Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0014-2005

Low Assurance Protection Profile

for a

Software based Personal Firewall for home Internet use Version 1.2

developed by

TNO ITSEF BV

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-0014-2005

Low Assurance Protection Profile
for a
Software based Personal Firewall for home Internet use
Version 1.2

Common Criteria Arrangement

developed by

TNO ITSEF BV

Assurance Package : EAL1

Bonn, July 08th, 2005

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

The Protection Profile mentioned above was evaluated at an accredited and licenced/approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.4 Revision 256 including Draft Interpretations #1 - #17 for conformance to the Common Criteria for IT Security Evaluation, Version 2.4, Revision 256.

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 (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 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].

According to the decree issued by the Bundesministerium des Innern (Federal Ministry of the Interior) on February 22nd, 2005 the BSI is authorised to issue certificates on the basis of CC, Version 2.4, Revision 256.

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 December 17th, 1990, Bundesgesetzblatt I p. 2834

Contents

Part A: Certification

Part B: Certification Results

Annex: Protection Profile

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 2.4, Revision 256 [1]
- Common Methodology for IT Security Evaluation, Version 2.4, Revision 256 with the CC v2.4 Draft Interpretations #1 - #17 [2]

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of December 17th, 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 July 07th, 1992, Bundesgesetzblatt I p. 1230

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

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 “Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, Version 1.2” has undergone the certification procedure at the BSI.

The evaluation of the “Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, Version 1.2” was conducted by SRC Security Research & Consulting GmbH. The evaluation facility of SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by BSI.

Author is TNO ITSEF BV.

The certification was concluded with

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

This work was completed by the BSI on July 08th, 2005.

[5] Information Technology Security Evaluation Facility

4 Publication

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

The “Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, 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 BSI[6]. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] 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 2

3 Assurance Package 3

4 Strength of Functions 3

5 Results of the Evaluation 4

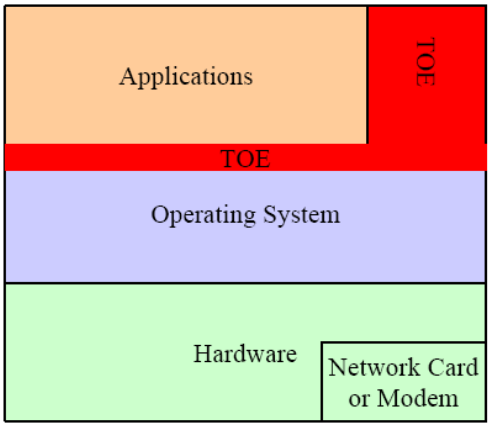
6 Definitions 5

7 Bibliography 6

1 PP Overview

This „Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, Version 1.2“ is established by TNO ITSEF BV as basis for the development of STs for TOEs that protect a personal computer which is connected to the internet and is used in a typical home computing environment.

The diagram below shows where the TOE can be placed in its environment: the TOE can operate as an application (from the home users point of view) or as part of the OS (from the computer applications point of view) and may also operate at both levels.



The TOE is used to regulate the flow of network traffic to and from the environment in which it is installed. As the TOE is connected to the Internet, the types of traffic that is regulated are:

- outgoing traffic: data that flows from the computing environment to the Internet
- incoming traffic: data that flows from the Internet to the computing environment.

The TOE intercepts, respectively, incoming and outgoing traffic that attempts to enter and exit the computing environment and applies a set of rules that define under which conditions network traffic is either allowed to proceed or is discarded.

The TOE may warn the user of the home PC when certain violations of the rules governing network traffic to and from the TOE occurs. A warning could relate to:

- A single violation of the rules, for example, an application attempts to make a outbound connection during installation in order to send customer information to a remote site
- A combination of violations of the rules, for example, a hacker runs a port scan on the computer in order to identify possible attack entry points
- The TOE also keeps an event log of violations.

The TOE is not a stand-alone device, and requires a supporting computing platform with at least one network interface.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a TOE claiming compliance to the Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, Version 1.2.

All functional requirements are drawn from Common Criteria Part 2.

SFRs	Component-Name
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MTD.1	Management of TSF data
FMT_MTD.3	Secure TSF data
FMT_SMR.1	Security roles
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_ARP.1	Security alarms

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 EAL1 (Evaluation Assurance Level 1).

4 Strength of Functions

A strength of function claim is no longer part of the CC, Version 2.4, Revision 256.

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 [4] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL1 and the class APE for the Protection Profile evaluation) are summarised in the following table.

CC Aspect	Result
CC Class APE	PASS.
APE_CCL.1	PASS.
APE_ECD.1	PASS.
APE_INT.1	PASS.
APE_OBJ.0	PASS.
APE_REQ.1	PASS.

The Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, Version 1.2 meets the requirements for Protection Profiles as specified in class APE and Draft Interpretation #2 of the CC, Version 2.4, Revision 256.

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

LAPP Low Assurance Protection Profile

PP Protection Profile

SF Security Function

SFP Security Function Policy

ST Security Target

TOE Target of Evaluation

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.

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 2.4, Revision 256

[2] Common Methodology for Information Security Evaluation, Version 2.4, Revision 256 with the CC v2.4 Draft Interpretations #1 - #17

[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] Low Assurance Protection Profile for a Software based Personal Firewall for home Internet use, Version 1.2, 06.04.2005

[7] Evaluation Technical Report (ETR), Version 1.03, 28.04.2005

This page is intentionally left blank.

Annex: Protection Profile