Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0392-2007

for

MICARDO V3.0 R1.0 HPC V1.0

from

Sagem Orga GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0392-2007

Health Professional Card

MICARDO V3.0 R1.0 HPC V1.0

from

Sagem Orga GmbH

Common Criteria Arrangement
for components up to EAL4

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, Version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0018-2007-MA-01**
Functionality:	**Protection Profile BSI-PP-0018-2007-MA-01 conformant** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 / augmented by** **ADV_IMP.2 - Implementation of the TSF** **ATE_DPT.2 - Testing: Low-Level Design** **AVA_MSU.3 - Analysis and Testing for Insecure States** **AVA_VLA.4 - Highly Resistant**

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, 25. May 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

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 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

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 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

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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been 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). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of 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 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

This evaluation contains the components ADV_IMP.2 - Implementation of the TSF, ATE_DPT.2 - Testing: Low-Level Design, AVA_MSU.3 - Analysis and Testing for Insecure States, AVA_VLA.4 - Highly Resistant, 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 V3.0 R1.0 HPC V1.0 has undergone the certification procedure at BSI.

The evaluation of the product MICARDO V3.0 R1.0 HPC V1.0 was conducted by SRC Security Research & Consulting GmbH. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor and distributor is:

Sagem Orga GmbH
Heinz-Nixdorf-Ring 1
33106 Paderborn, Germany

The certification is concluded with

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

This work was completed by the BSI on 25. May 2007.

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-30 and D1 to D-4.

The product MICARDO V3.0 R1.0 HPC V1.0 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 +49 228 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] Sagem Orga GmbH
Heinz-Nixdorf-Ring 1
33106 Paderborn, Germany

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

The IT product MICARDO V3.0 R1.0 HPC V1.0 was evaluated by SRC Security Research & Consulting GmbH. The evaluation was completed on 01. February 2007. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The evaluation of the TOE was conducted as a composition evaluation and uses the evaluation results of the CC evaluation of the underlying semiconductor “Philips SmartMX P5CC036V1D Secure Smart Card Controller” provided by Philips Semiconductors GmbH (Certification ID BSI-DSZ-CC-0293).

The TOE is realised as a Smart Card Integrated Circuit (IC with contacts) with Smart Card Embedded Software, consisting of the MICARDO V3.0 Operating System platform and the dedicated Health Professional Card Application (HPC Application) and Signature Application (SIG Application) as intended to be used for the German Health Care System.

The TOE claims conformance to the Protection Profile for the German Health Professional Card [9]. As outlined in chap. 1.3 the Security Target [6], the Security Target of the TOE is also based on the Protection Profile for the Secure Signature-Creation Device [10]. More detailed information about the Protection Profile claim can be found in chapters 7.1 and 7.2 of the Security Target [6].

The TOE`s HPC Application and SIG Application are based on the MICARDO V3.0 Operating System platform which is designed as multifunctional platform for high security applications.

The TOE is intended to be used as a Health Professional Card (HPC) within the German Health Care System. The HPC Application running on the underlying MICARDO V3.0 Operating System platform is implemented according to the requirements in [11] and [12].

Furthermore, the TOE is intended to be used as a Secure Signature-Creation Device (SSCD) for qualified electronic signatures and takes into account contents of the Protection Profile for the Secure Signature-Creation Device [10] which defines security requirements for SSCD in accordance with the European Directive 1999/93/EC on electronic signatures [13].

The TOE is designed as SSCD of the so-called Type 3, i.e. as device with oncard - generation of the Signature-Creation Data / Signature-Verification Data (SCD/SVD key pair), the secure storage of the SCD/SVD key pair and the secure creation of electronic signatures by using the dedicated SCD key. Hence, the Security Target for the TOE resp. its SIG Application is based on the related Protection Profile [10]. Please note that the TOE does not implement a Signature-Creation Application (SCA).

---

[8] Information Technology Security Evaluation Facility

The TOE comprises the following components:

- Integrated Circuit (IC) "Philips SmartMX P5CC036V1D Secure Smart Card Controller" provided by Philips Semiconductors GmbH (Certification ID BSI-DSZ-CC-0293)
- Smart Card Embedded Software comprising the MICARDO V3.0 Operating System platform (designed as native implementation) (Certification ID BSI-DSZ-CC-0390) including Dedicated HPC Application and SIG Application for the German Health Care System provided by Sagem Orga GmbH

The IC incl. its IC Dedicated Software has been 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-0293.

The configuration of the TOE as HPC will be done by Sagem Orga GmbH prior to the delivery of the product. The TOE contains at its delivery unalterable identification information on the delivered configuration.

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

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

The sponsor , and vendor and distributor of the TOE is

Sagem Orga GmbH
Heinz-Nixdorf-Ring 1
33106 Paderborn, Germany

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 Annex 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
+ ADV_IMP.2	Development – Implementation of the TSF
+ ATE_DPT.2	Testing – Low-Level Design
+ AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+ AVA_VLA.4	Vulnerability assessment – Highly resistant

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

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

The following SFRs are relevant for the TOE:

Security Functional Requirement	**Addressed issue**
SFRs for the TOE´s HPC Application according to PP HPC [9]	
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FCS_RND.1	Quality Metric for Random Numbers
FDP	**User data protection**
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_RIP.1	Subset Residual Information Protection
FDP_SDI.2	Stored Data Integrity Monitoring and Action
FDP_UCT.1	Basic Data Exchange Integrity
FDP_UIT.1	Data Exchange Integrity
FIA	**Identification and authentication**
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_UAU.1	Timing of Authentication
FIA_UAU.4	Single-use Authentication Mechanisms
FIA_UAU.6	Re-Authenticating
FIA_UID.1	Timing of Identification
FMT	**Security Management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT	**Protection of the TOE Security Functions**
FPT_EMSEC.1	TOE Emanation

Security Functional Requirement	Addressed issue
FPT_FLS.1	Failure with Preservation of Secure State
FPT_PHP.3	Resistance to Physical Attack
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_TST.1	TSF Testing
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF Trusted Channel
SFRs for the TOE´s SIG Application according to PP SSCD Type 3 [10]	
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FDP	**User data protection**
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_ETC.1	Export of User Data without Security Attributes
FDP_ITC.1	Import of User Data without Security Attributes
FDP_RIP.1	Subset Residual Information Protection
FDP_SDI.2	Stored Data Integrity Monitoring and Action
FDP_UIT.1	Data Exchange Integrity
FIA	**Identification and authentication**
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_UAU.1	Timing of Authentication
FIA_UID.1	Timing of Identification
FMT	**Security Management**
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MSA.1	Management of Security Attributes
FMT_MSA.2	Secure Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions

Security Functional Requirement	Addressed issue
FMT_SMR.1	Security Roles
FPT	**Protection of the TOE Security Functions**
FPT_AMT.1	Abstract Machine Testing
FPT_EMSEC.1	TOE Emanation
FPT_FLS.1	Failure with Preservation of Secure State
FPT_PHP.1	Passive Detection of Physical Attack
FPT_PHP.3	Resistance to Physical Attack
FPT_TST.1	TSF Testing
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted Path

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined, they are a subset of the SFRs of the table above:

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_RND.1	Quality Metric for Random Numbers
FMT	**Security Management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FPT	**Protection of the TOE Security Functions**
FPT_EMSEC.1	TOE Emanation

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6] chapter 5.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
SFRs for the IT-Environment for Certification Generation Application (CGA) according to PP SSCD Type 3 [10]	
FCS	**Cryptographic support**
FCS_CKM.2	Cryptographic Key Distribution
FCS_CKM.3	Cryptographic Key Access
FDP	**User data protection**
FDP_UIT.1	Data Exchange Integrity

Security Functional Requirement	Addressed issue
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF Trusted Channel
SFRs for the IT-Environment for Signature Creation Application (SCA) according to PP SSCD Type 3 [10]	
FCS	**Cryptographic support**
FCS_COP.1	Cryptographic Operation
FDP	**User data protection**
FDP_UIT.1	Data Exchange Integrity
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted Path

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6] chapter 5.2.

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

TOE Security Function	Addressed issue
Access Control	
F.ACS_SFP	Security Attribute Based Access Control
Identification and Authentication	
F.IA_AKEY	Key Based User / TOE Authentication Based on Asymmetric Cryptography
F.IA_SKEY	Key Based User / TOE Authentication Based on Symmetric Cryptography
F.IA_PWD	Password Based User Authentication
Integrity of Stored Data	
F.DATA-_INT	Stored Data Integrity Monitoring and Action
Data Exchange	
F.EX_CONF	Confidentiality of Data Exchange
F.EX_INT	Integrity and Authenticity of Data Exchange
Object Reuse	
F.RIP	Residual Information Protection
Protection	

TOE Security Function	Addressed issue
F.FAIL_PROT	Hardware and Software Failure Protection
F.SIDE_CHAN	Side Channel Analysis Control
F.SELFTEST	Self Test
Cryptographic Operations	
F.CRYPTO	Cryptographic Support
F.RSA_KEYGEN	RSA Key Pair Generation
F.GEN_DIGSIG	RSA Generation of Digital Signatures
F.VER_DIGSIG	RSA Verification of Digital Signatures
F.RSA_ENC	RSA Encryption
F.RSA_DEC	RSA Decryption

Table 5: Security Functions for the TOE ES

For more details please refer to the Security Target [6], chapter 6.

For the definition of the TOE Security Functions (TSF) related to the TOE-IC refer to [22], chap. 6.1.1.

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

1.3 Strength of Function

The TOE's strength of functions is claimed 'high' (SOF-High) for specific functions as indicated in the Security Target [6], chapter 6.2.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Paragraph. 3, Clause 2). For details see chapter 9 of this report.

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

The threats and Organisational Security Policies (OSPs) which were assumed for the evaluation and averted by the TOE are specified in the Security Target [6].

The threats to the TOE are given in chapter 3.3 of [6].The assets which are affected by the threats are described in chapter 3.1 of [6].

Based on the character of the Security Target the threats are subdivided into three groups.

The first group (see chapter 3.3.1 of [6]) consists of general threats of the TOE. The description of these threats is given by a reference to the ST of the underlying platform [16].

The threats of the underlying platform are given here in short:

General threats of the TOE-ES/BS (Basic Software) (chapter 3.3.1 of [6])	
Name	**Definition**
Threats on all Phases	
T.CLON	Cloning of the TOE
Threats on Phase 1	
T.DIS_INFO	Disclosure of IC Assets
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
Specific threats of the TOE-ES/BS (Basic Software) (chapter 3.3.1 of [6])	
Name	**Definition**
T.KEYGEN	RSA Key Pair Generation

Table 6: Threats of the TOE-ES/BS (Basic Software)

The second group of threats is built by the threats according the TOE's dedicated HPC Application. These threats are given in the ST in section 3.3.2 using a reference to the Protection Profile concerning the HPC application [9]. These threats are reproduced here in short:

Specific threats of the TOE-ES/AS (Application Software) (chapter 3.3.2 of [6])	
Name	**Definition**
Threats on Phase 7	
T.Compromise_Internal_Data	Compromise of confidential User or TSF data
T.Forge_Internal_Data	Forge of User or TSF data
T.Misuse	Misuse of TOE functions
T.Intercept	Interception of Communication
Specific threats of the TOE-ES/AS (Application Software) and TOE-IC (chapter 3.3.2 of [6])	
Threats on Phase 7	
T.Abuse_Func	Abuse of Functionality
T.Information_Leakage	Information Leakage from Smart Card
T.Malfunction	Malfunction due to Environmental Stress
T.Phys_Tamper	Physical Tampering

Table 7: Threats of the TOE-ES/AS (Application Software) and TOE-IC

The third group of threats deals with the TOE's dedicated SIG Application in section 3.3.3 of [6]. These threats are partially described using a reference to the Protection Profile concerning the Signature Application [10] as well as added within the ST. Also in this case the threats are reproduced here in short:

Specific threats of the TOE-ES/AS (Application Software) and TOE-IC (chapter 3.3.3 of [6])	
Name	**Definition**
Threats on Phase 7	
T.Hack_Phys	Physical attacks through the TOE interfaces

T.SCD_Divulg	Storing, copying, and releasing of the signature-creation data
T.SCD_Derive	Derive the signature-creation data
T.Sig_Forgery	Forgery of the electronic signature
T.Sig_Repud	Repudiation of signatures
T.SVD_Forgery	Forgery of the signature-verification data
T.DTBS_Forgery	Forgery of the DTBS-representation
T.SigF_Misuse	Misuse of the signature-creation function of the TOE
T.SIG_PERS_Aut	Authentication for Personalisation Process of SIG Application
T.SIG_PERS_Data	Modification or Disclosure of Personalisation Data of SIG Application

Table 8: Threats of the TOE-ES/AS (Application Software) and TOE-IC

The Organisational Security Policies for the TOE are given in chapter 3.4 of [6]. Also in this case the OSPs are subdivided into three groups.

The first group deals with the general organisational security policies for the underlying platform of the TOE. These OSPs are described using a reference to the ST of the underlying platform [16]. They are reproduced here in short:

General Organisational Security Policies for the TOE (chapter 3.4.1 of [6])	
Name	**Definition**
P.Process-Card	Protection during Packaging, Finishing and Personalisation
P.Design-Software	Design of the Smartcard Embedded Software

Table 9: General Organisational Security Policies for the TOE

The second group deals with the OSPs concerning the HPC Application. A reference to the Protection Profile of the HPC [9] is used in section 3.4.2 of the ST [6] to describe them. Also in this case the OSPs are reproduced here in short:

Organisational Security Policies concerning the HPC Application for the TOE (chapter 3.4.2 of [6])	
Name	**Definition**
OSP.HPC_Spec	Compliance to HPC specifications
OSP.Manufact	Manufacturing of the Smart Card
OSP.Limit_Usage	Limitation of HPC usage

Table 10: Organisational Security Policies concerning the HPC Application for the TOE

The OSPs concerning the TOE's dedicated SIG Application are given in the third group as a reference to the Protection Profile [10] in section 3.4.3 of the ST [6]. Also these OSPs are reproduced here with their name and short definition:

Organisational Security Policies concerning the SIG Application for the TOE (chapter 3.4.3 of [6])	
Name	**Definition**
P.CSP_QCert	Qualified certificate
P.QSign	Qualified electronic signatures
P.Sigy_SSCD	TOE as secure signature-creation device

Table 11: Organisational Security Policies concerning the SIG Application for the TOE

Note: Only the titles of the threats and OSPs are provided. For more details please refer to the Security Target [6], chapter 3, where also assets and subjects of the TOE are described.

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 finished. Alternatively, the TOE is delivered in form of initialised and tested modules. In this case, the smart card finishing process (embedding of the delivered modules, final card tests) is task of the customer.

In technical view the HPC is realised as a proprietary operating system with an Application Layer directly set-up on this operating system layer.

The HPC is based on the microcontroller "Philips SmartMX P5CC036V1D Secure Smart Card Controller" provided by Philips Semiconductors GmbH. The IC incl. its Dedicated Software is 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-0293).

The TOE is composed from the following parts:

- Integrated Circuit (IC) with its proprietary IC Dedicated Software (TOE-IC)
- Smart Card Embedded Software (TOE-ES) consisting of
  - Basic Software (TOE-ES/BS)
  - Application Software (TOE-ES/AS)

While the Basic Software consists of the MICARDO V3.0 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 V3.0 Operating System platform and implements the specific HPC Application and SIG Application. The two predefined applications belonging to the TOE comprise own dedicated file and data systems with dedicated security

structures, i.e. with application specific access rights and with application specific security mechanisms and PIN and key management. The design and implementation of the TOE´s dedicated HPC Application and SIG Application and their security structure follow the requirements in the specifications [11] and [12].

The Application Software will be brought into the smart card in cryptographically secured form during the initialisation process within phase 5 of the smart card product life cycle (see chap. 2.2 of the Security Target [6]). The initialisation process uses the specific initialisation routines of the TOE´s operating system, and the Application Software will be stored in the EEPROM area of the IC.

The HPC offers the capability to check its authenticity. For this purpose, the TOE contains the private part of a dedicated RSA authentication key pair over which by an internal authentication procedure the authenticity of the HPC can be proven.

1.6 Assumptions about the operating environment

The assumptions for the environment of the TOE are given in chapter 3.2 of the ST [6]. These assumptions are described in three different parts.

The first part of the assumptions (chapter 3.2.1 of [6]) relates to the underlying platform of the TOE and is included in the ST as a reference to the ST of the platform [16]. The assumptions are assigned to the different phases of the life cycle of the TOE, and are given here in short for the convenience of the reader:

Assumptions for the TOE environment (chapter 3.2.1 of [6])	
Name	**Definition**
Assumptions on Phases 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 6	
A.PERS	Protection of the TOE under Personalisation

Assumptions on Phase 7	
A.USE_DIAG	Secure Communication with the terminal

Table 12: Assumptions for the TOE environment related to the underlying platform of the TOE

The second part of the assumptions relates to the dedicated HPC Application and is described by a link to the HPC specific Protection Profile [9]. Also in this case the assumptions are given here in short:

Assumptions for the TOE environment (chapter 3.2.2 of [6])	
Name	**Definition**
Assumptions on Phases 6 and 7	
A.Pers_Agent	Personalization and management of the Smart Card
A.Users	Adequate usage of TOE and IT-Systems

Table 13: Assumptions for the TOE environment related to the dedicated HPC Application

The last part of the assumptions is built by the assumptions that relate to the dedicated SIG Application of the TOE. These assumptions are also described by a reference to the Protection Profile [10] and are completed with the SIG Application specific assumption A.SIG_PERS in chapter 3.2. of the ST [6]. For the convenience of the reader these assumptions are repeated here in short:

Assumptions for the TOE environment (chapter 3.2.3 of [6])	
Name	**Definition**
Assumptions on Phase 6	
A.SIG_PERS	Security of the Personalisation Process for the SIG Application
Assumptions on Phase 7	
A.CGA	Trustworthy certification-generation application
A.SCA	Trustworthy signature-creation application

Table 14: Assumptions for the TOE environment related to the dedicated SIG Application of the TOE

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:

MICARDO V3.0 R1.0 HPC V1.0

The following table outlines the TOE deliverables:

The TOE consists of:

TOE component	Designation	Type	Transfer Form
TOE-IC	Philips SmartMX P5CC036V1D Secure Smart Card Controller (incl. its IC Dedicated Software)	HW / SW	---
TOE-ES/BS	Smartcard Embedded Software / Part Basic Software (implemented in ROM/EEPROM of the microcontroller) ROM-Maske: MICARDO_EHC_R4.0	SW	Source Code (implemented in ROM and EEPROM of the micro-controller)
TOE-ES/AS	Smartcard Embedded Software / Part Application Software (containing the HPC Application and SIG Application, implemented in the EEPROM of the microcontroller)	SW	Source Code (implemented in EEPROM of the micro-controller)
User Guide / User of the MICARDO platform	User guidance for the Administrator / User of the MICARDO Card [17]	DOC	Document in paper / electronic form
User Guide / User of the HPC Card	User guidance for the User of the HPC Card (in particular, HPC Application and SIG Application) [18]	DOC	Document in paper / electronic form
User Guide / Personaliser of the HPC Card	User guidance for the Personaliser of the HPC Card (in particular, HPC Application and SIG Application) [19]	DOC	Document in paper / electronic form
Identification Data Sheet of the HPC Card	Data Sheet with information on the actual identification data and configuration of the HPC Card delivered to the customer [20]	DOC	Document in paper / electronic form
Aut-Key of the	Public part of the authentication key pair relevant	KEY	Document in

TOE component	Designation	Type	Transfer Form
HPC Card	for the authenticity of the HPC Card		paper form / electronic file
Pers-Key of the HPC Card	Personalisation key relevant for the personalisation of the HPC Card	KEY	Document in paper form / electronic file

Table 15: Deliverables of the TOE

AID of MF: D2 76 00 00 28 41 30 00

AID of HPC: D2 76 00 00 40 02

AID of SIG: D2 76 00 00 66 01

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.

3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and will be used as Health Professional Card (HPC) within the German Health Care System. Furthermore, the TOE is intended to be used as Secure Signature-Creation Device (SSCD) for qualified electronic signatures. The security policy is to provide protection against

- Cloning of the TOE,
- modification and disclosure of IC assets / smart card embedded software / application data ,
- modification of program behaviour (including program loading and execution),
- compromise / forge / misuse of confidential user or TSF data including information leakage,
- interception of communication,
- abuse of TOE functionality (including its SIG and HPC applications),
- malfunction due to environmental stress as well as physical tampering,
- physical attacks through the TOE interfaces,
- storing, copying, releasing and deriving the signature creation data by an attacker,
- forgery of the electronic signature, of the signature-verification data, or of the DTBS-representation,
- repudiation of signatures,

- misuse of the signature creation function of the TOE.

4 Assumptions and Clarification of Scope

The assumptions for the environment of the TOE are given in chapter 3.2 of the ST [6]. These assumptions are described in three different parts.

The first part of the assumptions (chapter 3.2.1 of the ST [6]) relate to the underlying platform of the TOE and is included in the ST as a reference to the ST of the platform [16]. The assumptions are assigned to the different phases of the life cycle of the TOE, and are given here in short:

Assumptions for the TOE environment (chapter 3.2.1 of [6])	
Name	**Definition**
Assumptions on Phases 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 6	
A.PERS	Protection of the TOE under Personalisation
Assumptions on Phase 7	
A.USE_DIAG	Secure Communication with the terminal

Table 16: Assumptions related to the underlying platform of the TOE

The second part of the assumptions relates to the dedicated HPC Application and are described by a link to the HPC specific Protection Profile [9]. Also in this case the assumptions are given here in short:

Assumptions for the TOE environment (chapter 3.2.2 of [6])	
Name	**Definition**
Assumptions on Phases 6 and 7	

A.Pers_Agent	Personalization and management of the Smart Card
A.Users	Adequate usage of TOE and IT-Systems

Table 17: Assumptions related to the dedicated HPC Application of the TOE

The last part of the assumptions is built by the assumptions related to the dedicated SIG Application of the TOE. These assumptions also described by a reference to a Protection Profile [10] and completed with the SIG Application specific assumption A.SIG_PERS. These assumptions are repeated here in short:

Assumptions for the TOE environment (chapter 3.2.3 of [6])	
Name	**Definition**
Assumptions on Phase 6	
A.SIG_PERS	Security of the Personalisation Process for the SIG Application
Assumptions on Phase 7	
A.CGA	Trustworthy certification-generation application
A.SCA	Trustworthy signature-creation application

Table 18: Assumptions related to the dedicated SIG Application of the TOE

4.3 Clarification of scope

Additional threats that are not addressed by the TOE and its evaluated security functions were not addressed by this product evaluation.

5 Architectural Information

The TOE is composed of an Integrated Circuit (IC) and a Smart Card Embedded Software (TOE-ES), consisting of Basic Software (TOE-ES/BS) and Application Software (TOE-ES/AS). The Basic Software consists of the MICARDO V3.0 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 V3.0 Operating System platform and implements the specific HPC Application and SIG 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, the Philips SmartMX P5CC036V1D Secure Smart Card Controller. For details concerning the CC evaluation of the Philips IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-0293.

The security functions of the TOE are "Security Attribute Based Access Control", "Key Based User / TOE Authentication Based on Asymmetric Cryptography", "Key Based User / TOE Authentication Based on Symmetric

Cryptography", "Password Based User Authentication", "Stored Data Integrity Monitoring and Action", "Confidentiality of Data Exchange", "Integrity and Authenticity of Data Exchange", "Residual Information Protection", "Hardware and Software Failure Protection", "Side Channel Analysis Control", "Self Test", "Cryptographic Support", "RSA Key Pair Generation", "RSA Generation of Digital Signatures", "RSA Verification of Digital Signatures", "RSA Decryption" and "RSA Encryption".

6 Documentation

The following documentation is provided with the product by the developer to the customer (see also table 8 of this report):

User Guidance for the Administrator / User of the MICARDO Card, Version V1.02, 06.12.2006, Sagem ORGA GmbH [17]

User Guidance for the User of the HPC Card (in particular, HPC Application and SIG Application) , Version V1.02, 31. January 2007, Sagem ORGA GmbH [18]

User Guidance for the Personaliser of the HPC Card (in particular, HPC Application and SIG Application) , Version V1.01, 25. October 2006, Sagem ORGA GmbH [19]

Data Sheet with information on the actual identification data and configuration of the HPC Card delivered to the customer, Version V1.01, 25.10.2006, Sagem ORGA GmbH [20]

7 IT Product Testing

The developer tested all TOE Security Functions either on real cards or with simulator and emulator tests. All command APDU with valid and invalid inputs were tested as well as all functions with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests.

Since many Security Functions can be tested by ISO-7816 APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developers tests include a full coverage of all security functionality with emulator tests. Tests with emulators were chosen by the evaluators 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 covered

- testing APDU commands related to Access Control,
- testing APDU commands related to External Authenticate and Internal Authenticate based on asymmetric cryptography,
- testing APDU commands related to External Authenticate and Internal Authenticate based on symmetric cryptography,
- testing the PIN functionality of the card,

- testing the mechanisms of encryption and MAC calculation for Secure Messaging,
- testing the correct erasure of secret data after use,
- testing the integrity check of the card state,
- APDU command tests for the commands using cryptographic mechanisms,
- APDU command tests for the commands generating RSA key pairs,
- APDU command tests for the commands using digital signatures,
- APDU command tests for the commands used for RSA encryption and decryption.

Tests were performed on installed (initialised) cards, on personalized Health Professional Cards as well as on cards in non-initialised states.

Source code analysis was also performed during the evaluation.

Some test of the platform BSI-DSZ-CC-0390 are also valid for this certification and were therefore reused, however, most tests were either repeated or specifically performed for this evaluation.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing. The tests included the resistance of the RSA and Triple-DES Implementation against Side Channel Analysis.

The achieved test results correspond to the expected test results.

8 Evaluated Configuration

The TOE is defined uniquely by the name and version number MICARDO V3.0 R1.0 HPC V1.0.

With regard to the smart card product life cycle of the TOE (for more details about the TOE life cycle phases please read the Overview of the TOE Life Cycle explained in the ST [6], chapter 2.2), the different development and production phases of the TOE with its IC incl. its IC Dedicated Software and with its Smart Card Embedded Software (Basic Software, Application Software) are part of the evaluation of the TOE. For the delivery of the TOE different ways are established:

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

The form of the delivery of the TOE does not concern the security features of the TOE. However, the initialisation process at Sagem Orga GmbH in Flintbek,

Germany is considered within the framework of the CC evaluation of the Sagem Orga GmbH product. The responsibility for the delivery of the personalised TOE to the end user is up to the Card Issuer.

The development of the TOE is done in Sagem Orga GmbH Paderborn; production and if necessary initialisation of the TOE takes place at Sagem Orga GmbH Flintbek. Regarding the development and production environment of the underlying IC please refer to Annex A of the certification report of the chip [21].

The evaluation results are restricted to chip cards containing the TOE with HPC and SIG application that have been inspected during the evaluation process and that are listed in chapter 2 of this report. See also chapter 1.5 of this report.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] 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.

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [8] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36].

The ETR [8] builds up on the ETR-lite for Composition documents of the evaluation of the underlying hardware "Philips SmartMX P5CC036V1D Secure Smart Card Controller" ([21]). The ETR-lite for Composition documents was provided by the ITSEF T-Systems GEI GmbH according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]) and was validated by a recent re-assessment.

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 smart card 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 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**
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

Assurance classes and components		Verdict
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
Installation, generation, and start-up procedures	ADO_IGS.1	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
Vulnerability assessment	CC Class AVA	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 19: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the PP BSI-PP-0018-2007-MA-01
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended,
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ADV_IMP.2 - Implementation of the TSF, ATE_DPT.2 - Testing: Low-Level Design, AVA_MSU.3 - Analysis and Testing for Insecure States, AVA_VLA.4 - Highly Resistant,
- the following TOE Security Functions fulfil the claimed Strength of Function:

F.IA_AKEY	Key Based User / TOE Authentication Based on Asymmetric Cryptography
F.IA_SKEY	Key Based User / TOE Authentication Based on Symmetric Cryptography
F.IA_PWD	Password Based User Authentication
F.CRYPTO	Cryptographic Support
F.RSA_KEYGEN	RSA Key Pair Generation
F.GEN_DIGSIG	RSA Generation of Digital Signatures
F.RSA_DEC	RSA Decryption.

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

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Paragraph 3, Clause 2) that are present namely in the Security Functions F.EX_CONF, F.EX_INT, F.CRYPTO, F.GEN_DIGSIG, and F.RSA_DEC.

The results of the evaluation are only applicable to the MICARDO V3.0 R1.0 HPC V1.0 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [6] and the chapters 2, 4 and 8 of this report).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for recertification or assurance continuity 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 operational documentation (refer to chapter 6 of this report) 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 [6] 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.

Furthermore an appropriate protection during packaging, finishing, and personalisation must be ensured up to delivery to the end user to prevent any possible copy, modification, retention, theft, or unauthorised use of the TOE and of its manufacturing and test data (the assumption A.Process-Card from the ST of the hardware platform [22]).

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 sanitized version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

ACM	Assurance class configuration management
ADO	Assurance class delivery and operation
AGD	Assurance class guidance documentation
ALC	Assurance class life cycle support activity
APDU	Application Protocol Data Unit
AS	Application Software
ATE	Assurance class test activity
ATR	Answer To Reset
AVA	Assurance class Vulnerability Assessment Activity
BS	Basic Software
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria
CEM	Evaluation Methodology
CM	Card Manager
DES	Data Encryption Standard
DFA	Differential Fault Analysis

DOC	Document
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electronically Erasable Programmable Read Only Memory
EHC	Electronic Health Card
ES	Embedded Software
ETR	Evaluation Technical Report
FSP	Functional Specification
HLD	High-level Design
HPC	Health Professional Card
IC	Integrated Circuit
IFD	Interface Device
IMP	Implementation Representation
INI	Initialisation Module
IT	Information Technology
JIL	Joint Interpretation Library
LLD	Low-level Design
MAC	Message Authentication Code
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
PW	Password
RSA	Rivest-Shamir-Adleman Algorithm
SF	Security Function
SFP	Security Function Policy
SIG	Signature
SM	Secure Messaging
SMC	Security Module Card
SOF	Strength of Function
SPA	Simple Power Analysis
SPM	TOE Security Policy Model
ST	Security Target
TOE	Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Function

TSP TOE Security Policy

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 2.3, 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.

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

[6] Security Target – MICARDO V3.0 R1.0 HPC V1.0, Version V1.02, Sagem ORGA GmbH, 09.05.2007 (confidential document)

[7] Security Target ST-Lite – MICARDO V3.0 R1.0 HPC V1.0, Version V1.01, Sagem ORGA GmbH, 23.05.2007 (sanitized public document)

[8] Evaluation Technical Report, Version 1.2 Datum 10-05.2007, Titel MICARDO V3.0 R1.0 HPC V1.0 (confidential document)

[9] Protection Profile – Health Professional Card (HPC) – Heilberufsausweis (HBA), BSI-PP-0018-2007-MA-01, Version 1.1, 2. April 2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[10] Protection Profile – Secure Signature-Creation Device Type 3 “EAL 4+”, BSI-PP-0006-2002, Version 1.05, July 25th 2001, CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures

[11] German Health Professional Card and Security Module Card, Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.1.0, 21.02.2006, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH

[12] German Health Professional Card and Security Module Card, Part 2: HPC Applications and Functions, Version 2.1.0, 21.02.2006, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH

[13] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rah-menbedingungen für elektronische Signaturen; Amtblatt der Europäischen Gemeinschaften, L13/12-L13/20; 19.01.2001; Europäisches Parlament und Rat der Europäischen Union

[14] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften; Bundesgesetzblatt Nr. 22, S. 876; 16.05.2001

[15] Verordnung zur elektronischen Signatur; Bundesgesetzblatt Nr. 509, S. 3074; 16.11.2001

[16] Security Target – MICARDO V3.0 R1.0, Version V1.01, Sagem ORGA GmbH, 06.September 2006

[17] User Guidance, MICARDO V3.0 R1.0, Version V1.02, 06.12.2006, Sagem ORGA GmbH

[18] User Guidance, MICARDO V3.0 R1.0 HPC V1.0, Version V1.02, 31. January 2007, Sagem ORGA GmbH

[19] User Guidance for the Personaliser, MICARDO V3.0 R1.0 HPC V1.0, Version V1.01, 25. October 2006, Sagem ORGA GmbH

[20] Data Sheet MICARDO V3.0 R1.0 HPC V1.0, Version V1.01, 25.10.2006, Sagem ORGA GmbH

[21] Certification Report BSI-DSZ-CC-0293-2005 for Philips P5CC036V1D and P5CC009V1D with specific IC Dedicated Software Secure Smart Card Controller from Philips Semiconductors GmbH Business Line Identification, Bundesamt für Sicherheit in der Informationstechnik, BSI

[22] Security Target - Evaluation of the Philips P5CC036V1D Secure Smart Card Controller, BSI-DSZ-CC-0293, Version 1.0, March 18th 2005, Philips Semiconductors GmbH

This page is intentionally left blank.

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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 1: 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 6: 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

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0392-2007

Evaluation results regarding development and production environment

The IT product MICARDO V3.0 R1.0 HPC V1.0 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005), extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC15408: 2005).

As a result of the TOE certification, dated 25. May 2007, the following results regarding the development and production environment apply. The Common Criteria 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.1) 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:

- Sagem Orga GmbH, Heinz-Nixdorf-Ring 1, 33106 Paderborn (embedded software development)
- Sagem Orga GmbH, Konrad-Zuse-Ring 1, 24220 Flintbek (card production and initialisation site)

For development and productions sites regarding the "Philips SmartMX P5CC036V1D Secure Smart Card Controller" refer to the certification report BSI-DSZ-CC-0293.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target BSI-DSZ-0392-2007, MICARDO V3.0 R1.0 HPC V1.0, Sagem Orga GmbH, Version V1.01, 22.11.2006 [7].

The evaluators verified, that the threats, policies and security objective for the life cycle phases 1 to 5 up to delivery within or at the end of phase 5 as stated in the TOE Security Target [7] are fulfilled by the procedures of these sites.

This page is intentionally left blank.