Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0002-2001

for

Smartcard IC Platform Protection Profile
Version 1.0

developed by

Atmel Smart Card ICs
Hitachi Europe Limited
Infineon Technologies AG
Philips Semiconductors Hamburg

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-0002-2001

Smartcard IC Platform Protection Profile Version 1.0

developed by

Atmel Smart Card ICs, Hitachi Europe Limited, Infineon Technologies AG, Philips Semiconductors Hamburg

Assurance Package : **EAL4 augmented**

Common Criteria Arrangement

Bonn, 11 July 2001

The President of the Bundesamt für Sicherheit in der Informationstechnik

Dr. Henze L.S.

The Protection Profile mentioned above was evaluated by the evaluation facility of BSI 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.

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.

The Certification Report contains the technical description of the security functionality of the certified Protection Profile, the details of the evaluation (strength and weaknesses) and instructions for the user.

[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]
- Interim 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 agreement 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 agreement 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 Smartcard IC Platform Protection Profile Version 1.0 has undergone the certification procedure at the BSI.

The evaluation of the Smartcard IC Platform Protection Profile Version 1.0 was conducted by the evaluation facility of the BSI.

Sponsors and developers are Atmel Smart Card ICs, Hitachi Europe Limited, Infineon Technologies AG and Philips Semiconductors Hamburg.

The certification was concluded with

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

This work was completed by the BSI on 11 July 2001.

4 Publication

The following Certification Results contain pages B-1 to B-8.

The Smartcard IC Platform Protection Profile 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 0228/9582-111.

Further copies of this Certification Report may be ordered from the sponsors[6]. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] **Atmel Smart Card ICs**, Maxwell Building, Scottish Enterprise Technology Park, East Kilbride, Scotland, G75 0QR, United Kingdom;
Hitachi Europe Limited, Smart Card Business, Lower Cookham Road, Maidenhead, Berkshire SL6 8YA, United Kingdom;
Infineon Technologies AG, Postfach 80 09 49, D-81609 München;
Philips Semiconductors Hamburg, Unternehmensbereich der Philips GmbH, Business Unit Identification, P.O. Box 54 02 40, D-22502 Hamburg;

B Certification Report

Content of the Certification Report

1 PP Overview

1.1 Introduction

The CC is rapidly becoming the de facto standard in the smartcard marketplace, as a means to guarantee suitable, sufficient and consistent security assurance for these versatile products.

In order to make the CC process as rapid, flexible and cost effective as possible for its users, a group of the major smartcard IC manufacturers has proposed a new approach to evaluating the IC itself. This new approach is intended to take full advantages of the possibilities of modularity and reuse allowed under the CC, to ensure that each silicon platform need only be evaluated once, and the results can then be directly applied to whatever applications are built on that platform.

This concept is embodied in the new IC platform PP, jointly developed by the following Integrated Circuits manufacturers:

- Atmel Smart Card ICs,
- Hitachi Europe Limited,
- Infineon Technologies AG and
- Philips Semiconductors Hamburg

in co-operation with debis Systemhaus Information Security Services GmbH (T-Systems IT Security Services) and with extensive consultation with the Certification Body.

In this PP, the Target of Evaluation (TOE) is a smartcard integrated circuit which is composed of a processing unit, security components, I/O ports (contact or contactless) and volatile or non-volatile memories (hardware). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is often used for testing purposes during production only but may also provide additional services to facilitate usage of the hardware and/or to provide additional services (for instance in the form of a library). In addition to the IC Dedicated Software the Smartcard Integrated Circuit may also comprise hardware to perform testing. All other software is called Smartcard Embedded Software and is not part of the TOE.

The increase in the number and complexity of applications in the smartcard market is reflected in the increase of the level of data security required. The security needs for a smartcard can be summarised as being able to counter those who want to defraud, gain unauthorised access to data and control a system using a smartcard. Therefore it is mandatory to:

- maintain the integrity and the confidentiality of the content of the smartcard memory as required by the application(s) the smartcard is built for and

- maintain the correct execution of the software residing on the card.

This requires that the smartcard integrated circuit especially maintains the integrity and the confidentiality of its security enforcing and security relevant architectural components.

The intended environment is very large. Once issued the smartcard can be used anywhere in the world, at any time, and no control can be assumed with regard to the operational environment.

The evaluation of the smartcard integrated circuit according to this Protection Profile is independent of the evaluation of the Smartcard Embedded Software. The developer of the Smartcard Embedded Software decides if the platform (evaluated smartcard integrated circuit) is suitable for the application. An evaluation of a smartcard can be built on the results of the evaluation of the smartcard integrated circuit conforming to this Protection Profile.

The whole life-cycle of the card will be considered during evaluations using this Protection Profile as far as the developer/manufacturer of the TOE is directly involved. An organisational security policy and a security objective is defined to ensure that this is covered. A complex of details is given in terms of refinements of the Common Criteria assurance components concerning the development and production processes.

The Common Criteria depict an ideal development process starting with a definition of the requirements and then having the design process, implementation, test, acceptance, delivery and usage. However, the smartcard development and production process is more complex. For instance the external interfaces of the IC designer / IC manufacturer are complex: Not only the delivery of the final product (“die” or wafer to smartcard embedding and personalisation) must be considered. The IC designer / IC manufacturer interacts with the Smartcard Embedded Software development, the mask manufacturer and may also exchange critical information with the card manufacturer.

Therefore, Common Criteria assurance requirements will be refined to ensure that this Protection Profile exactly reflects the requirements for the exchange of information and material between the developer/manufacturer of the TOE and its partners. So, the details regarding secure exchange (delivery and receipt) of assets are not specified in terms of threats. The necessity of appropriate security measures is established and emphasised by an organisational security policy.

This Protection Profile will describe the security problems related to smartcard integrated circuits (and the corresponding security objectives and requirements) in a more general way though addressing all important issues. Attack scenarios will be mentioned whenever appropriate but only to illustrate the corresponding security problem. The information about attack scenarios can not be considered as being complete.

It is not possible (because of differences between the chips) nor desirable (confidentiality; do not instruct the attackers) to specify all the specific attack scenarios and all the security features on a Protection Profile level. The Security Target may describe the Smartcard IC in more detail without necessarily disclosing construction details.

Hardware and software together shall build an integrated secure whole. There can be a lot of interdependencies between the two. Information for developing secure software has to be provided by the User Guidance. Therefore, in this PP, requirements for the Smartcard Embedded Software are specified as Security Requirements for the Non-IT Environment.

2 Security Functional Requirements

The following Security Functional Requirements from Part 2 of the CC are used in the present Protection Profile:

Security Functional Requirement	Identifier
FRU	**Resource utilisation**
FRU_FLT.2	Limited fault tolerance
FPT	**Protection of the TOE Security Functions**
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_SEP.1	TSF domain separation
FPT_PHP.3	Resistance to physical attack
FDP	**User data protection**
FDP_ITT.1	Basic internal transfer protection
FDP_IFC.1	Subset information overflow control

The predefined CC Security Functional Requirements are extended by the following requirements:

Security Functional Requirement	Identifier
FAU	**Security Audit**
FAU_SAS.1	Audit storage
FCS	**Cryptographic support**
FCS_RND.1	Quality metric for random numbers
FMT	**Security management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability

3 Assurance Package

The following Security Assurance Requirements from Part 3 of the CC are used in the present Protection Profile:

Requirement	Identifier
EAL4	Methodically designed, tested and reviewed
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_MSU.3	Analysis and testing of insecure states
AVA_VLA.4	Highly resistant

4 Strength of Functions

The strength of functions postulated for this Protection Profile is

SoF-high.

5 Results of the Evaluation

The Smartcard IC Platform Protection Profile Version 1.0 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