Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0243-2004

for

Tachograph Card Version 1.1 128/64 R1.0

from

ORGA Kartensysteme GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0243-2004

Smartcard with Tachograph Application

Tachograph Card Version 1.1 128/64 R1.0

from

ORGA Kartensysteme GmbH

IT Security Certified

SOGIS-MRA

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0*, extended by advice of the Certification Body for components beyond EAL4 and Smartcard specific guidance, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

Functionality:	**Product specific Security Target according to Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002, amending Regulation (EEC) no. 3821/85 on recording equipment in road transport; Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant, EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4; Equivalent to ITSEC E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 06. February 2004

The Vice President of the Federal Office
for Information Security

Common Criteria

Hange L.S.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Tachograph Card Version 1.1 128/64 R1.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0205-2003.

The evaluation of the product Tachograph Card Version 1.1 128/64 R1.0 was conducted by SRC Security Research & Consulting GmbH (ITSEF)[6]. SRC Security Research & Consulting GmbH is an evaluation facility recognised by BSI.

The sponsor and vendor and distributor is ORGA Kartensysteme GmbH.

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 06. February 2004.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-28.

The product Tachograph Card Version 1.1 128/64 R1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] ORGA Kartensysteme GmbH, Am Hoppenhof 33, 33104 Paderborn

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

Target of Evaluation (TOE) and subject of the Security Target (ST) [6] and [7] is the smartcard product “Tachograph Card Version 1.1 128/64 R1.0”.

The TOE will be used within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment.

The basic functions of the Tachograph Card are:

- 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 life cycle (phase 7 of life-cycle as described), vehicle units only may write user data to the card. A Tachograph Card is either of the type Driver Card or Control Card or Workshop Card or Company Card as outlined in the ST [7], chapter 2.4.

The TOE comprises the following components:

- Integrated Circuit (IC) "Philips P16WX064V0C Secure 16-bit Smart Card Controller " provided by Philips Semiconductors GmbH
- Caernarvon Cryptographic Library on Philips Smart *XA*2 as IC Dedicated Support Software provided by Philips Semiconductors GmbH
- Smartcard Embedded Software based on a Java Card Platform Version 2.1.1 with a specific Java Card Applet for the Tachograph Application provided by ORGA Kartensysteme GmbH.

The Java Card Applet for the Tachograph Application consists of a fix part containing the executable code and another configurable 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. Additionally, a General Tachograph Card is available that can be irreversibly converted into one of the different types Driver Card, Control Card, Workshop Card and Company Card by using a specific card command after initialisation resp. prior to the personalisation of the card.
- 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 developed and constructed in full accordance with the Tachograph Card Specification [8], Annex 1B 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, part 2, part 3, part 4 and part 8; ISO/IEC 10373 Identification cards – Test methods.

In order to achieve the required system security, the Tachograph Card and the corresponding ST [6] and [7] meet all the security requirements and evaluation conditions defined in the Tachograph Card's "Generic Security Target" in [8], Appendix 10 under consideration of the interpretations in [9].

The life-cycle of the TOE conforms to the smartcard life cycle described in Appendix 10 of [8] referring to PP/9911 [13]. The following table outlines this life-cycle for the TOE:

Phase		**Description**
Phase 1	Smartcard Embedded Software Development	The Smartcard Embedded Software Developer (ORGA Kartensysteme GmbH, Paderborn) is in charge of the Smartcard Embedded Software (Basic Software, Application Software) development and the specification of IC initialisation and pre-personalisation requirements.
Phase 2	IC Development	The IC Designer (Philips Semiconductors GmbH) designs the IC, develops 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. The IC Designer constructs the smartcard IC database, necessary for the IC photomask fabrication.
Phase 3	IC Manufacturing and Testing	The IC Manufacturer (Philips Semiconductors GmbH) generates the masks for the IC manufacturing based upon an output from the smartcard IC database. He is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalisation.
Phase 4	IC Packaging and Testing	The IC Packaging Manufacturer (ORGA Kartensysteme GmbH, Flintbek) is responsible for the IC packaging (production of modules) and testing.
Phase 5	Smartcard Product Finishing Process	The Smartcard Product Manufacturer (ORGA Kartensysteme GmbH, Flintbek) is responsible for the initialisation of the TOE (in form of initialisation of the modules of phase 4) and its testing. In this phase the TOE becomes either the type Driver Card or Control Card or Workshop Card or

Phase		Description
		Company Card. The smartcard product finishing process comprises the embedding of the initialised modules for the TOE and the card production what is done alternatively by ORGA Kartensysteme GmbH or by the customer.
Delivery of the TOE		Two different ways for delivery are established: (i) The TOE is delivered to the customer in form of a complete (initialised) smartcard. (ii) Alternatively, the TOE is delivered to the customer in form of an initialised module. In this case, the smartcard finishing process (embedding, final tests) is task of the customer.
Phase 6	Smartcard Personalisation	The Personaliser is responsible for 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.

Table 1: Life cycle of the TOE

The evaluation of the TOE was conducted as a composition evaluation making use of the platform evaluation results of the CC evaluations

- of the underlying semiconductor "Philips P16WX064V0C Secure 16-bit Smart Card Controller" provided by Philips Semiconductors GmbH [18] and
- of the underlying semiconductor "Philips P16WX064V0C Secure 16-bit Smart Card Controller with Caernarvon Cryptographic Library on Philips Smart *XA*2 as IC Dedicated Support Software" provided by Philips Semiconductors GmbH.

For the re-certification, a reassessment of the hardware platform (Philips P16WX064V0C Secure 16-bit Smart Card Controller with Caernarvon Cryptographic Library) had been successfully carried out by T-Systems GEI GmbH.

Both, the IC itself and the IC with its IC Dedicated Software were evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high based on the Protection Profile BSI-PP-0002 [12]. These platform evaluations were performed by T-Systems GEI GmbH.

The Embedded Software of the “Tachograph Card Version 1.1 128/64 R1.0” and the overall composition was evaluated by SRC Security Research & Consulting GmbH.

The concept for composition as outlined in CC Supporting Document [4, AIS 36] was used.

The evaluation was completed on 03 February 2004. Both, the SRC Security Research & Consulting GmbH and the evaluation facility of T-Systems GEI GmbH are evaluation facilities (ITSEF)[8] recognised by BSI. The sponsor, vendor and distributor of the Tachograph Card Version 1.1 128/64 R1.0 is ORGA Kartensysteme GmbH.

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Part C or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: Methodically designed, tested, and reviewed
+: ADO_IGS.2	Delivery and operation - Generation log
+: ADV_IMP.2	Development - Implementation of the TSF
+: ATE_DPT.2	Tests - Testing: low-level design
+: AVA_VLA.4	Vulnerability assessment – Highly resistant

Table 2: Assurance components and EAL-augmentation

The level of assurance and the augmentations are chosen in order to allow the confirmation of equivalence to ITSEC [10] E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] and outlined in JIL Security Evaluation and Certification of Digital Tachographs [9].

1.2 Functionality

The TOE Security Functional Requirements (SFR) and TOE Security Functions are based on Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] specified in the document JIL Security Evaluation and Certification of Digital Tachographs [9].

The TOE Security Functional Requirements selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

[8] Information Technology Security Evaluation Facility

Security Functional Requirement[9]	**Identifier**	**CC Part 2 conformant/ extended**
FCS_COP.1	Cryptographic operation (Triple-DES of HW only)	Conformant
FDP_ACC.1 [MEM]	Subset access control (Memory)	Conformant
FDP_ACC.1 [SFR]	Subset access control (Special Function Register)	Conformant
FDP_ACF.1 [MEM]	Security Attribute based access control (Memory)	Conformant
FDP_ACF.1 [SFR]	Security Attribute based access control (Special Function Register)	Conformant
FDP_IFC.1	Subset information flow control	Conformant
FDP_ITT.1	Basic internal transfer protection	Conformant
FPT_FLS.1	Failure with preservation of secure state	Conformant
FPT_ITT.1	Basic internal TSF data transfer protection	Conformant
FPT_PHP.3	Resistance to physical attack	Conformant
FPT_SEP.1	TSF domain separation	Conformant
FRAU_FLT.2	Limited fault tolerance	Conformant
FMT_MSA.3 [MEM]	Static attribute initialisation (Memory)	Conformant
FMT_MSA.3 [SFR]	Static attribute initialisation (Special Function Register)	Conformant
FMT_MSA.1 [MEM]	Management of security attributes (Memory)	Conformant
FMT_MSA.1 [SFR]	Management of security attributes (Special Function Register)	Conformant
FMT_SMF.1	Specification of Management Functions	Conformant
FAU_SAS.1	Audit storage	Extended see PP [12]
FCS_RND.1	Quality metric for random numbers	Extended see PP [12]
FMT_LIM.1	Limited capabilities	Extended see PP [12]
FMT_LIM.2	Limited availability	Extended see PP [12]
FRU_VRC.1	Simple value range check	Extended see ST of IC [19]

Table 3: Security Functional Requirements for the IC part of the TOE (see [18] and [19] for BSI-DSZ-CC-0203-2003).

Security Functional Requirement[10]	**Identifier**	**CC Part 2 conformant/ extended**
FCS_COP.1+1	Cryptographic operation (Triple-DES of SW using HW)	Conformant

[9] The brackets [xxx] after a component name indicates a specific iteration of the component

[10] The indicator +n after a component name indicates a specific iteration of the component

Security Functional Requirement[10]	Identifier	CC Part 2 conformant/ extended
FCS_COP.1+2	Cryptographic operation (RSA)	Conformant
FCS_COP.1+4	Cryptographic operation (SHA-1)	Conformant
FDP_IFC.1	Subset information flow control	Conformant
FDP_ITT.1	Basic internal transfer protection	Conformant
FDP_RIP.1	Subset residual information protection	Conformant
FPT_FLS.1	Failure with preservation of secure state	Conformant
FPT_ITT.1	Basic internal TSF data transfer protection	Conformant
FCS_RND.2	Random number generation	Extended see ST [7]
FPT_TST.2	Subset TOE security testing	Extended see ST [7]

Table 4: Security Functional Requirements for the IC dedicated SW part of the TOE

Security Functional Requirement[11]	Identifier	CC Part 2 conformant/ extended
FAU_SAA.1	Potential violation analysis	Conformant
FCO_NRO.1	Selective Proof of origin	Conformant
FCS_CKM.1	Cryptographic Key Generation (for Triple-DES Keys)	Conformant
FCS_CKM.2-1	Cryptographic Key Distribution (for Triple-DES Keys)	Conformant
FCS_CKM.2-2	Cryptographic Key Distribution (for public RSA Keys)	Conformant
FCS_CKM.2-3	Cryptographic Key Distribution (for static Triple-DES Keys)	Conformant
FCS_CKM.3-1	Cryptographic Key Access (to private RSA Key)	Conformant
FCS_CKM.3-2	Cryptographic Key Access (to public RSA Key)	Conformant
FCS_CKM.3-3	Cryptographic Key Access (to private RSA Key)	Conformant
FCS_CKM.3-4	Cryptographic Key Access (to public RSA Key)	Conformant
FCS_CKM.3-5	Cryptographic Key Access (to Triple-DES Key)	Conformant
FCS_CKM.4-1	Cryptographic Key Destruction (of Triple-DES Key)	Conformant
FCS_CKM.4-2	Cryptographic Key Destruction (of public RSA Key)	Conformant
FCS_COP.1-1	Cryptographic operation (explicit signature generation and verification)	Conformant
FCS_COP.1-2	Cryptographic operation (implicit signature generation and verification)	Conformant
FCS_COP.1-3	Cryptographic operation (implicit encryption and decryption operation)	Conformant

[11] The brackets -n after a component name indicates a specific iteration of the component

Security Functional Requirement[11]	**Identifier**	**CC Part 2 conformant/ extended**
FCS_COP.1-4	Cryptographic operation (encryption and decryption operation concerning symmetric cryptography)	Conformant
FCS_COP.1-5	Cryptographic operation (MAC generation and verification)	Conformant
FDP_ACC.2-1	Complete access control (for AC_SFP)	Conformant
FDP_ACC.2-2	Complete access control (for PERS-AC_SFP)	Conformant
FDP_ACF.1-1	Security attribute based access control (for AC_SFP)	Conformant
FDP_ACF.1-2	Security attribute based access control (for PERS-AC_SFP)	Conformant
FDP_DAU.1	Basic data authentication	Conformant
FDP_ETC.1	Export of user data without security attributes	Conformant
FDP_ETC.2	Export of user data with security attributes	Conformant
FDP_ITC.1	Import of user data without security attributes	Conformant
FDP_RIP.1	Subset residual information protection	Conformant
FDP_SDI.2	Stored data integrity monitoring and action	Conformant
FIA_AFL.1-1	Authentication failure handling (of interface device)	Conformant
FIA_AFL.1-2	Authentication failure handling (of PIN check workshop card)	Conformant
FIA_ATD.1	User attribute definition	Conformant
FIA_UAU.1	Timing of authentication	Conformant
FIA_UAU.3	Unforgeable authentication	Conformant
FIA_UAU.4	Single-use authentication mechanisms	Conformant
FIA_UID.1	Timing of identification	Conformant
FIA_USB.1	User-subject binding	Conformant
FPR_UNO.1-1	Unobservability (of mutual authentication operation)	Conformant
FPR_UNO.1-2	Unobservability (of import and export of user data)	Conformant
FPR_UNO.1-3	Unobservability (of import of static personalisation key)	Conformant
FPT_FLS.1	Failure with preservation of secure state	Conformant
FPT_PHP.3	Resistance to physical attack	Conformant
FPT_SEP.1	TSF domain separation	Conformant
FPT_TDC.1	Inter-TSF basic TSF data consistancy	Conformant
FPT_TST.1	TSF testing	Conformant
FTP_ITC.1	Inter-TSF trusted channel	Conformant

Table 5: Security Functional Requirements for the Embedded SW part of the TOE

These Security Functional Requirements are implemented by the following TOE Security Functions:

Identifier	Security Function
F.RNG	Random Number Generator
F.HW_DEA	Triple-DES Co-processor
F.OPC	Control of Operating Conditions
F.PHY	Protection against Physical Manipulation
F.LOG	Logical Protection
F.COMP	Protection of Mode Control
F.MEM_ACC	Memory Access Control
F.SFR_ACC	Special Function Register Access Control
F.RANGE_CHK	Value Range Check
F.DES	DES Operation
F.RSA	RSA Operation
F.SHA-1	SHA-1 Computation
F.RNG_Access	Generation of Random Numbers
F.Object_Reuse	Reuse of Objects

Table 6: TOE Security Functions of IC and IC dedicated SW parts of the TOE

Identifier	Security Function
F.ACS	Security Attribute Based Access Control
F.IA_KEY	Key Based User / TOE Authentication
F.IA_PWD	Password Based User Authentication (only relevant for the Tachograph Card type Workshop Card)
F.DATA_INT	Stored Data Integrity Monitoring and Action
F.EX_CONF	Confidentiality of Data Exchange
F.EX_INT	Integrity and Authenticity of Data Exchange
F.RIP	Residual Information Protection
F.FAIL_PROT	Hardware and Software Failure Protection
F.SIDE_CHAN	Side Channel Analysis Control
F.SELFTEST	Self Test
F.GEN_SES	Generation of Session Keys
F.GEN_DIGSIG	Generation of Digital Signatures
F.VER_DIGSIG	Verification of Digital Signatures
F.ENC	Encryption
F.DEC	Decryption

Table 7: TOE Security Functions of the Embedded SW part of the TOE

Note: Only the titles of the Security Functional Requirements and of the TOE Security Functions are provided. For more details please refer to the Security Target [7], chapter 5.1.1 and 6.1.

All TOE Security Functions are applicable from TOE delivery to phase 7 of the smartcard life cycle model.

1.3 Strength of Function

The TOE's strength of functions is rated 'high' (SOF-high) for the following functions:

- F.RNG (Random Number Generator);
- F.RNG_Access (Generation of Random Numbers);
- F.LOG (Logical Protection) especially for the F.HW_DEA (Triple-DES Co-processor);
- F.LOG (Logical Protection) and F.SIDE_CHAN (Side Channel Analysis Control) for F.DES (DES Operation), F.RSA (RSA Operation, only decryption part, F.GEN_DIGSIG (Generation of Digital Signatures), F.DEC (Decryption) and F.IA_KEY (Key Based User / TOE Authentication);
- F.IA_PWD (Password Based User Authentication).

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats are subdivided into three groups affecting the IC, the general, or the Tachograph Card specific Embedded Software:

Name	Definition
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

Table 8: Threats of IC and IC dedicated SW parts of the TOE

Name	Definition
Threats on all Phases	
T.CLON	Cloning of the TOE
Threats on Phase 1	
T.DIS_INFO	Disclosure of IC Assets

Name	Definition
T.DIS_DEL	Disclosure of the Smartcard Embedded Software / Application Data during Delivery
T.DIS_ES1	Disclosure of the Smartcard Embedded Software / Application Data within the Development Environment
T.DIS_TEST_ES	Disclosure of Smartcard Embedded Software Test Programs / Information
T.T_DEL	Theft of the Smartcard Embedded Software / Application Data during Delivery
T.T_TOOLS	Theft or Unauthorized Use of the Smartcard Embedded Software Development Tools
T.T_SAMPLE2	Theft or Unauthorized Use of TOE Samples
T_MOD_DEL	Modification of the Smartcard Embedded Software / Application Data during Delivery
T.MOD	Modification of the Smartcard Embedded Software / Application Data within the Development Environment
Threats on Delivery from Phase 1 to Phases 4 / 5 / 6	
T.DIS_DEL1	Disclosure of Application Data during Delivery
T.DIS_DEL2	Disclosure of Delivered Application Data
T.MOD_DEL1	Modification of Application Data during Delivery
T.MOD_DEL2	Modification of Delivered Application Data
Threats on Phases 4 to 7	
T.DIS_ES2	Disclosure of the Smartcard Embedded Software / Application Data
T.T_ES	Theft or Unauthorized Use of TOE
T.T_CMD	Use of TOE Command-Set
T.MOD_LOAD	Program Loading
T.MOD_EXE	Program Execution
T.MOD_SHARE	Modification of Program Behaviour
T.MOD_SOFT	Modification of Smartcard Embedded Software / Application Data

Table 9: Threats of the TOE-ES (Basic Software) parts of the TOE

Name	Definition
T.Ident_Data	Modification of Identification Data
T.Activity_Data	Modification of Activity Data
T.Data_exchange	Modification of Activity Data during Data Transfer
T.Pers_Data	Authentication for Personalisation
T.Pers_exchange	Modification or Disclosure of Personalisation Data during Data

Name	Definition
	Transfer

Table 10: Threats of the TOE-ES (Tachograph Card Specific Threats)

The Organisational Security Policies for the TOE are defined as:

Name	Definition
P.Process-Card	Protection during Packaging, Finishing and Personalisation
P.Design-Software	Design of the Smartcard Embedded Software

Table 11: OSPs for the TOE

Note: Only the titles of the threats and OSPs are provided. For more details please refer to the Security Target [7], chapter 3.

1.5 Special configuration requirements

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 tests) is task of the customer.

A Tachograph Card may be of the following types: Driver Card, Control Card, Workshop Card or Company Card as defined in [8] depending on the specific applet and data loaded into the card. Alternatively, in case of the card type General Tachograph Card, the applet may contain code with a prepared file system for the four card types. In that case, after initialisation resp. prior to the personalisation of the card, one of the four prepared card types has to be created by usage of a specific card command.

Two personalisation schemes are provided by the Tachograph Card:

- Dynamic scheme with Secure Messaging using a session key:

  The Tachograph Card 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 and makes use of asymmetric keys. The keys necessary on the card for the authentication procedure are part of the Application Software resp. the Tachograph Applet 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.

- 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 key has to be loaded with a specific card command in encrypted form.

In each case, the personalisation of the Tachograph Card requires a preceding authentication of the external world (personalisation unit). At the end of the personalisation process, the card is switched to the end-user operational phase.

There are no special security measures for the start-up of the TOE besides the requirement that the TOE has to be used under the well-defined operating conditions and that the requirements on the personalisation and usage have to be applied as described in the user documentation [15], [16] and [17].

1.6 Assumptions about the operating environment

The TOE is intended to be used within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment as specified in [8].

There do not exist any Tachograph Card specific assumptions for the environment of the TOE. The following general assumptions are made based on the PP/9911 [13] and PP/9806 [14] referenced in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] (Generic Security Target).

Name	Definition
Assumptions on Phase 1 to 5:	
A.DEV_ORG	Protection of the TOE under Development and Production
Assumptions on the TOE Delivery Process (Phases 4 to 7)	
A.DLV_PROTECT	Protection of the TOE under Delivery and Storage
A.DLV_AUDIT	Audit of Delivery and Storage
A.DLV_RESP	Responsibility within Delivery
Assumptions on Phases 4 to 6	
A.USE_TEST	Testing of the TOE
A.USE_PROD	Protection of the TOE under Testing and Manufacturing
Assumptions on Phase 7	
A.USE_DIAG	Secure Communication

Table 12: General assumptions for the TOE

Additionally, an assumption (A.PERS) on secure generation and handling of personalisation data is made because 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. The security of the personalisation process of the TOE is supported by the TOE itself.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Tachograph Card Version 1.1 128/64 R1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW / SW	Tachograph Smartcard Consisting of: - Philips P16WX064V0C Secure 16-bit Smart Card Controller, C013C including IC Dedicated Test ROM Software version 2.1 dated 03 Sept.2001 - IC Dedicated Support Software Caervarnon Cryptographic Library version 4.2.2 dated 13 June 2003 - Embedded Software, Version 1.1 128/64 R1.0 including Basic Software and Tachograph Application with Application Data (Depending on card type)	1.1 128/64 R1.0		Initialised and tested smartcards or initialised and tested modules
2	DOC	User documentation for personalisation, Tachograph Card Version 1.1 128/64 R1.0	V1.00	19 January 2004	Document in paper / electronic form [15]
3	DOC	User documentation for Tachograph Card issuer, Tachograph Card Version 1.1 128/64 R1.0	V1.00	19 January 2004	Document in paper / electronic form [17]
4	DOC	User documentation for developers of card interface devices, Tachograph Card Version 1.1 128/64 R1.0	V1.00	19 January 2004	Document in paper / electronic form [16]
5	DOC	Tachograph Card Version 1.1 128/64 R1.0 Data Sheet [12]	V1.00	19 January 2004	Document in paper / electronic form [20]

[12] see chapter 6

No	Type	Identifier	Release	Date	Form of Delivery
6	Keys	Keys for verification of the TOE and for personalisation (ORGA Key, Card Key, Personalisation Unit Key [if applicable], Static Pers-Key [if applicable])	Customer specific		Either on paper or in electronic format

Table 13: Deliverables of the TOE

To ensure that the customer receives this evaluated version, the delivery procedures described in the User documentation for personalisation [15] have to be followed. The Tachograph Card Version 1.1 128/64 R1.0 Data Sheet includes File Control Information (FCI) which can be used for identification of the five different card types.

3 Security Policy

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.

The TOE is the composition of the IC, IC Dedicated Software and Smartcard Embedded Software. The security policy is to provide:

- protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations, against access for code and data memory and against abuse of functionality
- secure storage of user data and TSF data
- access control to user data and TSF data according to the specified rules
- secure communication to the vehicle unit of the Tachograph System

as specified in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8].

4 Assumptions and Clarification of Scope

The TOE is intended to be used within the Tachograph System as a security medium which carries a specific Tachograph Application intended for its use with the recording equipment as specified in [8].

There do not exist any Tachograph Card specific assumptions for the environment of the TOE as the definition of the card type is done before the TOE personalisation in phase 6 before delivery.

General assumptions are made based on the PP/9911 [13] and PP/9806 [14] referenced in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8]

(Generic Security Target). These general assumptions are structured according to the phases of the life cycle. Some of these assumptions are related to procedures in phases 1 to 5. These phases were part of the TOE evaluation. As delivery of the TOE is defined within or at the end of phase 5 of the life cycle. (see table 1), the phases 6 and 7 are the usage phases of the TOE. Procedures related to assumptions on these phases and the additional assumption A.PERS on secure generation and handling of personalisation data are outlined in the user documentation.

The TOE is the Tachograph Card Version 1.1 128/64 R1.0 providing security functions as required in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] (Generic Security Target). Threats on the overall Tachograph System which are not related to the Tachograph Smartcards were not addressed by this product evaluation.

5 Architectural Information

The TOE is a product. It is composed from an Integrated Circuit (IC) with its proprietary IC Dedicated Software and a Smartcard Embedded Software (ES), consisting of Basic Software (BS) and Application Software (AS). The Design of the Embedded Software is based on the Java Card Platform Version 2.1.1 with a dedicated Java Card Applet for the Tachograph Card application. The four different card types are distinguished as they contain a specific applet each, and specific data structures and data.

As all parts of TOE software are running inside the IC, the external interface of the TOE to its environment can be defined as the external interface of this IC, the Philips P16WX064V0C Secure 16-bit Smart Card Controller. The external interface is divided into a physical / electrical interface and a logical interface.

The physical / electrical interface of the P16WX064V0C are the pads to connect the lines supply voltage, reset input, clock input, ground and I/O. An external voltage and timing supply as well as a data interface are necessary for the operation of the IC. Beyond the physical behaviour, the data interface is defined by the Smart Card Embedded Software (ES). A user would use the physical interface via the Chip card contacts. The electrical and physical characteristics fulfilled are given in the Tachograph Cards Specification [8]. The location and dimensions of the Chip card contacts comply with the ISO/IEC 7816-2. The electronic signals, the working of the card as well as the power consumption are in accordance with ISO/IEC 7816.

The logical interface consists of two parts: (i) everything below the command level and (ii) the accessing of the Tachograph Cards by commands via the command interface. Commands and protocols of the Tachograph Application for phase 7 are fully described in the Tachograph Cards Specification [8] with the exception of one newly introduced command, “GET DATA” which does not read any security relevant data. Specific commands for the personalisation phase (phase 6) are described in the User Guidance for the Personaliser [15].

The subsystems of the TOE are described in the ST [7], chapter 2.1. The TOE Summary Specification (chapter 6 of the ST [7]) describes the TOE Security Functions with relation to the IC and Cryptographic Library and to the Embedded Software.

6 Documentation

The user of the TOE is

(i) the developer of a vehicle unit who needs information how the TOE interacts with the vehicle unit

(ii) the personaliser of the Tachograph Cards who needs information about security procedures and how the TOE supports the personalisation process

(iii) the issuer of the Tachograph Cards who needs information how to use the 4 different card types after personalisation, information on specific aspects of the issuance of the Tachograph Cards and information to be passed to the end-user of the Tachograph Cards (card-holder, e.g. the driver).

For these three types of users separate user documentation is provided (see [15], [16] and [17]). Additionally, the Tachograph Card Version 1.1 128/64 R1.0, Data Sheet [20] is provided by ORGA. It contains Answer To Reset (ATR) information and File Control Information (FCI) as identification information for the Tachograph Cards. As some data contained in the Data Sheet can be customer specific, it will be provided individually for specific customers.

7 IT Product Testing

Tests of the TOE were done (i) with real cards using a card reader and a PC and (ii) in an emulator test environment.

For those tests, where real cards are used, the specified method was used to identify the Tachograph Card version and the correct card configuration for every test. The real cards used for testing were either in initialised state (i. e. ready for personalisation) or in operational state (i. e. personalisation completed). Using specific commands for reading FCI-data, the life cycle state of the applet and the type of the card could be determined.

For identification of the correct versions of the electronic data used for tests in the emulator test environment, and to determine whether the initial condition of each test is satisfied, the methods of the evaluated Configuration Management System were used. The version control mechanism can guarantee that the design files and the initial data used for testing are those provided by the developers for the specific version of the TOE under evaluation.

As specific subsystems are the same in all card types and others are different, some tests had to be performed on all four card types, others could be re-used. Tests after modifications of the TOE during the evaluation process were re-done as necessary depending on the specific change.

For re-evaluation, a subset of the developer and independent evaluator tests of BSI-DSZ-CC-0205-2003 had to be repeated. Especially tests covering product changes were performed again.

Developer tests:

For developer tests, the test cases were mapped to Security Functions. All Security Functions with their security properties and their interfaces were covered. In addition, the test cases were mapped to subsystems of the High-Level Design and to modules of the Low-Level Design. All subsystems and modules with their security properties and their interfaces were covered. The developer tested each property of the design specification. All command APDU with valid and invalid inputs are tested and all functions are tested with valid and invalid inputs. All test results were documented in log-files. All security functions were tested with overall positive results.

Independent evaluator tests:

Most tests of the evaluator were done by ISO-7816 APDU command sequences using a real card. Tests with emulators were chosen by the evaluators only for those security functions, where internal resources of the card needed to be modified or observed during the test (e.g. Anti-DPA-Measures and Residual Information protection).

Several issues have been checked extensively by functional tests and by source code analysis (e.g. I/O-testing, making sure that the protocol levels of the TOE interface below ISO command level have stable behaviour; functional Tachograph command testing including all possible error cases showing that no undesired behaviour exits on command level which might be exploitable by an attacker).

Side channel attacks on DES and RSA were tested and analysed during the evaluation of BSI-DSZ-CC-0205-2003. The result of these analysis is still valid. It showed that secret keys could not be extracted.

In addition, tests according to Appendix 9 of the EU Tachograph Card Commission Regulation [8] have been performed. Preliminary, the personalisation process of the cards has been carried out and thereby tested. The tests have been performed for all four different types of ORGA Tachograph Cards. For the Appendix 9 tests, cards with the final ROM mask and the actual Tachograph Applet have been used. The achieved test results correspond to the expected test results (see Annex A of this report).

8 Evaluated Configuration

The TOE is delivered within or at the end of phase 5 in form of initialised and tested complete cards or in form of initialised and tested modules (see table 1). A Tachograph Card may be of the following types: Driver Card, Control Card, Workshop Card or Company Card depending on the specific applet and data loaded into the card. Additionally, a General Tachograph Card is available that can be irreversibly converted into one of the different card types by using a specific card command after initialisation resp. prior to the personalisation of the card. These five different card types are considered as different configurations of the TOE.

All procedures for personalisation and configuration for the end-user necessary after delivery are described in the user documentation [15].

9 Results of the Re-Evaluation

The Evaluation Technical Report (ETR) [11] was provided by the ITSEF SRC Security Research & Consulting GmbH according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [11] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Compo sition: Annex A Composite smartcard evaluation [4, AIS 36].

The ETR [11] builds up on the *ETR-lite for Composition* documents of the evaluations of the underlying „Philips P16WX064V0C Secure 16-bit Smart Card Controller“ and of the underlying „Philips P16WX064V0C Secure 16-bit Smart Card Controller with Caernarvon Cryptographic Library on Philips Smart *XA*2 as IC Dedicated Support Software". These *ETR-lite for Composition* documents were provided by the ITSEF T-Systems GEI GmbH according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]).

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body. For smartcard specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used. For specific methodology on random number generator evaluation the scheme interpretations AIS 20 and AIS 31 (see [4]) were used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components	**Verdict**

Assurance classes and components		Verdict
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Generation log	ADO_IGS.2	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS

Assurance classes and components		Verdict
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 14: Verdicts for the assurance components

The evaluation has shown that:

- the Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the TOE provides the functionality according to Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8] and stated more precisely in the document JIL Security Evaluation and Certification of Digital Tachographs [9]
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4
- the assurance of the TOE is equivalent to ITSEC [10] E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [8]
- the TOE fulfils the claimed strength of function SOF-high for the functions as outlined in chapter 1.6. Therefore the scheme interpretations AIS 20, AIS 26 and AIS 31 (see [4]) were used. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).
- specific tests required by Appendix 9 of the EU Tachograph Card Commission Regulation [8] are fulfilled (see Annex A of this report).

The underlying hardware had been successfully reassessed by T-Systems GEI GmbH.

The results of the evaluation are only applicable to the Tachograph Card Version 1.1 128/64 R1.0. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The User Guidance documentation (refer to chapter 6) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

11 Annexes

none

12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document. It is a sanitised version of the complete Security Target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

AC_SFP	SFP Access Control
APDU	Application Protocol Data Unit
BS	Basic Software
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for IT Security Evaluation
CM	Card Manager
DES	Data Encryption Standard; symmetric block cipher algorithm
DFA	Differential Fault Analysis
DOC	Document
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electronically Erasable Programmable Read Only Memory
ES	Embedded Software
ETR	Evaluation Technical Report
FCI	File Control Information
IC	Integrated Circuit
IFD	Interface Device
INI	Initialisation Module
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JC	Java Card Platform
JCAPI	Java Card Application Programming Interface
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine

JIL	Joint Interpretation Library
MAC	Message Authentication Code
MMU	Memory Management Unit
OS	Operating System
OTP	One Time Programmable (a certain part of the EEPROM)
PERS-AC_SFP	SFP Personalisation Access Control
PIN	Personal Identification Number
PP	Protection Profile
PW	Password
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Secure Messaging
SOF	Strength of Function
SPA	Simple Power Analysis
ST	Security Target
TA	Tachograph Applet
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
VU	Vehicle Unit

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125, Version 5.1, January 1998)

[4] Application Notes and Interpretations of the Scheme (AIS), e.g.

AIS 20: Functionality classes and evaluation methodology for deterministic random number generators AIS 20, Version 1, 2 December,1999

AIS 25 for: CC-Supporting Document: The application of CC to Integrated Circuits, Version 2, July 2002

AIS 26 for: CC-Supporting Document: Application of Attack Potential to Smartcards, Version 2, August 2002

AIS 31: Functionality classes and evaluation methodology of physical random number generators, Version 1, 25 September 2001

AIS 35 for: CC-Supporting Document: ST-lite, Version 1.1, July 2002

AIS 36 for: CC-Supporting Documents: ETR-lite for Composition, Version 1.1, July 2002 and
ETR-lite for composition: Annex A Composite smartcard evaluation: Recommended best practice, Version 1.2, March 2002

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target, BSI-DSZ-0243-2004, Version 1.00, 19 January 2004, ORGA Kartensysteme GmbH (confidential document)

[7] Security Target Lite, BSI-DSZ-0243-2004, Version 1.00, 28 January 2004, ORGA Kartensysteme GmbH (sanitized public document)

[8] 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.), 05.08.2002, Commission of the European Communities

Appendix 2 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 – Tachograph Cards Specification

Appendix 7 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Data downloading protocols

Appendix 9 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 – Type Approval – List of Minimum Required Tests

Appendix 10 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Generic Security Targets

Appendix 11 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Common Security Mechanisms

[9] Joint Interpretation Library (JIL) - Security Evaluation and Certification of Digital Tachographs, Version 1.12, June 2003, JIL Working Group (BSI, CESG, DCSSI, NLNCSA)

[10] Information Technology Security Evaluation Criteria (ITSEC), CEC, Version 1.2, June 1991.

[11] Evaluation Technical Report, Version 2.01, 03 February 2004 for Tachograph Card Version 1.1 128/64 R1.0 (confidential document)

[12] Smart Card IC Platform Protection Profile, Version 1.0, July 2001, registered at the German Certification Body under number BSI-PP-0002-2001

[13] Smart Card Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 99. Registered at French certification body under the number PP/9911.

[14] Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806.

[15] User Guidance for the Personaliser of the Tachograph Card - Tachograph Card Version 1.1 128/64 R1.0, Version V1.00, ORGA Kartensysteme GmbH, 19.01.2004

[16] User Guidance for the Vehicle Unit Developer - Tachograph Card Version 1.1 128/64 R1.0, Version V1.00, ORGA Kartensysteme GmbH, 19.01.2004

[17] User Guidance for the Issuer of the Tachograph Card - Tachograph Card Version 1.1 128/64 R1.0, Version V1.00, ORGA Kartensysteme GmbH, 19.01.2004

[18] Certification Report, BSI-DSZ-CC-0203-2003 for Philips Smart Card Controller P16WX064V0C from Philips Semiconductors GmbH Business Line Identification, 18 June 2003, Bundesamt für Sicherheit in der Informationstechnik

[19] Security Target Lite BSI-DSZ-CC-0203, Version 1.2, May 8th, 2003, Evaluation of Philips P16WX064V0C Secure 16-bit Smart Card Controller, Philips Semiconductors (sanitized public document)

[20] Tachograph Card Version 1.1 128/64 R1.0, Data Sheet, Version V1.00, ORGA Kartensysteme GmbH, 19.01.2004

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential."

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A:

Functional Tests according to Appendix 9 of Annex I (B) of Council Regulation (EEC) No. 1360/2002

In addition to the ordinary evaluator tasks of the Common Criteria evaluation at level EAL4+ (equivalent to ITSEC E3 high), functional tests according to Appendix 9 of the EU Tachograph Card Commission Regulation [8] have been performed.

The following list shows the results of these tests:

N°	Test	Description	Related requirements	Result
1	Administrative examination			
1.1	Documentation	Correctness of documentation	-	**Confirmed**
4	Protocol tests			The evaluators have assured themselves in detail of the fact that the functional tests have been performed successfully.
4.1	ATR	Check that the ATR is compliant.	ISO/IEC 7816-3 TCS 304, 307, 308	**Confirmed**
4.2	T=0	Check that T=0 protocol is compliant.	ISO/IEC 7816-3 TCS 302, 303, 305	**Confirmed**
4.3	PTS	Check that the PTS command is compliant by setting T=1 from T=0.	ISO/IEC 7816-3 TCS 309 to 311	**Confirmed**
4.4	T=1	Check that T=1 protocol is compliant.	ISO/IEC 7816-3 TCS 303, / 306	**Confirmed**
5	Card Structure			
5.1		Test that the file structure of the card is compliant by checking the presence of the mandatory files in the card and their Access Conditions.	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419	**Confirmed**

N°	Test	Description	Related requirements	Result
6	Functional tests			
6.1	Normal Processing	Test at least once each allowed usage of each command (ex: test the UPDATE BINARY command with CLA = '00', CLA = '0C' and with different P1,P2 and Lc parameters). Check that the operations have actually been performed in the card (ex: by reading the file the command has been performed on).	TCS 313 to TCS 379	**Confirmed**
6.2	Error Messages	Test at least once each error message (as specified in Appendix 2) for each command. Test at least once every generic error (except ‘6400’ integrity errors checked during security certification).		**Confirmed**