification data and configuration of the Tachograph Card delivered to the customer	DOC	Document in paper / electronic form
Aut-Key of the Tachograph Card	Public part of the authentication key pair relevant for the authenticity of the Tachograph Card Note: The card´s authentication key pair is generated by Sagem Orga GmbH and depends on the TOE's configuration delivered to the customer. Furthermore, the key pair may be chosen customer specific.	KEY	Document in paper form / electronic file
Pers-Key of the Tachograph Card	Public part of the personalisation key pair of the Tachograph Card necessary for the personalisation process at the personaliser	KEY	Document in paper form / electronic file

TOE component	Description / Additional Information	Type	Transfer Form
	Note: The card´s personalisation key pair is generated by Sagem Orga GmbH and may depend on the TOE's configuration delivered to the customer. Furthermore, the key pair may be chosen customer specific.		
Pers-Key Pair of the Personalisation Unit (if applicable)	Personalisation key pair for the personalisation unit necessary for the personalisation of the Tachograph Card delivered to the personaliser Note: The personalisation key pair is generated by the personaliser itself or alternatively by Sagem Orga GmbH. In case of a generation at Sagem Orga GmbH, the key pair may depend on the TOE's configuration delivered to the customer and may be chosen customer specific.	KEY PAIR	Document in paper form / electronic file
Static Pers-Key (if applicable)	Static personalisation key for the personalisation unit necessary for the personalisation of the Tachograph Card delivered to the personaliser Note: The static personalisation key is generated by the personaliser itself or alternatively by Sagem Orga GmbH. In case of a generation at Sagem Orga GmbH, the key may depend on the TOE's configuration delivered to the customer and may be chosen customer specific.	KEY	Document in paper form / electronic file

Note: Deliverables in paper form require a personal passing on. For deliverables in electronic form an integrity and authenticity attribute will be attached.

2.2 TOE Life-Cycle

The smartcard product life-cycle of the TOE is decomposed into seven phases. In each of these phases different authorities with specific responsibilities and tasks are involved:

Phase		Description
Phase 1	**Smartcard Embedded Software Development**	The **Smartcard Embedded Software Developer (Sagem Orga GmbH)** is in charge of • the Smartcard Embedded Software (Basic Software, Application Software) development and • the specification of IC initialisation and pre-personalisation requirements (though the actual data for IC initialisation and pre-personalisation come from Phase 4, 5 resp. 6). The purpose of the Embedded Software designed during phase 1 is to control and protect the TOE during phases 4 to 7 (product

		usage).The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases.
Phase 2	**IC Development**	The **IC Designer (NXP Semiconductors GmbH)** • designs the IC, • develops the IC Dedicated Software, • provides information, software or tools to the Smartcard Embedded Software Developer, and • receives the Smartcard Embedded Software (only Basic Software) from the developer through trusted delivery and verification procedures. From the IC design, IC Dedicated Software and Smartcard Embedded Software, the **IC Designer (NXP Semiconductors GmbH)** • constructs the smartcard IC database, necessary for the IC photomask fabrication.
Phase 3	**IC Manufacturing and Testing**	The **IC Manufacturer (NXP Semiconductors GmbH)** is responsible for • producing the IC through three main steps: - IC manufacturing, - IC testing, and - IC pre-personalisation. The **IC Mask Manufacturer (NXP Semiconductors GmbH)** • generates the masks for the IC manufacturing based upon an output from the smartcard IC database.
Phase 4	**IC Packaging and Testing**	The **IC Packaging Manufacturer (Sagem Orga GmbH)** is responsible for • the IC packaging (production of modules) and • testing.
Phase 5	**Smartcard Product Finishing Process**	The **Smartcard Product Manufacturer (Sagem Orga GmbH)** is responsible for • the initialisation of the TOE (in form of initialisation of the modules of phase 4) and • its testing. The smartcard product finishing process comprises the embedding of the initialised modules for the TOE and the card production what is done alternatively by **Sagem Orga GmbH or by the customer.** Independent of the type of the TOE's delivery (initialised module, initialised card), testing of the initialisation process and result is performed by Sagem ORGA prior to the delivery of the product. Final card tests only aim at checking the quality of the card production, in particular concerning the bonding and implantation of the modules.
Phase 6	**Smartcard**	The **Personaliser** is responsible for

	Personalisation	• the smartcard personalisation and • final tests.
Phase 7	**Smartcard End-Usage**	The **Smartcard Issuer** is responsible for • the smartcard product delivery to the smartcard end-user, and the end of life process.

Appropriate procedures for a secure delivery process of the TOE or parts of the TOE under construction from one development resp. production site to another site within the smartcard product life-cycle are established. This concerns any kind of delivery performed from phase 1 to 5, including:

- intermediate delivery of the TOE or parts of the TOE under construction within a phase,
- delivery of the TOE or parts of the TOE under construction from one phase to the next.

In particular, the delivery of the Crypto Library from NXP Semiconductors GmbH to Sagem Orga GmbH follows the dedicated secured delivery process defined in the security evaluations of the NXP Crypto Library on different members of the P5 IC family. The delivery of the ROM mask and the EEPROM pre-personalisation data from Sagem Orga GmbH to NXP Semiconductors GmbH is done by using the dedicated secured delivery procedure specified by NXP Semiconductors GmbH following the so-called NXP Order Entry Form.

The IC manufacturer NXP Semiconductors GmbH delivers the IC with its IC Dedicated Software and the ROM mask supplied by Sagem Orga GmbH at the end of phase 3 in form of. The IC Dedicated Test Software stored in the Test-ROM is disabled before the delivery of the IC and cannot be used in the following phases.

The FabKey procedure described in the security evaluations of IC of the P5 family is replaced by the following procedure which provides at least equivalent security: The TOE's operating system puts in the non-initialised status the command "Verify ROM" at disposal, with which a SHA-1 hash value over the complete ROM and data freely chosen by the external world can be generated. Prior to the initialisation of the IC, the authenticity of the IC with its ROM mask will be proven by using the functionality "Verify ROM" and comparing the new generated hash value over the ROM data and the data freely chosen with a corresponding external reference value which is accessible only for Sagem Orga GmbH.

With regard to the smartcard product life-cycle of the MICARDO product described above, the different development and production phases of the TOE with its IC incl. its IC Dedicated Software and with its Smartcard Embedded Software (Basic Software, Application Software) are part of the evaluation of the TOE. Two different ways for the delivery of the TOE are established:

- The TOE is delivered at the end of phase 5 in form of complete cards, i.e. after the initialisation process of the TOE has been successfully finished, final tests have been successfully conducted and the card production has been fulfilled.
- Alternatively, the TOE is delivered in form of initialised and tested modules. In this case, the smartcard finishing process (embedding of the delivered modules, final card tests) is task of the customer.

2.3 TOE Environment

Considering the TOE and its life-cycle described above, four types of environments can be distinguished:

- development environment corresponding to phase 1 and 2,
- production environment corresponding to phase 3 to phase 5,
- personalisation environment corresponding to phase 6,
- end-user environment corresponding to phase 7.

2.3.1 Development Environment

Phase 1 - Smartcard Embedded Software Development

To assure security of the development process of the Smartcard Embedded Software, a secure development environment with appropriate personnel, organisational and technical security measures at Sagem Orga GmbH is established.

Only authorized and experienced personnel which understands the importance and the rigid implementation of the defined security procedures is involved in the development activities.

The development process comprises the specification, the design, the coding and the testing of the Smartcard Embedded Software. For design, implementation and test purposes secure computer systems preventing unauthorized access are used. For security reasons the coding and testing activities will be done independently of each other.

All sensitive documentation, data and material concerning the development process of the Smartcard Embedded Software are handled in an appropriately and sufficiently secure way. This concerns both the transfer as well as the storing of all related sensitive documents, data and material. Furthermore, all development activities run under a configuration control system which guarantees for an appropriate traceability and accountability.

The Smartcard Embedded Software of the developer, more precise the Basic Software part dedicated for the ROM of the IC, is delivered to the IC manufacturer through trusted delivery and verification procedures. The Application Software and additional parts of the Basic Software are delivered in form of a cryptographically secured initialisation file as well through trusted delivery and verification procedures to the initialisation center.

Phase 2 – IC Development

During the design and layout process only people involved in the specific development project for the IC have access to sensitive data. Different people are responsible for the design data of the IC and for customer related data. The security measures installed at NXP Semiconductors GmbH ensure a secure computer system and provide appropriate equipment for the different development tasks.

2.3.2 Production Environment

Phase 3 - IC Manufacturing and Testing

The verified layout data are provided by the developers of NXP Semiconductors GmbH directly to the wafer fab. The wafer fab generates and forwards the layout data related to the relevant photomask to the IC mask manufacturer (NXP Semiconductors GmbH).

The photomask is generated off-site and verified against the design data of the development before usage. The accountability and traceability is ensured among the wafer fab and the photomask provider.

The production of the wafers includes two different steps regarding the production flow. In the first step the wafers are produced with the fixed mask independent of the customer. After that step the wafers are completed with the customer specific mask and the remaining mask. The computer tracking ensures the control of the complete process including the storage of the semifinished wafers.

The test process of every die is performed by a test centre of NXP Semiconductors GmbH.

Delivery processes between the involved NXP Semiconductors GmbH sites provide accountability and traceability of the produced wafers. The delivery of the ICs from NXP Semiconductors GmbH to Sagem Orga GmbH is made in form of wafers whereby non-functional ICs are marked on the wafer.

Phase 4 – IC Packaging and Testing

For security reasons the processes of IC packaging and testing at Sagem Orga GmbH are done in a secure environment with adequate personnel, organisational and technical security measures.

Only authorized and experienced personnel which understands the importance and the rigid implementation of the defined security procedures is involved in these activities.

All sensitive material and documentation concerning the production process of the TOE is handled in an appropriately and sufficiently secure way. This concerns both the transfer as well as the storing of all related sensitive material and documentation. All operations are done in such a way that appropriate traceability and accountability exist.

Phase 5 - Smartcard Product Finishing Process

To assure security of the initialisation process of the TOE, a secure environment with adequate personnel, organisational and technical security measures at Sagem Orga GmbH is established.

Only authorized and experienced personnel which understands the importance and the rigid implementation of the defined security procedures is involved in the initialisation and test activities.

The initialisation process of the TOE comprises the loading of the TOE's Application Software and the remaining EEPROM-parts of the TOE's Basic Software which have been specified, coded, tested and cryptographically secured in phase 1 of the product life-cycle. The TOE allows only the initialisation of the intended initialisation file with its Application Software and its parts of the Basic Software. For security reasons, secure systems within a separate network and preventing unauthorized access are used for the initialisation process.

If the TOE is delivered in form of initialised and tested modules, the smartcard finishing process, i.e. the embedding of the delivered modules and final tests, is task of the customer.

Otherwise, the smartcard finishing process is part of the production process at Sagem Orga GmbH, and the TOE is delivered in form of complete (initialised) cards.

All sensitive documentation, data and material concerning the production processes of the TOE at Sagem Orga GmbH within phase 5 are handled in an appropriately and sufficiently secure way. This concerns both the transfer as well as the storing of all related sensitive documents, data and material. Furthermore, all operations run under a control system which supplies appropriate traceability and accountability.

At the end of this phase, the TOE is complete as smartcard and can be supplied for delivery to the personalisation centre for personalisation.

2.3.3 Personalisation Environment

Note: The phases from the TOE delivery at the end of phase 5 to phase 7 in the smartcard product life-cycle are not part of theTOE development and production process in the sense of this Security Target. Information about the phases 6 and 7 are just included to describe how the TOE is used after its development and production. The development and production of the TOE are done in such a way that the security features of the TOE are independent of the user data loaded during the TOE's personalisation and cannot be disabled by the personalisation data in the phases afterwards.

Phase 6 - Smartcard Personalisation

The security of the personalisation process of the TOE is supported by the TOE and its Application Software itself. The following personalisation schemes are provided by the Tachograph Card:

- Dynamic scheme with Secure Messaging using a session key:

  The TOE allows a personalisation only after a successful preceding mutual authentication between the TOE and the external world with agreement of a session key and send sequence counter. The authentication protocol follows the procedure described in the Tachograph Card Specification /TachAn1B/, Appendix 11, chap. 4 and makes use of asymmetric keys. The keys necessary on the card for the authentication procedure, i.e. the public key of the personalisation unit and the personalisation key pair of the card, are part of the Application Software (Tachograph Application) and are loaded onto the card in the framework of the initialisation. The following data transfer of the personalisation data has to be conducted with Secure Messaging according to /TachAn1B/, Appendix 11, chap. 5 using the session key and send sequence counter negotiated during the preceding authentication process.

- Static scheme with Secure Messaging using a static key:

  The TOE allows a personalisation only under usage of a static symmetric personalisation key which is stored on the card during the initialisation of the card or later within an additional pre-personalisation phase. In the latter case, the symmetric personalisation key has to be loaded with a specific card command in encrypted form (using the public key of the card´s asymmetric personalisation key pair stored during initialisation). The data transfer of the personalisation data has to be conducted with Secure Messaging according to /TachAn1B/, Appendix 11, chap. 5 using the static personalisation key (and the send sequence counter set by the card). Usage of the static personalisation key for securing the data transfer of the personalisation data is only possible after a successful preceding external authentication of the external world (personalisation unit).

In each case, the personalisation of the Tachograph Card requires a preceding authentication of the external world (personalisation unit). Key material necessary for securing the personalisation process is delivered by Sagem Orga GmbH, if applicable, in a trusted manner.

The personalisation schemes permitted by the delivered configuration of the Tachograph Card are set up within the Tachograph Application and are defined in the framework of the generation of the Tachograph Application within phase 1 of the product life-cycle.

The establishment of a secure environment for the personalisation process with adequate personnel, organisational and technical security measures is in the responsibility of the personalisation centre itself. Furthermore, the secure key management and handling of the cryptographic keys for securing the data transfer within the personalisation process and the secure handling of the personalisation data itself is task of the external world resp. the personalisation centre.

2.3.4 End-User Environment

Phase 7 – Smartcard End-usage

The TOE after its personalisation is destinated for use in the Tachograph System as a security medium and data carrier for different user types which is secured against forgery and tampering. For further details concerning the use of the Tachograph Card refer to chap. 2.4.

The TOE is constructed in such a manner that it implements all security requirements of the Tachograph Card Specification /TachAn1B/. There is no possibility, even in an unsecure end-user environment, to disable or to circumvent the security features of the TOE.

2.4 TOE Intended Usage

In this section, the intended usage of the TOE within the end-usage phase of the product life-cycle (phase 7), i.e. in personalised form will be considered more detailed.

According to the Tachograph Card Specification /TachAn1B/ and the interpretations in /JILDigTacho/ a Tachograph Card is defined as a smartcard product compliant to the Protection Profiles /PP9806/ resp. /BSI-PP-IC/ and /PP9911/ and carrying a specific application intended for its use with the recording equipment. Tachograph Cards allow for identification of the identity (or identity group) of the cardholder by the recording equipment and allow for data transfer and storage.

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; identifies the driver and allows for storage of driver activity data
- Control Card:
  a Tachograph Card issued by the authorities of a Member State to a national competent control authority; identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading
- 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; identifies the cardholder and allows for testing, calibration and/or downloading of the recording equipment
- Company Card:
  a Tachograph Card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment; identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company

The basic functions of the Tachograph Card are the following:

- 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

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

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

Regarding the security of the Tachograph System, the system security aims at:

- protecting integrity and authenticity of data exchanged between the cards and the recording equipment
- protecting the integrity and authenticity of data downloaded from the cards
- allowing certain write operations onto the cards to recording equipment only
- ruling out any possibility of falsification of data stored in the cards
- preventing tampering and detecting any attempt of that kind

Especially the following security mechanisms are relevant for the Tachograph Card:

- mutual authentication between a vehicle unit and a Tachograph Card, including session key agreement
- confidentiality, integrity and authentication of data transferred between a vehicle unit and a Tachograph Card
- integrity and authentication of data downloaded from a Tachograph Card to external storage media

The Tachograph Card offers a classical RSA public-key cryptographic system to provide the following security mechanisms:

- authentication between a vehicle unit and a Tachograph Card
- transport of Triple-DES session keys between a vehicle unit and a Tachograph Card
- digital signature of data downloaded from a Tachograph Card to external media

Furthermore, the Tachograph Card offers a Triple DES symmetric cryptographic system to provide a mechanism for data integrity during user data exchange between a vehicle unit and a Tachograph Card, and to provide, where applicable, confidentiality of data exchange between a vehicle unit and a Tachograph Card.

3 TOE Security Environment

3.1 Assets

Assets are security–relevant elements to be directly protected by the TOE whereby assets have to be protected in terms of confidentiality and integrity. Confidentiality of assets is always intended with respect to untrusted users of the TOE and its security-critical components, whereas the integrity of assets is relevant for the correct operation of the TOE and its security-critical components.

The confidentiality of the code of the TOE is included in this ST for several reasons. Firstly, the confidentiality is needed for the protection of intellectual/industrial property on security or effectiveness mechanisms. Secondly, though protection shall not rely exclusively on code confidentiality, disclosure of the code may weaken the security of the involved application. For instance, knowledge about the implementation of the operating system or the Tachograph Application itself may benefit an attacker. This also applies to internal data of the TOE, which may similarly provide leads for further attacks.

For a description of the TOE's assets refer to /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target), /PP9911/, chap. 3.1, /BSI-PP-IC/, chap. 3.1, /ST_IC/, chap. 3.1. The assets of the TOE sorted in primary and seconday assets are listed in the tables below:

Primary Assets	
Part of the TOE	**Definition**
IC	---
Smartcard Embedded Software / Basic Software	---
Smartcard Embedded Software / Application Software	- application specific user data (refer to /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 2.2) as - identification data (card identification data, cardholder identification data) - activity data (cardholder activities data, events and faults data, control activity data)

Secondary Assets	
Part of the TOE	**Definition**
IC	- logical design data - physical design data - IC Dedicated Software - initialisation data - pre-personalisation data - specific development aids - test and characterisation related data - material for software development support - photomasks - the special functions for the communication with an external interface device - the cryptographic co-processor for Triple-DES - the FameX co-processor for basic arithmetic functions to perform asymmetric cryptographic algorithms - the random number generator - TSF data
Smartcard Embedded Software / Basic Software	- specifications - code - related documentation - system specific data - initialisation data - specific development aids - test and characterisation related data - material for software development support - TSF data
Smartcard Embedded Software / Application Software	- specifications - code - related documentation - system specific data - initialisation data - specific development aids - test and characterisation related data - material for software development support - user data related documentation - TSF data, especially the application specific security data (refer to /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 2.2)

3.2 Assumptions

3.2.1 General Assumptions for the TOE

The general assumptions made on the environment of the TOE are defined according to /PP9911/, chap. 3.2 and are suitably supplemented for the TOE. The complete set of assumptions is listed in the table below.

Note:

In the following table, items of /PP9911/ which are common with /PP9806/ are indicated by a "*".

Assumptions for the Environment of the TOE	
Name	**Definition**
Assumptions on Phase 1 to 5	
A.DEV_ORG* (PP9911+supplement)	**Protection of the TOE under Development and Production** Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity of the Smartcard Embedded Software (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation ...) shall exist and be applied in software development. All authorities involved in the development and production of the TOE shall carry out their development and production activities in a suitable and secure environment. Each party has to ensure that the development and production of the TOE (incl. IC with its Dedicated Software, Smartcard Embedded Software) is secure so that no information is unintentionally made available for the later operational phase of the TOE. In particular, the confidentiality and integrity of design information and test data shall be guaranteed, access to development and test tools, samples and other sensitive material shall be restricted to authorised persons only etc.
Assumptions on the TOE Delivery Process (Phases 4 to 7)	
A.DLV_PROTECT* (PP9911)	**Protection of the TOE under Delivery and Storage** Procedures shall ensure protection of TOE material / information under delivery and storage.
A.DLV_AUDIT* (PP9911)	**Audit of Delivery and Storage** Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

A.DLV_RESP* (PP9911)	**Responsibility within Delivery** Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.
Assumptions on Phases 4 to 6	
A.USE_TEST* (PP9911)	**Testing of the TOE** It is assumed that appropriate functionality testing of the TOE is used in phases 4, 5 and 6.
A.USE_PROD* (PP9911)	**Protection of the TOE under Testing and Manufacturing** It is assumed that security procedures are used during all manufacturing and test operations through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).
Assumptions on Phase 6	
A.PERS	The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE handles the personalisation data in an adequate secure manner. This concerns especially the security data to be personalised as secret cryptographic keys and PINs. The storage of the personalisation data at the originator and at the personalisation center as well as the transfer of these data between the different sites is conducted with respect to data integrity and confidentiality. Furthermore, the personalisation center treats the data for securing the personalisation process, i.e. the personalisation keys suitably secure. It is in the responsibility of the originator of the personalisation data to garantuee for a sufficient quality of the personalisation data, especially of the cryptographic material to be personalised. The preparation and securing of the personalisation data appropriate to the Tachograph Card´s structure and according to the TOE's personalisation requirements is as well in the responsibility of the external world and is done with care.
Assumptions on Phase 7	
A.USE_DIAG* (PP9911)	**Secure Communication** It is assumed that secure communication protocols and procedures are used between smartcard and terminal.

3.2.2 Tachograph Card Specific Assumptions for the TOE

There do not exist any Tachograph Card specific assumptions for the environment of the TOE.

3.3 Threats

The TOE is required to counter different type of attacks against its specific assets. A threat agent could try to threaten these assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

Generally, threats can be split into the following types:

- threats against which a specific protection by the TOE is required
- threats against which a specific protection by the environment is required
- threats against which a specific protection by a combination of the TOE and the environment is required

Before listing the general threats for the TOE, several preliminary remarks about these threats:

<u>Threats on phase 1</u>

During phase 1, three types of threats have to be considered:

- threats on the TOE-ES and its development environment, such as unauthorized disclosure, modification or theft of the TOE-ES and/or initialisation data
- threats on the assets transmitted from the IC designer to the TOE-ES developer during the TOE-ES development
- threats on the TOE-ES and initialisation data transmitted during the delivery process from the TOE-ES software developer to the IC designer

Furthermore, one can consider the threats under the aspect of disclosure, theft, use or modification:

- Unauthorized disclosure of assets:

  This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

- Theft or unauthorized use of assets:

  Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such an attacker may personalize, modify or influence the product in order to gain access to the smartcard application system.

- Unauthorized modification of assets:

  The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threats includes the implementation of malicious Trojan horses.

Threats on delivery from phase 1 to phases 4 to 6

Threats on data transmitted during the delivery process from the TOE-ES developer to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.

Threats on phases 4 to 7

During these phases, the assumed threats could be divided in three types:

- Unauthorized disclosure of assets:

  This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.
- Theft or unauthorized use of assets:

  Potential attackers may gain access to the TOE and perform operation for which they are not allowed. For example, such attackers may personalize the product in an unauthorized manner, or try to gain fraudulently access to the smartcard system.
- Unauthorized modification of assets:

  The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threat includes the implementation of malicious Trojan horses, Trapdoors, downloading of viruses or unauthorized programs.

3.3.1 Threats of the IC (TOE-IC)

For the definition of the threats related to the TOE-IC refer to /BSI-PP-IC/, chap. 3.3, /ST_IC/, chap. 3.3 and /ST_IC_CL/, chap. 3.3. Here, only the threats concerning phase 7 of the product life-cycle are considered.

3.3.2 General Threats of the Smartcard Embedded Software (TOE-ES)

The table below lists the general threats to the assets of the TOE-ES against which specific protection within the TOE or its environment is required. Several groups of threats are distinguished according to the means used in the attack and to the phases of the TOE that are affected. The threats to the TOE-ES are defined as indicated in /PP9911/, chap. 3.3.

Note:

In the following table, items of /PP9911/ which are common with /PP9806/ are indicated by a "*".

Threats / TOE-ES	
Name	**Definition**
Threats on all Phases	
T.CLON* (PP9911)	**Cloning of the TOE** Unauthorized full or partional functional cloning of the TOE. Note: This threat is derived from specific threats combining unauthorized disclosure, modification or theft of assets at different phases.
Threats on Phase 1	
T.DIS_INFO* (PP9911)	**Disclosure of IC Assets** Unauthorized disclosure of the assets delivered by the IC designer to the Smartcard Embedded Software developer, such as sensitive information on IC specification, design and technology, software and tools if applicable.
T.DIS_DEL* (PP9911)	**Disclosure of the Smartcard Embedded Software / Application Data during Delivery** Unauthorized disclosure of the Smartcard Embedded Software and any additional application data (such as IC Pre-personalization requirements) during the delivery from the Smartcard Embedded Software developer to the IC designer.
T.DIS_ES1 (PP9911)	**Disclosure of the Smartcard Embedded Software / Application Data within the Development Environment** Unauthorized disclosure of the Smartcard Embedded Software (technical or detailed specifications, implementation code) and/or Application Data (such as secrets, or control parameters for protection system, specification and implementation for security mechanisms) within the development environment.
T.DIS_TEST_ES (PP9911)	**Disclosure of Smartcard Embedded Software Test Programs / Information** Unauthorized disclosure of the the Smartcard Embedded Software test programs or any related information.
T.T_DEL* (PP9911)	**Theft of the Smartcard Embedded Software / Application Data during Delivery** Theft of the Smartcard Embedded Software and any additional application data (such as pre-personalization requirements) during the delivery process from the Smartcard Embedded Software developer to the IC designer.
T.T_TOOLS (PP9911)	**Theft or Unauthorized Use of the Smartcard Embedded Software Development Tools**

	Theft or unauthorized use of the Smartcard Embedded Software development tools (such as PC, development software, data bases).
T.T_SAMPLE2 (PP9911)	**Theft or Unauthorized Use of TOE Samples** Theft or unauthorized use of TOE samples (e.g. bond-out chips with the Smartcard Embedded Software).
T_MOD_DEL* (PP9911)	**Modification of the Smartcard Embedded Software / Application Data during Delivery** Unauthorized modification of the Smartcard Embedded Software and any additional application data (such as IC prepersonalization requirements) during the delivery process from the Smartcard Embedded Software developer to the IC designer.
T.MOD (PP9911)	**Modification of the Smartcard Embedded Software / Application Data within the Development Environment** Unauthorized modification of the Smartcard Embedded Software and/or Application Data or any related information (technical specifications) within the development environment.
Threats on Delivery from Phase 1 to Phases 4 / 5 / 6	
T.DIS_DEL1 (PP9911)	**Disclosure of Application Data during Delivery** Unauthorized disclosure of Application Data during delivery from the Smartcard Embedded Software developer to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.
T.DIS_DEL2 (PP9911)	**Disclosure of Delivered Application Data** Unauthorized disclosure of Application Data delivered from the Smartcard Embedded Software developer to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.
T.MOD_DEL1 (PP9911)	**Modification of Application Data during Delivery** Unauthorized modification of Application Data during delivery from the Smartcard Embedded Software developer to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.
T.MOD_DEL2 (PP9911)	**Modification of Delivered Application Data** Unauthorized modification of Application Data delivered from the Smartcard Embedded Software developer to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.
Threats on Phases 4 to 7	
T.DIS_ES2	**Disclosure of the Smartcard Embedded Software / Application Data**

(PP9911)	Unauthorized disclosure of the Smartcard Embedded Software and Application Data (such as data protection systems, memory partitioning, cryptographic programs and keys).
T.T_ES (PP9911)	**Theft or Unauthorized Use of TOE** Theft or unauthorized use of the TOE (e.g. bound out chips with the Smartcard Embedded Software).
T.T_CMD (PP9911)	**Use of TOE Command-Set** Unauthorized use of instructions or commands or sequence of commands sent to the TOE.
T.MOD_LOAD (PP9911)	**Program Loading** Unauthorized loading of programs.
T.MOD_EXE (PP9911)	**Program Execution** Unauthorized execution of programs.
T.MOD_SHARE (PP9911)	**Modification of Program Behavior** Unauthorized modification of program behavior by interaction of different programs.
T.MOD_SOFT* (PP9911)	**Modification of Smartcard Embedded Software / Application Data** Unauthorized modification of the Smartcard Embedded Software and Application Data.

3.3.3 Tachograph Card Specific Threats

The following table lists the specific threats relevant for the Tachograph Application within the TOE-ES. The threats are provided by the Tachograph Card Specification /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 3.3 and are supplemented for the TOE's personalisation.

Threats / TOE-ES (Tachograph Card Specific Threats)	
Name	**Definition**
T.Ident_Data	**Modification of Identification Data** A successful modification of identification data held by the TOE (e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.
T.Activity_Data	**Modification of Activity Data**

	A successful modification of activity data stored in the TOE would be a threat to the security of the TOE.
T.Data_ex-change	**Modification of Activity Data during Data Transfer** A successful modification of activity data (addition, deletion, modification) during import or export would be a threat to the security of the TOE.
T.Pers_Data	**Authentication for Personalisation** A successful storage of personalisation data without authorisation (of the external world) would be a threat to the security of the TOE.
T.Pers_ex-change	**Modification or Disclosure of Personalisation Data during Data Transfer** A successful modification or disclosure of personalisation data during data import would be a threat to the security of the TOE.

3.4 Organisational Security Policies of the TOE

The TOE reaches is specific security functionality only by a correct and effective implementation of the underlying IC and its security functionality by the Smartcard Embedded Software (TOE-ES). In particular this means, that the TOE-ES must fulfill the assumptions for the TOE-ES as defined in the Security Target for the TOE-IC.

The relevant assumptions for the TOE-ES as given in /ST_IC_CL/, chap. 3.2 (refer also to /ST_IC/, chap. 3.2 and /BSI-PP-IC/, chap. 3.2) are suitably redefined in terms of Organisational Security Policies for the TOE as follows:

Organisational Security Policy for the TOE	
Name	**Definition**
P.Process-Card (A.Process-Card in ST-IC)	**Protection during Packaging, Finishing and Personalisation** Security procedures shall be used after TOE-IC delivery up to delivery to the end-user to maintain confidentiality and integrity of the TOE-IC and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
P.Design-Software (A.Plat-Appl, A.Resp-Appl, A.Check-Init, A.Key-Function, in ST-IC)	**Design of the Smartcard Embedded Software** To ensure that the TOE-IC is used in a secure manner the Smartcard Embedded Software (TOE-ES) shall be designed so that the requirements from the following documents are met: - hardware data sheet for the TOE-IC, - TOE-IC application notes, Security relevant user data (especially cryptographic keys) are treated by the Smartcard Embedded Software (TOE-ES) as required by the security needs of

	the specific application context. For example the Smartcard Embedded Software (TOE-ES) will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal. The Smartcard Embedded Software shall provide a function to check initialisation data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability. The check shall include at least the Fabkey Data that is agreed between the TOE-ES developer and the TOE-IC Manufacturer. Key-dependent functions shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks.

4 Security Objectives

4.1 Security Objectives for the TOE

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

- integrity and confidentiality of the TOE's assets
- protection of the TOE and its associated documentation and environment during the development and production phases.

4.1.1 Security Objectives for the TOE-IC

For the definition of the security objectives related to the TOE-IC refer to /BSI-PP-IC/, chap. 4.1, /ST_IC/, chap. 4.1 and /ST_IC_CL/, chap.4.1. Here, only the security objectives concerning phase 7 of the product life-cycle are considered.

4.1.2 General Security Objectives for the TOE-ES

Nearly all security objectives mentioned in the table below concern the general security objectives for the TOE-ES as defined in /PP9911/, chap. 4.1. These security objectives are supplemented by security objectives drawn from /BSI-PP-IC/, chap. 4.2, /ST_IC/, chap. 4.2 and /ST_IC_CL/, chap. 4.2, which will be in the current scope switched from assumptions resp. security objectives for the environment of the IC to security objectives for the TOE-ES. The complete set of security objectives for the TOE-ES is listed in the table below.

Note:

For clarity, within the description of the security objectives in the following table as indicated in /BSI-PP-IC/, /ST_IC/ resp. /ST_IC_CL/ the word „TOE“ is replaced by „TOE-IC“ and the term „Smartcard Embedded Software“ is supplemented by „TOE-ES“.

Note:

In the following table, items of /PP9911/ which are common with /PP9806/ are indicated by a “*”.

Security Objectives / TOE-ES	
Name	**Definition**
O.CLON* (PP9911)	**Cloning** The TOE functionality must be protected from cloning.
O.OPERATE* (PP9911)	**Correct Operation**

	The TOE must ensure continued correct operation of its security functions.
O.FLAW* (PP9911)	**Flaws** The TOE must not contain flaws in design, implementation or operation.
O.DIS_MEMORY* (PP9911)	**Disclosure of Memory Contents** The TOE shall ensure that sensitive information stored in memories is protected against unauthorized disclosure.
O.MOD_MEMORY* (PP9911)	**Modification of Memory Contents** The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.
O.TAMPER_ES (PP9911)	**Tampering of the Smartcard Embedded Software** The TOE must prevent tampering with its security critical parts. Security mechanisms have especially to prevent the unauthorized change of functional parameters, security attributes and secrets such as the life cycle sequence flags and cryptographic keys. The Smartcard Embedded Software must be designed to avoid interpretations of electrical signals from the hardware part of the TOE.
O.DIS_MECHANISM2 (PP9911)	**Disclosure of Security Mechanisms of the Smartcard Embedded Software** The TOE shall ensure that the Smartcard Embedded Software security mechanisms are protected against unauthorized disclosure.
O.Plat-Appl (OE.Plat-Appl in ST_IC)	**Usage of Hardware Platform** To ensure that the TOE-IC is used in a secure manner the Smartcard Embedded Software (TOE-ES) shall be designed so that the requirements from the following documents are met: - hardware data sheet for the TOE-IC, - TOE-IC application notes,
O.Resp-Appl (OE.Resp-Appl in ST_IC)	**Treatment of User Data** Security relevant user data (especially cryptographic keys) shall be treated by the Smartcard Embedded Software (TOE-ES) as required by the security needs of the specific application context. For example the Smartcard Embedded Software (TOE-ES) shall not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.
O.Check-Init (OE.Check-Init in ST_IC)	**Check of initialisation data by the Smartcard Embedded Software** To ensure the receipt of the correct TOE-IC, the Smartcard Embedded Software (TOE-ES) shall provide a function to check initialisation data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability. The check shall include at least the Fabkey Data that is agreed between the TOE-ES developer and the TOE-IC Manufacturer.
O.Key-Function (A.Key-Function in ST_IC)	**Usage of Key-dependent Functions** Key-dependent functions shall be implemented in the Smartcard Embedded Software (TOE-ES) in a way that they are not susceptible to leakage attacks.

4.1.3 Tachograph Card Specific Security Objectives

The following table lists the specific security objectives relevant for the Tachograph Application. The security objectives are drawn from the Tachograph Card Specification /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 3.4 and 3.5 and are supplemented by an additional security objective for the personalisation of the TOE.

Security Objectives / TOE-ES (Tachograph Card Specific Security Objectives)	
Name	**Definition**
O.Card_Identification_Data	**Storage of Identification Data** The TOE must preserve card identification data and cardholder identification data stored during card personalisation process.
O.Card_Activity_-Storage	**Storage of Activity Data** The TOE must preserve user data stored in the card by vehicle units.
O.Data_Access	**User Data Write Access** The TOE must limit user data write access rights to authenticated vehicle units.
O.Pers_Access	**Personalisation Data Write Access (supplement)** The TOE must limit personalisation data write access rights to authenticated personalisation units.
O.Secure_-Communications	**Secure Communications** The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the application.

4.2 Security Objectives for the Environment

4.2.1 General Security Objectives for the Environment of the TOE

Nearly all general security objectives for the environment of the TOE are defined in /PP9911/, chap. 4.2. These security objectives are supplemented by security objectives drawn from /BSI-PP-IC/, chap. 4.2, /ST_IC/, chap. 4.2 and /ST_IC_CL/, chap. 4.2, and a further specific security objective for the TOE's personalisation.

All of these security objectives have to be fulfilled by organisational measures, thus they are security objectives for the Non-IT-Environment of the TOE. Security objectives for the IT-Environment of the TOE are not present.

The complete set of security objectives for the environment is listed in the table below.

Note:

For clarity, within the description of the security objectives in the following table as given in /BSI-PP-IC/, /ST_IC/ resp. /ST_IC_CL/ the word „TOE" is replaced by „TOE-IC" and the term „Smartcard Embedded Software" is supplemented by „TOE-ES".

Note:

In the following table, items of /PP9911/ which are common with /PP9806/ are indicated by a "*".

Security Objectives for the Environment of the TOE	
Name	**Definition**
Objectives on Phase 1	
O.DEV_TOOLS* (PP9911)	**Development Tools for the Smartcard Embedded Software** The Smartcard Embedded Software shall be designed in a secure manner, by using exclusively software development tools (compilers assemblers, linkers, simulators, etc.) and software-hardware integration testing tools (emulators) that will result in the integrity of program and data.
O.DEV_DIS_ES (PP9911)	**Development of the Smartcard Embedded Software** The Smartcard Embedded Software developer shall use established procedures to control storage and usage of the classified development tools and documentation, suitable to maintain the integrity and the confidentiality of the assets of the TOE. It must be ensured that tools are only delivered and accessible to the parties authorized personnel. It must be ensured that confidential information on defined assets are only delivered to the parties authorized personnel on a need to know basis.
O.SOFT_DLV* (PP9911)	**Protection of the Delivery of the Smartcard Embedded Software** The Smartcard Embedded Software must be delivered from the Smartcard Embedded Software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.
O.INIT_ACS (PP9911)	**Access to Initialisation Data** Initialisation Data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures).
O.SAMPLE_ACS (PP9911)	**Access to Samples**

	Samples used to run tests shall be accessible only by authorized personnel.
Objectives on the TOE Delivery Process (Phases 4 to 7)	
O.DLV_PROTECT* (PP9911)	**Protection of the Delivery of TOE Material / Information** Procedures shall ensure protection of TOE material / information under delivery including the following objectives: - non-disclosure of any security relevant information - identification of the element under delivery - meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgement) - physical protection to prevent external damage - secure storage and handling procedures (including rejected TOE's) - traceability of TOE during delivery including the following parameters: - origin and shipment details - reception, reception acknowledgement - location material/information
O.DLV_AUDIT* (PP9911)	**Audit of Delivery** Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.
O.DLV_RESP* (PP9911)	**Responsibility** Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.
Objectives on Delivery from Phase 1 to Phases 4, 5 and 6	
O.DLV_DATA (PP9911)	**Delivery of Application Data** The Application Data must be delivered from the Smartcard Embedded Software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.
Objectives on Phases 4 to 6	
O.TEST_OPERATE* (PP9911)	**Testing of the TOE** Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE

	and its manufacturing and test data.
O.Process-Card (OE.Process-Card in ST-ICNXP+Lib)	**Protection during Packaging, Finishing and Personalisation** Security procedures shall be used after TOE-IC Delivery up to delivery to the end-user to maintain confidentiality and integrity of the TOE-IC and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
Objectives on Phase 6	
O.PERS	**Maintaining of Personalisation Data** The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE shall handle the personalisation data in an adequate secure manner. This concerns especially the security data to be personalised as secret cryptographic keys and PINs. The storage of the personalisation data at the originator and at the personalisation center as well as the transfer of these data between the different sites shall be conducted with respect to data integrity and confidentiality. Furthermore, the personalisation center shall treat the data for securing the personalisation process, i.e. the personalisation keys suitably secure. It is in the responsibility of the originator of the personalisation data to garantuee for a sufficient quality of the personalisation data, especially of the cryptographic material to be personalised. The preparation and securing of the personalisation data appropriate to the Tachograph Card´s structure and according to the TOE's personalisation requirements is as well in the responsibility of the external world and shall be done with care.
Objectives on Phase 7	
O.USE_DIAG* (PP9911)	**Secure Communication** Secure communication protocols and procedures shall be used between the smartcard and the terminal.

5 IT Security Requirements

5.1 TOE Security Requirements

This section consists of the subsections “TOE Security Functional Requirements” and ”TOE Security Assurance Requirements”.

5.1.1 TOE Security Functional Requirements

The TOE Security Functional Requirements (SFRs) define the functional requirements for the TOE using functional requirement components drawn from /CC 2.3 Part2/, functional requirement components of /CC 2.3 Part2/ with extension as well as self-defined functional requirement components (only for the IC with its IC Dedicated Software). This chapter contains the SFRs concerning the IC (TOE-IC) as far as they are relevant for the composite evaluation as well as the SFRs concerning the Smartcard Embedded Software (TOE-ES).

Note:

The SFRs for the TOE are listed in the following chapters within tables. Thereby, the tables contain in the left column the original definition of the respective SFR and its elements, dependencies, hierarchical information, management and audit functions. The right column supplies the iterations, selections, assignments and refinements chosen for the TOE.

For the SFRs of the TOE-ES, the SFRs are numbered by taking the original name of the SFRs resp. its elements and adding “-x” for the x-th iteration.

The following section gives a survey of the SFRs related to the TOE’s Smartcard Embedded Software as required in the Tachograph Card Specification /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target) and the JIL interpretation /JILDigTacho/, Annex B.

5.1.1.1 Security Function Policies

The Tachograph Card distinguishes between two different phases, more precise between the personalisation phase and the end-usage (operational) phase, each of it with its own Security Function Policy (SFP). The SFPs for these different phases of the Tachograph Card will be described in detail in the following.

For a **non-personalised** Tachograph Card, the TOE-ES maintains a Security Function Policy as defined as follows:

SFP Personalisation Access Control (PERS-AC_SFP)

The SFP PERS-AC_SFP is only relevant for the personalisation phase of the Tachograph Card, i.e. after the initialisation of the card has been completed and no personalisation has been conducted.

Subjects:

- personalisation unit
- other card interface devices

Security attributes for subjects:

- USER_GROUP
  (PERSO_UNIT, NON_PERSO_UNIT)

Objects:

- data fields for user data as:
  - identification data (card identification data, cardholder identification data)
  - activity data (cardholder activities data, events and faults data, control activity data)
- data fields for security data as:
  - card´s signature key pair
  - public keys
  - PIN (only relevant for Workshop Card)
  - static personalisation key (if applicable and if the key is loaded during pre-personalisation)
- security data (loaded during initialisation resp. pre-personalisation or negotiated during personalisation):
  - card´s private personalisation key
  - card´s public personalisation key
  - personalisation unit´s public personalisation key
  - static personalisation key (if applicable)
  - session keys
  - card´s private authentication key
- TOE software code
- TOE file system (incl. file structure, additional internal structures, access conditions)
- identification data of the TOE concerning the IC and the Smartcard Embedded Software
- data field for identification data of the TOE's personalisation concerning the date and time of the personalisation

Security attributes for objects:

Access Rules for:

- data fields for user data
- data fields for security data
- security data
- TOE file system
- identification data of the TOE
- data field for identification data of the TOE’s personalisation

Operations (Access Modes):

- data fields for user data as:
  - identification data: selecting (command Select), writing (command Update Binary)
  - activity data: selecting (command Select), writing (command Update Binary)
- data fields for security data as:
  - card´s signature key pair: loading (command Put Key)
  - public keys: loading (command Put Key)
  - PIN (only relevant for Workshop Card): loading (command Put Key)
  - static personalisation key (if applicable and if the key is loaded during pre-personalisation): loading (command Store Kpers)
- security data:
  - card´s private personalisation key: internal authentication (command Internal Authenticate), external authentication (command External Authenticate), import of static personalisation key (if applicable; command Store Kpers)
  - card´s public personalisation key: referencing over a MSE-command (for further usage within cryptographic operations as authentication)
  - personalisation unit´s public personalisation key: referencing over a MSE-command (for further usage within cryptographic operations as authentication)
  - static personalisation key (if applicable): activating (command Copy Kpers), afterwards securing of personalisation commands with Secure Messaging
  - session keys: securing of personalisation commands with Secure Messaging
  - card´s private authentication key: internal authentication (command Internal Authenticate)
- TOE software code: ---
- TOE file system (incl. file structure, additional internal structures, access conditions): blowing-up the file system for a chosen type of Tachograph Card (command Complete Filesystem)
- identification data of the TOE: selecting (command Select), reading (command Get Data)

- data field for identification data of the TOE's personalisation (date and time of personalisation): selecting (command Select), writing (command Append Record), reading (command Get Data)

The SFP PERS-AC_SFP controls the access of subjects to objects on the basis of security attributes.

The TOE maintains the following **type of security attributes**:

- Access Rule (AR) consisting of one or more Partial Access Rules (PAR) whereat each PAR consists of one Access Mode (AM) and one or more Access Conditions (AC)

The AM indicates the command type for accessing the object. The AC defines the conditions under which a command executed by a subject is allowed to access the object.

The access modes to the above mentioned objects are defined above. Further, the TOE maintains the following **types of elementary ACs**:

- **NEV (Never)**
  The command can never be executed.
- **ALW (Always)**
  The command can be executed without restrictions.
- **AUT (Key based user authentication)**
  The right corresponding to a successful external key based authentication must be opened up (done by the command External Authenticate) before the command can be executed.
- **PWD (Password based user authentication)**
  The right corresponding to a successful password based authentication must be opened up (done by the command Verify PIN) before the command can be executed.
- **SM CMD MAC, SM RSP MAC (Secure Messaging providing data integrity and authenticity for command resp. response)**
  The command must be secured with a cryptographic checksum using Secure Messaging as defined in the Tachograph Card Specification (/TachAn1B/, Appendix 11, chap. 5, Appendix 2, chap. 3.6.2.2, 3.6.3.2).
- **SM CMD ENC, SM RSP ENC (Secure Messaging providing data confidentiality for command resp. response)**
  The command must be secured with an encryption using Secure Messaging as defined in the Tachograph Card Specification (/TachAn1B/, Appendix 11, chap. 5, Appendix 2, chap. 3.6.2.2, 3.6.3.2).
- **OR**
  Boolean OR relation.

For rule decisions, the PERS-AC_SFP uses the actual security status set in the card as reference value.

The PERS-AC_SFP explicitly authorises access of subjects to objects based on the following rules:

- The TSF allows access to an object for a defined access mode, if the object's access condition is valid for this access mode.
- The TSF evaluates within an AC resp. PAR the logical expression of elementary AC elements according to the following rules:
  - AC element NEV is set to "false".
  - AC element AUT is set to "true", if AUT complies with the actual security status (preceding external authentication has been conducted successfully).
  - AC element SM CMD MAC / SM RSP MAC is set to "true", if SM CMD MAC, SM RSP MAC complies with the user indication for SM CMD MAC, SM RSP MAC and SM CMD MAC, SM RSP MAC complies with the actual security status (preceding external authentication has been conducted successfully).
  - AC element SM CMD ENC, SM RSP ENC is set to "true", if SM CMD ENC, SM RSP ENC complies with the user indication for SM CMD ENC, SM RSP ENC and SM CMD ENC, SM RSP ENC complies with the actual security status (preceding external authentication has been conducted successfully).

The SFP PERS-AC_SFP restricts the access of subjects to the **identification data of the TOE** to the commands Select and Get Data. There are no further restrictions for the access to these data areas with identification data of the TOE.

The SFP PERS-AC_SFP restricts the access of subjects to the **data field for identification data of the TOE's personalisation** to the commands Select, Append Record and Get Data. There are no further restrictions for the access to these data areas.

The SFP PERS-AC_SFP controls the access of subjects to **security data,** which are loaded during initialisation (i.e. card´s personalisation key pair, personalisation unit´s public personalisation key, card´s private authentication key, static personalisation key (if applicable and loaded within the initialisation)) resp. during pre-personalisation (static personalisation key, if applicable) or are negotiated during personalisation (session keys) by access rules. Except for the static personalisation key, there are no further restrictions for the execution of the above mentioned access modes concerning these secret data. The usage resp. activation of the static personalisation key is regulated by security attributes as specified below.

The SFP PERS-AC_SFP controls the access of subjects to the **data fields for user data**. Generally, an object of type user data can only be accessed if an access mode exists and an access rule has been attached to the object during its creation. For each type of Tachograph Card the access rules for the different data fields for user data are implemented as follows: The personalisation of the Tachograph Card´s data fields for user data is done by using the access modes selecting and writing whereat Secure Messaging is required. The key used for Secure Messaging is either a session key which is negotiated during a preceding mutual authentication process with the initialised card´s and the personalisation unit´s personalisation keys. Otherwise a static personalisation key is used which is loaded during initialisation or within an additional pre-personalisation phase. In any case, each security relevant personalisation command is combined with the elementary AC elements AUT, PRO SM and ENC SM (logical AND), thus personalisation is only possible with an authenticated personalisation unit and in a secured mode with encryption and MAC-securing using the negotiated session key resp. static personalisation key and a related send sequence counter.

The SFP PERS-AC_SFP controls the access of subjects to the **data fields for security data** for personalisation purposes as follows: The loading of the secrets is only possible with Secure Messaging with the same properties as described above for the personalisation of the data fields for user data. In particular, loading of a static personalisation key after initialisation is either denied or only possible after a preceding external authentication (using the initialised card´s and personalisation unit´s personalisation keys). Furthermore, the loading of the card´s signature key pair is connected in an atomar process with the change of the Tachograph Card´s status from „initialised status“ to „operational status“. Afterwards, the personalisation commands are no longer available, and from now on only the SFP_access_rules (AC_SFP) as loaded in the framework of the initialisation is relevant.

The SFP PERS-AC_SFP controls the access of subjects to the **static personalisation key** for personalisation purposes as follows: The activation of the key is either denied or only possible after a preceding external authentication (using the initialised card´s and personalisation unit´s personalisation keys).

The SFP PERS-AC_SFP controls the access of subjects to the **TOE file system**. Blowing up the file system for a chosen type of Tachograph Card is either denied or only possible after a preceding external authentication (using the initialised card´s and personalisation unit´s personalisation keys).

The access rules for loading and activating a static personalisation key as well as the access rule for blowing up the TOE file system are pre-defined during production of the Tachograph Card and cannot be changed after delivery of the TOE. These access rules allow for a configuration of the TOE (choice of personalisation scheme, choice of file system status at delivery time) .

For a **personalised** Tachograph Card, the TOE-ES maintains a Security Function Policy as defined as follows:

<u>SFP_access_rules (AC_SFP)</u>

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 and the Tachograph Application is in the „operational status“.

Subjects:

- vehicle units (in sense of the Tachograph Card specification)
- other card interface devices (non-vehicle units)

Security attributes for subjects:

- USER_GROUP
  (VEHICLE_UNIT, NON_VEHICLE_UNIT)
- USER_ID
  (Vehicle Registration Number (VRN) and Registering Member State Code (MSC), where USER_ID is only known to USER_GROUP = VEHICLE_UNIT)

Objects:

- user data:
  - identification data (card identification data, cardholder identification data)
  - activity data (cardholder activities data, events and faults data, control activity data)
- security data:
  - card´s private signature key
  - public keys (in particular card´s public signature key; keys stored permanently on the card or imported into the card in form of certificates)
  - session keys
  - PIN (only relevant for Workshop Card)
  - card´s private authentication key
- TOE software code
- TOE file system (incl. file structure, additional internal structures, access conditions)
- identification data of the TOE concerning the IC and the Smartcard Embedded Software
- identification data of the TOE's personalisation concerning the date and time of the personalisation

Security attributes for objects:

Access Rules for:

- user data
- security data
- TOE file system
- identification data of the TOE
- identification data of the TOE's personalisation

Operations (Access Modes):

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

  - card´s private signature key: generation of a digital signature (command PSO Compute Digital Signature), internal authentication (command Internal Authenticate), external authentication (command External Authenticate)
  - public keys (in particular card´s public signature key): referencing over a MSE-command (for further usage within cryptographic operations as authentication, verification of a digital signature etc.)
  - session keys: securing of commands with Secure Messaging
  - PIN (only relevant for Workshop Card): verification (command Verify PIN)
  - card´s private authentication key: internal authentication (command Internal Authenticate)
- TOE software code: ---
- TOE file system (incl. file structure, additional internal structures, access conditions): ---
- identification data of the TOE: selecting (command Select), reading (command Get Data)
- identification data of the TOE's personalisation (date and time of personalisation): selecting (command Select), reading (command Get Data)

The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. A description of the security attributes maintained by the TOE is given above (see SFP PERS-AC_SFP).

For rule decisions, the AC_SFP uses the actual security status set in the card as reference value.

The AC_SFP explicitly authorises access of subjects to objects based on the following rules:

- The TSF allows access to an object for a defined access mode, if the object's access condition is valid for this access mode.
- The TSF evaluates within an AC resp. PAR the logical expression of elementary AC elements according to the following rules:
  - AC element ALW is set to "true".
  - AC element NEV is set to "false".
  - AC element AUT is set to "true", if AUT complies with the actual security status (preceding external authentication has been conducted successfully).
  - AC element PWD is set to "true", if PWD complies with the actual security status (preceding PIN verification has been conducted successfully).
  - AC element SM CMD MAC / SM RSP MAC is set to "true", if SM CMD MAC / SM RSP MAC complies with the user indication for SM CMD MAC / SM RSP MAC and SM CMD MAC / SM RSP MAC complies with the actual security status (preceding external authentication has been conducted successfully).
  - AC element SM CMD ENC / SM RSP ENC is set to "true", if SM CMD ENC / SM RSP ENC complies with the user indication for SM CMD ENC / SM RSP ENC and SM CMD ENC / SM RSP ENC complies with the actual security status (preceding external authentication has been conducted successfully).
- For the command Read Binary, the following special rules hold:

- The TSF allows read access to an object as well in that case, that there does not exist an SM CMD MAC / SM RSP MAC element in the object's AC, but SM CMD MAC / SM RSP MAC is indicated by the user. (The command will then be secured accordingly with Secure Messaging.)

For each type of Tachograph Card the access rules for the different objects and access modes are implemented according to the requirements in the Tachograph Card Specification /TachAn1B/, Appendix 2, chap. 4.

The AC element PWD is only relevant for the Tachograph Card type Workshop Card. For a Workshop Card the actual security status reached by the AC element PWD will be evaluated. 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.

Generally, an object of type **user data** or **security data** can only be accessed if an access mode exists and an access rule has been attached to the object (during its creation). The SFP AC_SFP controls the access of subjects to **user data** and **security data** by access rules.

The SFP AC_SFP restricts the access of subjects to the **identification data of the TOE** to the commands Select and Get Data. There are no further restrictions for the access to these data areas with identification data of the TOE.

The SFP AC_SFP restricts the access of subjects to the **data field for identification data of the TOE's personalisation** to the commands Select and Get Data. There are no further restrictions for the access to this data area.

5.1.1.2 Security Functional Requirements

FAU **Security Audit**	
FAU_SAA **Security Audit Analysis**	
FAU_SAA.1 **Potential Violation Analysis**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.5
FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. **FAU_SAA.1.2** The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation; b) [assignment: *any other rules*].	**FAU_SAA.1-1:** **FAU_SAA.1.1-1** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. **FAU_SAA.1.2-1** The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [- **cardholder authentication failure (5 consecu-**

Hierarchical to: No other components Dependencies: - FAU_GEN.1 Audit data generation Management: a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules Audit: a) Minimal: Enabling and disabling of any of the analysis mechanisms b) Minimal: Automated responses performed by the tool	**tive unsuccessful PIN checks),** - **self test error,** - **stored data integrity error,** - **activity data input integrity error** - **error in the framework of securing of data exchange (concerning data integrity and / or data confidentiality)** - **software / hardware failure**] known to indicate a potential security violation; b) [**none**]. Hierarchical to: No other components Dependencies: Not applicable Management: Not applicable

FCO **Communication**	
FCO_NRO **Non-Repudiation of Origin**	
FCO_NRO.1 **Selective Proof of Origin**	TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.8.2
FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the [selection: *originator, recipient,* [assignment: *list of third parties*]]. **FCO_NRO.1.2** The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] 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 [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*]. Hierarchical to: No other components Dependencies: - FIA_UID.1 Timing of identification	**FCO_NRO.1-1:** **FCO_NRO.1.1-1** The TSF shall be able to generate evidence of origin for transmitted [**user data (download function)**] at the request of the [**recipient**]. **Refinement** DEX_304: The TOE shall be able to generate an evidence of origin for data downloaded to external media. **FCO_NRO.1.2-1** The TSF shall be able to relate the [**card identity given by the card´s specific private signature key**] of the originator of the information, and the [**hash value of the data area of the currently selected transparent elementary file**] of the information to which the evidence applies. **Refinement** DEX_306: The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be veri-

Management: a) The management of changes to information types, fields, originator attributes and recipients of evidence. Audit: a) Minimal: The identity of the user who requested that evidence of origin would be generated. b) Minimal: The invocation of the non-repudiation service. c) Basic: Identification of the information, the destination, and a copy of the evidence provided. d) Detailed: The identity of the user who requested a verification of the evidence.	fied. **FCO_NRO.1.3-1** The TSF shall provide a capability to verify the evidence of origin of information to [**the recipient**] given [**no limitation**]. **Refinement** DEX_305: The TOE shall be able to provide a capability to verify the evidence of origin of downloaded data to the recipient. Hierarchical to: No other components Dependencies: - FIA_UID.1-1 Timing of identification Management: Not applicable

FCS **Cryptographic Support**	
FCS_CKM **Cryptographic Key Management**	
FCS_CKM.1 **Cryptographic Key Generation**	TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.9
FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)	**FCS_CKM.1/SM:** **FCS_CKM.1.1/SM** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**generation of a 2TDES session key**] and specified cryptographic key sizes [**of double length (128 bits with 112 effective bits, no parity bits set)**] that meet the following: [- **ISO/IEC 9798-3 Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 2: Entity Authentication Using a Public Key Algorithm, Second Edition 1998** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.1.3 (CSM_012), 3.2 (CSM_015), 4 (CSM_020)**]. **Refinement** CSP_301: If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic

Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	key sizes. (...) Hierarchical to: No other components Dependencies: - [FCS_CKM.2-1 Cryptographic key distribution] - FCS_CKM.4/SMFCS_CKM.4/SM Cryptographic key destruction Management: Not applicable
FCS_CKM.2 **Cryptographic Key Distribution**	TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.9
FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components 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 - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	**FCS_CKM.2-1:** **FCS_CKM.2.1-1** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**3-DES session key agreement (with send sequence counter) by an internal-external authentication mechanism**] that meets the following: [- **ISO/IEC 9798-3 Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 2: Entity Authentication Using a Public Key Algorithm, Second Edition 1998** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.1.3 (CSM_012), 4 (CSM_020), Appendix 2, chap. 3.6.8, 3.6.9**]. **Refinement** CSP_302: If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods. Hierarchical to: No other components Dependencies: - [FCS_CKM.1/SM Cryptographic key generation] - FCS_CKM.4/SMFCS_CKM.4/SM Cryptographic key destruction Management: Not applicable
	FCS_CKM.2-2: **FCS_CKM.2.1-2** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**import of public RSA-keys by certificates (non self-descriptive card verifiable certificates in**

	conformance with ISO/IEC 7816-8)] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.3, esp. 3.3.1 (CSM_017), 3.3.2 (CSM_018) and 3.3.3 (CSM_019), Appendix 2, chap. 3.6.7 (esp. TCS_346)**]. **Refinement** CSP_302: If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/RSA Cryptographic key destruction Management: Not applicable
	FCS_CKM.2-3: **FCS_CKM.2.1-3** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**import of a static 3-DES key**] that meets the following: [- **Cryptographically secured import (encryption using the public part of a dedicated RSA-key pair of the card)**]. **Refinement** CSP_302: If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/SM Cryptographic key destruction Management: Not applicable
FCS_CKM.3 **Cryptographic Key Access**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.9
FCS_CKM.3.1	**FCS_CKM.3-1:**

The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components 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 - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	**FCS_CKM.3.1-1** The TSF shall perform [**the access to a private RSA-key for the generation of a digital signature**] in accordance with a specified cryptographic key access method [**access to the key by its implicitly known reference within the execution of the command PSO Compute Digital Signature resp. the command Internal Authenticate**] that meets the following: [- **Tachograph Card specification,** /TachAn1B/ **Appendix 2, chap. 3.6.13 (TCS_373), 3.6.8 (TCS_350)**]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] Management: Not applicable
	FCS_CKM.3-2: **FCS_CKM.3.1-2** The TSF shall perform [**the access to a public RSA-key for the verification of a digital signature**] in accordance with a specified cryptographic key access method [**access to the key by its reference explicitly set before within the execution of the command PSO Verify Digital Signature resp. the command External Authenticate resp. the command PSO Verify Certificate**] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 2, chap. 3.6.14 (TCS_377), 3.6.9 (TCS_355), 3.6.7 (TCS_347)**]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/RSA Cryptographic key destruction Management:

	Not applicable
	FCS_CKM.3-3: **FCS_CKM.3.1-3** The TSF shall perform [**the access to a private RSA-key for the decryption operation**] in accordance with a specified cryptographic key access method [**access to the key by its implicitly known reference within the execution of the command External Authenticate resp. the command Store Kpers**] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 2, 3.6.9 (TCS_355)** - **PKCS#1 V2.0 (RSA primitive for decryption)**]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] Management: Not applicable
	FCS_CKM.3-4: **FCS_CKM.3.1-4** The TSF shall perform [**the access to a public RSA-key for the encryption operation**] in accordance with a specified cryptographic key access method [**access to the key by its reference explicitly set before within the execution of the command Internal Authenticate**] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 2, chap. 3.6.8 (TCS_350)** - **PKCS#1 V2.0 (RSA primitive for encryption)**]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/RSA Cryptographic key destruction Management: Not applicable
	FCS_CKM.3-5: **FCS_CKM.3.1-5** The TSF shall perform [**the encryption, decryption, MAC generation and MAC verification operations**

	with a 3-DES session key resp. with a static 3-DES key for Secure Messaging] in accordance with a specified cryptographic key access method [**access to the session key resp. static key by its reference implicit set by the card before within the execution of the command Read Binary resp. the command Update Binary, if Secure Messaging is required**] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.1.3 (CSM_013), Appendix 2, chap. 3.6.2.2, 3.6.3.2**]. **Refinement** CSP_301: (...) Generated cryptographic session keys shall have a limited (TBD by manufacturer and not more than 240) number of possible use. Hierarchical to: No other components Dependencies: - [FCS_CKM.1/SM Cryptographic key generation] (for session key), [FDP_ITC.1-1 Import of user data without security attributes] (for static key) - FCS_CKM.4/SM Cryptographic key destruction Management: Not applicable
FCS_CKM.4 **Cryptographic Key Destruction**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.9
FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components 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] - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period,	**FCS_CKM.4/SM:** **FCS_CKM.4.1-1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**erasing of 3-DES session keys resp. of a static 3-DES key**] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.1.3 (CSM_013), Appendix 2, chap. 3.6.8 (TCS_353)** - **Physical erasing (overwriting with zero)**]. Hierarchical to: No other components Dependencies: - [FCS_CKM.1/SM Cryptographic key generation] (for session key), [FDP_ITC.1-1 Import of user data without security attributes] (for static key) Management: Not applicable

and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	
	FCS_CKM.4/RSA: **FCS_CKM.4.1-/RSA** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**erasing of imported public RSA-keys and references to public RSA-keys**] that meets the following: [- **Tachograph Card specification** /TachAn1B/**, Appendix 2, chap. 3.6.10 (TCS_363)**]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] Management: Not applicable
FCS_COP **Cryptographic Operation**	
FCS_COP.1 **Cryptographic Operation**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.9
FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Hierarchical to: No other components 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_COP.1/CSA:** **FCS_COP.1.1/CSA** The TSF shall perform [**the explicit signature generation and verification (commands PSO Compute Digital Signature and PSO Verify Digital Signature)**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**of 1024 bits**] that meet the following: [- **PKCS#1 (with SHA-1) signature generation / verification scheme, RSA Encryption Standard Version 2.0, October 1998** - **SHA-1, FIPS Pub. 180-1, NIST, April 1995** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 2.2.1 (CSM_003), 2.2.2 (CSM_004), 6.1 (CSM_034) and 6.2 (CSM_035)**]. Hierarchical to:

- FMT_MSA.2 Secure security attributes Management: --- Audit: a) Minimal: Success and failure, and the type of cryptographic operation b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/RSA Cryptographic key destruction Management: ---
	FCS_COP.1/CCA: **FCS_COP.1.1/CCA** The TSF shall perform [**the implicit signature generation and verification (commands Internal Authenticate, External Authenticate and PSO Verify Certificate)**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**of 1024 bits**] that meet the following: [- /ISO 9796-2/ **(DS scheme 1)** - **SHA-1, FIPS Pub. 180-1, NIST, April 1995** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 2.2.1 (CSM_003), 2.2.2 (CSM_004), 4 (CSM_020), 3.3.2, 3.3.3**]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/RSA Cryptographic key destruction Management: ---
	FCS_COP.1/ASYM: **FCS_COP.1.1/ASYM** The TSF shall perform [**the implicit encryption and decryption operations concerning asymmetric cryptography (commands Internal Authenticate, External Authenticate and Store Kpers)**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**of 1024 bits**] that meet the following: [- **PKCS#1 encryption / decryption primitive, RSA Encryption Standard Version 2.0, October 1998** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 2.2.1 (CSM_003), 4**]. Hierarchical to:

	No other components Dependencies: - [FDP_ITC.1-1 Import of user data without security attributes] - FCS_CKM.4/RSA Cryptographic key destruction Management: ---
	FCS_COP.1/SYM: **FCS_COP.1.1/SYM** The TSF shall perform [**the encryption and decryption operations concerning symmetric cryptography**] in accordance with a specified cryptographic algorithm [**2TDES in CBC mode with ICV = 0**] and cryptographic key sizes [**of 128 bits (112 effective bits, no parity bits set)**] that meet the following: [- **Data Encryption Standard, FIPS Pub. 46-3, NIST, Draft 1999** - **ANSI X9.52 Triple Data Encryption Algorithm Modes of Operations 1998** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 2.2.3 (CSM_005) and 5.4 (CSM_031)**]. Hierarchical to: No other components Dependencies: - [FCS_CKM.1/SM Cryptographic key generation] (for session key), [FDP_ITC.1-1 Import of user data without security attributes] (for static key) - FCS_CKM.4/SM Cryptographic key destruction Management: ---
	FCS_COP.1/MAC: **FCS_COP.1.1/MAC-** The TSF shall perform [**the MAC generation and the MAC verification concerning symmetric cryptography**] in accordance with a specified cryptographic algorithm [**DES Retail-MAC (with consideration of the send sequence counter)**] and cryptographic key sizes [**of 128 bits (112 effective bits, no parity bits set)**] that meet the following: [- **ANSI X9.19 Financial Institution Retail Message Authentication 1986** - **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 2.2.3 (CSM_005) and 5.3 (CSM_028))**].

	Hierarchical to: No other components Dependencies: - [FCS_CKM.1/SM Cryptographic key generation] (for session key), [FDP_ITC.1-1 Import of user data without security attributes] (for static key) - FCS_CKM.4/SM Cryptographic key destruction Management: ---

FDP **User Data Protection**	
FDP_ACC **Access Control Policy**	
FDP_ACC.2 **Complete Access Control**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.3.1, 4.4
FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] 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 in the TSC and any object within the TSC are covered by an access control SFP. Hierarchical to: FDP_ACC.1 Dependencies: - FDP_ACF.1 Security attribute based access control Management: --- Audit: ---	**FDP_ACC.2-1:** **FDP_ACC.2.1-1** The TSF shall enforce the [**AC_SFP**] on [**subjects:** - **vehicle units (in the sense of the Tachograph Card specification)** - **other card interface devices (non-vehicle units)** **objects:** - **user data:** - **identification data (card identification data, cardholder identification data)** - **activity data (cardholder activities data, events and faults data, control activity data)** - **security data:** - **card´s private signature key** - **public keys (in particular card´s public signature key, imported public keys)** - **session keys** - **PIN (only relevant for workshop card)** - **card´s private authentication key** - **TOE software code** - **TOE file system (incl. file structure, add. internal structures, access conditions)** - **identification data of the TOE (-IC, -ES)** - **identification data of the TOE’s personalisation**]

	and all operations among subjects and objects covered by the SFP. **FDP_ACC.2.2-1** The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. Hierarchical to: FDP_ACC.1 Dependencies: - FDP_ACF.1-1 Security attribute based access control Management: ---
	FDP_ACC.2-2: **FDP_ACC.2.1-2** The TSF shall enforce the [**PERS-AC_SFP**] on [**subjects:** - **personalisation units** - **other card interface devices (non-personalisation units)** **objects:** - **data fields for user data as:** - **identification data (card identification data, cardholder identification data)** - **activity data (cardholder activities data, events and faults data, control activity data)** - **data fields for security data as:** - **card´s signature key pair** - **public keys** - **PIN (only relevant for workshop card)** - **static personalisation key (if applicable)** - **security data:** - **card´s private personalisation key** - **card´s public personalisation key** - **personalisation unit´s public personalisation key** - **static personalisation key (if applicable)** - **session keys** - **card´s private authentication key** - **TOE software code** - **TOE file system (incl. file structure, add. internal structures, access conditions)** - **identification data of the TOE (-IC, -ES)** - **data field for identification data of the TOE's personalisation**] and all operations among subjects and objects covered by the SFP.

	FDP_ACC.2.2-2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. Hierarchical to: FDP_ACC.1 Dependencies: - FDP_ACF.1-2 Security attribute based access control Management: ---
FDP_ACF **Access Control Functions**	
FDP_ACF.1 **Security Attribute Based Access Control**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.3.2, 4.4 / JILDigTacho, chap. 2.6
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects cotrolled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]. **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]. **FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]. **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]. Hierarchical to: No other components Dependencies: - FDP_ACC.1 Subset access control - FMT_MSA.3 Static attribute initialisation Management: a) Managing the attributes used to make explicit ac-	**FDP_ACF.1-1:** **FDP_ACF.1.1-1** The TSF shall enforce the [**AC_SFP**] to objects based on [**subjects:** - **vehicle units (in the sense of the Tachograph Card specification)** - **other card interface devices (non-vehicle units)** **objects:** - **user data:** - **identification data (card identification data, cardholder identification data)** - **activity data (cardholder activities data, events and faults data, control activity data)** - **security data:** - **card´s private signature key** - **public keys (in particular card´s public signature key, imported public keys)** - **session keys** - **PIN (only relevant for workshop card)** - **card´s private authentication key** - **TOE software code** - **TOE file system (incl. file structure, add. internal structures, access conditions)** - **identification data of the TOE (-IC, -ES)** - **identification data of the TOE's personalisation** **security attributes for subjects:** - **USER_GROUP**

cess or denial based decisions Audit: a) Minimal: Successful requests to perform an operation on an object covered by the SFP b) Basic: All requests to perform an operation on an object covered by the SFP c) Detailed: The specific security attributes used in making an access check	- **USER_ID** **security attributes for objects:** - **access rules**]. **FDP_ACF.1.2-1** 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 VEHICLE_UNIT only;** - **IDENTIF_WRITE:** **all card types: identification data may only be written once and before the end of phase 6 of card's life-cycle; 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 TOE by VEHICLE_UNIT 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 end of phase 5 of TOE's life-cycle 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 end of phase 5 of card's life-cycle; no user may write or modify these identification data during phase 6 or end-usage phase of card's life-cycle;** - **IDENTIF_ TOE_ PERS_WRITE:** **all card types: identification data of the TOE's personalisation may only be written once and within phase 6 of card's life-cycle; no user may write or modify these identification data during end-usage phase of card's life-cycle** - **SECDATA_ACCESS:** **access to secret data stored in the framework of the initialisation or personalisation of the TOE is done by an implicit connection with the respective command whereat the access to the card´s private signature key for an external**

authentication, to session keys or to the PIN is only successful for VEHICLE_UNIT; for all other secret data any user will succeed
].

Note
/TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2 and 4.3.2 (FDP_ACF.1.2 GENERAL_READ) say that only control cards may have an authentication process before exporting cardholder identification data, but /TachAn1B/, Appendix 2 TCS_415 says that authentication is mandatory for exporting cardholder identification data. Furthermore, there are no TSF mediated actions defined in FIA_UAU.1.1 for the company card.

Agreed interpretation in /JILDigTacho/, chap. 2.6: The allowed actions for a company card seems to be missing in the specification of FIA_UAU.1 in the generic security target of /TachAn1B/, Appendix 10. From the context it is clear that a company card should allow the actions as specified by /TachAn1B/, Appendix 2 (which are the same for a control card). Therefore, the specification of the TOE SFRs in /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target should be read as follows:

- GENERAL_READ: User data may be read from the TOE by any user, except cardholder identification data which may be read from control cards **or company cards** by VEHICLE_UNIT only.

Refinements
ACT_301: The TOE shall hold permanent identification data.

ACT_302: There shall be an indication of the time and date of the TOE's personalisation. This indication shall remain unalterable.

FDP_ACF.1.3-1
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4-1
The TSF shall explicitly deny access of subjects to objects based on the [**none**].

Hierarchical to:
No other components

Dependencies:
- FDP_ACC.2-1 Subset access control

Management:
Not applicable

FDP_ACF.1-2:

FDP_ACF.1.1-2
The TSF shall enforce the [**PERS-AC _SFP**] to objects based on
[
subjects:

- **personalisation units**
- **other card interface devices (non-personalisation units)**

objects:

- **data fields for user data as:**
  - **identification data (card identification data, cardholder identification data)**
  - **activity data (cardholder activities data, events and faults data, control activity data)**
- **data fields for security data as:**
  - **card´s signature key pair**
  - **public keys**
  - **PIN (only relevant for workshop card)**
  - **static personalisation key (if applicable)**
- **security data:**
  - **card´s private personalisation key**
  - **card´s public personalisation key**
  - **personalisation unit´s public personalisation key**
  - **static personalisation key (if applicable)**
  - **session keys**
  - **card´s private authentication key**
- **TOE software code**
- **TOE file system (incl. file structure, add. internal structures, access conditions)**
- **identification data of the TOE (-IC, -ES)**
- **data field for identification data of the TOE’s personalisation**

security attributes for subjects:

- **USER_GROUP**
- **USER_ID**

security attributes for objects:

- **access rules (for data fields for user data, data fields** for **security data, static personalisation key, TOE file system)**

].

FDP_ACF.1.2-2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
- **IDENTIF_WRITE:**
  all card types: identification data may only be written before the end of phase 6 of card’s life-cycle; within phase 6, identification data may be written by PERSO_UNIT only

	- **ACTIVITY_WRITE:** **all card types: activity data may only be written during the end-usage phase of card’s lifecycle** - **SECDATA_WRITE:** **all card types: security data as the card´s personalisation key pair, the personalisation unit´s public personalisation key and the card´s private authentication key may only be loaded before the end of phase 5 of card´s lifecycle; the card´s static personalisation key (if applicable) may only be loaded in phase 5 resp. in phase 6 of card´s life-cycle; the card´s signature key pair and the PIN (workshop card) may only be loaded within phase 6** - **SECDATA_ACCESS:** **access to secret data stored in the framework of the initialisation, pre-personalisation (if applicable) or personalisation of the TOE is done by an implicit connection with the respective command whereat the access to the card´s private personalisation key for an external authentication or for the import of the static personalisation key, to session keys or to the static personalisation key is only successful for PERSO_UNIT; for all other secret data any user will succeed** - **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 end of phase 5 of TOE’s life-cycle and then locked from any future modification or deletion by any user (Note: This requirement holds for each configuration of the Tachograph Card delivered to the customer; in particular, if the card is delivered at the end of phase 5 with a prepared file system, it is only possible to blow up one of the four pre-defined Tachograph Card file system types whereat no modification is possible.)** - **IDENTIF_TOE_READ:** **all card types: identification data of the TOE or 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 end of phase 5 of card’s life-cycle; no user may write or modify these identification data during phase 6 phase of card’s life-cycle or later;** - **IDENTIF_ TOE_ PERS_WRITE:** **all card types: identification data of the TOE’s personalisation may only be written within phase 6 of card’s life-cycle; no user may write or modify these identification data during end-usage phase of card’s life-cycle**

	]. **Refinements** ACT_301: The TOE shall hold permanent identification data. ACT_302: There shall be an indication of the time and date of the TOE's personalisation. This indication shall remain unalterable. **FDP_ACF.1.3-2** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4-2** The TSF shall explicitly deny access of subjects to objects based on the [**none**]. Hierarchical to: No other components Dependencies: - FDP_ACC.2-2 Subset access control Management: Not applicable
FDP_DAU **Data Authentication**	
FDP_DAU.1 **Basic Data Authentication**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.6.2
FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*]. **FDP_DAU.1.2** The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information. Hierarchical to: No other components Dependencies: No dependencies Management: a) The assignment or modification of the objects for which data authentication may apply could be configurable in the system Audit: a) Minimal: Successful generation of validity evidence b) Basic: Unsuccessful generation of validity evi-	**FDP_DAU.1-1:** **FDP_DAU.1.1-1** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [**activity data**]. **FDP_DAU.1.2-1** The TSF shall provide [**any subject (i.e. vehicle units and other card interface devices (non-vehicle units))**] with the ability to verify evidence of the validity of the indicated information. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable

dence c) Detailed: The identity of the subject that requested the evidence	
FDP_ETC **Export to Outside TSF Control**	
FDP_ETC.1 **Export of User Data without Security Attributes**	PP9911
FDP_ETC.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TSC. **FDP_ETC.1.2** The TSF shall export the user data without the user data's associated security attributes. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Management: --- Audit: a) Minimal: Successful export of information b) Basic: All attempts to export information	**FDP_ETC.1-1:** **FDP_ETC.1.1-1** The TSF shall enforce the [**for phase 6 of the product´s life-cycle: PERS-AC_SFP; for phase 7 of the product´s life-cycle: AC_SFP**] when exporting user data, controlled under the SFP(s), outside of the TSC. **FDP_ETC.1.2-1** The TSF shall export the user data, without the user data's associated security attributes. Hierarchical to: No other components Dependencies: - [FDP_ACC.2-1 Subset access control] - [FDP_ACC.2-2 Subset access control] Management: ---
FDP_ETC.2 **Export of User Data with Security Attributes**	TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.8.2
FDP_ETC.2.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TSC. **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 TSC, 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 TSC: [assignment: *additional exportation control rules*].	**FDP_ETC.2-1:** **FDP_ETC.2.1-1** The TSF shall enforce the [**AC_SFP**] when exporting user data **within the card data download function**, controlled under the SFP(s), outside of the TSC. **FDP_ETC.2.2-1** The TSF shall export the user data with the user data's associated security attributes. **Refinement** DEX_306: The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be verified. **FDP_ETC.2.3-1** The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously

Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Management: a) The additional exportation control rules could be configurable by a user in a defined role. Audit: a) Minimal: Successful export of information b) Basic: All attempts to export information	associated with the exported user data. **FDP_ETC.2.4-1** The TSF shall enforce the following rules when user data is exported from the TSC: [**none**] Hierarchical to: No other components Dependencies: - [FDP_ACC.2-1 Subset access control] Management: Not applicable
FDP_ITC **Import from Outside TSF Control**	
FDP_ITC.1 **Import of User Data without Security Attributes**	PP9911
FDP_ITC.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when importing user data, controlled under the SFP, from outside of the TSC. **FDP_ITC.1.2** The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. **FDP_ITC.1.3** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*]. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - FMT_MSA.3 Static attribute initialisation Management: a) The modification of the additional control rules used for import Audit: a) Minimal: Successful import of user data, including any security attributes b) Basic: All attempts to import user data, including any security attributes c) Detailed: The specification of security attributes for	**FDP_ITC.1-1:** **FDP_ITC.1.1-1** The TSF shall enforce the [**for phase 6 of the product´s life-cycle: PERS-AC_SFP; for phase 7 of the product´s life-cycle: AC_SFP**] when importing user data, controlled under the SFP, from outside of the TSC. **FDP_ITC.1.2-1** The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. **FDP_ITC.1.3-1** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**none**]. Hierarchical to: No other components Dependencies: - [FDP_ACC.2-1 Subset access control] - [FDP_ACC.2-2 Subset access control] Management: Not applicable

imported user data supplied by an authorised user	
FDP_RIP **Residual Information Protection**	
FDP_RIP.1 **Subset Residual Information Protection**	PP9911
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE Audit: ---	**FDP_RIP.1-1:** **FDP_RIP.1.1-1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**deallocation of the resource from**] the following objects: [**security relevant material (e.g. cryptographic KEYs, PINs, ...)**]. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable
FDP_SDI **Stored Data Integrity**	
FDP_SDI.2 **Stored Data Integrity Monitoring and Action**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.6.1
FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*]. **FDP_SDI.2.2** Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*]. Hierarchical to: FDP_SDI.1 Dependencies: No dependencies Management: a) The actions to be taken upon the detection of an integrity error could be configurable Audit:	**FDP_SDI.2-1:** **FDP_SDI.2.1-1** The TSF shall monitor user data **(incl. stored secrets)** stored within the TSC for [**integrity error before access and processing**] on all objects, based on the following attributes: [**user data value, user data object**]. **FDP_SDI.2.2-1** Upon detection of a data integrity error, the TSF shall [**warn the entity connected**]. Hierarchical to: FDP_SDI.1 Dependencies: No dependencies Management: Not applicable

a) Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check b) Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed c) Detailed: The type of integrity error that occurred d) Detailed: The action taken upon detection of an integrity error	

FIA **Identification and Authentication**	
FIA_AFL **Authentication Failures**	
FIA_AFL.1 **Authentication Failure Handling**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.3
FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], “*an administrator configurable positive integer within* [assignment: *range of acceptable values*]“] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*]. **FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*]. Hierarchical to: No other components Dependencies: - FIA_UAU.1 Timing of authentication Management: a) management of the threshold for unsuccessful authentication attempts b) management of actions to be taken in the event of an authentication failure Audit: a) Minimal: the reaching of the threshold for the unsuccesful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	For all card types: Card reaction for each single user authentication failure: **FIA_AFL.1-1:** **FIA_AFL.1.1-1** The TSF shall detect when [**1**] unsuccessful authentication attempt occurs related to [**authentication of a card interface device**]. **FIA_AFL.1.2-1** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**warn the entity connected, assume the user as NON_VEHICLE_UNIT (phase 7 of product´s life-cycle) resp. NON_PERSO_UNIT (phase 6 of product´s life-cycle)**]. Hierarchical to: No other components Dependencies: - FIA_UAU.1-1 Timing of authentication Management: Not applicable
	For workshop cards only: Card reaction in the case of a failure of the additional PIN-authentication mechanism:

	FIA_AFL.1-2: **FIA_AFL.1.1-2** The TSF shall detect when [**5**] unsuccessful authentication attempts occur related to [**PIN check (workshop card)**]. **FIA_AFL.1.2-2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**warn the entity connected, block the PIN check procedure such that any subsequent PIN check attempt will fail, be able to indicate to subsequent users the reason of the blocking**]. **Note** Agreed interpretation in /JILDigTacho/, chap. 2.6: To ensure that the Tachograph Card takes care of unsuccessful authentication events, the sentence “The following assignments describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.” (/TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.3) should be read as follows: “**Additionally** the following assignments describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.” This should ensure that the Tachograph Card (here only the workshop card) only allows a mutual authentication with the Vehicle Unit after a successful PIN verification of a human user. Hierarchical to: No other components Dependencies: - FIA_UAU.1-1 Timing of authentication Management: Not applicable
FIA_ATD **User Attribute Definition**	
FIA_ATD.1 **User Attribute Definition**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.1
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*]. Hierarchical to: No other components Dependencies:	**FIA_ATD.1-1:** **FIA_ATD.1.1-1** The TSF shall maintain the following list of security attributes belonging to individual users: [**phase 6 of the product´s life-cycle:** - **USER_GROUP (PERSO_UNIT, NON_PERSO_UNIT)**

No dependencies Management: a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users Audit: ---	**phase 7 of the product´s life-cycle:** - **USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)** - **USER_ID (VRN and Reg. MSC, where USER_ID is only known to USER_GROUP = VEHICLE_UNIT)**]. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable
FIA_UAU **User Authentication**	
FIA_UAU.1 **Timing of Authentication**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.2 / JILDigTacho, chap. 2.6
FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated. **FIA_UAU.1.2** The TSF shall require each user to be successfully authenticated before allowing any other TSF- mediated actions on behalf of that user. Hierarchical to: No other components Dependencies: - FIA_UID.1 Timing of identification Management: a) management of the authentication data by an administrator b) management of the authentication data by the associated user c) managing the list of actions that can be taken before the user is authenticated Audit: a) Minimal: Unsuccessful use of the authentication mechanism b) Basic: All use of the authentication mechanism c) Detailed: All TSF mediated actions performed before authentication of the user	(Only phase 7 of the product´s life-cycle) **FIA_UAU.1-1:** **FIA_UAU.1.1-1** The TSF shall allow [**driver card, workshop card: export of user data with security attributes (card data download function),** **control card, company card: export of user data without security attributes except export of cardholder identification data**] on behalf of the user to be performed before the user is authenticated. **Note** /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2 and 4.3.2 (FDP_ACF.1.2 GENERAL_READ) say that only control cards may have an authentication process before exporting cardholder identification data, but /TachAn1B/, Appendix 2 TCS_415 says that authentication is mandatory for exporting cardholder identification data. Furthermore, there are no TSF mediated actions defined in FIA_UAU.1.1 for the company card. Agreed interpretation in /JILDigTacho/, chap. 2.6: The allowed actions for a company card seems to be missing in the specification of FIA_UAU.1 in the generic security target of /TachAn1B/, Appendix 10. From the context it is clear that a company card should allow

	the actions as specified by /TachAn1B/, Appendix 2 (which are the same for a control card). Therefore, the specification of the TOE SFRs in /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target should be read as follows: - Control **and company** card**s**: Export of user data without security attributes except cardholder identification data **FIA_UAU.1.2-1** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. **Refinements** UIA_301: Authentication of a vehicle unit shall be performed by means of proving that it possesses security data that only the system could distribute. UIA_302: The workshop card shall provide an additional authentication mechanism by checking a PIN code (This mechanism is intended for the vehicle unit to ensure the identity of the cardholder, it is not intended to protect workshop card content). Hierarchical to: No other components Dependencies: - FIA_UID.1-1 Timing of identification Management: Not applicable
FIA_UAU.3 **Unforgeable Authentication**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.2
FIA_UAU.3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF. **FIA_UAU.3.2** The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit:	**FIA_UAU.3-1:** **FIA_UAU.3.1-1** The TSF shall [**prevent**] use of authentication data that has been forged by any user of the TSF. **FIA_UAU.3.2-1** The TSF shall [**prevent**] use of authentication data that has been copied from any other user of the TSF. Hierarchical to: No other components Dependencies: No dependencies Management: ---

a) Minimal: Detection of fraudulent authentication data b) Basic: All immediate measures taken and results of checks on the fraudulent data	
FIA_UAU.4 **Single-use Authentication Mechanisms**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.2
FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(*s)]. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: a) Minimal: Attempts to reuse authentication data	**FIA_UAU.4-1:** **FIA_UAU.4.1-1** - The TSF shall prevent reuse of authentication data related to [**key based authentication mechanisms**]. Hierarchical to: No other components Dependencies: No dependencies Management: ---
FIA_UID **User Identification**	
FIA_UID.1 **Timing of Identification**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.2.1 / JILDigTacho, chap. 2.6
FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified. **FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. Hierarchical to: No other components Dependencies: No dependencies Management: a) the management of the user identities b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists Audit: a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided b) Basic: All use of the user identification mechanism,	(Only phase 7 of the product´s life-cycle) **FIA_UID.1-1:** **FIA_UID.1.1-1** The TSF shall allow [**none of the TSF-mediated actions**] on behalf of the user to be performed before the user is identified. **Note** In /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, FIA_UID.1.1(TSF mediated actions) states that the card shall allow no operations before the identification of the user, and, FDP_ACF.1.2 (GENERAL_READ) states "User data may be read from the TOE by any user, ...". However, /TachAn1B/, Appendix 11 defines a process to identify and authenticate a VEHICLE_UNIT, but no process is defined to identify other users. Agreed interpretation in /JILDigTacho/, chap. 2.6: In /TachAn1B/, Appendix 10, Tachograph Card Generic Security Target the following types of users are identified:VEHICLE_UNIT and NON_VEHICLE_UNIT. The user NON_VEHICLE_UNIT is identified by the Tacho-

including the user identity provided	graph Card by just putting it into a card reading device (which could be a Vehicle Unit). After a successful mutual authentication between Tachograph Card and Vehicle Unit, the Tachograph Card assumes the user VEHICLE_UNIT to be identified. (Note: This interpretation shall be applied by analogy for the TOE's personalisation phase resp. personalisation units.) **FIA_UID.1.2-1** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable
FIA_USB **User-Subject Binding**	
FIA_USB.1 **User-Subject Binding**	PP9911
FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*]. **FIA_USB.1.2** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*]. **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: *rules for the changing of attributes*]. Hierarchical to: No other components Dependencies: - FIA_ATD.1 User attribute definition Management: a) an authorised administrator can define default subject security attributes b) an authorised administrator can change subject security attributes	**FIA_USB.1-1:** **FIA_USB.1.1-1** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**phase 6 of the product´s life-cycle:** - **USER_GROUP (PERSO_UNIT, NON_PERSO_UNIT)** **phase 7 of the product´s life-cycle:** - **USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)** - **USER_ID (VRN and Reg. MSC, where USER_ID is only known to USER_GROUP = VEHICLE_UNIT)**]. **FIA_USB.1.2-1** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**assignment in the framework of the TOE's access rule mechanism**]. **FIA_USB.1.3-1** The TSF shall enforce the following rules governing

Audit: a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject) b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject)	changes to the user security attributes associated with subjects acting on the behalf of users: [**no change of user security attributes possible**]. Hierarchical to: No other components Dependencies: - FIA_ATD.1-1 User attribute definition Management: Not applicable

FPR **Privacy**	
FPR_UNO **Unobservability**	
FPR_UNO.1 **Unobservability**	PP9911
FPR_UNO.1.1 The TSF shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) the management of the behaviour of the unobservability function Audit: a) Minimal: The invocation of the unobservability mechanism	**FPR_UNO.1-1:** **FPR_UNO.1.1-1** The TSF shall ensure that [**within phase 6 of the product´s life cycle: non-personalisation units,** **within phase 7 of the product´s life-cycle: non-vehicle units**] are unable to observe the operation [**mutual authentication (for the agreement of session keys and send sequence counters)**] on [**authentication tokens**] by [**within phase 6 of the product´s life cycle: a personalisation unit,** **within phase 7 of the product´s life-cycle: a vehicle unit**]. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable

	FPR_UNO.1-2: **FPR_UNO.1.1-2** The TSF shall ensure that [**within phase 6 of the product´s life cycle: non-personalisation units,** **within phase 7 of the product´s life-cycle: non-vehicle units**], **if required,** are unable to observe the operation [**import function of user data, export function of user data**] on [**user data**] by [**within phase 6 of the product´s life cycle: a personalisation unit,** **within phase 7 of the product´s life-cycle: a vehicle unit**]. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable
	FPR_UNO.1-3: **FPR_UNO.1.1-3** The TSF shall ensure that [**within phase 6 of the product´s life cycle: non-personalisation units**] are unable to observe the operation [**import**] **(if applicable)** on [**a static personalisation key**] by [**within phase 6 of the product´s life cycle: a personalisation unit**]. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable

FPT **Protection of the TSF**	
FPT_FLS **Fail Secure**	

FPT_FLS.1 **Failure with Preservation of Secure State**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.7.3, 4.7.4
FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*]. Hierarchical to: No other components Dependencies: - ADV_SPM.1 Informal TOE security policy model Management: --- Audit: a) Basic: Failure of the TSF	**FPT_FLS.1-1:** **FPT_FLS.1.1-1** The TSF shall preserve a secure state when the following types of failures occur: [- **reset** - **power supply cut-off** - **power supply variations** - **unexpected abortion of the execution of the TSF due to external or internal events (esp. break of a transaction before completion)** - **system breakdown** - **internal Hardware- or Software failure** - **card life cycle corruption** - **application life cycle corruption**]. **Refinements** RLB_306: The TOE shall preserve a secure state during power supply cut-off or variations. RLB_307: If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly. Hierarchical to: No other components Dependencies: - ADV_SPM.1 Informal TOE security policy model Management: ---
FPT_PHP **Physical Protection**	
FPT_PHP.3 **Resistance to Physical Attack**	PP9911
FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices /elements*] by responding automatically such that the TSP is not violated. Hierarchical to: No other components Dependencies: No dependencies	**FPT_PHP.3-1:** **FPT_PHP.3.1-1** The TSF shall resist [**side channel attacks like SPA-attacks, DPA-attacks, DFA-attacks and timing attacks concerning all critical cryptographic operations**] to the [**TSF interfaces**] by responding automatically such that the TSP is not violated. Hierarchical to: No other components

Management: a) management of the automatic responses to physical tampering Audit: ---	Dependencies: No dependencies Management: Not applicable
FPT_SEP **Domain Separation**	
FPT_SEP.1 **TSF Domain Separation**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.7.2
FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. **FPT_SEP.1.2** The TSF shall enforce separation between the security domains of subjects in the TSC. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: ---	**FPT_SEP.1-1:** **FPT_SEP.1.1-1** The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. **FPT_SEP.1.2-1** The TSF shall enforce separation between the security domains of subjects in the TSC. **Refinements** RLB_304: There shall be no way to analyse, debug or modify TOE's software in the field. RLB_305: Inputs from external sources shall not be accepted as executable code. Hierarchical to: No other components Dependencies: No dependencies Management: ---
FPT_TDC **Inter-TSF TSF Data Consistency**	
FPT_TDC.1 **Inter-TSF Basic TSF Data Consistency**	PP9911
FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product. **FPT_TDC.1.2** The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.	**FPT_TDC.1-1:** **FPT_TDC.1.1-1** The TSF shall provide the capability to consistently interpret [- **authentication tokens with their input data for session keys and send sequence counters** - **session keys and send sequence counters themselves**

Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: a) Minimal: Successful use of TSF data consistency mechanisms b) Basic: Use of the TSF data consistency mechanisms c) Basic: Identification of which TSF data have been interpreted d) Basic: Detection of modified TSF data	- **PINs and their formats** - **imported certificates, their format and their included signature** - **imported signatures for verification** - **imported keys (in particular, personalisation keys)**] when shared between the TSF and another trusted IT product. **FPT_TDC.1.2-1** The TSF shall use [- **rules for the interpretation of the input data for session keys and send sequence counters within authentication tokens for the creation of session keys and send sequence counters: Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 4, 3.2, Appendix 2, chap. 3.6.8, 3.6.9** - **rules for the interpretation of session keys and send sequence counters within Secure Messaging:** **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 5, 3.2, Appendix 2, chap. 3.6.2.2, 3.6.3.2** - **rules for the interpretation of imported PINs: Tachograph Card specification** /TachAn1B/**, Appendix 2, chap. 3.6.5** - **rules for the interpretation of imported certificates, their format and their included signature:** **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.3** - **rules for the interpretation of imported signatures for verification:** **Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 6.2** - **rules for the interpretation of imported keys: Tachograph Card specification** /TachAn1B/**, Appendix 11, chap. 3.3, specification of the TOE concerning the TOE's personalisation schemes and procedures**] when interpreting the TSF data from another trusted IT product. Hierarchical to: No other components Dependencies: No dependencies Management: ---
FPT_TST **TSF Self Test**	

FPT_TST.1 **TSF Testing**	PP9911 / TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.7.1
FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*]. **FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*]. **FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. Hierarchical to: No other components Dependencies: - FPT_AMT.1 Abstract machine testing Management: a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions b) management of the time interval if appropriate Audit: a) Basic: Execution of the TSF self tests and the results of the tests	**FPT_TST.1-1:** **FPT_TST.1.1-1** The TSF shall run a suite of self tests [**during initial start-up, periodically during normal operation**] to demonstrate the correct operation of [**the TSF**]. **Note** During initial start-up means before code is executed. **Refinements** RLB_301: The TOE's self tests shall include the verification of the integrity of any software code not stored in ROM. RLB_302: Upon detection of a self test error the TSF shall warn the entity connected. RLB_303: After operating system testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state. The term “periodically during normal operation” is understood as follows: It is assumed that the TOE performs at least one reset-operation each day, so that the self test at each initial start-up suffices the requirement of performing the self test periodically during normal operation. **FPT_TST.1.2-1** The TSF shall provide authorised users with the capability to verify the integrity of [**TSF data**]. **Refinement** In this framework, the Smartcard Embedded Software of the TOE (TOE-ES) itself is understood as „authorised user“. **FPT_TST.1.3-1** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. **Refinement** This requirement concerns only the production phase, more precise the initialisation phase of the TOE (phase 5 of the product´s life cycle). Prior to the initialisation of the TOE, the ROM-code of the TOE shall be verifiable by the Smartcard Embedded Software developer. The integrity of the EEPROM-code shall be provable by the TOE during the initialisation process.

	Hierarchical to: No other components Dependencies: Not applicable Management: Not applicable

FTP **Trusted Path/Channels**	
FTP_ITC **Inter-TSF Trusted Channel**	
FTP_ITC.1 **Inter-TSF Trusted Channel**	TachAn1B, Appendix 10, Tachograph Card Generic Security Target, chap. 4.8.1
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product 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** The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted channel, if supported Audit: a) Minimal: Failure of the trusted channel functions b) Minimal: Identification of the initiator and target of failed trusted channel functions c) Basic: All attempted uses of the trusted channel functions d) Basic: Identification of the initiator and target of all trusted channel functions	**FTP_ITC.1-1:** **FTP_ITC.1.1-1** The TSF shall provide a communication channel between itself and a remote trusted IT product **(vehicle unit, personalisation 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. **Refinements** DEX_301: The TOE shall verify the integrity and authenticity of data imported from a vehicle unit. DEX_302: Upon detection of an imported data integrity error, the TOE shall: - warn the entity sending the data, - not use the data. DEX_303: The TOE shall export user data to the vehicle unit with associated security attributes, such that the vehicle unit will be able to verify the integrity and authenticity of data received. **Note** The refinements above from the Tachograph Card specification shall be applied by analog for the personalisation phase of the TOE. The integrity and authenticity resp. the confidentiality, if required, of the data transfer between the Tachograph Card and the remote trusted IT product (vehicle unit, personalisation unit) shall be conducted with Secure Messaging in accordance with ISO/IEC 7816-4 (using a 3-DES session key or a static 3-DES key). **FTP_ITC.1.2-1**

	The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel. **FTP_ITC.1.3-1** The TSF shall initiate communication via the trusted channel for [**user data import from a remote trusted IT product, user data export to a remote trusted IT product**]. Hierarchical to: No other components Dependencies: No dependencies Management: Not applicable

5.1.2 SOF Claim for TOE Security Functional Requirements

According to the requirements in the Tachograph Card specification /TachAn1B/, main body and Appendix 10 (Tachograph Card Generic Security Target), and to the JIL interpretations /JILDigTacho/, the required level for the Strength of Function of the TOE security functional requirements listed in the preceding chap. 5.1.1 is “SOF-high”. This correlates to the claimed assurance level with its augmentation by the assurance component AVA_VLA.4 (refer to the following chap. 5.1.3).

The following restriction of the strength of function claim has to be defined for the security functions using RSA keys: The claim “SOF-high” is no longer made *as far as the key length of the RSA keys is concerned*. Due to the development of the attack potential in the recent years, a RSA key length of 1024 bit is no longer considered to be resistant against a high attack potential. On the other hand, the functional specification of the Tachograph Card still requires that the product uses 1024 bit RSA keys. To resolve this issue, the strength of function claim is relaxed for the security evaluation. However, the relaxation is only related to the key length – i.e. only brute force attacks on the RSA key are not rated against a high attack potential. All other mechanisms like the resistance against side channel analysis etc. are still rated against a high attack potential which is state-of-the-art at the time of the security evaluation. This way, the Tachograph product combines the minimal restriction imposed by the external functional specification with the state-of-the art security mechanisms supplied by the MICARDO platform.

5.1.3 TOE Security Assurance Requirements

The evaluation of the Tachograph Card according to ITSEC E3 high as required in the Tachograph Card Specification /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target) will be replaced by a comparable evaluation according to Common Criteria, whereby the requirements in the JIL interpretations /JILDigTacho/, Annex A have to be considered. The TOE security assurance level is fixed as

EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4, thus the CC evaluation of the TOE matches the evaluation assurance requirements stated in the Tachograph Card Specification /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target).

The following table lists the security assurance requirements (SARs) for the TOE:

SAR	
Class ACM **Configuration Management**	ACM_AUT.1 Partial CM Automation
	ACM_CAP.4 Generation Support and Acceptance Procedures
	ACM_SCP.2 Problem Tracking CM Coverage
Class ADO **Delivery and Operation**	ADO_DEL.2 Detection of Modification
	ADO_IGS.**2** Generation Log
Class ADV **Development**	ADV_FSP.2 Fully Defined External Interfaces
	ADV_HLD.2 Security Enforcing High-Level Design
	ADV_IMP.**2** Implementation of the TSF
	ADV_LLD.1 Descriptive Low-Level Design
	ADV_RCR.1 Informal Correspondence Demonstration
	ADV_SPM.1 Informal TOE Security Policy Model
Class AGD **Guidance Documents**	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Class ALC **Life Cycle Support**	ALC_DVS.1 Identification of Security Measures
	ALC_LCD.1 Developer Defined Life-Cycle Model

	ALC_TAT.1 Well-defined Development Tools
Class ATE **Tests**	ATE_COV.2 Analysis of Coverage
	ATE_DPT.**2** Testing: Low-Level Design
	ATE_FUN.1 Functional Testing
	ATE_IND.2 Independent Testing – Sample
Class AVA **Vulnerability Assessment**	AVA_MSU.2 Validation of Analysis
	AVA_SOF.1 Strength of TOE Security Function Evaluation
	AVA_VLA.**4** Highly Resistant

5.1.4 Refinements of the TOE Security Assurance Requirements

All assurance components given in the table of chap. 5.1.3 are used as defined in /CC 2.3 Part3/ and /CEM 2.3/. Additionally, according to /JILDigTacho/, Annex A.3, Note 2 and 9 the following refinements resp. interpretations are taken into account:

ADO_IGS.2

ADO_IGS.2 is interpreted resp. refined according to ITSEC E3.32 and ITSEC-JIL, Section 16.2 as follows:

- The term “generation” is always interpreted as “installation”.
- "While installing the TOE, any configuration options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how the TOE was initially configured and when the TOE was installed."

AVA_MSU.2

ITSEC 3.33 additionally requires evaluator tests where necessary. This testing, can be part of the penetration testing under AVA_VLA. It is decided on a case by case basis if the evaluator performs misuse-testing as additional part of penetration testing to confirm or disprove the misuse analysis. Specifically, if high attack potential is assumed, such independent misuse-testing is performed.

5.2 Security Requirements for the Environment of the TOE

5.2.1 Security Requirements for the IT-Environment

There are no security requirements for the IT-Environment of the TOE defined.

5.2.2 Security Requirements for the Non-IT-Environment

There are no security requirements for the Non-IT-Environment of the TOE defined.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 TOE Security Functions / TOE-IC

For the definition of the TOE Security Functions (TSF) related to the TOE-IC refer to the Security Targets /ST_IC/, chap. 6.1 and /ST_IC_CL/, chap. 6.1.

The TSFs defined for the TOE-IC cover the following functions which are relevant for the TOE: F.RNG, F.HW_DES, F.OPC, F.PHY, F.LOG, F.COMP, F.MEM_ACC, F.SFR_ACC, F.DES, F.RSA, F.SHA-1, F.RNG_Access, F.Object_Reuse, F.LOG

6.1.2 TOE Security Functions / TOE-ES

The following section gives a survey of the TSFs of the TOE's Smartcard Embedded Software under consideration of the requirements in the Tachograph Card Specification /TachAn1B/, Appendix 10 (Tachograph Card Generic Security Target).

TOE Security Functions / TOE-ES	
Access Control	
F.ACS	**Security Attribute Based Access Control**
	The TSF enforces for the personalisation phase of the TOE the SFP Personalisation Access Control (PERS-AC_SFP) and for the end-usage phase of the TOE the SFP_access_rules (AC_SFP) as defined in chap. 5.1.1.1.
Identification and Authentication	
F.IA_AKEY	**Key Based User / TOE Authentication**
	Users of the TOE can be authenticated with regard to the TOE by means of a challenge-response procedure using random numbers (external authentication). Vice versa, the TOE itself can be authenticated with regard to the external world as well by means of a challenge-response procedure using random numbers (internal authentication). In both cases, the TSF makes use of asymmetric cryptography (with encryption, decryption, generation of a digital signature resp. verification of a digital signature) and of the generation of random numbers and is therefore connected with the TSFs F.RSA_ENC, F.RSA_DEC, F.GEN_DIGSIG, F.VER_DIGSIG and the IC´s TSF F.RNG_Access for random number access.

	For an internal authentication, the TSF generates and returns an authentication token by using the operations “generation of a digital signature” and “encryption” on random numbers of the external world and of the TOE itself. In detail, the TSF uses the relevant private key to sign the authentication data including the randoms and then uses the public key currently selected to encrypt the signature and form the authentication token which will be returned to the external world. For an external authentication, the TSF verifies an authentication token delivered by the external world (containing random numbers of the external world and of the TOE itself) by using the operations “decryption” and “verification of a digital signature”. In detail, the TSF uses the currently selected public key to decrypt the authentication token and uses then the relevant private key to verify the signature within the delivered authentication token. The external authentication process needs a preceding Get Challenge - operation. The private key necessary on the card´s side for authentication purposes is stored on the card (during initialisation resp. personalisation of the TOE) and is implicitly connected with the corresponding commands. The necessary public keys whereas are already stored on the card or have to be imported in the form of certificates. In each case, they have to be explicitly referenced for usage. The import of a public key by a certificate is connected with the verification of the respective certificate under use of the TSF F.VER_DIGSIG. The access to the keys is controlled by the SFP Personalisation Access Control (PERS-AC_SFP) within the personalisation phase of the TOE and by the SFP_access_rules (AC_SFP) within the end-usage phase of the TOE as defined in chap. 5.1.1.1, which is realised by the TSF F.ACS. In case of a successful external authentication attempt a corresponding actual security state is set. The combination of a successful internal authentication process followed by a successful external authentication process leads to the generation of a new session key (with send sequence counter) which will be used for securing the following data transfer. In detail, the following conditions are valid: If the internal authentication process does not fail, the current session key, if existing, is erased and no longer available. In order to have a new session key available, a following external authentication process must be successfully performed. If the external authentication does not fail, and if the first part of the session key is available from the preceding successful internal authentication, the session key is generated and set for future commands using Secure Messaging. If the first session key part is not available from a previous internal authentication, the second part of the session key, sent by the external world within the authentication token, is not stored in the card. The generation of session keys is task of the TSF F.GEN_SES. For the Tachograph card type Workshop Card the mutual authentication process described above is only possible after a successful preceding password based user authentication (see F.IA_PWD).
F.IA_PWD	**Password Based User Authentication**
	Users of the TOE can be authenticated by means of a card holder authentication process. For the card holder authentication process, the TSF compares the cardholder verification information, here a password (PIN), provided by a subject with a corresponding secret reference data stored in the card. The TSF is internally connected with the card´s unique password stored on the card (set to a default value during initialisation resp. loaded in the framework of the TOE’s personalisation). The access to the password is controlled by the SFP_access_rules (AC_SFP) as defined in chap. 5.1.1.1, which is realised by the TSF F.ACS. The TSF detects when a defined number of consecutive unsuccessful authentication attempts

	occurs related to the card holder authentication process. Each consecutive unsuccessful comparison of the presented password with the reference value stored on the card is recorded by the TSF in order to limit the number of further authentication attempts with the password. For this purpose, the TSF manages a mandatory error counter for the password. In case of a successful authentication attempt a corresponding actual security state for the password is set and the error counter is reinitialised. If an authentication attempt with the password fails, the corresponding actual security state is reset and the password´s error counter is decreased. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF blocks the corresponding password. There is no way to reset the error counter in order to unblock the password so that the password is invalid for each further authentication process. For security reasons, the initial value for the error counter is set to a sufficiently small finite value (here: 5). The TSF does not check the quality of the used password, this check is in responsibility of the external world. Furthermore, there is no possibility to change the password while the card is in operational status. The transfer of the password to the TOE for authentication attempts is executed in unsecured mode (i.e. without use of Secure Messaging) or optional in secured mode with Secure Messaging. In the latter case, the TSFs F.EX_CONF and F.EX_INT are involved.
Integrity of Stored Data	
F.DATA_INT	**Stored Data Integrity Monitoring and Action**
	The TSF monitors data stored within the TOE for integrity errors. This concerns all elementary files and dedicated files as well as all secrets (esp. passwords and cryptographic keys) stored outside the file system within the EEPROM area. The monitoring is based on the following attributes: - a checksum (CRC) attached to each header of a file - a checksum (CRC) attached to the data contained in a file - a checksum (CRC) attached to each secret stored outside the file system within the EEPROM area Before the TOE accesses to an elementary or dedicated file or a secret stored outside the file system, the TSF carries out an integrity check on base of the mentioned attributes. Upon detection of a data integrity error, the TSF informs the user about this fault. If the checksum of the header of a file has been detected as corrupted, the data contained in the affected file is no longer accessible. If the data contained in a file is not of integrity, the affected data will be treated in the following way: - For the Read access, the affected data will be exported, but the data export will be connected with a warning. (Exception: The command Get Data of the Tachograph Application for reading out the EF_Application_Identification will not export data in case of a corrupt checksum.) - For the Update access, the integrity error of the affected data will be ignored, and the data imported by the command will be stored and a new checksum will be computed. - For all remaining access modes, the affected data will not be used for data processing.

	If a secret stored outside the file system is corrupted, the secret will not be processed.
Data Exchange	
F.EX_CONF	**Confidentiality of Data Exchange**
	The TSF provides the capability to ensure that secret data which is exchanged between the TOE and the user remains confidential during transmission. For this purpose, encryption based on symmetric cryptography is applied to the secret data. The TSF ensures that the user and the user data's access condition have indicated confidentiality for the data exchange. Securing the data transfer with regard to data confidentiality will be done by Secure Messaging according to the standards ISO/IEC 7816-4 and /TachAn1B/, Appendix 11, chap. 5. The cryptographic key used for securing the data transfer is either a symmetric session key which is generated during a preceding mutual authentication process between the card and the external world (realised by the TSFs F.IA_AKEY and F.GEN_SES) or a static symmetric key. For encryption, the TSF makes use of the TSF F.DES of the underlying IC resp. its Dedicated Support Software.
F.EX_INT	**Integrity and Authenticity of Data Exchange**
	The TSF provides the capability to ensure that data which is exchanged between the TOE and the user remains integer and authentic during transmission. For this purpose, cryptographic checksums based on symmetric cryptography are applied to the data. The TSF ensures that the user and the user data's access condition have indicated integrity and authenticity for the data exchange. Securing the data transfer with regard to data integrity and authenticity will be done by Secure Messaging according to the standards ISO/IEC 7816-4 and /TachAn1B/, Appendix 11, chap. 5. The cryptographic key used for securing the data transfer is either a symmetric session key which is generated during a preceding mutual authentication process between the card and the external world (realised by the TSFs F.IA_AKEY and F.GEN_SES) or a static symmetric key. For checksum securing, the TSF makes use of the TSF F.DES of the underlying IC resp. its Dedicated Support Software.
Object Reuse	
F.RIP	**Residual Information Protection**
	The TSF ensures that any previous information content of a resource is explicitly erased upon the deallocation of the resource used for any of the following components: - volatile and non-volatile memories used for operations in which security relevant material (e.g. secret keys or other secrets like passwords) is involved The TSF makes use of the TSF F.Object_Reuse of the underlying IC resp. its Dedicated Sup-

	port Software.
Protection	
F.FAIL_PROT	**Hardware and Software Failure Protection**
	The TSF preserves a secure operation state of the card when the following types of failures occur: - induced hardware or software failures (transient or permanent) during the execution of an operation resp. command, in particular: - Power supply cut-off - Power supply variations - Manipulation of executable code - Environmental stress - Manipulation resp. insufficient quality of the HW-RNG - HW and/or SW induced reset - Unexpected abortion of the TSF due to external or internal events (in particular, break of a transaction before completion) - System breakdown - Internal HW and/or SW failure - Corruption of status information (as e.g. card status information, object life cycle state, actual security state related to key and password based authentication, ...) - Environmental stress - Input of inconsistent or improper data - tampering The TSF makes use of hardware and software based security features and corresponding mechanisms to monitor and detect induced hardware and software failures and tampering attacks. In particular, the TSF is supported by the IC specific TSFs F.OPC and F.PHY. Upon the detection of a failure of the above mentioned type the TSF reacts in such a way that the TSP is not violated. The TOE changes immediately to a locked state and cannot be used any longer within the actual session. Depending on the type of the detected attack to the underlying IC (incl. its Dedicated Software) or to the Smartcard Embedded Software code the TOE will be irreversible locked resp. can be reactivated by a reset.
F.SIDE_CHAN	**Side Channel Analysis Control**
	The TSF manages suitable hardware and software based mechanisms to prevent attacks by a side channel analysis like Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and Timing attacks. The TSF ensures that all countermeasures available are used in such a way that they support each other. In particular, the TSF is supported by the TSF F.LOG of the underlying IC and its Dedicated Support Software. The TSF acts in such a manner that all security relevant operations of the TOE (esp. the TOE's cryptographic operations) are suitably secured by these hardware and software coun-

	termeasures. The TSF guarantees that information on IC power consumption, information on command execution time and information on electromagnetic emanations do not lead to useful information on processed security critical data as secret cryptographic keys or passwords. In particular, the IC contacts as Vcc, I/O and GND or the IC surface do not make it possible for an attacker to gain access to security critical data as secret cryptographic keys or passwords. The TSF enforces that a secure session is installed before any cryptographic key is generated, loaded into volatile / non-volatile memories (esp. of dedicated IC cryptographic modules) and processed in a cryptographic operation or in an authentication process.
F.SELFTEST	**Self Test**
	The TSF provides the capability of conducting a self test during initial start-up, i.e. after each reset to demonstrate the correct operation of its TSFs. Under the assumption that the TOE performs at least one reset-operation each day, the self test fulfills the requirement of being performed periodically during normal operation. The TOE's self tests consist of the verification of the integrity of any software code stored in the EEPROM area by checking a related checksum of the code. Furthermore, the TSF provides authorised users - here the Smartcard Embedded Software of the TOE (TOE-ES) itself - with the capability to verify the integrity of TSF data. For this task, the TSF is supported by the TSF F.DATA_INT. Additionally, the TSF provides authorised users with the capability to verify the integrity of stored TSF executable code. This concerns only the production phase, more precise the initialisation phase of the TOE (phase 5 of the product´s life cycle). Prior to the initialisation of the TOE, the ROM-code of the TOE can be verified by the Smartcard Embedded Software developer. The integrity of the EEPROM-code is checked by the TOE during the storage of the initialisation file in the framework of the initialisation. The TSF supports all other TSFs defined for the Smartcard Embedded Software (TOE-ES).
Cryptographic Operations	
F.CRYPTO	**Cryptographic Support**
	The TSF provides cryptographic support for the other TSFs using cryptographic mechanisms. The TSF supports: - DES/TDES algorithm accodring to the standard /FIPS 46-3/ resp. /ANSI X9.52/. - RSA core algorithm according to the standard /PKCS1/ with key lengths of up to 2048 bit modulus lengths - Random number generation by a pseudo RNG. The generator is seeded by teh hardware random number generator. - hash value calculation - Negotiation of TDES session keys The resistance of the TSF against SPA, DPA, DFA and TA is part of the TSF F.SIDE_CHAN. The random number generation is in particular used for RSA and DES key generation and authentication mechanisms.

	The mechanism for the generation of session keys is directly connected with the TSFs F.IA_AKEY which realise internal and external authentication processes. Furthermore, the generation of random numbers of high quality, and depending on the authentication type, the SHA-256 hash value calculation of TSF F.CRYPTO are involved. The TSF is directly supported by the TSFs of the underlying IC and its Cryptographic Library which supply cryptographic functionality. In particular, the TSFs F.RNG, F.HW_DES, F.DES, F.RSA_encrypt, F.RSA_sign, F.RSA_public, F.SHA and F.RNG_Access are involved. Due to the requirements of the Tachograph specification /TachAn1B/, the RSA keys in the Tachograph cards use only a key length of 1024 bit and the only available hashing algorithm is SHA-1. Please refer to Section 6.2 for an assessment of the situation.
F.GEN_SES	**Generation of Session Keys**
	The TSF generates session keys for symmetric cryptography used for securing the data exchange between the TOE and the external world with regard to data confidentiality and data integrity and authenticity. The TSF enforces that the key material meets the following requirements: - random numbers generated by the card and used in the key generation process have a high quality The TSF for generation of session keys is connected with the TSF F.RNG_Access for the generation of random numbers with high quality. Furthermore, the TSF for generation of session keys is directly connected with the TSF F.IA_AKEY which realises the internal and external authentication process.
F.GEN_DIGSIG	**Generation of Digital Signatures**
	The TSF provides a digital signature functionality based on asymmetric cryptography. The TSF digital signature function will be used for several purposes with different signature keys and different formats for the digital signature input: - Explicit generation of digital signatures of data using the signature scheme with appendix (signature generation operation) according to the standard /PKCS1/ and with a hash algorithm supplied by F.CRYPTO. In this case, the TSF digital signature function is implicitly combined with the Tachograph Card´s dedicated and unique private signature key stored in the card. - Within authentication processes for the creation of authentication tokens using the signature scheme with message recovery (signature generation operation) according to the standard ISO 9796-2 and with a hash algorithm supplied by F.CRYPTO. In this case, the TSF digital signature function is implicitly combined with the Tachograph Card´s dedicated private personalisation key (during the personalisation phase) resp. with the Tachograph Card´s dedicated and unique private signature key (during the end-usage phase of the card). - For proving the authenticity of the ORGA Tachograph Card: creation of an authentication token using the signature scheme with message recovery (signature generation operation) according to the standard ISO 9796-2 and with hash algorithm supplied by F.CRYPO.

	In this case, the TSF digital signature function is implicitly combined with the Tachograph Card´s dedicated private authentication key stored in the card. Random numbers necessary for the generation of digital signatures are generated by using the TSF F.RNG_Access of the underlying IC resp. its Dedicated Support Software for random number generation. For the signature mechanism itself, the TSF makes use of the services supplied by F.CRYPTO. For the computation of hash values the a hash function supplied by TSF F.CRPYTOis used. Furthermore, the security of the TSF is supported by the TSFs F.LOG and F.SIDE_CHAN of the IC and its Dedicated Support Software resp. the Smartcard Embedded Software. Note: Each pivate key used for the signature generation function is generated by the external world and loaded onto the card (during initialisation resp. personalisation). It is in the responsibility of the external world to guarantee for a sufficient cryptographic strength of the private key and to handle the private key outside the card in a sufficient secure manner. Under the assumption that the external world meets the requirements on the key handling set above, the TSF digital signature function works in such a manner that the private key cannot be derived from the signature and the signature cannot be generated by other individuals not possessing that secret. Furthermore, the TSF digital signature function works in a manner that no information about the private key may be disclosed during the generation of the digital signature. Due to the requirements of the Tachograph specification /TachAn1B/, the signature schemes are restricted - to RSASSA_PKCS1-v1_5 with hashing function SHA-1 for the scheme according to /PKCS1/ - and to RSA_ISO9796_2_DSS1 with hashing function SHA-1 for the scheme according to /ISO 9796-2/
F.VER_-DIGSIG	**Verification of Digital Signatures**
	The TSF provides a functionality to verify digital signatures based on asymmetric cryptography, particularly the RSA algorithm with cryptographic primitives supplied by F.CRPYTO. The TSF function to verify a digital signature will be used for several purposes with different keys and different formats for the digital signature input: - Explicit verification of digital signatures of data using the signature scheme with appendix (signature verification operation) according to the standard PKCS#1 V2.0 and with a hashing algorithm provided by F.CRYPTO. - Within authentication processes for the verification of authentication tokens using the signature scheme with message recovery (signature verification operation) according to the standard ISO 9796-2 and with a hashing algorithm supplied by F.CRYPTO. - Within the verification and unwrapping of imported certificates using the signature scheme with message recovery (signature verification operation) according to the standard ISO 9796-2 and with a hashing algorithmsupplied by F.CRYPTO. In all cases, the TSF function to verify a digital signature uses the public key which has been referenced before. In this connection, the public key is either stored in the card (e.g. within a certificate) or is loaded onto the card within a certificate by a suitable preceding operation. Due to the requirements of the Tachograph specification /TachAn1B/, the signature scheme are restricted to the - RSASSA_PKCS1-v1_5_VERIFY with hashing function SHA-1 according to /PKCS1/ - and RSA_ISO9796_2_DSS1_VERIFY with hashing function SHA-1 according to /ISO

	9796-2/ .
F.RSA_ENC	**Encryption**
	The TSF provides a functionality to encrypt data based on asymmetric cryptography, particularly the RSA algorithm with a key length of up to 2048 bit. The TSF encryption function will be used for the following purpose: - Within authentication processes for the generation of authentication tokens using the encryption primitive according to the standard /PKCS1/ The TSF encryption function uses the public key which has been referenced before. In this connection, the public key is either stored in the card (e.g. within a certificate) or is loaded onto the card within a certificate by a suitable preceding operation. For the encryption mechanism itself, the TSF makes use of the TSF F.RSA of the underlying IC resp. its Dedicated Support Software. Due to the requirements of the Tachograph specification /TachAn1B/, the encryption scheme is restricted to RSAES_PKCS1_V1_5 and a RSA key length of 1024 bit.
F.RSA_DEC	**Decryption**
	The TSF provides a functionality to decrypt data based on asymmetric cryptography, particularly the RSA algorithm with a key length of up to 2048 bit. The TSF decryption function will be used for the following purposes: - Within authentication processes for the verification of authentication tokens using the decryption primitive according to the standard /PKCS1/. - For the secured import of a static symmetric personalisation key (only relevant for the personalisation phase): decryption of the imported cryptogram with the personalisation key using the decryption primitive according to the standard /PKCS1/ and recovering the key from the encryption input (remove of padding). The TSF decryption function is implicitly combined with the Tachograph Card´s dedicated private personalisation key (during the personalisation phase) resp. with the Tachograph Card´s dedicated and unique private signature key (during the end-usage phase of the card). The functionality for a secure import of a static personalisation key is only relevant for the personalisation phase. Note: Each pivate key used for the decryption function is generated by the external world and loaded on the card (during initialisation resp. personalisation). It is in the responsibility of the external world to guarantee for a sufficient cryptographic strength of the private key and to handle the private key outside the card in a sufficient secure manner. Under the assumption that the external world meets the requirements on the key handling set above, the TSF decryption function works in such a manner that no information about the private key may be disclosed during the decryption operation. For the decryption mechanism itself, the TSF makes use of the TSF F.RSA of the underlying IC resp. its Dedicated Support Software. Furthermore, the security of the TSF is supported by the TSFs F.LOG and F.SIDE_CHAN of the IC and its Dedicated Support Software resp. the Smartcard Embedded Software.

	Due to the requirements of the Tachograph specification /TachAn1B/, the encryption scheme is restricted to RSAES_PKCS1_V1_5 and a RSA key length of 1024 bit.

6.2 SOF Claim for TOE Security Functions

According to Common Criteria, /CC 2.3 Part1/ and /CC 2.3 Part3/, all TOE Security Functions (TSF) which are relevant for the assurance requirement AVA_SOF.1 are identified in this section.

The TOE Security Functions using mechanisms which can be analysed for their permutational or probabilistic properties and which contribute to AVA_SOF.1 are the following:

- The generation of random numbers by the hardware RNG within the TSF F.RNG resp. by the software RNG within the TSF F.RNG_Access can be analysed with probabilistic methods.
- The quality of the mechanisms contributing to the resistance against leakage attacks of the TSF F.LOG, especially for the TSF F.HW_DES can be analysed using permutational or probabilistic methods on power consumption of the TOE.
- The implementations of the algorithms for F.DES, F.RSA_sign, F.RSA_encrypt, F.GEN_DIGSIG and F.RSA_DEC are resistant to Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks. This concerns as well all security critical mechanisms of the TSF F.IA_AKEY. The quality of these mechanisms against leakage attacks can be analysed using permutational or probabilistic methods.
- The implementation of the password based authentication mechanism as used within the TSF F.IA_PWD can be analysed with permutational methods.

For each of the TOE Security Functions given in the preceding list an explicit claim of "SOF-high" is made with the following restriction:

According to /ALGCAT/ neither RSA keys of 1024 bits length nor the SHA-1 hashing function is still considered to be strong enough for the generation of qualified electronic signatures, which implies that the strength of function claim of SOF-high is questionable. Furthermore, /PKCS1/ recommends the use of the RSAES_OAEP encryption scheme while the Tachograph specification still postulates the use of the PKSC1_V1.5 scheme.

The Micardo Tachograph product adheres to the Tachograph specification even though a gradual transition to stronger cryptographic mechanisms is needed to a achieve the unrestricted SOF claim of high. However, the developer *stresses* that the limitations imposed by the Tachograph specification only affect the assessment of the *algorithmic* strength of the functions. The implementation of the algorithms in particular the SPA/DPA and DFA resistance is rated against a *state-of-the-art* high attack potential.This significantly increases the protection of and the assurrance in the product, even if the restrictions of the specification do not permit to use appropriate key lengths and the most modern algorithms.

Notes:

The implementation of the TSF F.DATA_INT will be realised by attaching CRC-checksums to defined data areas. Hereby, the mechanisms of generating and checking CRC-checksums can be analysed with permutational or probabilistic methods. But these mechanisms are not relevant for AVA_SOF.1, as the securing of data areas by CRC-checksums is intended only to secure against accidental data modification.

The implementations of the TSFs F.RSA_public (of the underlying IC), F.VER_DIGSIG and F.RSA_ENC use only public keys and do not need to be considered with regard to high attack potential so that securing of the implementations against Differential Fault Analysis (DFA) because no promising DFA attack paths on public key computations are known. However, SPA and DPA resistance of the implementation of F.RSA_ENC and F.VER_DIGSIG is considered in the composite evaluation because public key operations are involved in processing confidential operations like encryption and decryption of session keys.

The implementation for the TSF F.SHA-1 can be analysed with permutational or probabilistic methods, but the TSF does not contribute to AVA_SOF.1 as the developers of the Crypto Library and the Smartcard Embedded Software do not see the hash algorithm as a cryptographic mechanism in the sense of the Common Criteria (CC). Nevertheless, this TSF is secured by appropriate hardware security features.

The TOE’s cryptographic algorithms itself can also be analysed with permutational or probabilistic methods but this is not in the scope of CC evaluations.

6.3 Assurance Measures

Appropriate assurance measures will be employed by the developer of the TOE to satisfy the security assurance requirements defined in chap. 5.1.3. For the evaluation of the TOE, the developer will provide appropriate documents describing these measures and containing further information supporting the check of the conformance of these measures against the claimed assurance requirements.

For the Smartcard Embedded Software part of the TOE (TOE-ES), the following table gives a mapping between the assurance requirements and the documents containing the relevant information for the respective requirement. All these documents concerning the TOE-ES are provided by the developer of the TOE-ES. The table below contains only the directly related documents, references to further documentation can be taken from the mentioned documents.

Overview of Developer´s TOE-ES related Documents		
Assurance Class	**Family**	**Document containing the relevant information**
ACM Configuration Management	ACM_AUT	- Document Configuration Control System
	ACM_CAP	- Document Life-Cycle Model - Document Configuration Control System
	ACM_SCP	- Document Configuration Control System - Document Life-Cycle Model
ADO Delivery and	ADO_DEL	- Document Life-Cycle Model

Operation	ADO_IGS	- Document Installation, Generation and Start-Up Procedures
ADV Development	ADV_FSP	- Document Functional Specification
	ADV_HLD	- Document High-Level Design - Detailed development documents as system specifications, design specifications, etc.
	ADV_LLD	- Document Low-Level Design - Detailed development documents as system specifications, design specifications, etc.
	ADV_IMP	- Source Code - Detailed development documents as system specifications, design specifications, etc.
	ADV_RCR	- Functional Specification - High-Level Design - Low-Level Design
	ADV_SPM	- Document TOE Security Policy Model
AGD Guidance Documents	AGD_ADM	--- (Part of the User Guidances.)
	AGD_USR	- User Guidance for the Personaliser of the Tachograph Card - User Guidance for the Operation of Tachograph Cards
ALC Life Cycle Support	ALC_DVS	- Document Security of the Development Environment
	ALC_LCD	- Document Life-Cycle Model
	ALC_TAT	- Configuration List
ATE Tests	ATE_COV	- Document Test Documentation - Detailed test documentation as system test specifications, test protocols, etc.
	ATE_DPT	- Document Test Documentation - Detailed test documentation as system test specifications, test protocols, etc.
	ATE_FUN	- Document Test Documentation - Detailed test documentation as system test specifications, test protocols, etc.
	ATE_IND	- Samples of the TOE - Source Code
AVA Vulnerability Assessment	AVA_MSU	- Document Analysis of the Guidance Documents
	AVA_SOF	- Document TOE Security Function Evaluation
	AVA_VLA	- Document Vulnerability Analysis

As mentioned, the evaluation of the TOE will be done as composite evaluation on basis of the evaluated IC "NXP SmartMX P5CC037V0A Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH. Therefore, for the TOE-IC the following documents will be at least provided by the IC developer:

Overview of Developer´s TOE-IC related Documents	
Class	Documents
Security Target	Security Target of the IC evaluation, /ST_IC/
	Security Target of the IC evaluation incl. Crypto Library, /ST_IC_CL/
User Guidances	User Guidance for the IC, /UG_IC/
	Data Sheet for the IC, /DS_IC/
	User Guidances for the Crypto Library, /UG_CL/, /UG_CL_RNG/, /UG_CL_DES/, /UG_CL_SHA/, /UG_CL_RSA/

7 PP Claims

Not applicable. Refer to chap. 1.3.

8 Rationale

The following chapters cover the security objectives rationale, the security requirements rationale and the TOE summary specification rationale. Furthermore, the chapter contains a statement of compatibility between the platform security target and this composite security target according to the requirements of /AIS36/.

The chapter is not disclosed in the ST-Lite.

Reference

I Bibliography

/CC 2.3 Part1/

Title:	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model
Identification:	CCMB-2005-08-001
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.3 Part2/

Title:	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements
Identification:	CCMB-2005-08-002
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.3 Part3/

Title:	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements
Identification:	CCMB-2005-08-003
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CEM 2.3/

Title:	Common Methodology for Information Technology Security Evaluation - Evaluation Methodology
Identification:	CCMB-2005-08-004
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/AIS32/

Title:	Übernahme international abgestimmter CC Interpretationen
Identification:	AIS 32
Date:	02.07.2001
Publisher:	Bundesamt für Sicherheit in der Informationstechnik

/AIS36/

Title: Kompositionsevaluierung
Identification: AIS 36, Version 2
Date: 12.11.2007
Publisher: Bundesamt für Sicherheit in der Informationstechnik

/JILDigTacho/
Title: JIL Security Evaluation and Certification of Digital Tachographs
Version: Version 1.12
Date: June 2003
Author: JIL Working Group (BSI, CES, DCSSI, NLNCSA)

/PP9806/
Title: Protection Profile - Smartcard Integrated Circuit
Identification: Registered at the French Certification Body (DCSSI) under the number PP/9806
Version: Version 2.0
Date: Sept. 1998
Author: Motorola Semiconductors, Philips Semiconductors, Service Central de la Securite des Systemes d´Information, Siemens AG Semiconductors, ST Microelectronics, Texas-Instruments Semiconductors

/DCSSI_PP_IC/
Title: Protection Profile - Smartcard Integrated Circuit
Identification: Registered at the French Certification Body (DCSSI) under the number PP/9806
Version: Version 2.0
Date: Sept. 1998
Author: Motorola Semiconductors, Philips Semiconductors, Service Central de la Securite des Systemes d´Information, Siemens AG Semiconductors, ST Microelectronics, Texas-Instruments Semiconductors

/PP9911/
Title: Protection Profile - Smartcard Integrated Circuit with Embedded Software
Identification: Registered at the French Certification Body (DCSSI) under the number PP/9911
Version: Version 2.0
Date: June 1999
Author: Atmel Smart Card ICs, Bull-SC&T, De la Rue – Card Systems, Eurosmart, Gemplus, Giesecke & Devrient GmbH, Hitachi Europe Ltd, Infineon Technologies AG, Microelectronica Espana, Motorola SPS, NEC Electronics, Oberthur Smart Card, ODS, ORGA Kartensysteme GmbH, Philips Semiconductors Hamburg, Schlumberger Cards Devision, Service Central de la Securite des Systemes d´Information, ST Microelectronics

/DCSSI_PP_ICES/
Title: Protection Profile - Smartcard Integrated Circuit with Embedded Software
Identification: Registered at the French Certification Body (DCSSI) under the number PP/9911
Version: Version 2.0
Date: June 1999
Author: Atmel Smart Card ICs, Bull-SC&T, De la Rue – Card Systems, Eurosmart, Gemplus, Giesecke & Devrient GmbH, Hitachi Europe Ltd, Infineon Technologies AG, Microelectronica Espana, Motorola SPS, NEC Electronics, Oberthur Smart Card, ODS, ORGA Kartensysteme GmbH, Philips Semiconductors Hamburg, Schlumberger Cards Devision, Service Central de la Securite des Systemes d´Information, ST Microelectronics

/BSI-PP-IC/
Title: Smartcard IC Platform Protection Profile
Identification: Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002
Version: Version 1.0
Date: July 2001
Author: Atmel Smart Card ICs, Hitachi Europe Ltd, Infineon Technologies AG, Philips Semiconductors

/CompPP9806-BSIPP0002/
Title: Assessment on the Substitution of an Evaluation based on PP/9806 by an Evaluation based on BSI-PP-0002-2001
Version: Version 1.1
Date: May 2002
Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI)

/DS_IC/
Title: Product Data Sheet: P5xC012/02x/037/052 family – Secure dual interface and contact PKI smart card controller
Version: Revision 3.6
Date: 6th April 2009
Publisher: NXP Semiconductors GmbH

/UG_IC/
Title: Guidance, Delivery and Operation Manual for the P5xC012/02x/037/052 family
Version: Revision 1.5
Date: 23rd January 2008
Publisher: NXP Semiconductors GmbH

/UG_CL/

Title: Secured Crypto Library on the P5xC012/02x/037/052 Family
Version: Revision 1.4
Date: 7th October 2009
Publisher: NXP Semiconductors GmbH

/UG_CL_RNG/
Title: Secured Crypto Library on the SmartMX, User guidance manual: Random Number Generator
Version: Revision 5.0
Date: 24nd Aug. 2007
Publisher: NXP Semiconductors GmbH

/UG_CL_DES/
Title: Secured Crypto Library on the SmartMX, User guidance manual: DES Library
Version: Revision 3.0
Date: 24th Aug. 2007
Publisher: NXP Semiconductors GmbH

/UG_CL_SHA/
Title: Secured Crypto Library on the SmartMX, User guidance manual: SHA Library
Version: Revision 4.1
Date: 12th June 2008
Publisher: NXP Semiconductors GmbH

/UG_CL_RSA/
Title: Secured Crypto Library on the SmartMX, User guidance manual: RSA Library
Version: Revision 4.2
Date: 7th October 2009
Publisher: NXP Semiconductors GmbH

/ST_IC/
Title: Security Target Lite – P5CC037V0A
Identification: BSI-DSZ-CC-0465-2008(-MA-1b)
Version: Revision 1.6
Date: 9th July 2009
Publisher: NXP Semiconductors GmbH

/ST_IC_CL/
Title: Security Target Lite – Crypto Library Version 2.2 on the P5CC037V0A
Identification: BSI-DSZ-CC-612-2008()
Version: Revision 1.2

Date: 07th Oct 2009
Publisher: NXP Semiconductors GmbH

/TachAn1B/
Title: Annex 1B of Commission Regulation (EC) No.1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, L 207 / 1 ff.)
Date: 05.08.2002
Publisher: Commission of the European Communities

/ISO9796-2/
Title: Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2: Mechanisms Using a Hash Function
Identification: ISO/IEC 9796-2
Version: First Edition
Date: 1997
Publisher: ISO / IEC

/ISO9798-3/
Title: Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 3: Entity Authentication Using a public key algorithm
Identification: ISO/IEC 9798-3
Version: Second Edition
Date: 1998
Publisher: ISO / IEC

/ISO 7816-4/
Title: Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interchange
Identification: ISO/IEC 7816-4
Version: First edition
Date: September 1.1995
Publisher: International Organization for Standardization/International Electrotechnical Commission

/ISO 7816-8/
Title: Integrated circuit(s) cards with contacts. Part 8: Interindustry commands for interchange
Identification: ISO/IEC FDIS 7816-8
Date: June 1998
Publisher: International Organization for Standardization/International Electrotechnical Commission

/ISO 7816-9/
Title: Integrated circuit(s) cards with contacts. Part 9: Enhanced inter-industry commands
Identification: ISO/IEC 7816-9
Version: First Edition
Date: Sept. 2000
Publisher: International Organization for Standardization/International Electrotechnical Commission

/ALGCAT/
Title: Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs.1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Anschnitt I Nr. 2 SigV vom 22. Nov. 2001
Identification: Bundesanzeiger (published 04.02.2010, Nr 19, pp426)
Date: 06.01.2010
Publisher: Bundesnetzagentur

/SHA-1/
Title: Secure Hash Standard
Identification: FIPS Publication 180-1
Date: April 1995
Publisher: National Institute of Standards and Technology (NIST)

/FIPS 46-3/
Title: Data Encryption Standard (DES)
Identification: FIPS Publication 46-3
Date: October 1999
Publisher: National Institute of Standards and Technology (NIST)

/ANSI X9.52/
Title: Triple Data Encryption Algorithm Modes of Operation
Identification: ANSI X9.52
Date: 1998
Publisher: American National Standards Institute (ANSI)

/PKCS1/
Title: PKCS #1 v2.1: RSA Cryptography Standard
Date: June 2002
Publisher: RSA Laboratories

/ISO 9796-2/
Title: Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2: Integer Factorization Based Mechanisms
Identification: ISO/IEC 9796-2
Version: Second Edition
Date: 2002
Publisher: ISO / IEC

/TDES/
Title: Data Encryption Standard
Identification: FIPS Publication 46-3
Date: Draft 1999
Publisher: National Institute of Standards and Technology (NIST)

/TDES-OP/
Title: Triple Data Encryption Algorithm Modes of Operation
Identification: ANSI X9.52
Date: 1998
Publisher: American National Standards Institute

/PKCS1/
Title: RSA Encryption Standard
Identification: PKCS#1
Version: Version 2.0
Date: Oct. 1998
Publisher: RSA Laboratories

II Summary of abbreviations

2TDES	Triple DES using two 8 byte keys (effective key length 128 or 112 bit)
3TDES	Triple DES using three 8 byte keys (effective key length 192 or 168 bit)
A.x	Assumption
AC	Access Condition
AID	Application Identifier
ALW	Always
AM	Access Mode
AR	Access Rule
AS	Application Software
ATR	Answer To Reset
AUT	Key Based Authentication
BS	Basic Software
CC	Common Criteria
DES	Data Encryption Standard
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EF	Elementary File
ES	Embedded Software
IC	Integrated Circuit
IFD	Interface Device
ITSEC	Information Technology Security Evaluation Criteria
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MF	Master File
O.x	Security Objective
OS	Operating System

PAR	Partial Access Rule
P.x	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
PW	Password
PWD	Password Based Authentication
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Secure Messaging
SOF	Strength of Functions
SPA	Simple Power Analysis
SPM	TOE Security Policy Model
SSC	Send Sequence Counter
ST	Security Target
T.x	Threat
TDES	Triple DES, uses three base operations ENC, DEC, ENC
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VU	Vehicle Unit

III Glossary

For explanation of technical terms refer to the following documents:

/PP9911/, Annex A

/BSI-PP-IC/, Chap. 8.7

/ST_IC_CL/, Glossary

/TachAn1B/, main body, Chap. I Definitions

/TachAn1B/, Appendix 10, Tachograph Card Generic Security Target, Chap. 2