Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0186-2004

for

SafeGuard® Easy, Version 3.20 SR1 for Microsoft Windows® 2000

from

Utimaco Safeware AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0186-2004

SafeGuard® Easy, Version 3.20 SR1

for Microsoft Windows® 2000

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)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

Functions:	**Product specific Security Target** **Common Criteria part 2 conformant**
Assurance Package:	**Common Criteria part 3 conformant** **EAL3**

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 German Federal Office for Information Security (BSI) 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, 24. September 2004

The President of the Federal Office
for Information Security

IT Security Certified

Dr. Helmbrecht L.S. SOGIS-MRA

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 Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security 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 Federal Office for Information Security (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 Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

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 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)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 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 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium 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. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

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, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

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, Version 3.20 SR1[6] for Microsoft Windows® 2000[7] has undergone the certification procedure at BSI.

The evaluation of the product SafeGuard® Easy, Version 3.20 SR1 for Microsoft Windows® 2000 was conducted by T-Systems GEI GmbH. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

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 24. September 2004.

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] Service Release 1

[7] Microsoft Windows® 2000 is called in the following only Windows 2000.

[8] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B -20.

The product SafeGuard® Easy, Version 3.20 SR1 for Windows 2000 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[9] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[9] Utimaco Safeware AG, Hohemarkstraße 22, D-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 3

2 Identification of the TOE 8

3 Security Policy 8

4 Assumptions and Clarification of Scope 9

5 Architectural Information 11

6 Documentation 13

7 IT Product Testing 13

8 Evaluated Configuration 15

9 Results of the Evaluation 16

10 Evaluator Comments/Recommendations 17

11 Annexes 18

12 Security Target 18

13 Definitions 18

14 Bibliography 20

1 Executive Summary

The Target of Evaluation (TOE) is the SafeGuard® Easy, Version 3.20 SR1 for Windows 2000.

SafeGuard Easy (SGE) is a software product to ensure secure access to data on Personal Computers (PCs). It works on a high security level but is easy to install, maintain and use.
This product under evaluation is designed for the Microsoft operating system Windows 2000. (Versions of SGE also are available for other PC operating systems, but are not part of this evaluation).
The security of SGE 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 Target of Evaluation (TOE) consists of

(i) the installable program code including the installation program of SafeGuard® Easy, Version 3.20 SR1 for Windows 2000, English and German program version, delivered on the SafeGuard Easy program CD-ROM, identified as “[SafeGuard® Easy 3.20 SR1]”, where only the following parts of the installed programs implement the security functionality of the TOE:

(a) the system kernel of SGE,
(b) the master boot record of SGE,
(c) the drivers needed for encrypting and decrypting user data,
(d) the installation program and the administration program,

(ii) the User's Guide for using and administrating SGE, called "SafeGuard Easy – Data protection by encryption – Version 3.20 SR1, User’s Manual, Utimaco Safeware AG, 2003” (English Version, pdf file) and
"SafeGuard Easy – Zugangsschutz durch Verschlüsselung – Version 3.20 SR1, Handbuch, Utimaco Safeware AG, 2003" (German Version, pdf file)

(iii) the User's Guide Enhancement for secure operation, called "SafeGuard Easy Version 3.20 SR1 – Manual for certification compliant operation – Utimaco Safeware AG, September 2004" (English Version) and
"SafeGuard Easy Version 3.20 SR1 – Handbuch für den zertifizierungskonformen Betrieb – Utimaco Safeware AG, September 2004" (German Version)

The IT product SafeGuard Easy,Version 3.20 SR1 for Windows 2000 was evaluated by T-Systems GEI GmbH. The evaluation was completed on 15. September 2004. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[10] recognised by BSI.

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 EAL3 (Evaluation Assurance Level 3).

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

Tabelle B1: TOE security functional requirements

1.3 Strength of Function

The TOE's minimum strength of function is rated 'SOF-medium'. The strength of function is only claimed for the security function "Pre Boot Authentication (PBA)" (refer to [6], chapter7.1.1). There is no strength applied to the security function "Protection of Data on Hard Disk Partitions" because the assessment of crytographic strength is out of scope.

[10] Information Technology Security Evaluation Facility

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

The following threats should be averted by the TOE:

<T.ACCESS> An unauthorised individual <S.UNAU> attempts to perform a substantial access <ACC.SUB> to any data stored on encrypted hard disk partitions <D.USER>. This attack is expected to be performed after having the PC switched off. ("Substantial access" means reading, writing or modifying information; "any data" means data files, program files, operating system files and file system information).

<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.

There were no organisational security policies defined.

1.5 Special configuration requirements

<u>System configuration during installation:</u>
The following settings have to be selected during the installation and first configuration of SafeGuard Easy:

- Installation Type: Complete System
- Installation Options: None of the options “Secure Auto Logon” (SAL), “Configuration File Wizard”, “Response Code Wizard” and “Automatic SmartCard Logon” (SCAL) shall be selected.
- Installation Mode: Define system settings interactively
- Encryption Mode: Standard (full hard disk encryption)
- Workstation settings: PBA enabled (“Password at system start”) and hidden password entry set
- Workstation settings: Minimum password length: 8 characters. Caution: This requires an explicit modification of the initial default settings, which in this case is 6 characters.
- Encryption Algorithm for hard disk encryption: AES-128, AES-256, Rijndael-256, DES or IDEA
- Encryption keys: It is strongly recommended to select a random key for hard disk encryption. When despite defining a hard disk encryption key manually, it has to be observed, that the 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 (please see also [10] and [11]).

  Caution: Once you have selected random key, do not edit the Key or Repeat Key Field any more.

- Selection of passwords: To prevent passwords from being guessed or systematically tested (dictionary attack) do not choose passwords from your private environment (e.g. names of family members or other relatives). Also do not choose trivial passwords like ASCII or keyboard sequences (e.g. “abcdefgh”, 12345678..” or “asdfghjk...”). SafeGuard Easy tests passwords for triviality and issues an appropriate warning. (please see also “Error Corrections of User’s Manual” at the end of this brochure). Inserting one ore more of the allowed special characters like “$%&?=...” increases resistance against dictionary attacks significantly.
- Master Boot Record: From MBR Protection select “Standard Action”, “Display Warning” and “Restore MBR”. The selection “MBR Options” with its subcategory “Keep original MBR” is with Windows 2000 available only on Compaq PCs having a bootable setup partition. Please select this option only when needed to correctly operate your PC.

Settings for additional users:
When defining new users for an installation of SafeGuard Easy, it shall be in mind, that in the scope of certification all users are on the same level as the user “System”. So the following settings for a new user are required:

- Simplified Remote logon: off
- Template: none
- Expiration date: no expiration
- Change password at next logon: no
- Password change: no period to change password
- Rights: all available rights set

Note: During installation SafeGuard Easy creates a user named “User”, who initially does have neither a password nor any rights set. Since user names cannot be changed, you shall delete this user and create new ones with meaningful names following the above rules.

1.6 Assumptions about the operating environment

Hardware Requirements

The TOE runs on personal computer systems with 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, SGE is especially suitable for the protection of user data on mobile computers.

Software Requirements

Operating System:

The version of SGE under this evaluation is provided for the following operating system:

> Microsoft Windows 2000
> (Professional and Server, International versions for support of Western character sets)

SGE works with all available file systems under Windows 2000: FAT, FAT32, NTFS4, and NTFS5 (EFS).

Application Software Requirements:

The TOE 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.

Connectivity Aspects:

SGE works on any PC which meets hardware and software requirements, not regarding, if the PC is stand alone or if it is 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 SGE 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.

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 Federal Office for Information Security (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

SafeGuard® Easy, Version 3.20 SR1 for Windows 2000, English and German programm version	Version 3.20 SR1	CD-ROM
"SafeGuard® Easy Version 3.20 SR1 – Data protection by encryption – Windows® 95, Windows® 98 SE, Windows® NT 4.0, Windows® 2000, Windows® XP – User's Manual, Utimaco Safeware AG, 2003" (English Version)	Version 3.20 SR1 2003	.pdf-file
"SafeGuard® Easy Version 3.20 SR1 – Zugangsschutz durch Verschlüsselung – Windows® 95, Windows® 98 SE, Windows® NT 4.0, Windows® 2000, Windows® XP – Handbuch, Utimaco Safeware AG, 2003" (German Version)	Version 3.20 SR1 2003	.pdf-file
"SafeGuard® Easy Version 3.20 SR1 – Manual for certification compliant operation – Utimaco Safeware AG, September 2004" (English Version)	Version 3.20 SR1 September 2004	paper
"SafeGuard Easy Version 3.20 SR1 – Handbuch für den zertifizierungskonformen Betrieb – Utimaco Safeware AG, September 2004" (German Version)	Version 3.20 SR1 September 2004	paper

3 Security Policy

SafeGuard Easy is a software product installed on a PC to prevent unauthorised access to user data stored on hard disk partitions. In this context, user data means all files on hard disk partitions, i.e. data files, program files and even files of the operating system. The protection of the user data stored on hard disk partitions is realised by encryption. Encryption guarantees the confidentiality of data and is done on sector level - not on file level. This provides the advantage of being independent from the behaviour of application programs and processing files difficult to handle, like temporary file areas or paging files of the operating system.

User identification and authentication is done by PBA (Pre Boot Authentication) prior to booting the operating system. Only after a successful authentication, the user has access to the data on the hard disk partition. In this way, the access to data is restricted to the authorised individuals only. On a running system, after authentication, the encryption is completely transparent to the user, so that he is normally not aware of the security mechanisms behind. After shutting down the operating system and switching off the PC, the entire hard disk partitions are encrypted and therefore secured. Booting the PC from any device circumventing PBA results in a view to encrypted hard disk partitions.

Authentication bases upon user names and secret passwords. The cryptographic key necessary to encrypt the user data stored on the hard disk is encrypted with the password of each user and is secured in this way.

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. Especially the encryption of the hard disk partitions shall not be switched off.
- 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 booting from any other device than the hard disk by appropriate measures. This provides protection against "Trojan Horse" attacks within the normal environment of an authorized user. In case of a stolen PC the "Trojan Horse" attack is not relevant, because the intermediate "help" of an authorized user is not available.

- Each user has to keep his selected password(s) secret. It is recommended not to record passwords either manually or electronically. If despite of this passwords are written down, the records have to be kept in a secret place.
- A Challenge Code (cf. Manual, par. 6.4) shall not be generated nor sent to anyone else. If an attacker gets hold of both the Challenge- and the corresponding Response Code, the password for the current installation may be disclosed. If nevertheless this function is used, it must be ensured, that challenge and response is transmitted via secure channels and a secure identification of the requesting user takes place.
- If the safety feature “Kernel Backup” is used, the created backups have to be stored on removable media and kept in a secure place.
- Within an authorized user’s normal environment it might be possible, to replace the user’s original PC by an externally identical but specially prepared one. This can only be detected by checking the identity of the PC prior to identification to PBA.
- When leaving the workstation for a short time the Windows screen blanking should be enabled (button [Lock workstation]); leaving the workstation for a longer period of time, the PC should be switched off and then rebooted.

4.2 Environmental assumptions

- The PC, where SafeGuard Easy is installed, and the environment, where the PC is operated by any authorized user has to be secured against devices, which are capable of recording the password entered by an authorized 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.

4.3 Clarification of scope

The threats listed below have to be averted in order to support the TOE security capabilities but are not addressed by the TOE itself. They have to be addressed by the operating environment of the TOE (for detailed information about the threats refer to the Security Target [6]).

The following threats should 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 by the authorised user (Trojan horse), unnoticed (virus), or accidentally (both). 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.

Furthermore SGE is not intended to be used on servers in a network (however it will work there).

SGE can not guarantee complete integrity of data, as e.g. sectors of the hard disk are not physically write protected. So, for example, the hard disk may be formatted, if it is possible to boot the system from a different booting device than the built-in hard disk. Usually, physical sector modifications on an encrypted hard disk will be detected, because (after decryption) they will at least generate unuseful random nonsense data.

Floppy disk encryption and device encryption of removable devices are not included within the scope of the certified security functions.

5 Architectural Information

The SGE 3.20 SR1 hard disk protection is a software (SW) consisting of the following main components:

Real mode kernel working on BIOS level, together with a modified Master Boot Record, Windows 32-bit filter driver, and administration and installation programs; here this mainly refers to the SafeGuard Easy 32-bit administration application.

Additionally a real mode program can be generated to be started from an extern bootable medium (e.g. floppy disk) called Emergency Administration Program.
A top level description and a list of subsystems can be found within the TOE description of the “Security Target”, [6]. The complete software description and the complete instruction set of the SGE 3.20 SR1 hard disk protection can be found in the Guidance Documents [8], [9], [10] and [11].

For the implementation of the TOE Security Functions basically the components mentioned above are realized within the software.

TSF enforcing	non TSF enforcing
Subsystems of main component [C1], Real mode kernel working on BIOS level, together with a modified Master Boot Record:	
[S1.2] PBA Module	[S1.1] Modified Master Boot Record
[S1.3] PBA Support Module	
[S1.4] Real Mode Kernel Data Handler	
[S1.5] Real Mode Encryption Driver & Plugins	
Subsystems of main component [C2], Windows 32-bit filter driver:	
[S2.1] Windows 32-bit Filter Driver Frame	
[S2.2] Windows 32-bit Crypto Modules	
Subsystems of main component [C3], Administration and installation programs:	
[S3.1] Main Installation Program	[S3.4] Device and Floppy Encryption Switching Program
[S3.2] Deinstallation Program	[S3.5] Emergency Disk Wizard
[S3.3] Windows 32-bit Administration Program	[S3.7] Response Generator
[S3.6] Windows 16-bit Emergency Administration Program	[S3.8] Configuration File Wizard

Table B5: Subsystems defined by the High-Level Design catogorized into TSP enforcing and other

6 Documentation

The following documents are provided for a customer, who purchases the TOE:

SafeGuard® Easy Version 3.20 Service Release 1 – Data Protection by Encryption — Windows® 95, Windows® 98 SE, Windows® NT 4.0, Windows® 2000, Windows® XP – User's Manual, Utimaco Safeware AG, 2003 (English Version, pdf file) [8]
SafeGuard® Easy Version 3.20 Service Release 1 – Zugangsschutz durch Verschlüsselung — Windows® 95, Windows® 98 SE, Windows® NT 4.0, Windows® 2000, Windows® XP – Handbuch, Utimaco Safeware AG, 2003 (German Version, pdf file) [9]
SafeGuard Easy Version 3.20 SR1, – Manual for certification compliant operation – Utimaco Safeware AG, September 2004 (English Version) [10]
SafeGuard Easy Version 3.20 SR1 – Handbuch für den zertifizierungskonformen Betrieb – Utimaco Safeware AG, September 2004 (German Version) [11]

Table B6: Documentation delivered with the TOE

7 IT Product Testing

The test effort provided by the developer is described in the documents 'Functional Test for Certified Operation' [12] and 'Test Documentation' [13]. The latter comprises the test plan and sufficiency rationales that has to be provided for the assurance requirements given by the class ATE and has to be seen as an overview document. The test preparation, procedures, expected and actual results are included by 'Functional Test for Certified Operation' [12].

The developer additionally provided a 'Testspecification' [14] that comprises the whole functional testing effort for the product SGE 3.20 SR1. Most of these tests are not applicable to the TOE that has to be installed and operated with strict value settings to meet the CC conformant configuration.

The developer tested the TOE on two different hardware environments (PC with IDE hard disk (>8 MB) with a NTFS partition and a PC with a IDE hard disk (>16 MB) with two FAT32 partitions). Both environments were operated with Windows 2000. The configuration was set with valid parameters with respect to the 'Security Target' [6] and the guidance [8], [9], [10] and [11]. The TOE conformant parameters are especially specified in the supplementary guidance [10] and [11].

All of the performed tests are manually executed, guided by the test description specified in 'Functional Test for Certified Operation' [12]. These tests directly influence the user interfaces. The developer divided the test cases into the functional units of the TOE as specified within the FSP. For this, the test cases are divided into concise parts, so that the security functions with their behaviour could be sufficiently tested and assessed.

To test the encryption and decryption behaviour of the TOE (hard disk interface) the developer analysed the hard disk with appropriate tools. Single sectors of the physical hard disk device are read out (Disk edit) in encrypted an decrypted mode. These data were analysed with a reference implementation (Crypto Test) of the cryptographic algorithms for equality.

In case that the observed actual test results meet the expected test results the tester has confirmed this within the document ‘Functional Test for Certified Operation’ [12]. Therefore every test case comprises a table for the result confirmation. For each test the tester had to be named, and the results had to be signed manually. The developer provided a copy of a completely filled out document version for the evaluation process.

As required by the CEM [2], work unit [3:ATE_IND.2-11], the evaluator shall report in the ETR the evaluator testing effort, outlining the testing approach, configuration, depth and results.

The evaluators have carried out a subset of test cases to examine the correct implementation of the security functions. The test subset chosen by the evaluators comprises two parts. The first part is given by a sample of developer tests as specified in ‘Functional Test for Certified Operation’ [12] being repeated.

The evaluators repeated the following tests:

1.1 Installation and Initial Hard Disk Encryption

1.2 Deinstallation and Final Hard Disk Decryption

1.3 Encryption Algorithms

1.8 Real Mode Encryption /Transistion to Protected Mode

2.1 PBA Installation

2.2 (a, b, c, d, e) PBA Authentication (correct password, invalid user name check, invalid password check, delay time after reboot, reset delay after correct username and password entry)

2.3 (a, b, c) Password Change during PBA (Successful password change after authentication, behaviour on incorrect authentication, check security attributes against insecure values)

3.1 Administration Program Login

3.2 Password Change with Administration Program

3.4 (a) Changing Default Settings within the TOE valid ranges (Increase password length)

3.5 (a, b, c) Emergency Administration (correct password, incorrect password entry check, system de-installation)

The other test part comprises independent evaluator tests. These can be devided into functional tests and penetration tests.

The evaluator has carried out 19 individual test cases, comprising five penetration tests. Some independent tests have been adopted by the developer during the evaluation process (e.g. Test 5, 6, 7 ,8, 11 and 14).

For both parts of test activity the evaluators have repeated at least one developer test for each TSF.

Overall the evaluators would like to point out that the developer provided sufficient tests for each TSF. These tests have been verified and extended by the evaluators as appropriate. Because of the positive testing results the evaluators are convinced that the TOE correctly implements the TSF.

8 Evaluated Configuration

The TOE is a software product to ensure secure access to and protection of data on Personal Computers (PCs). After installation the TOE provides a transparent encryption (write process) and decryption (read process) of the hard disk data for authorised users. Users are authorised by password authentication processes.

The TOE is defined uniquely by the name SafeGuard Easy 3.20 SR1 for Windows 2000 (short: SGE 3.20 SR1). Its implementation representation and its (unique) configuration are specified by the Configuration List the in appendices of the document “SafeGuard Easy Version 3.20 SR1 – Configuration Management Documentation, Utimaco Safeware AG, Version 1.02, 12.08.2003“.

The “Single Evaluation Report: Safe Guard Easy – Configuration Management” states that the product is uniquely referenced by a version number (3.20 SR1 for the TOE). The configuration list is given by “SafeGuard Easy Version 3.20 SR1 – Configuration List, Utimaco Safeware AG, Configuration List Version 1, 11.07.2003” and “SafeGuard Easy Version 3.20SR1 – Configuration List for Evaluation Documentation, Utimaco Safeware AG, Configuration List Version 11, 07.09.2004”. The Version “3.20 SR1” is stored and printed on a CD-R.

SafeGuard® Easy 3.20 SR1,

Application for Windows 95 / 98 / Me /NT 4.0 / 2000 / XP

English German French

Copyright © 2003

Utimaco Safeware AG

Note: The evaluation started with the TOE version “SGE 3.0” and was changed during the evaluation process to the version “SGE 3.20 SR1”. Between the two versions of the TOE no security functionality has changed. A detailed analysis is given by “Differences SGE 3.20 SR1 vs 3.00”.

The SafeGuard Easy program CD-ROM containing the installable program code and the installation program was used to perform the TOE evaluator tests in the evaluator's laboratory and at the developer's site.
The TOE used to perform the tests was provided by Utimaco in Oberursel. The TOE is labelled as stated above.

9 Results of the Evaluation

The verdicts of each Single Evaluation Report is given in the following table:

Single Evaluation Report	Verdict
Security Target	**PASS**
Functional Specification, incl. Correspondence Demonstration	**PASS**
High-level Design, incl. Correspondence Demonstration	**PASS**
Configuration Management	**PASS**
Delivery and Operation	**PASS**
Life Cycle support	**PASS**
Guidance Documentation	**PASS**
Test	**PASS**
Vulnerability Assessment	**PASS**

Table B9: Results of the Single Evaluation Reports

In accordance to the CEM [2] (together with the Final Interpretations according to [4]) the evaluators report here the conclusions of the evaluation, which will relate to whether the TOE has satisfied its associated ST, in particular the overall verdict as defined in CC Part 1 Chapter 5, and determined by application of the verdict assignment described in Section 1.4 of the CEM.
The TOE was evaluated in accordance to the Evaluation Assurance Level **EAL3** provided by part 3 of the CC [1]. There where no augmentations:
Therefore the evaluation is considered to be **Part 3 Conformant**.
The Security Target [6] claims, that the TOE (SafeGuard Easy 3.20 SR1 for Windows 2000) will fulfil the TOE security functional requirements (**Part 2 Conformant**) given in chapter B 1.2 of this document that are taken from CC Part 2.

These security functional requirements are claimed to be realised by the TSF

<SF1> Pre Boot Authentication (PBA)
<SF2> Protection of Data on Hard Disk Partitions
<SF3> Installation and Secure Administration

(for further details see [6]). The evaluation in accordance to EAL3 has shown that the TOE security functional requirements are correctly realised by the three TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE meets the security objectives claimed in the "Security Target" [6] effectively.
The evaluators determines that the Security Target does not claim conformance to a Protection Profile.
The evaluators have checked that the statements of all Single Evaluation Reports listed in above are valid and assessed with a PASS assessment.
The classification of subsystems of the TOE as indicated in chapter B5 is valid.
On the basis of the evaluation results of the Single Evaluation Reports the evaluators come to following verdict:

1. The requirements of the evaluation level **EAL3** are **fulfilled**.
2. The minimum strength of functions is: **medium**

The evaluation has shown that the TOE will effectively fulfil this strength of function claim.

Note that there is no strength applied to the in <SF2> realised encryption / decryption mechanisms (DES, IDEA, AES-128, AES-256, Rijndael-256) because the assessment of cryptographic strength is out of scope.

10 Comments/Recommendations

Imposed conditions and directions to the developer

There are no imposed conditions or directions to the developer.

Recommendations and directions to the user

The guidance documentation [8], [9], [10] and [11] contains all necessary information about the usage of the TOE.
Besides the requirements

- to follow the instructions in the user guidance documents, especially in the supplementary documentation ([10] and [11]) and
- to ensure fulfilment of the assumptions about the environment in the Security Target (see [6]),

the evaluators have the following recommendation to the user of the TOE:

As the usage of the challenge response mechanism showed a vulnerability facilitating access to a valid system password, the evaluators recommend the user to block the response interface by setting up SYSTEM as the only user. With this a user is not able to generate a challenge at all and the chance of misuse is completely eliminated. It has to be stressed that [10] and [11] contain sufficient information to guide the user or the administrator not to use the challenge response mechanism.

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. This document represents the complete Security Target used for evaluation.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
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
SGE	SafeGuard Easy
PBA	Pre Boot Authentication

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC 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.

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.

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-0186, Version 1.06.00, 2004-04-30, Utimaco Safeware AG

[7] Evaluation Technical Report, Version 1.0, 08.09.2004 (confidential document)

User Guidance Documentation:

[8] SafeGuard Easy – Data protection by encryption – Version 3.20SR1, User’s Manual, Utimaco Safeware AG, 2003

[9] SafeGuard Easy – Zugangsschutz durch Verschlüsselung – Version 3.20SR1, Handbuch, Utimaco Safeware AG, 2003

[10] SafeGuard Easy Version 3.20SR1 – Manual for certification compliant operation – Utimaco Safeware AG, September 2004

[11] SafeGuard Easy Version 3.20SR1 – Handbuch für den zertifizierungskonformen Betrieb – Utimaco Safeware AG, September 2004

Testdocumentation:

[12] SafeGuard Easy Evaluation Documentation for SafeGuard Easy Version 3.20SR1; Test Specification: Functional Test for Certified Operation, Roland Reinl, Version 1.03, 07.04.2004 (confidential document)

[13] SafeGuard Easy Evaluation Documentation for SafeGuard Easy Version 3.20SR1; Test Documentation, Roland Reinl, Version 1.03, 31.03.2004 (confidential document)

[14] SafeGuard Easy Evaluation Documentation for SafeGuard Easy Version 3.20SR1; Testspecification, Erwin Kümmel, Version 1.03, 25.03.2004 (confidential document)

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

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

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

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

Package name **Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

Package name **Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

PP **Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

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.“

This page is intentionally left blank.