Bundesamt
für Sicherheit in der
Informationstechnik

BSI-PP-0026-2006

Protection Profile

for

Machine Readable Travel Document with „ICAO Application“ Extended Access Control, Version 1.1

developed on behalf of the

Federal Ministry of the Interior, Germany

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

Bundesamt für Sicherheit in der Informationstechnik

Certificate BSI-PP-0026-2006

Protection Profile

for a

Machine Readable Travel Document with „ICAO Application“ Extended Access Control, Version 1.1

developed on behalf of the

Common Criteria Arrangement

Federal Ministry of the Interior, Germany

Assurance Package: **EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4**

Bonn, 11 December 2006

The Vice President of the Federal Office for Information Security

Hange 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 2.3 (ISO/IEC 15408)* applying the *Common Methodology for Information Technology Security Evaluation (CEM), Version 2.3* and including final interpretations.

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.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185 - 189 – D-53175 Bonn – Postfach 20 03 63 – D-53133 Bonn

Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (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 the Protection Profile is carried out on the instigation of the BSI. 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 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
- BSI Certification – Description of the Procedure [3]
- Procedure for the Issuance of a PP certificate by the BSI
- Common Criteria for Information Technology Security Evaluation, Version 2.3 [1][5]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)[4]

---

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 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Inneren 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 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 Machine Readable Travel Document with „ICAO Application" Extended Access Control, Version 1.1 has undergone the certification procedure at the BSI.

The evaluation of the Protection Profile for Machine Readable Travel Document with „ICAO Application" Extended Access Control, Version 1.1 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 ‘Federal Office for Information Security (BSI)‘ on behalf of the ‘Federal Ministry of the Interior, Germany’

The certification was concluded with

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

This work was completed by the BSI on 11 December 2006.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-11.

The Protection Profile for Machine Readable Travel Document with „ICAO Application" Extended Access Control, Version 1.1 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 BSI[7]. 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

The Protection Profile (PP) [7] defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTDs) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). It addresses the advanced security method Basic Access Control (BAC) Extended Access Control (EAC) and chip authentication similar to the Active Authentication in the Technical reports of the ICAO New Technology Working Group.

The Target of Evaluation (TOE) defined in the PP is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [8] and providing the Basic Access Control, the Extended Access Control according to the ICAO document and the chip authentication according to the technical report [9].

The TOE comprises the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors, the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software, the IC Embedded Software (operating system), the MRTD application and the associated guidance documentation. The TOE is usually integrated into a passport book of an MRTD holder for whom the issuing state or organisation has personalised the MRTD.

The TOE life cycle is described in terms of the four life cycle phases: Phase 1 "Development", Phase 2 "Manufacturing", Phase 3 "Personalization of the MRTD", Phase 4 "Operational Use". The intention of the PP is to consider at least the phases 1 and 2 as part of the evaluation and therefore define TOE delivery according to CC after phase 2 or later.

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 of logical MRTD
OT.Data_Int	Integrity of personal data
OT.Data_Conf	Confidentiality of personal Data
OT.Sens_Data_Conf	Confidentiality of sensitive biometric reference data
OT.Identification	Identification and Authentication of the TOE
OT.Chip_Auth_Proof	Proof of MRTD's chip authenticity
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 several categories:

Identifier for Sec. Objective	Issue addressed by the Security Objectiv
Security Objectives for the Development and Manufacturing Environment	
OD.Assurance	Assurance Security Measures in Development and Manufacturing Environment
OD.Material	Control over MRTD Material
Security Objectives for the Operational Environment	
OE.Personalization	Personalization of logical MRTD
OE.Pass_Auth_Sign	Authentication of logical MRTD by Signature
OE.Auth_Key_MRTD	MRTD Authentication Key
OE.Authoriz_Sens_Data	Authorization for Use of Sensitive Biometric Reference Data
For the Receiving State or organization	
OE.Exam_MRTD	Examination of the MRTD passport book
OE.Passive_Auth_Verif	Verification by Passive Authentication
OE.Prot_Logical_MRTD	Protection of data of the logical MRTD
OE.Ext_Insp_Systems	Authorisation of Extended Inspection Systems

Table 2: Security Objectives for the environment of the TOE

For details and application notes refer to the PP chapter 3.5. 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 claiming compliance 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/KDF_MRTD	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE
FCS_CKM.1/DH_MRTD	Cryptographic key generation – Diffie-Hellman Keys by the MRTD
FCS_CKM.4	Cryptographic key destruction – MRTD
FCS_COP.1/SHA_MRTD	Cryptographic operation – Hash for Key Derivation by MRTD
FCS_COP.1/TDES_MRTD	Cryptographic operation – Encryption / Decryption Triple DES
FCS_COP.1/MAC_MRTD	Cryptographic operation – Retail MAC
FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification by MRTD
FDP	**User data protection**
FDP_ACC.1 (PRIM)	Subset access control – Primary Access Control
FDP_ACC.1 (BASIC)	Subset access control – Basic Access control
FDP_ACF.1 (Basic)	Security attribute based access control – Basic Access Control
FDP_ACF.1 (PRIM)	Security attribute based access control – Primary Access Control
FDP_UCT.1/MRTD	Basic data exchange confidentiality - MRTD
FDP_UIT.1/MRTD	Data exchange integrity – MRTD
FIA	**Identification and authentication**
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.4/MRTD	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5/MRTD	Multiple authentication mechanisms
FIA_UAU.6/MRTD	Re-authenticating – Re-authenticating of Terminal by the TOE
FIA_AFL.1	Authentication failure handling

Security Functional Requirement	Identifier and addressed issue
FMT	**Security Management**
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Pre-personalization Data
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
FMT_MTD.1/CVCA_INI	Management of TSF data – Initialisation of CVCA Certificate and Current Date
FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifier Certification Authority
FMT_MTD.1/DATE	Date Management of TSF data – Current date
FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write
FMT_MTD.1/CAPK	Management of TSF data – Chip Authentication Private Key
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
FMT_MTD.3	Secure TSF data
FPT	**Protection of the TOE Security Functions**
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_PHP.3	Resistance to physical attack
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

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

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Identifier and addressed issue
FAU	**Security Audit**
FAU_SAS.1	Audit storage
FCS_RND	**Generation of random numbers**
FCS_RND.1/MRTD	Quality metric for random numbers
FIA_API	**Authentication Proof of identity**
FIA_API.1/CAP	Authentication Proof of identity-MRTD
FMT_LIM	**Limited capabilities and availability**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FPT_EMSEC	**TOE Emanation**
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 chapter 5.

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

Security Functional Requirement	**Identifier and addressed issue**
FDP	**User data protectiont**
FDP_DAU.1/DS	Basic data authentication - Passive Authentication
FDP_UCT.1/GIS	Basic data exchange confidentiality – General Inspection System
FDP_UIT.1/GIS	Data exchange integrity - General Inspection System
FCS	**Cryptographic support**
FCS_CKM.1/PKI	Cryptographic key generation – Document Verification PKI Keys
FCS_COP.1/CERT_SIGN	Cryptographic operation – Certificate Signing
FCS_CKM.1/KDF_BT	Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal
FCS_CKM.4/BT	Cryptographic key destruction – BT
FCS_COP.1/SHA_BT	Cryptographic-operation-Hash Function by the Basic Terminal
FCS_COP.1/ENC_BT	Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal
FCS_COP.1/MAC_BT	Cryptographic operation – Secure messaging Message Authentication Code by the Basic

Security Functional Requirement	Identifier and addressed issue
	Terminal
FCS_COP.1/SIG_SIGN_EIS	Cryptographic operation – Signature creation by EIS
FCS_COP.1/SHA_EIS	Cryptographic operation – Hash for Key Derivation by EIS
FCS_CKM.1/DH_GIS	Cryptographic key generation – Diffie-Hellman Keys by the GIS
FCS_COP.1/SHA_GIS	Cryptographic operation – Hash for Key Derivation by GIS
FIA	**Identification and authentication**
FIA_UAU.4/GIS	Single-use authentication mechanisms – Single-use authentication of the Terminal by the GIS
FIA_UAU.5/GIS	Multiple authentication mechanisms – General Inspection System
FIA_UAU.6/GIS	Re-authenticating of Terminal by the General Inspection System
FIA_UAU.4/BT	Single-use authentication mechanism-Basic Terminal
FIA_UAU.6/BT	Re-authentication Basic-Terminal
FIA_API.1/SYM_PT	Authentication Proof of Identity – Personalization Terminal Authentication with Symmetric Key

Table 5: SFRs for the IT-Environment, taken from CC part 2

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

The following CC part 2 extended SFRs are defined for the IT Environment of the TOE:

Security Functional Requirement	Identifier and addressed issue
FCS	**Cryptographic support**
FCS_RND.1/BT	Quality metric for random numbers-Basic Terminal
FIA	**Identification and authentication**
FIA_API.1/EIS	Authentication Proof of Identity –Extended Inspection System

Table 6: SFRs for the IT-Environment, CC part 2 extended

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 EAL4 (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
+: ALC_DVS.2	Sufficiency of security measures
+: AVA_MSU.3	Analysis and testing for insecure states
+: AVA_VLA.4	Highly resistant

Table 7: TOE security assurance requirements

4 Strength of Functions

The minimum strength of function level is claimed SOF-high and covers but is not limited to the TSF required by the SFR FIA_UAU.4, FCS_RND.1 and FPT_FLS.1 as far as probabilistic or permutational mechanisms are involved.

A TOEs implemented security functions shall meet this claimed strength from design and construction point of view. The strength of function available in a specific system context where the TOE is used depends on the selection of the data used to set up the communication to the TOE. Therefore the issuing state or organisation is responsible for the strength of function that can be achieved in a specific system context. This has to be assessed in the specific system context.

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 [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 8: Assurance class

The Protection Profile for Machine Readable Travel Document with „ICAO Application" Extended Access Control, Version 1.1 meets the requirements for Protection Profiles as specified in class APE of the CC.

6 Definitions

6.1 Acronyms

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

6.2 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.

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.

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.

7 Bibliography

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

[2] Common Methodology for Information Security Evaluation, Version 2.3

[3] BSI Certification – Description of the Procedure (BSI 7125)

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

[5] German IT Security Certificates (BSI 7148, BSI 7149)

[6] Evaluation Technical Report for a PP evaluation, Version 1.1, 7. September 2006, Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application" Extended Access Control, SRC (confidential document)

[7] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application" Extended Access Control, BSI-PP-0026, Version 1.1, 7. September 2006, BSI

[8] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[9] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

Annex: Protection Profile