BSI-PP-0005-2002

for

Protection Profile – Secure Signature-Creation Device Type 2, Version 1.04

developed by

CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures

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-0005-2002

Protection Profile – Secure Signature-Creation Device Type 2, Version 1.04

developed by

Common Criteria Arrangement

CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures

Assurance Package : **EAL4 augmented**

Bonn, 3. April 2002

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 [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

---

[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.

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.

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 ‘Secure Signature-Creation Device Type 2’, Version 1.04 has undergone the certification procedure at the BSI.

The evaluation of the Protection Profile ‘Secure Signature-Creation Device Type 2’, Version 1.04 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 CEN/ISSS Information Society Standardization System, Workshop on Electronic Signatures.

The certification was concluded with

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

This work was completed by the BSI on 3. April 2002.

[6] Information Technology Security Evaluation Facility

4 Publication

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

The Protection Profile ‘Secure Signature-Creation Device Type 2’, Version 1.04 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] CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures, Rue de Stassart 36, B-1050 Brussels, Belgium

B Certification Results

Content of the Certification Results

1 PP Overview

This Protection Profile ‘Secure Signature-Creation Devices (SSCD-PP) Type 2‘ is established by CEN/ISSS for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures as generally recognised standard for electronic-signature products.

The intent of this Protection Profile SSCD-PP Type 2 is to specify functional and assurance requirements for the signature-creation in conformance with Annex III of the Directive 1999/93/ec for secure signature-creation devices. Member States shall presume that there is compliance with the requirements laid down in Annex III of the directive when electronic signature products are evaluated according to Security Targets (ST) that are compliant with this PP and the PP for SSCD Type 1 [5] or the PP for SSCD Type 3 [6]. SSCD Type 1 represent the components for the generation of the Signature-Creation Data (SCD). The SSCD of Type 3 is a combination of SSCD Type 1 and SSCD Type 2.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a SSCD-PP Type 2 compliant TOE.

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

Component	Component-Name
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
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_UIT.1	Data exchange integrity
FDP_UCT.1	Basic data exchange confidentiality
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication

Component	Component-Name
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_AMT.1	Abstract machine testing
FPT_EMSEC.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
FTP_TRP.1	Trusted path

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
+: AVA_MSU.3	Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

4 Strength of Functions

The strength of functions postulated for this Protection Profile is

SoF-high.

5 Results of the Evaluation

The Protection Profile 'Secure Signature-Creation Device Type 2', Version 1.04 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.

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

[5] Protection Profile ‘Secure Signature-Creation Devices (SSCD-PP) Type 1‘, Version 1.05, 28.07.2001

[6] Protection Profile ‘Secure Signature-Creation Devices (SSCD-PP) Type 3‘, Version 1.05, 25.07.2001

Annex: Protection Profile