Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0661-2011

for

Micardo V3.6 R1.0 Tachograph V2.0

from

Sagem Orga GmbH (Morpho e-Documents Division)

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0661-2011

Digital Tachograph

Micardo V3.6 R1.0 Tachograph V2.0

from	Sagem Orga GmbH (Morpho e-Documents Division)
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3, extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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.

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.

Bonn, 7 April 2011

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Joachim Weber L.S.
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

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 Micardo V3.6 R1.0 Tachograph V2.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0358-2006. Specific results from the evaluation process BSI-DSZ-CC-0602-2009 were re-used.

The evaluation of the product Micardo V3.6 R1.0 Tachograph V2.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 22 March 2011. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Sagem Orga GmbH (Morpho e-Documents Division)

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Micardo V3.6 R1.0 Tachograph V2.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

6 Information Technology Security Evaluation Facility

7 Sagem Orga GmbH (Morpho e-Documents Division)
Riemekestraße 160
33106 Paderborn

This page is intentionally left blank.

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.

1 Executive Summary

The Target of Evaluation (TOE) is MICARDO V3.6 R1.0 Tachograph V2.0. It is a smart card product which will be employed within the Tachograph System as a security medium. It carries a specific Tachograph Application intended for its use with the recording equipment.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile but is written in view of the requirements of the „Generic Security Target“ for the Tachograph Cards within the Tachograph Card Specification [15], Appendix 10 (Tachograph Card Generic Security Target) and the JIL interpretations and requirements in [16].

The TOE Security Assurance Requirements (SAR) 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 the Evaluation Assurance Level EAL 4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5.1.1.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended. (Note: The supplement „extended“ is only relevant for the SFRs of the underlying IC with its IC Dedicated Support Software.)

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

TOE Security Function	Addressed issue
F.ACS	Security Attribute Based Access Control
F.IA_AKEY	Key Based User / TOE Authentication
F.IA_PWD	Password Based User Authentication
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.RSA_ENC	Encryption
F.DEC_ENC	Decryption
F.CRYPTO	Cryptographic Support

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.1.1 for the IC part of the TOE and 6.1.2.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 6.2 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.2 - 3.4.

This certification covers the following configurations of the TOE:

The TOE is delivered in form of initialised complete cards or in form of initialised modules (see table 2). A Tachograph Card may be of the following types: Driver Card, Control Card, Workshop Card or Company Card, depending on the specific application 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 [13]. For details, refer to Chapter 8.

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:

Micardo V3.6 R1.0 Tachograph V2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW / SW	NXP SmartMX P5CC037V0A Secure Smart Card Controller (incl. its IC Dedicated Software, covering in particular the Crypto Library, and incl. the ROM mask)	MICARDO V3.6 R1	Delivery of initialised modules or smartcards
2	SW	Smartcard Operating System Software (implemented in ROM / EEPROM of the microcontroller)	MICARDO V3.6 R1.0	Delivery of initialised modules or smartcards

No	Type	Identifier	Release	Form of Delivery
3	SW	Tachograph Application Software	Indicated in the Data Sheet	In electronic form (within initialised module or smartcard)
4	DOC	User guidance for the Personaliser of the Tachograph Card	Version V2.00, 09.03.2011 [12]	Document in paper / electronic form
5	DOC	User guidance for the Operation of Tachograph Cards by Issuer and Vehicle Unit Developer	Version V2.00, 09.03.2011 [13]	Document in paper / electronic form
6	DOC	Data Sheet MICARDO V3.6 R1.0 Tachograph V2.0	Version 1.0.0 with customer specific completions [14]	Document in paper / electronic form
7	KEY	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.	Indicated in the Data Sheet [14]	Document in paper / electronic form
8	KEY	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 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.	Dependent on the TOE's configuration	Document in paper / electronic form

No	Type	Identifier	Release	Form of Delivery
9	KEY PAIR	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.	Dependent on the TOE's configuration	Document in paper / electronic form
10	KEY	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.	Dependent on the TOE's configuration	Document in paper / electronic form

Table 2: Deliverables of the TOE

Initialised cards/modules can be authenticated with the command INTERNAL AUTHENTICATE. The procedure and the expected answer of the command is described in the Data Sheet ([14], ch. 3.5).

The card types can be differentiated by the Cold and Warm EEPROM ATR in the following way:

Cold EEPROM ATR:

```
3b dd 18ffc0 80 b1 fe451f C3 00 68 d2760000280409 XX 009000 YY
```

Warm EEPROM ATR:

```
3b cd ff80 31 fe45 00 68 d2760000280409 XX 009000 ZZ
```

In both ATRs, d276000028 is the international RID of Orga, 04 identifies the producer of the semiconductor, and 09 identifies the TOE Micardo V3.6 Tachograph 2.

The values for XX, YY and ZZ are image specific with the following values:

Card type	XX	YY	ZZ
Driver Card	11	C4	50
Workshop Card	21	F4	60
Control Card	31	E4	70
Company Card	41	94	00
General Card	71	A4	30

Table 3: Deliverables of the TOE

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

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 [15].

The TOE is the composition of the IC, IC Dedicated Software and Smart Card 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 [15].

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 [15].

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 and PP/9806 referenced in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [15] (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, 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 Micardo V3.6 R1.0 Tachograph V2.0 providing security functions as required in Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [15] (Generic Security Target). Threats on the overall Tachograph System which are not related to the Tachograph Smart Cards were not addressed by this product evaluation.

5 Architectural Information

The TOE is a product that is composed from an Integrated Circuit with its proprietary IC Dedicated Software and a Smartcard Embedded Software, consisting of Basic Software and Application Software. While the Basic Software consists of the MICARDO V3.6 R1.0 Operating System platform of the TOE (realised as native implementation), the Application Software covers the Application Layer which is directly set-up on the MICARDO V3.6 R1.0 Operating System platform and implements the specific Tachograph Application. As all these parts of 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, microcontroller "NXP Smart Card Controller P5CC037V0A” with the Crypto Library “Secured Cryptographic Library on P5CC037V0A” as IC Dedicated Support Software provided by NXP Semiconductors. The IC incl. its Dedicated Software was evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high (refer to Certification ID BSI-DSZ-CC-0465). The Crypto Library was evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high and is listed under the Certification ID BSI-DSZ-CC-0612.

According to the high-level design (HLD) the security functions of the TOE are enforced by the following subsystems:

- Security Functions related to the TSFI (Key Based User / TOE Authentication (F.IA_AKEY), Password Based User Authentication (F.IA_PWD), Confidentiality of Data Exchange (F.EX_CONF), Integrity and Authenticity of Data Exchange (F_EX_INT), Cryptographic Support (F.CRYPTO), Generation of Session Keys (F.GEN_SES), Generation of Digital Signatures (F.GEN_DIGSIG), Verification of Digital Signatures (F.VER_DIGSIG), Encryption (F.RSA_ENC) and Decryption (F.RSA_DEC)): Commands, Initialisation
- Security Attribute Based Access Control (F.ACS): Commands, High-Level OS, Application Layer, Initialisation
- Data Integrity Protection (F.DATA_INT): Commands, High-Level OS, Low-Level OS
- Residual Information Protection (F.RIP): High-Level OS, Low-Level OS
- Failure Protection (F.FAIL_PROT): High-Level OS; Low-Level OS, Crypto IC
- Side Channel Control (F.SIDE_CHAN): High-Level OS; Low-Level OS, Crypto IC
- Self-Tests (F.SELFTEST): Low-Level OS, Initialisation

More information on architecture of the TOE and a schematic picture is found in the Security Target [6] and [9], chapter 2.1.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The TOE test configuration is defined by the denotation MICARDO V3.6 R1.0 Tachograph V2.0 and coincides with the evaluated configuration.

As a basis for the tests, real cards as well as an emulator were used. Real cards were used mainly for APDU tests, while emulator tests were used for tests which cannot be performed with real cards, e.g. tests where a checksum error is provoked by the tester by manipulating the checksum during the test.

The developer tested all TOE Security Functions either on real cards or with emulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set was tested, e.g. all command APDUs and functions were tested with valid and invalid inputs. Repetition of developer tests was performed during the independent evaluator tests.

Since many Security Functions can be tested by APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of the security functionality. 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.

During their independent testing, the evaluators performed

- APDU command testing related to
  - initialisation, personalisation and usage phase,
  - the access control of files and cryptographic keys,
  - external and internal authentication based on asymmetric cryptography,
  - correct PIN functionality of the workshop card,
  - the correct execution of Secure Messaging,
  - the correct execution of cryptographic mechanisms,
- emulator testing related to
  - the correct reaction to checksum errors for stored data,
  - the correct erasure of secret data after use,
  - the correct reaction to a corruption of the card life cycle state,

- further
  - side channel analysis for SHA-1, DES and RSA,
  - fault injection attacks (laser attacks),
  - source code analysis.

The evaluators tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results corresponded to the expected test results in almost all cases. Regarding the exceptional test cases, it was sufficiently explained and justified why they gave no indications for an unexpected behaviour of security functions of the TOE.

8 Evaluated Configuration

The TOE is delivered in form of initialised and tested complete cards or in form of initialised and tested modules (see table 2). A Tachograph Card may be of the following types: Driver Card, Control Card, Workshop Card or Company Card depending on the specific application 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 [13].

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF 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.

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards and

(iii) ETR-lite – for Composition and ETR-lite – for Composition: Annex A Composite smartcard evaluation: Recommended best practice

(see [4], AIS 25, AIS 26 and AIS 36) were used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)

- The components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0358-2006, re-use of specific evaluation tasks was possible. Specific results from the evaluation process BSI-DSZ-CC-0602-2009 were also re-used.

Formally, the evaluation is a re-evaluation of the Tachograph Card certified under BSI-DSZ-CC-0358-2006 (0358). On application level, changes were considered with regard to 0358. However, changes regarding the operating system, the Microkernel and the Initialisation Module are considered with regard to the Electronic Health Card certification BSI-DSZ-CC-0602-2009, since the operating system used there (MICARDO V3.5) is much more comparable to the operating system used in the current evaluation (MICARDO V3.6) than that of the 0358 certification (MICARDO V3.0). The focus of this re-evaluation was on the changes that are mainly a different IC with crypto library, adoptions of the operating system and commands to fit the Tachograph interface and minor changes in the application software.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
  (Note: The supplement „extended“ is only relevant for the SFRs of the underlying IC with its IC Dedicated Support Software.)
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function : high
  - the generation of random numbers (connected with security functions F.RNG for HW generation and/or F.RNG_Access for SW generation);
  - the mechanisms against leakage attacks (as defined in F.LOG);
  - the mechanisms F.DES, F.GEN_DIGSIG, F.RSA_DEC and the critical mechanisms of F.IA_KEY, as far as resistance against SPA, DPA, DFA and timing attacks is concerned;
  - the password based authentication mechanism (connected with F.IA_PWD).

  The functions F.RSA_sign and F.RSA_encrypt, as far as resistance against SPA, DPA, DFA and timing attacks is concerned, were rated SOF high in the certification of the Crypto Lib.
  No SOF claims are made for the CRC checksum mechanism, for F.RSA_public, F.VER_DIGSIG, F.RSA_ENC, F.SHA-1, and for the cryptographic algorithms themselves.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The TOE is conformant to the requirements of the „Generic Security Target“ for the Tachograph Cards within the Tachograph Card Specification [15], Appendix 10

(Tachograph Card Generic Security Target) and the Tachograph JIL interpretations and requirements in [16].

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

- hash functions:

  SHA-1

- algorithms for the encryption and decryption:

  RSA 1024, Triple-DES, Retail-MAC

This holds for the following security functions:

- F.GEN_DIGSIG, F.VER_DIGSIG, F.IA_AKEY, F.CRYPTO, F.EX_CONF, F.EX_INT, F.RSA_ENC, F.RSA_DEC

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to [15] the algorithms are suitable for authentication and data integrity between vehicle units and tachograph cards and digital signature of data downloaded from vehicle units or tachograph cards to external media.

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptograhic algortithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AIS Application Notes and Interpretations of the Scheme

APDU Application Protocol Data Unit

ASE Security Target evaluation class

ATR Answer to Reset

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

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

DPA Differential Power Analysis

EAL Evaluation Assurance Level

EEPROM Electronically Erasable Programmable Read Only Memory

ES Embedded Software

ETR Evaluation Technical Report

IC Integrated Circuit

ISO International Organization for Standardization

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

JIL Joint Interpretation Library

MAC Message Authentication Code

OS Operating System

PC Personal Computer

PIN Personal Identification Number

PP Protection Profile

RNG Random Number Generator

ROM Read Only Memory

RSA Rivest-Shamir-Adleman Algorithm

SAR Security Assurance Requirements

SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOF	Strength of Function
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE security functions interface
TSP	TOE Security Policy
TSS	TOE Summary Specification

12.2 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.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

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

[6] Security Target BSI-DSZ-0661-2011, MICARDO V3.6 R1.0 Tachograph V2.0, Version V1.00, Sagem ORGA GmbH, 9.03.2011 (confidential document)

[7] Evaluation Technical Report, Version 1.3, Date 11.03.2011, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration list for the TOE, MICARDO V3.6 R1.0 Tachograph V2.0, Version X.1.00.3, 28.09.2010, Sagem ORGA GmbH, file name ORGA_MIC_V36_R10_P5_TC_ConfList_X1003.pdf (confidential document)

[9] Security Target ST Lite - MICARDO V3.6 R1.0 Tachograph V2.0, Version V1.02, Sagem ORGA GmbH, 12.05.2011 (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product Crypto Library V2.2 on P5CC037V0A, Version 2.0, 03.08.2010, Brightsight (confidential document)

[11] ETR for composite evaluation according to AIS 36 for the Product NXP P5CC037V0A Secure Smart Card Controller, Version 1.3, 28.09.2010, T-Systems GEI GmbH (confidential document)

[12] User Guidance for the Personaliser of the Tachograph Card, MICARDO, V3.6 Tachograph V2, Version Version V2.00, 9.03.2011, Sagem ORGA GmbH, file name ORGA_MIC_V36_R10_TC2_USR_PERS_X2002.pdf

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 September 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[13] User Guidance for the Operation of the Tachograph Card, MICARDO V3.6 Tachograph V2, Version V2.00, 9.03.2011, Sagem ORGA GmbH, file name ORGA_MIC_V36_R10_TC2_USR_OPR_X2002.pdf

[14] MICARDO V3.6 R1.0 Tachograph V2.0, Data Sheet, V1.0.0, Sagem ORGA GmbH, file name ORGA_MIC_V36_R10_TC2_DataSheetForm_X1002.doc

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

[16] JIL Security Evaluation and Certification of Digital Tachographs, Version 1.12, JIL Working Group (BSI, CESG, DCSSI, NLNCSA), June 2003.

[17] Certification Report, for Crypto Library V2.2 on P5CC037V0A from NXP Semiconductors Germany GmbH, Certification ID BSI-DSZ-CC-0612-2010, 5 August 2010.

[18] 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, 22.12.2010, Bundesnetzagentur

[19] Tachograph Product Update – Impact Analysis Report, Version X1.00.1, Sagem ORGA GmbH, 03.09.2009, file name ORGA_MIC_V36_TC_IAR_X1001.doc

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„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 CC Part 2 (functional requirements), CC 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:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC 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:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 4 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
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)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 6: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 CC 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 11.1)

“Table 6 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 7 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 standard 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 7: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 11.4)

“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 11.5)

“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 11.6)

“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 11.7)

“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 11.8)

“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 11.9)

“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 19.3)

“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 19.4)

"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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment 37

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0661-2011

Evaluation results regarding development and production environment

The IT product Micardo V3.6 R1.0 Tachograph V2.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)..

As a result of the TOE certification, dated 7 April 2011, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.2) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

(a) Sagem Orga GmbH (Morpho e-Documents Division), Riemekestraße 160, Office Center Almepark, Building G, level 04 and 05, 33104 Paderborn (embedded software development and testing)

(b) Sagem Orga GmbH (Morpho e-Documents Division), Konrad-Zuse-Ring 1, 24220 Flintbek (production of modules/cards, initialisation and delivery)

(c) For development and productions sites regarding the "Crypto Library V2.2 on P5CC037V0A" from NXP Semiconductors Germany GmbH refer to the certification report BSI-DSZ-CC-0612-2010 [17].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.