



BSI-PP-0018-2005

Protection Profile

for

**Health Professional Card (HPC) –
Heilberufsausweis (HBA),
Version 1.0**

developed on behalf of the

Federal Ministry of Health, Germany

Certification Report

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



Certificate BSI-PP-0018-2005

Protection Profile

for

Health Professional Card (HPC) – Heilberufsausweis (HBA), Version 1.0



Common Criteria Arrangement

developed on behalf of the

Federal Ministry of Health, Germany

Assurance Package: EAL 4 augmented with
ADV_IMP.2, AVA_MSU.3 and AVA_VLA.4

Bonn, December 14th, 2005

The President of the Federal
Office for Information Security

Dr. Helmbrecht

L.S.

The Protection Profile mentioned above was evaluated at an accredited and licenced/approved evaluation facility on the basis of the *Common Criteria for Information Technology Security Evaluation (CC), Version 2.1 (ISO/IEC 15408)* applying the *Common Methodology for Information Technology Security Evaluation (CEM), Part 1 Version 0.6, Part 2 Version 1.0* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

This certificate applies only to the specific version and release of the Protection Profile and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the Federal Office for Information Security. 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 Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG¹ Act, the Bundesamt für Sicherheit in der Informationstechnik (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of TOEs which are intended to meet common consumer needs for IT security. The development and certification of a PP or the reference to an existent one gives consumers the possibility to express their IT security needs without referring to a special product. Product or system certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued.

Certification of a Protection Profile is carried out on the instigation of the author, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1].

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

¹ Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

Part A: Certification

Part B: Certification Results

Annex: Protection Profile

A Certification

1 Specifications of the Certification Procedure

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

- BSIG²
- BSI Certification Ordinance³
- BSI Schedule of Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011
- BSI Certification - Description of the Procedure (BSI 7125)
- Procedure for the Issuance of a PP certificate by the BSI
- Common Criteria for Information Technology Security Evaluation, Version 2.1⁵
- Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

² Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

³ Ordinance on the Procedure for Issuance of a Certificate by the Bundesamt für Sicherheit in der Informationstechnik (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 22 September 2000

2 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of Protection Profile certificates under certain conditions was agreed.

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005 and India in April 2005.

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 Protection Profile for Health Professional Card (HPC) – Heilberufsausweis (HBA), Version 1.0 has undergone the certification procedure at the BSI.

The evaluation of the Protection Profile for Health Professional Card (HPC) – Heilberufsausweis (HBA), Version 1.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation facility of SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)⁶ recognised by BSI.

Developer is the 'T-Systems GEI GmbH, Prüfstelle IT-Sicherheit' on behalf of the 'Federal Ministry of Health, Germany'.

The certification was concluded with

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

This work was completed by the BSI on December 14th, 2005.

⁶ Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-10.

The Protection Profile for Health Professional Card (HPC) – Heilberufsausweis (HBA), Version 1.0 has been included in the BSI list of certified and registered Protection Profiles, which is published regularly (see also Internet: <http://www.bsi.bund.de>). Further information can be obtained via the BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report may be ordered from the BSI⁷. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁷ **BSI** - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

B Certification Results

Content of the Certification Results

| | | |
|---|---------------------------------------|---|
| 1 | PP Overview..... | 2 |
| 2 | Security Functional Requirements..... | 4 |
| 3 | Assurance Package | 6 |
| 4 | Strength of Functions | 6 |
| 5 | Results of the Evaluation..... | 6 |
| 6 | Obligation for ST writer..... | 7 |
| 7 | Definitions..... | 7 |
| 8 | Bibliography..... | 8 |

1 PP Overview

The Protection Profile (PP) [7] defines the security objectives and requirements for the electronic Health Professional Card (HPC, German: "Heilberufsausweis") based on the regulations for the German health care system. It address the security services provided by this card, mainly:

- Authentication of the card holder by use of a PIN,
- Mutual Authentication between the HPC and a electronic Health Card (eHC) or the HPC and a Security Module Card (SMC),
- Document key decipherment for an external application,
- Client-server authentication for a client.

This Protection profile does not address the use of the HPC as secure-signature creation device for qualified electronic signature (see PP [7], chapter 9 Informative Annex: HPC as SSCD [13] for details).

The Target of Evaluation (TOE) defined in the PP is the Health Professional Card (HPC, German "Heilberufsausweis"). HPC is a contact based smart card which is conformant to the specification documents [8] and [9].

The TOE comprises of:

- TOE_IC, consisting of:
 - the circuitry of the HPC's chip (the integrated circuit, IC) and
 - the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- TOE_ES
 - the IC Embedded Software (operating system)
- TOE_APP
 - the HPC applications (data structures and their content)
- TOE_GD
 - the guidance documentation delivered together with the TOE.

The TOE is used by an individual acting as accredited health profession

- to authenticate themselves for access to the application data of a patient which are handled by the eHC or by the infrastructure of the health care service,
- to authorise health employees using a Security Module Card (SMC) for access to medications data and medical data on the eHC or handled by the infrastructure of the health care service in case of emergency,
- to decrypt keys of encrypted application data.

The TOE life cycle is described in terms of seven life cycle phases: Phase 1 "Smart Card Embedded Software Development", Phase 2 "IC Development",

Phase 3 “IC Manufacturing and Testing”, Phase 4 “IC Packaging and Testing“, Phase 5 “ Smart Card Product Finishing Process”, Phase 6 “Smart Card Personalization” and Phase 7 “Smart Card End-usage”. For the evaluation of the HPC the phases 1 up to 4 as defined in Table 1 are part of the TOE development in the sense of the CC. The phases 6 and 7 are part of the operational use in the sense of the CC. The phase 5 may be part of one of these CC phases or may be split between them depending on the specific model used by the TOE developer. The writer of the ST shall define the exact boundary.

The PP defines the following Security Objectives for the TOE:

| Identifier for Sec.Objective | Issue addressed by the Security Objective |
|------------------------------|---|
| OT.AC_Pers | Access Control for Personalization and Management |
| OT.Data_Confident | Confidentiality of internal Data |
| OT.Data_Integrity | Integrity of internal Data |
| OT.Trusted_Channel | Trusted Channel |
| OT.AC_Serv | Access Control for TOE Security Services |
| OT.Prot_Abuse_Func | Protection against Abuse of Functionality |
| OT.Prot_Inf_Leak | Protection against Information Leakage |
| OT.Prot_Phys_Tamper | Protection against Physical Tampering |
| OT.Prot_Malfunction | Protection against Malfunctions |

Table 1: Security Objectives for the TOE

The PP defines the Security Objectives for the environment of the TOE divided into two categories:

| Identifier for Sec.Objective | Issue addressed by the Security Objective |
|---|--|
| Security Objectives for the Development and Manufacturing Environment | |
| OD.Assurance | Assurance Security Measures in Development and Manufacturing Environment |
| OD.Material | Control over Smart Card Material |
| Security Objectives for the Operational Environment | |
| OE.Perso | Secure Personalization and Management |
| OE.Users | Adequate Usage of TOE and IT-Systems |

Table 2: Security Objectives for the environment of the TOE

For details and application notes refer to the PP [7] chapter 4. Security Functional Requirements for the TOE and for the IT-Environment are derived from these Security Objectives as outlined in the following chapter.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a TOE which is compliant to the Protection Profile. 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 taken from CC part 2:

| Security Functional Requirement | Identifier and addressed issue |
|---------------------------------|--|
| FCS | Cryptographic support |
| FCS_CKM.1/ASYM | Cryptographic Key Generation – Asymmetric Card-to-Card Authentication with Key Agreement |
| FCS_CKM.1/SYM | Cryptographic Key Generation – Symmetric Card-to-Card authentication with Key Agreement |
| FCS_CKM.4 | Cryptographic Key Destruction |
| FCS_COP.1/SHA | Cryptographic Operation – Hash Algorithm |
| FCS_COP.1/CCA_SIGN | Cryptographic Operation – Digital Signature-Creation for Card-to-Card Authentication |
| FCS_COP.1/CCA_VERIF | Cryptographic Operation – Digital Signature-Verification for Card-to-Card Authentication |
| FCS_COP.1/CSA | Cryptographic Operation – Digital Signature-Creation for Client-Server Authentication |
| FCS_COP.1/RSA_DEC | Cryptographic Operation – RSA Decryption |
| FCS_COP.1/TDES | Cryptographic Operation – Triple DES Encryption / Decryption |
| FCS_COP.1/MAC | Cryptographic operation – Retail MAC |
| FDP | User data protection |
| FDP_ACC.2 | Complete access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_RIP.1 | Residual Information Protection |
| FDP_SDI.2 | Stored Data Integrity |
| FDP_UCT.1 | Basic data exchange confidentiality |
| FDP_UIT.1 | Data exchange integrity |
| FIA | Identification and authentication |
| FIA_AFL.1 | Authentication failure handling – HPC-PIN |
| FIA_ATD.1 | User attribute definition |
| FIA_UID.1 | Timing of identification |
| FIA_UAU.1 | Timing of authentication |
| FIA_UAU.4 | Single-use authentication mechanisms |

| Security Functional Requirement | Identifier and addressed issue |
|--|--|
| FIA_UAU.6 | Re-authenticating |
| FMT | Security Management |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security roles |
| FMT_MTD.1/INI | Management of TSF data – Writing of Initialisation Data and Pre-personalization Data |
| FMT_MTD.1/RAD_WR | Management of TSF data – Writing of Authentication Reference Data |
| FMT_MTD.1/RAD_MOD | Management of TSF data – Modification of Authentication Reference Data |
| FMT_MTD.1/PIN | Management of TSF data – Management of the Human user Authentication Data |
| FMT_MTD.1/RAD_CH | Management of TSF data – Protection of Human user Authentication Data |
| FPT | Protection of the TOE Security Functions |
| 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/Channel |
| FTP_ITC.1 | Inter-TSF trusted channel |

Table 3: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

| Security Functional Requirement | Identifier and 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 4: 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 PP [7] chapter 6.

3 Assurance Package

The security assurance requirements are based entirely on the assurance components defined in Part 3 of the Common Criteria. The assurance requirements comply with assurance level EAL 4 augmented (Evaluation Assurance Level 4 augmented).

The following table shows the augmented assurance components.

| Requirement | Identifier |
|--------------|--|
| EAL4 | TOE evaluation: Methodically designed and tested |
| +: ADV_IMP.2 | Implementation of the TSF |
| +: AVA_MSU.3 | Analysis and testing for insecure states |
| +: AVA_VLA.4 | Highly resistant |

Table 5: Augmented assurance components

4 Strength of Functions

The minimum strength of function level is claimed SOF-high. This protection profile does not contain any security functional requirement for which an explicit strength of function claim is required.

5 Results of the Evaluation

The Evaluation Technical Report (ETR), [6] 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 verdict for the CC, Part 3 assurance component (according the class APE for the Protection Profile evaluation) is summarised in the following table.

| CC Aspect | Result |
|--------------|--------|
| CC Class APE | PASS |
| APE_DES.1 | PASS |
| APE_ENV.1 | PASS |
| APE_INT.1 | PASS |
| APE_OBJ.1 | PASS |
| APE_REQ.1 | PASS |
| APE_SRE.1 | PASS |

Table 6: Verdict for Assurance class

The Protection Profile for Health Professional Card (HPC) – Heilberufsausweis (HBA), Version 1.0 meets the requirements for Protection Profiles as specified in class APE of the CC.

6 Obligation for ST writer

In case that phase 5 “Smart Card Product Finishing Process“ of the PP is not part of the CC phase “TOE Development“ (see PP [7], chapter 2.3) the ST writer has to add an assumption for a secure Smart Card Product Finishing environment (see PP [7], table 1) and an according objective for the environment.

7 Definitions

7.1 Acronyms

| | |
|----------------|---|
| CC | Common Criteria for IT Security Evaluation |
| EAL | Evaluation Assurance Level |
| eHC | electronic Health Card |
| ICAO | International Civil Aviation Organisation |
| IT | Information Technology |
| ITSEF | Information Technology Security Evaluation Facility |
| HPC | Health Professional Card |
| PP | Protection Profile |
| SF | Security Function |
| SFP | Security Function Policy |
| SMC | Security Module Card |
| SOF | Strength of Function |
| SSCD-PP | Protection Profile Secure Signature Creation Device |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |

7.2 Glossary

Augmentation - The addition of one or more assurance component(s) from 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.

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.

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.

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.

8 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999
- [3] BSI certification: Procedural Description (BSI 7125)

- [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] Evaluation Technical Report for a PP evaluation, Version 1.0, December 09th, 2005, Common Criteria Protection Profile Health Professional Card (HPC) – Heilberufsausweis (HBA), SRC Security Research & Consulting GmbH (confidential document)
- [7] Common Criteria Protection Profile Health Professional Card (HPC) – Heilberufsausweis (HBA), BSI-PP-0018, Version 1.0, December 12th, 2005, BSI
- [8] German Health Professional Card and Security Module Card Specification - Pharmacist & Physician – Part 2: HPC Applications and Functions, Version 2.1 draft, 19.11.2005
- [9] German Health Professional Card and Security Module Card Specification - Pharmacist & Physician - Part 3: SMC Applications and Functions, Version 2.1 draft, 19.11.2005
- [10] German Health Professional Card and Security Module Card Specification - Pharmacist & Physician - Part 3: SMC Applications and Functions, Version 2.1 draft, 19.11.2005
- [11] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, Version 0.99, 31.10.2005, BMGS
- [12] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendungsspezifische Strukturen, Version 0.99, 06.11.2005, BMGS
- [13] Protection Profile Secure Signature Creation Device Type 2 resp. Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0005-2002T resp. BSI-PP-0006-2002T

This page is intentionally left blank.

C Annex: Protection Profile

The Protection Profile (PP) [7] is provided within a separate document.