Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0176-2002

for

SafeGuard® Easy for Windows 2000, Version 1.0

from

Utimaco Safeware AG

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

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0176-2002

SafeGuard® Easy for Windows 2000, Version 1.0

from

Utimaco Safeware AG

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

Functions:	**product specific Security Target** **Common Criteria part 2 conformant**
Assurance Package:	**Common Criteria part 3 conformant** **EAL1**

This certificate applies only to the specific version and release of the product in its evaluated configuration 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 and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 22.04.2002

The President of the Bundesamt für
Sicherheit in der Informationstechnik

IT Security Certified

SOGIS-MRA

Dr. Henze L.S.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

This certificate is not an endorsement of the IT product 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 IT product by 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.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by 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 Results contain the technical description of the security functionality of the certified product, 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)
- The DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

[2] Act setting up the Bundesamt 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 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministeriums des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The agreement on the mutual recognition of IT security certificates based on the CC was extended up to and including the evaluation level EAL7.

2.2 CC - Certificates

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 product **SafeGuard® Easy for Windows 2000, Version 1.0** has undergone the certification procedure at BSI.

The evaluation of the product SafeGuard® Easy for Windows 2000, Version 1.0 was conducted by T-Systems ISS GmbH. The T-Systems ISS GmbH is an evaluation facility recognised by BSI (ITSEF)[6].

The sponsor, vendor and distributor is Utimaco Safeware AG.

The certification is concluded with

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

This work was completed by the BSI on 22.04.02.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-14.

The product SafeGuard® Easy for Windows 2000, Version 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Utimaco Safeware AG, Hohenmarkstr. 22, 61440 Oberursel

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

SafeGuard® Easy Version 1.0 (SGE) is a software product to ensure secure access to data on Personal Computers (PCs).

This product is designed for the Microsoft operating system Windows 2000. (Versions of SafeGuard® Easy also are available for other PC operating systems, but are not part of this evaluation).

The security of SafeGuard® Easy prevents unauthorised users from access to all data on the hard disk(s) of a PC operating under the named operating system.

Basically, the security provided by SGE bases upon the encryption of entire hard disk partitions. User authentication is done by PBA (Pre Boot Authentication) prior to booting the operating system. In this way, the access to data is restricted to authorised individuals only.

The IT product **SafeGuard® Easy for Windows 2000, Version 1.0** was evaluated by T-Systems ISS GmbH.The evaluation was completed on 19.03.02. The T-Systems ISS GmbH is an evaluation facility approved by BSI (ITSEF)[8]. The sponsor, vendor and distributor is Utimaco Safeware AG.

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria. The TOE meets the assurance requirements of assurance level EAL1 (Evaluation Assurance Level 1).

1.2 Functionality

TOE security functional requirements taken from Part 2 of the CC [1]

FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based on access control
FDP_ETC.1	Export of user data without security attributes
FDP_IFC.1	Subset information flow control
FDP_ITC.1	Import of user data without security attributes
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FMT_SMR.1	Security roles
FMT.MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes

[8] Information Technology Security Evaluation Facility

FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data

1.3 Strength of Function

The strength of the TOE security functions (SOF) was not claimed since this is not required for the evaluation assurance level EAL1.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

1.4.1 Threats addressd by the TOE

The following threats are to be averted by the TOE:

<T.ACCESS> An unauthorised individual <S.UNAU> attempts to perform substantial access <ACC.SUB> to any plain text data stored on hard disk partitions defined as encrypted by the TOE <D.USER>. This attack is expected to be performed when the PC is not in operational state.

<T.MANAGE> An unauthorised individual <S.UNAU> attempts to perform TOE management operations (changing the protection status of the TOE or modifying other TSF data <D.TSF>). This attack is expected to be performed when the PC is not in operational state.

1.4.2 Threats addressed by the environment

The following threats are to be averted by the environment:

<T.PASSW> An unauthorised individual <S.UNAU> gets the password <D.PASSW> of an authorised individual <S.USER> (any user knowing any valid user name/password combination of the current installation). This includes password recording using hardware devices or software tools. In the case of password disclosure, an unauthorised person becomes an authorised person. As a consequence, there is no longer protection against <T.ACCESS> and <T.MANAGE>.

<T.INTRUD> An intruder <S.UNAU> succeeds in placing non-trusted software on the PC's hard disk designed to attack (disclose or modify) the TOE software or its TSF data <D.TSF>. The attacker's program will be executed unnoticed by the authorised user (Trojan horse or a virus).

With such an attack, the attacker attempts (i) to disclose cryptographic keys or passwords in order to break or circumvent the certain security functions of the TOE, or (ii) to modify software of the TOE to cause the TOE's security functions or measures to fail or to operate against the security policy. In either cases, the attacker attempts to succeed in performing <T.ACCESS> or <T.MANAGE>.

<T.DIRECT> Non-trusted software, which does not use the respective Application Programming Interface of the OS platform for disk access, but directly accesses the hard disk by circumventing layers of the disk access system, is placed on the PC's hard disk or executed while the computer is operated. In this case, the threat <T.ACCESS> is no longer averted.

1.5 Special configuration requirements

There are no special configuration requirements defined
The following settings have to be selected during the installation and first configuration of SafeGuard® Easy

- Installation Type: Interactive,
- Encryption Mode: Standard (full hard disk encryption),
- PBA enabled,
- Minimum password length: 6 characters,
- Encryption Algorithm for hard disk ecnryption: DES or IDEA,
- When defining hard disk or floppy disk encryption keys manually, it has to be observed, that a maximum number of randomly selected characters is input (max. 32 characters). Trivial keys (like ”123456" or ”aaaaaaaa", for example) shall not be used, because they could easily be guessed by an attacker.

1.6 Assumptions about the operating environment

1.6.1 Hardware Requirements

The TOE runs on personal computer systems with the following minimum requirements:

- microprocessor Intel Pentium (or successor type like Pentium II) or compatible device, with 32-bit internal operation, suitable for Windows 2000,
- minimum system RAM of 32 MB,
- hard disk with a minimum of 4 MB free storage,
- CD-ROM drive for installation.

The TOE supports furthermore following hardware devices:

- up to four hard disks:
  hard disks may be accessed via IDE, Advanced IDE or SCSI controller, Because of its security measures, SafeGuard® Easy is especially suitable for the protection of user data on mobile computers.

1.6.2 Software Requirements

SafeGuard® Easy Version 1.0 is provided for the following operating system:

Microsoft Windows 2000 (Professional and Server).
SafeGuard® Easy works with all available file systems under Windows 2000: FAT, FAT32, NTFS4, and NTFS5 (EFS).

SafeGuard® Easy is working together with all application software, which is released for the mentioned operating system platform. However, application software, which is not using the respective Application Programming Interface of the OS platform for disk access, but circumventing some layers of the disk access system, may read encrypted sectors from the disk and therefore may not recognise the file structure on the disk correctly. Such software may also write plain text data directly onto a protected device. Then these data are not protected by the TOE against unauthorised disclosure.
In practice, such software has not been known to the vendor, except for special hard disk repair and copy functions. Using such software for hard disk repair and copy functions, while the TOE is installed, is not advised, as this also may - in extreme consequence - damage the TOE installation.

1.6.3 Connectivity Aspects

SafeGuard® Easy works on any PC which meets hardware and software requirements. The PC can be stand alone or be connected over a data line to any other computer system.
Data connection may include:

- Connection to a LAN (Local Area Network) or a WAN (Wide Area Network) by Ethernet, Arcnet or others
- Remote access connection to another computer system via serial line (serial cable, modem, USB connection).

In these cases it must be observed, that the security from SafeGuard® Easy extends only to the local disk drives, and that there is no encryption of virtual drives in network environments.
Security may be inactive, when the secured PC is operated while connected to another computer system and parts of the PC's hard disk(s) are accessible to other users or programs (via shared partitions/drives/volumes, directories or files) within this connection. In this case, any user having access to those shares has access to the plain text data stored in it.
For these reasons, the threats defined for the TOE restrict denial of access for unauthorised users to the state, where the PC is not in operational state and the unauthorised individual tries to access data by anyhow setting the PC into operation or removing the hard disk from the PC and examining the device separately.
Also attention has to be paid to the fact, that, when the PC - with the TOE installed on it - is operated in connection to any other computer system, it might be possible for unauthorised individuals to manipulate the TOE in a way, that its security functionality can be circumvented or deactivated (e.g. by installing “Trojan Horse”-type programs/scripts). Therefore no partition-/drive-/volume-, directory- or file-shares shall be defined on a PC secured by the TOE.

When the TOE is operated in a network with connection to the Internet, a correctly installed and maintained firewall system shall be established to prevent access to the protected PC's hard disk(s) and memory by unauthorised individuals from outside.
SafeGuard® Easy is not intended to be used on servers in a network (however it will work there).

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Bundesamt für Sicherheit in der Informationstechnik (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The following TOE deliverables are provided of a costomer who purchases the TOE:

SafeGuard® Easy for Windows 2000 English and German version,	Version 1.0	CD-Rom
SafeGuard® Easy Windows 2000 – Mobile/Desktop Security (English Version)	Version 1.0 August 2000	paper
SafeGuard® Easy Windows 2000 – Mobile/Desktop Security (German Version)	Version 1.0 August 2000	paper
SafeGuard® Easy – User`s Manual Supplement (English Version)	Version 1.0 November 2001	paper
SafeGuard® Easy – Handbuchergänzung (German Version)	Version 1.0 November 2001	paper

3 Security Policy

There are no additional organisational security policies defined.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

The following measures have to be taken, as long as SafeGuard® Easy is installed on a PC:

- The configuration selected during installation shall not be modified later.
- Floppy disk encryption, device encryption and Secure Auto Logon are not within the scope of the certified functions of SafeGuard® Easy.
- The logical access to the hard disk(s) after booting from floppy disk or a different boot device is protected., when the recommended system configuration is correctly installed. However, to obtain an additional protection of the system against spying out a SafeGuard® Easy password with the help of a ”Trojan Horse“ program, the PC has to be secured against unauthorised user booting from any other divice than the hard disk has to be secured against by appropriate measures.
- Each user has to keep his selected password(s) secret. It is recommended not to record passwords either manually or electronically. If passwords are written down, the records have to be kept in a secret place.

4.2 Environmental assumptions

- Untrusted software, which could disclose or modify the security functions of SafeGuard® Easy (especially ”Trojan Horses“ or viruses), shall not be placed on the PC. The PC has to be scanned with appropriate tools for those programs or program components.
- When the PC is integrated in a LAN, no partitions/drives/volumes, directories or files shall be shared with other users of this LAN. This is to avoid the intrusion of malicious program code which might disclose or modify the security functions of SafeGuard® Easy.
- When the TOE is operated in a network with connection to the Internet, additionally a correctly installed and maintained firewall system shall be established to prevent intrusion of malicious program code.
- Software which does not use the respective Application Programming Interface of the OS platform for hard disk or floppy disk access shall not be placed on the PC’s hard disk or executed while SafeGuard® Easy is installed. Failure to do so may result in damages to the OS file system causing the PC not to boot any more.
- The PC, where the TOE is installed, and the environment, where the PC is operated by any authorised user has to be secured against devices, which are capable of recording the password entered by an authorised user. Such devices may be keyboard grabbers in the cable between keyboard and PC, which are able to record the keystrokes as well as video cameras capturing the user during password entry.
- Before eventually processing the challenge/response, the user creating the response shall certainly make sure himself of the identity of the requesting

user; the transmitted data (challenge and response code) shall be transferred on a secure channel. Otherwise a password for the current installation may be disclosed.

4.3 Clarification of scope

The TOE is used to protect confidential information on the personal computers from being accessed by unauthorised persons.

The certification of SafeGuard® Easy is simply done under the assumption, that all users of an installed product have the same management rights for administering SafeGuard® Easy. In other words, a functional separation between the **different users or user roles is not part of the certification**.

The installation has to be performed by a user in interactive installation to ensure the correct setting of the configuration parameters. The installation by using configuration files is not within the scope of certified operation.

5 Architectural Information

There are no Development-High Level Design (ADV_HLD) documents by EAL1 postulated.

6 Documentation

The following documents are provided with the product by the developer to the consumer:

1. User's Guide for using and administrating SafeGuard® Easy, called SafeGuard® Easy Windows 2000 – Mobile/Desktop Security – Version 1.0**,** User’s Manual, Utimaco Safeware AG, August 2000" (English Version)
2. Guide for using and administrating SafeGuard® Easy, called SafeGuard® Easy Windows 2000 – Mobile/Desktop Security – Version 1.0, Handbuch, Utimaco Safeware AG, August 2000" (German Version)
3. User's Guide Enhancement for secure operation, called SafeGuard® Easy – User`s Manual Supplement, Utimaco Safeware AG, Version 1.0, November 2001" (English Version)
4. User's Guide Enhancement for secure operation, called SafeGuard® Easy– Handbuch-ergänzungen, Utimaco Safeware AG, Version 1.0, November 2001" (German Version)

7 IT Product Testing

In EAL1 there are no developer tests postulated.

The evaluators‘ independent tests were carried out using personal computer (PC – IBM compatible that fulfils the basic minimum requirements and that has only Microsoft Windows 2000 Professional operating system installed as the platform for SafeGuard® Easy part of the TOE.

The evaluators performed independent tests on allimportant TOE security functions provided by the TOE. All evaluator's independent tests are documented in the Evaluator Test Documentation.
The test strategy applied by the evaluators was, to test the most important TSFs with a substantial level of rigour that is adequate for the Assurance Level EAL1 and at the same time cost-effective.
Finally, the evaluators concluded that the independent tests carried out by them indicated that each aspect of TSF's tested are functioning correctly as one expects and would anticipate based on their descriptions given in ST [6], chapter 7 and Functional Specification respectively.

8 Evaluated Configuration

The following security functions of SafeGuard® Easy are certified:

- Pre-Boot Authentication (PBA): For a secure identification and authentication of authorised users with user name and password.
- Protection of Data on Hard Disk Partitions (using encryption): For denying access to hard disk contents for unauthorised users.
- Installation and Secure Administration: Functions for installing and maintaining SafeGuard® Easy.

Floppy disk encryption, device encryption and Secure Auto Logon are not within the scope of the certified functions of SafeGuard® Easy.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) 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) as relevant for the TOE.

The verdicts for the CC, part 3 assurance classes and components (according to EAL1 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components	EAL1 assurance component	Verdict
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS

Assurance classes and components	EAL1 assurance component	Verdict
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	CC Class ACM	PASS
CM capabilities	ACM_CAP.1	PASS
Delivery and operation	CC Class ADO	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
functional specification	ADV_FSP.1	PASS
Representation correspondence	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Tests	CC Class ATE	PASS
Independent testing	ATE_IND.1	PASS

10 Evaluator Comments/Recommendations

There are no imposed conditions and/or directions to the developer. The evaluators will like to recommend that **configuration file mode of operation be included in the next version of the TOE**, if the developer decides to do so.

The target audience (evaluators, public companies and private users respectively) should strictly abide to the recommendations and directions specified regarding measures for secure operation of the TOE that is available in the Security Target [6] and Manuals respectively.

11 Annexes

none

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
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

13.2 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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (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), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-CC-0176-2002, Version 1.04.00, Security Target, Utimaco Safeware AG

[7] Evaluation Technical Report, Version 1.0, vom 18.02.2002, Evaluation Technical Report of SafeGuard® Easy for Windows 2000 (confidential document)

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (Kapitel 5.4)

The pass result of evaluation shall be a statement that describes the extent to which the PP or TOE can be trusted to conform to the requirements. The results shall be caveated with respect to Part 2 (functional requirements), Part 3 (assurance requirements) or directly to a PP, as listed below.

a) **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are only based upon functional components in Part 2.

b) **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

c) **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are in the form of an **EAL** or **assurance package** that is based only upon assurance components in Part 3.

d) **Part 3 augmented** - A PP or TOE is Part 3 augmented if the assurance requirements are in the form of an **EAL** or **assurance package**, plus other assurance components in Part 3.

e) **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements are in the form of an **EAL** associated with additional assurance requirements not in Part 3 or an **assurance package** that includes (or is entirely made up from) assurance requirements not in Part 3.

f) **Conformant to PP** - A TOE is conformant to a PP only if it is compliant with all parts of the PP.“

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential."