Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0021-2006

for

BAROC Smart Card Protection Profile

Version 1.2

developed by

BAROC/FISC Smart Card Group

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

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

Certificate BSI-PP-0021-2006

BAROC Smart Card Protection Profile, Version 1.2

developed by

BAROC/FISC Smart Card Group

Assurance Package : EAL4 augmented with ADV_IMP.2 and AVA_VLA.4

Common Criteria Arrangement

Bonn, 18 January 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 2.1 (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.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 – D-53175 Bonn – Postfach 20 03 63 – D-53133 Bonn
Telefon (0228) 9582-0 – Telefax (0228) 9582-455 – Infoline (0228) 9582-111

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 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

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 [1], Version 2.1[5]
- Common Methodology for IT Security Evaluation [2], Part 1 Version 0.6, Part 2 Version 1.0

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 Bundesamtes 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 Bundesamtes 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, 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 BAROC Smart Card Protection Profile, Version 1.2 has undergone the certification procedure at the BSI.

The evaluation of the BAROC Smart Card Protection Profile, Version 1.2 was conducted by "Evaluation Body for IT Security of TÜVIT – member of TÜV NORD Group". The evaluation facility of TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

Sponsor is the Bankers Association of the Republic of China (BAROC).

The certification was concluded with

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

This work was completed by the BSI on 18 January 2006.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-6.

The BAROC Smart Card Protection Profile, Version 1.2 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 sponsor[7]. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] The Bankers Association of the Republic of China, 3F, No. 9, De-Huei St., Taipei 10461, Taiwan, R.O.C.

B Certification Results

Content of the Certification Results

1 PP Overview

The BAROC Smart Card Protection Profile, Version 1.2 is established by BAROC/FISC.

It is developed to serve as a baseline for the security of smartcards developed by different vendors. These smartcards will be used for the financial transactions within the FISC inter-bank system.

The Protection Profile focuses on a Financial Smart Card which consists of embedded software and a secure IC Controller. The TOE is used as a security token for inter-bank financial transactions, such as cash withdrawal, fund transfer, tax payment and online sale.

The TOE security functionality consists of:

TAC (Transaction Authentication Code) generation
The TOE calculates a TAC on transaction data. The TAC ensures authenticity and integrity of the transaction data. In addition to the TAC, the TOE also generates a transaction S/N (serial number) which participates in the calculation of the TAC. In order to generate a TAC, the user has to enter a PIN for confirmation.

Secure key update
The TOE is providing a secure means to update cryptographic keys (especially the key which is used for TAC generation) that will be stored in the TOE.

Protection of TSF and user data
The TOE protects its TSF and user data from unauthorized modification and disclosure.

It should be noted that it is considered by the Protection Profile authors to be impossible for the user to maintain confidentionality of their PIN, thus there is to be no threats „stealing“ a PIN from the environment. Rather, the functions of the TOE are to maintain the secrecy of the private key and generate „TAC's“.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a BAROC/FISC Smart Card Protection Profile compliant TOE.

All functional requirements are drawn from Common Criteria, Version 2.1, Part 2 except for Security Functional Component FPT_EMAN.1.

Component	Component-Name
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1/KEY	Subset access control for cryptographic keys
FDP_ACC.1/TAC	Subset access control for TAC generation

Component	Component-Name
FDP_ACF.1/ KEY	Security attribute based access control for cryptographic keys
FDP_ACF.1/TAC	Security attribute based access control for TAC generation
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_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_AFL.1/PIN	Authentication failure handling regarding the PIN
FIA_AFL.1/KEY	Authentication failure handling regarding the key
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
FMT_MSA.1/TAC	Management of security attributes for TAC
FMT_MSA.1/KEY	Management of security attributes for keys
FMT_MSA.2	Secure security attributes
FMT_MSA.3/TAC	Static attribute initialization for TAC
FMT_MSA.3/KEY	Static attribute initialization for keys
FMT_MTD.1	Management of TSF data
FMT_SMF.1/PIN	Specification of Management Functions for PIN
FMT_SMF.1/KEY	Specification of Management Functions for TAC
FMT_SMR.1	Security roles
FPT_AMT.1	Abstract machine testing
FPT_EMAN.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_ITC.1	Inter-TSF trusted channel

Table 1: TOE Security Functional Requirements

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 are 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 TSF
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 2: TOE security assurance requirements

4 Strength of Functions

The strength of functions postulated for this Protection Profile is

SoF-high.

5 Results of the Evaluation

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The 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 3: Verdict for assurance class

The BAROC Smart Card Protection Profile, Version 1.2 meets the requirements for Protection Profiles as specified in class APE of the CC.

6 Definitions

6.1 Acronyms

BAROC The Bankers Association of the Republic of China

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

FISC Financial Information Services Co., Ltd.

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 of the CC 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.

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.

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.

7 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1 (ISO/IEC 15408)

[2] Common Methodology for Information Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0

[3] BSI Certification – Description of the Procedure

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

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

[6] BAROC Smart Card Protection Profile, Version 1.2, 11.11.2005

[7] Evaluation Technical Report (ETR), Version 3.0, 01.12.2005 (confidentional document)

Annex: Protection Profile