Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0003-2001

for

Smart Card Security User Group
Smart Card Protection Profile
(SCSUG-SCPP)
Version 3.0

developed by

Smart Card Security User Group

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

Certificate BSI-PP-0003-2001

Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP) Version 3.0

developed by

Smart Card Security User Group

Assurance Package : **EAL4 augmented**

Common Criteria Arrangement

Bonn, 10th October 2001

The President of the Bundesamt für Sicherheit in der Informationstechnik

Dr. Henze 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.*

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 Bundesamt für Sicherheit in der Informationstechnik. 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 Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Bundesamt für Sicherheit in der Informationstechnik 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 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 [CC].

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 [BSI 7125]
- Procedure for the Issuance of a PP certificate by the BSI
- Common Criteria for Information Technology Security Evaluation [CC], Version 2.1[5]
- Common Methodology for IT Security Evaluation [CEM], Part 1 Version 0.6, Part 2 Version 1.0

---

[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 29 October 1992, Bundesgesetzblatt I p. 1838

[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.

In May 2000 an arrangement for the mutual recognition of IT security certificates up to the assurance package EAL4 and Protection Profiles based on the CC was signed by the national bodies of Australia, Canada, Finland, France, Germany, Great Britain, Greece, Italy, Netherlands, New Zealand, Norway, Spain an the USA. Israel joined the arrangement in November 2000.

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 Smart Card Security User Group - Smart Card Protection Profile Version 3.0 has undergone the certification procedure at the BSI.

The evaluation of the Smart Card Security User Group - Smart Card Protection Profile Version 3.0 was conducted by 'Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH - ein Unternehmen der RWTÜV-Gruppe'. The evaluation facility of TÜV Informationstechnik GmbH is an evaluation facility recognised by BSI (ITSEF)[6].

Sponsor is Europay International S.A. (on behalf of the Smart Card Security User Group). Developer is the Smart Card Security User Group. The members of the Smart Card Security User Group at time of the application for certification included:

- American Express
- Europay International
- JCB Co Ltd
- MasterCard International
- Mondex International
- Visa International
- National Institute of Standards and Technology (USA)
- National Security Agency (USA)

The certification was concluded with

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

This work was completed by the BSI on 10th Oktober 2001.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-7.

The Smart Card Security User Group - Smart Card Protection Profile Version 3.0 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 0228/9582-111.

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] **Europay International S.A.** (on behalf of the Smart Card Security User Group), Chaussée de Tervuren 198A, B-1410 Waterloo, Belgium

B Certification Report

Content of the Certification Report

1 PP Overview

This PP describes the IT security requirements for a smart card to be used in connection with sensitive applications, such as banking industry financial payment systems. Smart card as used in this PP means an integrated circuit containing a microprocessor, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory which may include RAM, ROM, and/or programmable non-volatile memory (typically EEPROM or Flash memory). The carrier is typically made of plastic and usually conforms to ISO 7810 and 7813 - Identification Cards, but may have the smaller size of a GSM (global system for mobile communications) subscriber identification module (SIM). The chip is embedded in a module which provides the capability for standardized connection to systems separate from the chip (typically through contacts in accordance with ISO 7816 or contactless in accordance with ISO 14443).

This PP covers the smart card's integrated circuit and operating software, but does not include specific applications. Application-specific PPs or security targets may use the Smart Card Security User Group - Smart Card Protection Profile Version 3.0 (SCSUG-SCPP) as a foundation for further work.

This PP is applicable to both contact and contactless smart cards, without special regard for form factor or physical card security features. This PP does not cover card features such as printing, the magnetic stripe (if present), security features such as holograms, or any other part of the card. It also does not cover security requirements for card acceptor devices (CADs) or networks interfacing with them.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a SCSUG-SCPP–compliant TOE.

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

Component	Component Name	Refined?	Operations Completed?
FAU_ARP.1	Security alarms	no	no
FAU_LST.1	Audit list generation	Explicitly stated	partial
FAU_SAA.1	Potential violation analysis	no	no
FAU_SEL.1	Selective audit	no	no
FAU_STG.1	Protected audit trail storage	no	yes

Component	Component Name	Refined?	Operations Completed?
FAU_STG.3	Action in case of possible audit data loss	no	no
FCS_CKM.1	Cryptographic key generation	no	no
FCS_CKM.3	Cryptographic key access	no	no
FCS_COP.1	Cryptographic operation	no	no
FDP_ACC.1	Subset access control	no	no
FDP_ACF.1	Security attribute based access control	no	no
FDP_ETC.1	Export of user data without security attributes	no	no
FDP_IFC.1	Subset information flow control	no	no
FDP_IFF.1	Simple security attributes	no	no
FDP_ITC.1	Import of user data without security attributes	no	no
FDP_ITT.1	Basic internal transfer protection	no	partial
FDP_RIP.1	Subset residual information protection	no	partial
FDP_UIT.1	Data exchange integrity	no	partial
FIA_AFL.1	Authentication failure handling	no	no
FIA_ATD.1	User attribute definition	no	no
FIA_UAU.1	Timing of authentication	no	no
FIA_UAU.7	Protected authentication feedback	no	yes
FIA_UID.1	Timing of identification	no	no
FMT_MOF.1	Management of security functions behavior	no	partial
FMT_MSA.1	Management of security attributes	no	no
FMT_MSA.2	Secure security attributes	no	N/A
FMT_MSA.3	Static attribute initialization	no	partial
FMT_MTD.1	Management of TSF data	no	no
FMT_MTD.2	Management of limits on TSF data	no	partial
FMT_MTD.3	Secure TSF data	no	N/A
FMT_REV.1	Revocation	no	no

Component	Component Name	Refined?	Operations Completed?
FPT_FLS.1	Failure with preservation of secure state	no	no
FPT_ITI.1	Inter-TSF detection of modification	no	no
FPT_ITT.1	Basic internal TSF data transfer protection	no	yes
FPT_PHP.3	Resistance to physical attack	no	partial
FPT_RCV.3	Automated recovery without undue loss	no	partial
FPT_RCV.4	Function recovery	no	yes
FPT_RPL.1	Replay detection	no	no
FPT_RVM.1	Non-bypassability of the TSP	no	N/A
FPT_SEP.1	TSF domain separation	no	N/A
FPT_TST.1	TSF testing	no	no
FTP_ITC.1	Inter-TSF trusted channel	no	no

3 Assurance Package

This section lists the IT security assurance components and indicates whether the component has been refined. Following the table, each requirement is listed with refinements identified. These requirements are chosen to be in support of specific objectives or are included consistent with an EAL4 augmented assurance level. Augmentation includes AVA_VLA.3 and ADV_INT.1.

Component	Component Name	Refined?
ACM_AUT.1	Partial CM automation	no
ACM_CAP.4	Generation support and acceptance procedures	no
ACM_SCP.2	Problem tracking CM coverage	yes
ADO_DEL.2	Detection of modification	no
ADO_IGS.1	Installation, generation, and start-up procedures	no
ADV_FSP.2	Fully defined external interfaces	no
ADV_HLD.2	Security enforcing high-level design	no
ADV_IMP.1	Subset of the implementation of the TSF	yes

Component	Component Name	Refined?
ADV_INT.1	Modularity	yes
ADV_LLD.1	Descriptive low-level design	no
ADV_RCR.1	Informal correspondence demonstration	no
ADV_SPM.1	Informal TOE security policy model	no
AGD_ADM.1	Administrator guidance	no
AGD_USR.1	User guidance	no
ALC_DVS.1	Identification of security measures	yes
ALC_LCD.1	Developer defined life-cycle model	no
ALC_TAT.1	Well-defined development tools	no
ATE_COV.2	Analysis of coverage	no
ATE_DPT.1	Testing: high-level design	no
ATE_FUN.1	Functional testing	no
ATE_IND.2	Independent testing - sample	no
AVA_MSU.2	Validation of analysis	no
AVA_SOF.1	Strength of TOE security function evaluation	no
AVA_VLA.3	Moderately resistant	yes

4 Strength of Functions

The strength of functions postulated for this Protection Profile is

SoF-high.

5 Results of the Evaluation

The Smart Card Security User Group - Smart Card Protection Profile Version 3.0 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 Part3 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.

7 Bibliography

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

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

[7125] BSI Certification – Description of the Procedure

[7148] German IT Security Certificates

C Protection Profile