debis

Services by DaimlerChrysler

Certification Report

SafeGuard® Easy Product Family
for DOS and Windows

Utimaco Safeware AG

debisZERT-DBZ-CC-01009-1999

debis IT Security Services

The Modern Service Provider

Preface

The SafeGuard® Easy Product Family for DOS and Windows[1] of Utimaco Safeware AG has been evaluated against the *Common Criteria for Information Technology Security Evaluation*. The evaluation has been performed under the terms of the certification scheme debisZERT of debis IT Security Services. The certification procedure applied conforms to the rules of service type 1: *Certificates in accordance with ITSEC / CC*.

The product family contains the following platform dependent versions of *SafeGuard Easy*:

SafeGuard Easy for DOS / Windows 3.x
Version 2.24, Utimaco, English and German language versions

SafeGuard Easy for Windows 95,
Version 1.13, Utimaco, English and German language versions,
Version 1.13, IBM, German language version

SafeGuard Easy for Windows 98,
Version 1.01, Utimaco, English and German language versions,

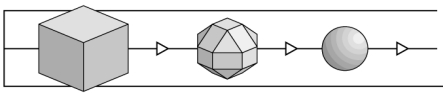
SafeGuard Easy for Windows NT,
Version 1.02, Utimaco, English and German language versions,
Version 1.02, IBM, German language version

The result is:

TOE Security Functions[2]:	Pre-Boot Authentication, Protection of Data on Hard Disk Partitions and Floppy Disks (by Encryption), Screen Blanking and Keyboard / Mouse Lock, Installation and Secure Administration
Evaluation Assurance Level:	EAL3
Minimum Strength of Function:	SOF-Medium

1 Information about the validity of the Registered Trademark can be obtained from the sponsor. In the following certification report the trademark sign is omitted.

2 The evaluated functionality and related options depend on the platform used; see chapter 3 “Security Target”.



For further information and copies of this report, please contact the certification body:

✉ debis IT Security Services	✆	+49-228-9841-110
- Certification Body -	Fax:	+49-228-9841-60
Rabinstr. 8	Email:	debiszert@itsec-debis.de
D-53111 Bonn, Germany	WWW:	www.itsec-debis.de

This is to certify that the evaluation has been performed compliant to the scheme debisZERT.

Bonn, 15.03.1999

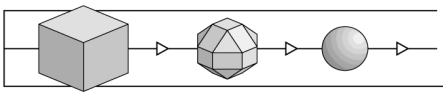
Certifier:	Head of the Certification Body:
Klaus-Werner Schröder	Dr. Heinrich Kersten

Revision List

The following revision list shows the history of this certification report.

Information on re-certifications due to product modifications are given in chapter 6.

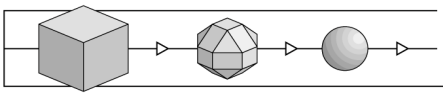
Revision	Date	Activity
0.9	24.08.98	Preversion (based on template report 1.3)
1.0	02.10.98	Initial release (based on template report 1.3)
1.1	15.03.99	Update: Win98 product version included (based on template report 1.4)



(This page is intentionally left blank.)

Contents

1 Introduction 9
1.1 Evaluation 9
1.2 Certification 9
1.3 Certification Report 10
1.4 Certificate 10
1.5 Application of Results 10
2 Evaluation Findings 13
2.1 Introduction 13
2.2 Evaluation Result 13
2.3 Further Remarks 14
3 Security Target 15
3.1 ST Introduction 15
3.1.1 ST Identification 15
3.1.2 ST Overview 15
3.1.3 CC Conformance 16
3.2 TOE Description 16
3.3 Security Environment 17
3.3.1 Assumptions 17
3.3.2 Threats 21
3.3.3 Organisational Security Policies 23
3.4 Security Objectives 24
3.4.1 TOE Security Objectives 25
3.4.2 Security Objectives for Environment 27
3.5 IT Security Requirements 28
3.5.1 TOE Security Requirements 28
3.5.2 Security Requirements for the IT Environment 38
3.6 TOE Summary Specification 40
3.6.1 TOE Security Functions 40
3.6.2 Assurance Measures 43
3.7 PP Claims 43
3.8 Rationale 43
3.8.1 Security Objectives Rationale 44
3.8.2 Security Requirements Rationale 45
3.8.3 TOE Summary Specification Rationale 48
3.8.4 PP Claims Rationale 50
3.9 Annexes 51
3.9.1 Annex A: Functional Components for <RF1> 51
3.9.2 Annex B: Functional Components for <RF2> 53
3.9.3 Annex C: Functional Components for <RF3> 54
3.9.4 Annex D: Functional Components for <RF4> 57
3.9.5 Annex E: Functional Components for <RF5> 60
4 Remarks and Recommendations concerning the Certified Object 63
5 Annex 65
5.1 Glossary 65



5.2 References 69
5.3 Abbreviations 70
6 Re-Certification 73

1 Introduction

1.1 Evaluation

1 The evaluation was sponsored by Utimaco Safeware AG, Dornbachstr. 30, D-61440 Oberursel, Germany.

2 The evaluation was carried out by the evaluation facility Prüflabor IT-Sicherheit of debis IT Security Services. The evaluation for all poduct versions except for the Win98 version was completed on 28.09.1998. The evaluation of the Win98 product version was completed on 12.03.1999.

3 The evaluation has been performed against the *Common Criteria for Information Technology Security Evaluation* /CC/. An overview on the basic structure of the CC and its terminology can be found in /CC/ Part 1: Introduction and General Model.

4 Currently, there is no officially approved evaluation manual for the Common Criteria; as far as reasonable, available draft manuals and the evaluation methodology in /ITSEM/ have been used.

1.2 Certification

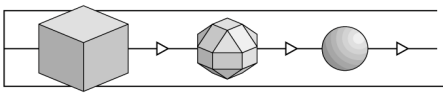
5 In currently discussed drafts for an evaluation manual the terms „overseer“ and „evaluation summary report“ (ESR) are used. Due to standard debisZERT terminology, an „overseer“ means a „certifier“ and „evaluation summary report“ is identical to „certification report“; furthermore, the process of overseeing the evaluation, producing, accepting and publishing the ESR, is called „certification“.

6 The certification was performed under the terms of the certification scheme debisZERT of debis IT Security Services. The Certification Body of debis IT Security Services complies to EN 45011 and was accredited with respect to this standard by the Deutsche Akkreditierungsstelle für Informations- und Telekommmunikationstechnik (DEKITZ) under DAR Registration Number DIT-ZE-005/98-00.

7 The Certification Body applied the certification procedure as specified in the following documents:

/Z01/ Certification Scheme

/V01/ Certificates in accordance with ITSEC/CC



1.3 Certification Report

8 The certification report states the outcome of the evaluation of SafeGuard® Easy Product Family for DOS and Windows - referenced as TOE = Target of Evaluation in this report.

9 The certification report is only valid for the specified version(s) of the TOE. It can be extended to new or different versions as soon as a successful re-evaluation has been performed.

10 The consecutively numbered paragraphs in this certification report are formal statements from the Certification Body. Unnumbered paragraphs contain statements of the sponsor (security target) or supplementary material.

11 The certification report is intended

- as a formal confirmation for the sponsor concerning the performed evaluation,
- to assist the user of SafeGuard® Easy Product Family for DOS and Windows when establishing an adequate security level.

12 The certification report contains pages 1 to 72. Copies of the certification report can be obtained from the sponsor or the Certification Body.

13 The certification report can be supplemented by statements of successful re-certification and by annexes on special technical problems. Such statements and annexes will also be published in

/Z02/ Certified IT Products, Systems and Services.

1.4 Certificate

14 A survey on the outcome of the evaluation is given by the security certificate debisZERT-DBZ-CC-01009-1999 dated 15.03.1999[3].

15 The contents of the certificate are published in the document

/Z02/ Certified IT Products, Systems and Services

and on the WWW.

1.5 Application of Results

16 The processes of evaluation and certification are performed with state-of-the-art expertise, but cannot give an absolute guarantee that the certified object is free

---

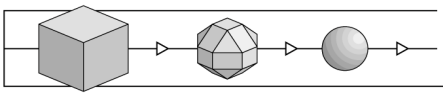
3 The certificate corresponding to version 1.0 of this certification report was dated 2.10.1998.

of vulnerabilities. With increasing evaluation level however, the probability of undiscovered exploitable vulnerabilities decreases.

17 It is highly recommended to read the certification report carefully to benefit from the evaluation. In particular, the information provided on the TOE security environment and the security objectives for the TOE are essential for the user.

18 The results of the evaluation are only valid under the assumption that all requirements specified in the certification report are met by the user.

Otherwise, the results of the evaluation are not fully applicable. In this case, there is a need of an additional analysis whether and to which degree the certified object can still offer security under the modified assumptions. The evaluation facility and the Certification Body can give support to perform this analysis.



(This page is intentionally left blank.)

2 Evaluation Findings

2.1 Introduction

19 The outcome of the evaluation is represented by the ETR (Evaluation Technical Report). The evaluation was performed against the security target specified in chapter 3.

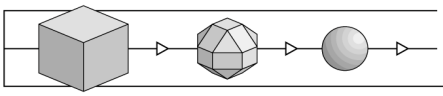
2.2 Evaluation Result

20 The evaluation facility came to the following conclusion:

- The security target meets the requirements of the corresponding class ASE (Security Target Evaluation) of the Common Criteria.
- The TOE meets all requirements of the assurance level EAL3 according to the Common Criteria. This level contains the following assurance components[4]:

Assurance class	Assurance components
Configuration management	**ACM_CAP.3 Authorisation controls** **ACM_SCP.1 TOE CM coverage**
Delivery and operation	ADO_DEL.1 Delivery procedures ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.1 Informal functional specification **ADV_HLD.2 Security enforcing high-level design** ADV_RCR.1 Informal correspondence demonstration
Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Life cycle support	**ALC_DVS.1 Identification of security measures**
Tests	**ATE_COV.2 Analysis of coverage** **ATE_DPT.1 Testing: high-level design** ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample

4 The entries marked in bold type indicate changes to the next lower EAL-level.



Assurance class	Assurance components	
Vulnerability assessment	**AVA_MSU.1**	**Examination of guidance**
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

- The Security Functions of the TOE have the following minimum Strength of Function (SOF) rating (where applicable): **SOF-Medium**

2.3 Further Remarks

21 The evaluation facility has formulated no further requirements to the sponsor.

22 The evaluation facility has formulated the following recommendation to the user: The user is advised to exactly follow the guidance given in the (product related) manuals.

3 Security Target

23 The Security Target (Version 2.4, 24.2.99) supplied by the sponsor for the evaluation is written in english language.

3.1 ST Introduction

The chapter *ST Introduction* is organised as follows: *ST Identification, ST Overview, CC Conformance*.

3.1.1 ST Identification

This Security Target is the basis for the evaluation of *SafeGuard Easy* products belonging to the *SafeGuard Easy* product family for DOS and Windows.

This product family consists of four products for different operating system platforms with almost the same functionality:

<P1> *SafeGuard Easy* for DOS / Windows 3.x, Version 2.24,

<P2> *SafeGuard Easy* for Windows 95, Version 1.13,

<P3> *SafeGuard Easy* for Windows 98, Version 1.01,

<P4> *SafeGuard Easy* for Windows NT, Version 1.02,

In all four cases, an English and German language versions are included into the evaluation.

For <P2> and <P4>, an IBM version in German language is included into the evaluation.

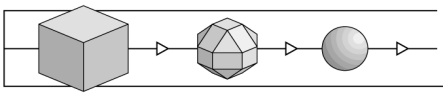
Though all products provide almost the same security functionality each product is evaluated separately (Target of Evaluation, TOE). The User's Guide (using and administrating SGE) for each version is part of the TOE as printed document.

The TOE is called "SGE" in the following. Differences between the four versions are indicated using the abbreviations <P1>, <P2>, <P3> and <P4>.

SafeGuard Easy for DOS / Windows version 2.02 (German and English) has already been certified according to ITSEC by the BSI under the certification ID: BSI-ITSEC-0012-1995.

3.1.2 ST Overview

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. The product family under evaluation is designed for PCs equipped with different Microsoft operating systems:



<P1> *SafeGuard Easy* for DOS / Windows 3.x, Version 2.24,

<P2> *SafeGuard Easy* for Windows 95, Version 1.13,

<P3> *SafeGuard Easy* for Windows 98, Version 1.01,

<P4> *SafeGuard Easy* for Windows NT, Version 1.02.

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.

SGE also offers the ability to encrypt floppy disks. It includes a function for screen and keyboard locking as a secure pause function in the products <P1>, <P2> and <P3>.

3.1.3 CC Conformance

The TOE claims to be *Part 2 conformant* and *Part 3 conformant*.

This means the *TOE security assurance requirements* correspond to an assurance level defined in Part 3 of the Common Criteria, and the functional requirements base upon those described in Part 2 of the Common Criteria.

The individual assurance components for measuring the achieved assurance are those defined by *EAL3 (Evaluation Assurance Level 3)* in Part 3 of the Common Criteria. The functional requirements are described in section 0.

3.2 TOE Description

SafeGuard Easy (SGE) is designed to protect user data on Personal Computers (PCs) operated in a standard office environment. *SafeGuard Easy* is a software product installed on a PC to prevent unauthorised access to user data stored in hard disk partitions. As an option, data stored on floppy disks may also be protected. SGE (for DOS and Windows 95 / 98) also offers a function to protect data on external devices (like ZIP drives, BERNOULLI drives etc.), but this function is not part of the evaluation. Only authorised individuals may start / boot the operating system from an encrypted device (especially from the hard disk). 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 the authorised individual only. The protection of the user data stored on hard disk partitions or on floppy disks is realised by encryption. As a result, the protection is effective even if the PC is not running. To extend this protection to user data displayed on the screen when the authorised user is temporarily absent, the screen is darkened either by the user or after an specific elapse of time. When the screen is darkened, mouse and keyboard input is locked too. To recover the screen content and to start programs, the user must re-authenticate himself. Authentication bases upon secret passwords. These passwords are also used to encrypt the cryptographic key necessary to encrypt the user data stored on the hard disk or on floppy disks.

SafeGuard Easy is installed from floppy disk. The installation program together with the administration program installs the system kernel of SGE on the hard disk, adds some drivers to the operating system, changes the master boot record, and one-time encrypts the hard disk. After having installed SGE, the PC is protected. The Target of Evaluation (TOE) consists of (i) the system kernel of SGE, (ii) the master boot record of SGE, (iii) the drivers needed for encrypting user data, (iv) the screen saver program to support screen blanking and keyboard / mouse locking including re-authentication and recovery, (v) the installation and administration program, (vi) the Response Generation Program for the Challenge Response Logon, and (vii) the User's Guide for using and administrating SGE.

Usually, user authentication is performed using passwords. SGE distinguishes between the „administrator" and the „user" primarily by checking passwords. In the standard user administration there is only one user and one administrator. In the extended user administration (not available for *SafeGuard Easy* for Windows NT) there might be different users and one administrator. User authentication is required prior to booting the operating system (PBA) and when starting the administration program. Although SGE allows the administrator to define rights of other users to perform administrative operations. The intended method of using the TOE in this evaluation is to put users on an equal footing with the administrator: So, it is assumed that the authorised user is allowed to perform all administration activities. Alternatively to the authentication using passwords, SGE offers the possibility for the Challenge Response Logon.

3.3 Security Environment

The chapter *Security Environment* is organised as follows: *Assumptions, Threats, Organisational Security Policies*.

3.3.1 Assumptions

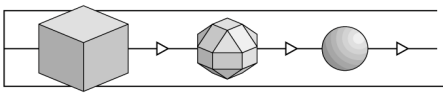
In this section several assumption (or requirements to use SGE) are described. The following subsections contain rather general information for users *Hardware Requirements, Software Requirements, Internetworking Considerations* whereas the subsection *Special Measures* includes physical, organisational and connectivity aspects which are relevant to guaranteeing the TOE's security.

Hardware Requirements

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

- microprocessor type 80386 (or higher), 32-bit internal operation,
- RAM as required by the appropriate operating system platform,
- hard disk with a minimum of 2 MB free storage.

The TOE supports furthermore following hardware devices:



- up to four hard disks
  hard disks may be accessed via IDE, Advanced IDE or SCSI controller,

- up to two floppy disk drives.

SGE provides special mechanisms for working with the suspend operation on different laptop or notebook computers. However, a correct functionality together with the suspend operation cannot be guaranteed for every transportable computer model.

Software Requirements

SGE is provided for the different platforms of Microsoft operating systems:

<P1> *SafeGuard Easy* for DOS / Windows 3.x

This product requires

- MS-DOS Version 3.3 or higher or

- compatible DOS operating system

This product supports Windows 3.1 and Windows for Workgroups 3.11. The hard disk encryption also works under 32-bit disk access of Windows for Workgroups 3.11.

The screen blanking and keyboard / mouse lock is also implemented for operation under Windows and in DOS boxes operating under Windows.

<P2> *SafeGuard Easy* for Windows 95

This product requires

- Windows 95

This product works under 16-bit as well as under 32-bit disk access of Windows 95. SGE supports the FAT32 file system available under Windows 95 B. The screen blanking and keyboard / mouse lock is implemented for the Windows 95 desktop and works also in full screen DOS boxes. The screen blanking and keyboard / mouse lock does not work, when Windows 95 is booted in safe mode or as command prompt.

<P3> *SafeGuard Easy* for Windows 98

This product requires

- Windows 98

This product works under 16-bit as well as under 32-bit disk access of Windows 98. The screen blanking and keyboard / mouse lock is implemented for the Windows 98 desktop and works also in full screen DOS boxes. The screen blanking and keyboard / mouse lock does not work, when Windows 98 is booted in safe mode or as command prompt.

<P4> *SafeGuard Easy* for Windows NT

This product requires

- Windows NT 3.51 Workstation or
- Windows NT 4.0 Workstation

This product works in a secure way with both available file systems: FAT and NTFS which are included within Windows NT. A screen blanking and keyboard / mouse lock is not implemented in this product, because the screen blanking function of Windows NT is secure enough to cover the pause functionality.

Platform Independent Software Requirements

The TOE is working together with all application software, which is released for the mentioned operating system platforms. 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 this data is not protected by the TOE against unauthorised disclosure.

Internetworking Considerations

SGE works on stand alone PCs as well as on workstations in a LAN or workstations connected as a terminal to a host.

In the latter cases it must be observed, that the security from SGE extends only over the local disk drives, not over virtual drives in network environments. Security is also inactive, when the secured PC is included in a peer-to-peer LAN and parts of its hard disk(s) are accessible to other users within this LAN.

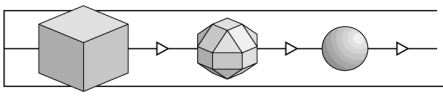
This has also to be observed, where PCs are connected to external hosts via modem or Intranet / Internet connections.

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

Special Measures

SafeGuard Easy (SGE) is designed to protect user data on Personal Computers (PCs) operated in a standard office environment. *SafeGuard Easy* is a software product installed on a PC to prevent unauthorised access to user data stored in hard disk partitions. As an option, data stored on floppy disks are also protected. Only authorised individuals may use the computer (start / boot the operating system from an encrypted device, especially from the hard disk).

The following measures have to be taken to guarantee the TOE's security:



<A1> Installation options

The system has to be installed directly by the system administrator, not using a configuration file. The system has to be configured observing the following options during installation:

- Standard installation (with PBA).
- Selection of an appropriate encryption algorithm (DES with 16 rounds or IDEA).
- Minimum password length set to 6 characters.
- Activation of floppy disk encryption.
- Activation of screen / keyboard lock (not applicable for <P4>, because this functionality is realised by the operating system).
- The user shall not select the encryption of the operating system areas, but the entire hard disk encryption.

These settings must not be changed. Some of these options ensure that the security functions of the TOE are *active* after having installed the product on a PC. In addition, users shall not use the device encryption offered by SGE to protect other storage devices like BERNOULLI drives, ZIP drives, PCMCIA fixed disks etc. because this configuration is not evaluated.

<A2> Operating instructions

The users have to be advised to activate the screen / keyboard lock manually when leaving the PC for a short time and to switch off or reboot the PC, when leaving the PC for a longer time.

The users have to be informed, that the screen / keyboard lock is not working, when Windows 95 or Windows 98 is booted in safe mode or as command prompt.

As an additional measure to prevent the system from spying out any SGE user name and password by using a "Trojan Horse" program (see discussion of weaknesses in construction), the boot sequence of the PC has to be protected against booting from floppy disk by using a mechanical lock or a system internal measure (e.g. boot password of the BIOS).

<A3> User rights' settings

Although the TOE allows the administrator to define rights of other users to perform administrative operations, the intended method of using the TOE in this evaluation is to put users on an equal footing with the administrator:

So, it is assumed that

- the authorised user is allowed to perform all administration activities.

So there is actually no difference between users and the administrator.

Whereas the assumptions <A1> and <A2> state that the TOE must be properly installed, administrated, and used, the assumption <A3> must be fulfilled to guarantee a complete definition of the threats.

3.3.2 Threats

Subjects

Subjects relevant for considering the security of the TOE are:

<S1> authorised user, i.e. all persons knowing a correct password (under standard user administration) or knowing a correct combination of user name and password (under extended user administration) for the current installation,

<S2> unauthorised person (all persons knowing none of the passwords or user name / password combinations; these persons may also use an installation of SGE in another domain but they do not know any password for the domain considered here).

Refer to section 3.3.3 for more detail.

Objects

Objects relevant for considering the security of the TOE are:

<O1> user data contained in encrypted partitions of the local hard disk drive(s),

<O2> user data stored on encrypted floppy disks,

<O3> contents of the screen,

<O4> processes (programs) on the PC,

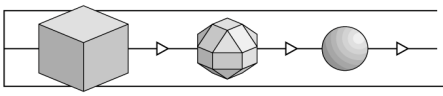
<O5> user and administrator passwords, and

<O6> TOE software and its TSF data.

Opportunities

To classify the threats, different moments must be considered:

<M1> The PC is switched off (not running), the operating system is not loaded, the authorised user is absent.



<M2> A floppy disk encrypted with the help of the TOE is not under supervision of the authorised user.

<M3> PC is running, the operating system is loaded, but the screen is darkened and the mouse / keyboard is locked, the authorised user is temporarily absent.

Expertise and available resources

The TOE should avert the threats even if the attackers may have moderate skill including know-how on some (rather general) TOE design principles and (cryptographic) algorithms used by the TOE. The means being available should not be that extensive that they cannot be employed by a medium-sized group without being noticed to a great extend. The time needed to perform the attack should not exceed four weeks.

Threats to be averted by the TOE

<T1> An unauthorised person <S2> attempts to perform a substantial access to any data stored on encrypted hard disk partitions <O1>. This attack is expected to be performed after having the PC switched off <M1>.

("Substantial access" means reading, writing or modifying information; "any data" means data files, program files and file system information)

<T2> An unauthorised person <S2> attempts to perform a substantial access to any data stored on an encrypted floppy disk <O2>. This attack is expected to be performed when a floppy disk encrypted with the help of the TOE is not under supervision of the authorised user <M2>.

("Substantial access" means reading, writing or modifying information; "any data" means data files, program files and file system information)

<T3> An unauthorised person <S2> attempts to perform administrative operations (changing the protection status of the TOE or modifying other TSF data <O6>). This attack is expected to be performed after having the PC switched off <M1>.

<T4>a Products <P1>, <P2> and <P3> only

An unauthorised person <S2> attempts to read the screen contents <O3> or to start a process <O4>. This attack is expected to be performed when the PC is running (the operating system is loaded), but the screen is darkened, the mouse / keyboard is locked, and the authorised user is temporarily absent <M3>.

Remark: The product <P4> for Windows NT does not cover <T4> by its own security functions. This threat is already covered by the operating system itself. The mechanism provided by the operating system is considered strong enough not to break the strength of mechanisms for the TOE.

Threats to be averted by the environment

<T4>b Product <P4> only

An unauthorised person <S2> attempts to read the screen contents <O3> or to start a process <O4>. This attack is expected to be performed when the PC is running (the operating system is loaded), but the screen is darkened, the mouse / keyboard is locked, and the authorised user is temporarily absent <M3>.

Remark: The product <P4> for Windows NT does not cover <T4> by its own security functions. This threat is already covered by the operating system itself. The mechanism provided by the operating system is considered strong enough not to break the strength of mechanisms for the TOE.

<T5> An unauthorised person <S2> gets the password <O5> of an authorised person (user and administrator). In either cases, an unauthorised person becomes an authorised person. As a consequence, there is no protection against <T1>, <T2>, <T3>, and <T4>.

<T6> An intruder <S2> succeeds in placing untrusted software on the PC's hard disk designed to attack (disclose or modify) the TOE software or its TSF data <O6>. The attacker's program will be executed by the authorised user (Trojan horse), unnoticed (virus), or accidentally (both).

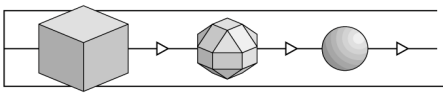
With such an attack, the attacker attempts (i) to disclose cryptographic keys or passwords in order to break or circumvent the certain security functions of the TOE, (ii) to modify software of the TOE to cause the TOE's security functions or measures to fail or to operate against the security policy. In either cases, the attacker attempts to succeed in performing <T1>, <T2>, <T3>, and <T4>.

<T7> Untrusted software is placed on the PC's hard disk or executed while the computer is operated which does not use the respective Application Programming Interface of the OS platform for disk access. Then this software circumvents layers of the disk access system. In this case, the threats <T1> and <T2> are not averted.

The PC is included in a peer-to-peer LAN, and any part of its hard disk(s) is shared with other users of this LAN. Then the remote host will have data access with the same rights as the user currently logged in. In this case, the threat <T1> is not averted.

3.3.3 Organisational Security Policies

The Security Objectives of the TOE (chapter 3.4) are only derived from the identified threats (section 3.3.2) together with assumptions (section 3.3.1). Therefore, the description of the *Organisational Security Policies* may be omitted.



Note that the *Assumptions* <A1> and <A2> contain fundamental statements that could be formulated as *Organisational Security Policies*. But it has been decided to include the corresponding statements as *Assumptions*, since no *Security Objectives* will address these issues. Nevertheless, the instructions contained in the assumptions just mentioned must be followed by the users.

To further explain the use of the TOE, additional information is given in the remaining part of this section. This is mainly to define the term „authorised user“ and distinguish him from other („unauthorised“) users:

1) The TOE distinguishes between the „administrator“ and the „user“ primarily by checking passwords. In the standard user administration configuration there is no name associated with an individual. In the extended user administration configuration each individual authorised to perform operations controlled by the TOE gets a name which is analysed by the TOE to check the right password. Nevertheless, the access control is assumed to be based upon roles.

2) The person who installs the TOE on a PC automatically becomes the „administrator“ by defining the corresponding password. This password (together with the Response Generation Program) is needed to perform the Challenge Response Logon.

3) The „administrator“ defines the user’s account by choosing the appropriate password. The „user“ is informed by the „administrator“ of the password.

4) Different individuals (authorised persons) may act as „user(s)“ or the „administrator“ by sharing the corresponding password (and name, if any).[5] **Hence, security is enforced by distinguishing between „authorised individuals (users)“ and „unauthorised individuals“.**

These rules must be taken into account when considering the definition of the subjects <S1> and <S2> in section 3.3.2. The definition of the subjects <S1> and <S2> in turn has been used to define the threats <Tx>. Hence all the rules above are already used to define the threats. Therefore, the Security Objectives of the TOE can only be derived from the identified threats together with assumptions (as claimed above) and there is no need to further consider the above rules explicitly.

3.4 Security Objectives

The chapter *Security Objectives* is organised as follows: *TOE Security Objectives*, *Security Objectives for Environment*.

5 Note that because of assumption <A2> there is actually no difference between users and the administrator.

The following *Security Objectives* can be traced back to the *Threats* as follows:

	<G1>	<G2>	<G3>	<G4>a	<G4>b	<G5>	<G6>	<G7>
<T1>	×							
<T2>		×						
<T3>			×					
<T4>a				×				
<T4>b					×			
<T5>						×		
<T6>							×	
<T7>								×

Nevertheless, the description of the *Security Objectives* contain additional information to indicate how the security problem (*Threat*) is addressed by the TOE. This is to provide a clear link to understand the *TOE Functional Requirements*.

3.4.1 TOE Security Objectives

The TOE is designed to prevent unauthorised users from access to data and programs on PCs and on encrypted floppy disks. It also prevents unauthorised users from operating a running, temporarily left-alone PC (especially prevents the screen output of running processes and inhibits the starting of new processes).

Although a TOE's *Security Function Policy (SFP)* is expected to be given when defining the *TOE Security Functional Requirements* it is given already here to provide background information for better understanding the *TOE's Security Objectives*.

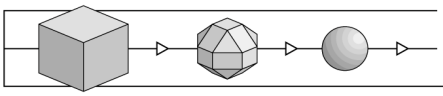
SFP1 Only „authorised individuals (users)" can access files on the hard disk or on floppy disks protected by the TOE. This means, access to user data is controlled (access control).

SFP2 Only „authorised individuals (users)" may perform administrative operations. This means, administration is the subject of access control.

SFP3 In order to realise the Security Function Policy SFP1 and SFP2 only authorised users may start / boot the operating system from an encrypted device (especially from the hard disk) to use the computer or start the administration program.

SFP4 The TOE shall provide means to protect the computer when the authorised user is temporarily absent without the need to switch it off. This is to support SFP1.

The strength of protection provided by TOE shall correspond to the scope of using SGE and the description of the environment in which it is used (refer to section 0 and 3.3.2).



The *TOE's Security Objectives*[6] are as follows:

<G1> Unauthorised individuals <S2> shall not be able to perform any substantial access to any data stored on encrypted hard disk partitions <O1>. This attempt is expected to be performed after having the PC switched off <M1>.

("Substantial access" means reading, writing or modifying information; "any data" means data files, program files and file system information)

Solution: These user data are protected by a TSF which encrypts the user data whenever being written onto the hard disk (exported out of the TSC). The functional requirements are described in section 3.5.1..3 (Protection of Data on Hard Disks <RF3>). Authorised individuals are identified by checking their respective password before the operating system is loaded. The corresponding functional requirements are described in section 3.5.1..2 (Pre-Boot Authentication (PBA) <RF2>). The latter function provides the cryptographic key necessary to access (decrypt) the data stored on protected hard disk partitions.

<G2> Unauthorised individuals <S2> shall not be able to perform any substantial access to any data stored on an encrypted floppy disk <O2>. This attempt is expected to be performed when a floppy disk encrypted with the help of the TOE is not under supervision of the authorised user <M2>.

("Substantial access" means reading, writing or modifying information; "any data" means data files, program files and file system information)

Solution: These user data are protected by a TSF which encrypts the user data whenever being written onto the floppy disk (exported out of the TSC). The functional requirements are described in section 3.5.1..4 (Protection of Data on Floppy Disks <RF4>). Authorised individuals are identified by checking their respective password before the operating system is loaded. The corresponding functional requirements are described in section 3.5.1..2 (Pre-Boot Authentication (PBA) <RF2>). The latter function provides the cryptographic key necessary to access (decrypt) the data stored on protected floppy disks.

<G3> Unauthorised individuals <S2> shall not be able to perform administrative operations (changing the protection status of the TOE or modifying other TSF data) <O6>. This attempt is expected to be performed after having the PC switched off <M1>.

Solution: Access to administrative operations is controlled by a TSF. Authorised individuals are identified by checking their respective password. To perform administrative operations TSF data must be accessed. This data is en-

---

6 The abbreviation <Gx> („Goal x") has been chosen instead of <Ox> („Objectives") to avoid confusion with the abbreviation of the objects (<Ox>).

crypted and can be accessed only if the correct password has been input. The functional requirements are described in section 3.5.1..1 (Installation and Secure Administration <RF1>).

<G4>a Products <P1>, <P2> and <P3> only

Unauthorised individuals <S2> shall not be able to read the screen contents <O3> or to start a process <O4>. This attempt is expected to be performed when the PC is running (the operating system is loaded), but the screen is darkened, the mouse / keyboard is locked, and the authorised user is temporarily absent <M3>.

Remark: Regarding <P4> refer to <G4>b.

Solution: The user data on the screen are protected by blanking the screen when the user is temporarily absent. Then, processes cannot be started since the keyboard and the mouse are locked. The screen blanking and keyboard / mouse lock is activated either by the user or automatically after an elapse of time. The functional requirements are described in section 3.5.1..5 (Screen Blanking and Keyboard / Mouse Lock <RF5>).

3.4.2 Security Objectives for Environment

The *Security Objectives for Environment* are as follows:

<G4>b Product <P4> only

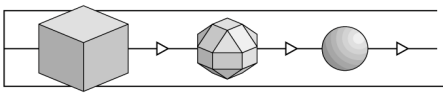
Unauthorised individuals <S2> shall not be able to read the screen contents <O3> or to start a process <O4>. This attempt is expected to be performed when the PC is running (the operating system is loaded), but the screen is darkened, the mouse / keyboard is locked, and the authorised user is temporarily absent <M3>.

Remark: The product <P4> for Windows NT does not cover <G4> by its own security functions. This must be ensured by the operating system itself. The mechanism provided by the operating system is considered strong enough not to break the strength of mechanisms for the TOE.

Solution: The user data on the screen are protected by blanking the screen when the user is temporarily absent. Then, processes cannot be started since the keyboard and the mouse are locked. The screen blanking and keyboard / mouse lock is activated either by the user or automatically after an elapse of time. This is realised by the Screen Saver of Windows NT.

<G5> Unauthorised individuals <S2> shall not get the password <O5> of an authorised person (user and administrator). If this is not guaranteed by the environment, the TOE will miss to provide the security defined above.

Solution: The users are instructed to keep their password secret.



<G6> An intruder <S2> shall not succeed in placing untrusted software on the PC's hard disk designed to attack (disclose or modify) the TOE software or its TSF data <O6>. The attacker's program will be executed by the authorised user (Trojan horse), unnoticed (virus), or accidentally (both). In this case the TOE will miss to provide the security defined above.

Solution: The users are instructed to use appropriate tools to scan for such untrusted software and to remove it.

<G7> Software which does not use the respective Application Programming Interface of the OS platform for disk access shall not be placed on the PC's hard disk or executed while the computer is operated. In addition, parts of the hard disk(s) shall not be shared with other users of this LAN. If this is not guaranteed by the environment, the TOE will miss to provide the security defined above.

Solution: The users are instructed to use appropriate means to look for such „bad" software and to remove it. The same holds for „bad" connections.

Note that the *Assumptions* <A1> and <A2> contain fundamental statements that could be formulated as *Security Objectives for Environment*. But there is little to be gained from that. The Common Criteria do not require security requirements for the non-IT environment to be a formal part of the Security Target. As a consequence, it has been decided to include the corresponding statements as *Assumptions*. Nevertheless, the instructions contained in the assumptions just mentioned must be followed by the users.

3.5 IT Security Requirements

The chapter *IT Security Requirements* is organised as follows: *TOE Security Requirements* (*TOE Functional Requirements*, *TOE Assurance Requirements*), *Security Requirements for the IT Environment*.

3.5.1 TOE Security Requirements

TOE Functional Requirements

The TOE offers the security functions described below. All listed product arrangements of the TOE are identical in their security enforcing and security relevant parts, functions and mechanisms. Product <P4> does not contain screen blanking / keyboard lock.

The claimed rating of the minimum strength of security functions for the configuration of the TOE mentioned in section 3.3.1 („Assumptions") is *SOF-medium*.

The *TOE Functional Requirements* response to the security problems defined in form of *Security Objectives* as follows:

	Functional Requirements	Part 2 Functional Components
<G1>	Protection of Data on Hard Disks <RF3>	refer to Annex C in section 3.9.3
	Pre-Boot Authentication (PBA) <RF2>	refer to Annex B in section 3.9.2
<G2>	Protection of Data on Floppy Disks <RF4>	refer to Annex D in section 3.9.4
	Pre-Boot Authentication (PBA) <RF2>	refer to Annex B in section 3.9.2
<G3>	Installation and Secure Administration <RF1>	refer to Annex A in section 3.9.1
<G4>a	Screen Blanking and Keyboard / Mouse Lock <RF5>	refer to Annex E in section 3.9.5

The *TOE Functional Requirements* are described using components taken from Part 2 of the Common Criteria.

Note regarding the functional requirements for <G1> and <G2>: The *Common Criteria* distinguish between *inter-TSF transfer* and *transfer outside TSF control*. The *inter-TSF transfer* is defined for a distributed TOE where the TOE communicates with a remote trusted IT product. Exchange of data is called *transfer outside TSF control* if there is no TSF (or its characteristics are unknown) on the remote IT product.

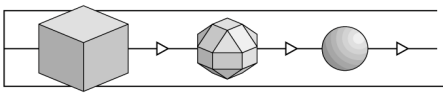
In the case of TOE the hard disk and the floppy disks can be regarded as external IT products. User data which are written onto hard disk or floppy disks are actually brought outside the *TSF Scope of Control (TSC)* since these encrypted user data are not under control of any TSF (but protected using the TOE) when the computer is switched off (refer to <T1> with <M1> and <T2> with <M2>). Hence, appropriate export and import functions are used to describe the behaviour of SGE. Refer to the Annexes for more detail.

3.5.1..1 Installation and Secure Administration <RF1>

SGE is installed from the installation disks to the hard disk using an installation program. This installation program is different for the different product versions of SGE.

For all platforms, it mainly unpacks the program files and copies them to the hard disk. After copying the files, the SGE administration program is automatically started and gives the chance to define the program options and to initiate the hard disk encryption.

[The system can be installed by using a predefined configuration file. In this case the configuration file contains the settings, with which SGE has to be installed and a system administrator is not required for installation. This feature must not be used, when the certified operation of SGE is required.]



User Administration

Administration of SGE is performed in a hierarchical user system with a system administrator on top. The system administrator is organised as a "role", i.e. there is one special user name (required only for the extended user administration) and one password for this role. Different persons can be associated as system administrator by knowing the password for this role.

Under the standard user administration a second user is defined, whose rights can be set by the system administrator. This user is also organised as a "role"; only his password is required for identification and authentication. More than one person may share the password.

For <P1>, <P2> and <P3> additionally an extended user administration is available. In this case the system administrator maintains different users (up to 16) with different user names and passwords and can assign different rights to the users available in the system. When a user is assigned the right to maintain the user settings, he can also behave as a system administrator and change the user rights.

However, according to the assumption <A3>, the intended method of using the TOE in this evaluation is to put users on an equal footing with the administrator: The authorised user is allowed to perform all administration activities. There is actually no difference between users and the administrator.

Administration Program

SGE comprises an administration program to perform these functions. The administration program checks the identity and authenticity of the user calling it by asking for his user name (only in the extended user administration) and the password. This is done before the user is allowed to perform any action described below. It is possible that not only the user logged in at the moment is able to call the administration program but also every authorised user is able to do so. Alternatively to entering the password it can be provided by Challenge Response Login (<P1> and <P2> only) when using the 16-bit version.

The administration program is an application of the appropriate platform and allows to

- change user passwords,
- set user rights,
- set password rules and PBA options,
- define status, encryption algorithms and keys for hard disk encryption, floppy disk encryption and device encryption (as far as available),
- define encrypted and non-encrypted partitions on the hard disks,
- define screen blanking options in <P1>, <P2> and <P3> only,

- set MBR-related options (boot virus check etc.),
- create a configuration file for remote installation,
- perform recovery operations like backup, restore or repair of the system kernel of SGE,
- perform deinstallation of the system kernel of SGE.

Each operation can be performed by any user, if his appropriate administration right has been set. The system administrator is authorised for all administration operations. (Refer to assumption <A3> for the users' rights settings valid for this evaluation.)

One-pass Hard Disk Encryption / Decryption

A primary hard disk encryption or final decryption is initiated automatically after changing the status of a partition (from non-encrypted to encrypted or vice versa) by the administration program. Under Windows NT in <P4> the encryption / decryption is running as a background process.

Recovery Operations

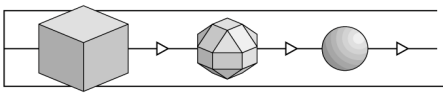
SGE provides some functions for recovery of faulty systems: the system kernel, which is the major part of an installed system, can be backed up (on a floppy disk for instance) and restored, when the system does not boot or recognise any user logon. This is done by booting the PC from a floppy disk and starting the administration program. Restore of a system kernel is only possible with the knowledge of the system administrator password belonging to that system kernel.

The system has also a component, which is able to repair the kernel (within some limits) when errors occur. This is done by a particular program which can be executed by every user. The program only fixes a special part of the system kernel trying to restore an initial state of the kernel but grants no access to the data stored on the PC.

Functional Requirements

The following functional requirements were selected from Part 2 of the Common Criteria to form the security behaviour described above:

- The function Management of Security Functions Behaviour (FMT_MOF.1) ensures that only the authorised persons can install SGE (enable the security functions; valid by definition), deinstall SGE (disable the security functions) or modify the behaviour of the security functions (refer to SFP 2 of the TOE's Security Function Policy (SFP)).
- The function Management of TSF Data (FMT_MTD.1) ensures that only the authorised persons can change TSF data (for example: change passwords, refer to SFP 2 of the TOE's Security Function Policy (SFP)).



- The supplementary function User authentication before any action (FIA_UAU.2) ensures that prior to using either of the above functions the user must authenticate himself (refer to SFP 3 of the TOE's Security Function Policy (SFP)). There is no need to include the function Timing of identification (FIA_UID.1) because the users are either not identified (standard user administration) or identification is inseparably linked up with the authentication process (extended user administration).

The components describing functional requirements selected from Part 2 of the Common Criteria are contained in Section 3.9.1 (Annex A: Functional Components for <RF1>).

3.5.1..2 Pre-Boot Authentication (PBA) <RF2>

Pre-Boot Authentication is a mechanism in SGE to check the user's authenticity before the operating system on a PC is booted from a hard disk.

With PBA installed, the system prompts for a password after starting the PC. Only a correct PBA password enables to boot an operating system. In case of an incorrect password entered, the PBA module waits for some time until the next password entry is possible. This time increases for each incorrect entry.

PBA includes a mechanism, which calculates the key for the boot partition from the password entered. SGE allows two versions of PBA administration.

In the standard version, two users are available: a system administrator and a standard user. To each user one password is assigned, the PBA is restricted to the entry of one of these passwords, and the system itself decides, what user has been logged in.

The extended user administration allows the definition of up to 16 users with both, a user name and a password. During PBA the user name and the password have to be entered for identification and authentication. The users known from the standard user administration are copied with the user names 'SYSTEM' and 'USER' to the user list. The extended user administration is not available under <P4>.

In both cases some rules for password selection, like password minimum length and password expiration, may be defined by the administrator. All users are enabled to change their user password during PBA logon.

During PBA a Challenge Response Logon is possible using a challenge response procedure. For this function, the PBA module generates a random challenge string, which can be transmitted by the user to a system administrator. With the Response Generation Program, the administrator creates a response string out of the challenge, his password and a function code. Then the user enters this response string at the PBA and is then enabled to perform the functions, which the system administrator has enabled to him. The response code is only valid for a single login.

Functional Requirements

The following functional requirements were selected from Part 2 of the Common Criteria to form the security behaviour described above:

- The function User authentication before any action (FIA_UAU.2) ensures that prior to booting the operating system the user must authenticate himself (refer to SFP 3 of the TOE's Security Function Policy (SFP)). There is no need to include the function Timing of identification (FIA_UID.1) because the users are either not identified (standard user administration) or identification is inseparable linked up with the authentication process (extended user administration).

- During PBA users may change the password. The function Management of TSF Data (FMT_MTD.1) ensures that only the authorised person can change his password (TSF data), refer to SFP 2 of the TOE's Security Function Policy (SFP)).

The components describing functional requirements selected from Part 2 of the Common Criteria are contained in Section 3.9.2 (Annex B: Functional Components for <RF2>).

3.5.1..3 Protection of Data on Hard Disks <RF3>

The major security feature of SGE is the encryption of the partitions of local hard disks (up to four hard disks of different hardware interfaces can be handled).

Available encryption algorithms are DES and IDEA.[7]

All data on the encrypted partitions of the hard disk(s) is held encrypted and encryption / decryption is performed during write or read accesses to the hard disk(s).

Booting a PC, where SGE is installed, from a floppy disk results in a state where information can't be retained from the hard disk(s) as a result of the encryption. When booting such a PC from hard disk, the control is handed from one part of SGE to another. First, the PBA module checks the authenticity of the user and calculates the encryption key for the boot partition. Next, an INT 13h handler is installed to decrypt the hard disk data during the boot phase. This handler remains active as long as hard disk access is performed during BIOS INT 13h (DOS e.g.). If a 32-bit operating system is booted, a device driver is automatically loaded, which is taking over hard disk on-line encryption and decryption during the 32-bit session.

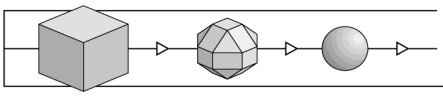
Functional Requirements

The following functional requirements were selected from Part 2 of the Common Criteria to form the security behaviour described above:

- According to the above SFP 1 of the TOE's Security Function Policy (SFP) only „authorised individuals (users)" can access files on the hard disk or on floppy

---

7 Note that due to <A1> BLOWFISH, STEALTH and XOR must not be used.



disks protected by the TOE. This means, access to user data is controlled (access control). This is stated by the policy Subset Access Control (FDP_ACC.1).

- This policy is enforced mainly by the function Export of user data without security attributes (FDP_ETC.1). Export of user data to the hard disk is controlled by the TSF when these data are designated for being stored on that device (brought outside TSC). These data are encrypted by the TOE before being written to the hard disk. So, the security attribute not being explicitly exported is „encrypted or confidential“ and the key is available only within the TSF.

- Import of user data from the hard disk is controlled by the TSF when these data are designated for being read from that device (brought from outside TSC). These data are decrypted by the TOE when being read from the hard disk. So, the security attribute being ignored is whether they are actually encrypted, and there are no extra rules being enforced by the TSF when data is imported. The key is available only within the TSF. These requirements are summarised as function Import of user data without security attributes (FDP_ITC.1).

- To use the export or the import function of the TOE, these functions need to get enabled and supplied with the key. The TSF is supplied with the key by the function Pre-Boot Authentication (PBA) <RF2> (see 3.5.1..2) when the user has successfully been authorised. Therefore, the default value for the present TSF is „restrict access“. This is one of the requirements of function Static attribute initialisation (FMT_MSA.3).

The components describing functional requirements selected from Part 2 of the Common Criteria are contained in Section 3.9.3 (Annex C: Functional Components for <RF3>).

Protection of Operating System Areas (informative only)

The minimum security function of SGE is the encryption of the system areas used by the file system. This includes:

- Bootsector, FAT and root directory of each available partition under DOS, Windows 3.x <P1>, Windows 95 <P2> or Windows 98 <P3>,

- Bootsector, FAT and root directory for FAT partitions respectively file system root area for NTFS partitions under Windows NT (<P4> only).

During installation of SGE the administrator has to decide, if the encryption of the system areas or a full partition encryption is installed.

When installing SGE according to the installation directives for certified operation below, the user shall not select the encryption of the operating system areas, but the entire hard disk encryption.

3.5.1..4 Protection of Data on Floppy Disks <RF4>

SGE supports the on-line encryption of floppy disks. The encryption algorithm can be selected out of the range of algorithms offered for hard disk encryption.

The system administrator can determine for each user, if he is allowed to switch on and switch off the floppy disk encryption during his session or if he is not allowed.

Functional Requirements

The following functional requirements were selected from Part 2 of the Common Criteria to form the security behaviour described above:

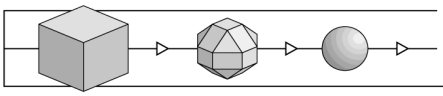
- According to the above SFP 1 of the TOE's Security Function Policy (SFP) only „authorised individuals (users)" can access files on the hard disk or on floppy disks protected by the TOE. This means, access to user data is controlled (access control). This is stated by the policy Subset Access Control (FDP_ACC.1).

- This policy is enforced mainly by the function Export of user data without security attributes (FDP_ETC.1). Export of user data to protected floppy disks is controlled by the TSF when these data are designated for being stored on that device (brought outside TSC). These data are encrypted by the TOE before being written to the floppy disk. So, the security attribute not being explicitly exported is „encrypted or confidential" and the key is available only within the TSF.

- Import of user data from protected floppy disk is controlled by the TSF when these data are designated for being read from that device (brought from outside TSC). These data are decrypted by the TOE when being read from the floppy disk. So, the security attribute being ignored is whether they are actually encrypted, and there are no extra rules being enforced by the TSF when data is imported. The key is available only within the TSF. These requirements are summarised as function Import of user data without security attributes (FDP_ITC.1).

- To use the export or the import function of the TOE, these functions needs to get enabled and supplied with the key. The TSF is supplied with the key by the function Pre-Boot Authentication (PBA) <RF2> (see 3.5.1..2) when the user has successfully been authorised. Therefore, the default value for the present TSF is „restrict access". This is one of the requirements of function Static attribute initialisation (FMT_MSA.3).

The components describing functional requirements selected from Part 2 of the Common Criteria are contained in Section 3.9.4 (Annex D: Functional Components for <RF4>).



3.5.1..5 Screen Blanking and Keyboard / Mouse Lock <RF5>

SGE in the versions <P1>, <P2> and <P3> includes a feature for screen blanking and keyboard and mouse lock.

After a lock request the screen is darkened and all keyboard inputs and mouse interactions are directly captured by the screen blanking program. Background processes (if there are any under Windows) keep on running, but their output cannot be seen and they cannot receive keyboard input any longer.

The lock is invoked either actively by the user or automatically by the system after some period (length configurable) of no user interaction. Pressing any key or moving the mouse during screen blanking and keyboard lock results in a login screen coming up.

The user authenticates himself by entering his password to release the lock function. Only the user currently logged in will be authenticated by the screen blanking program.

Functional Requirements

The following functional requirements were selected from Part 2 of the Common Criteria to form the security behaviour described above:

- According to SFP4 the TOE shall provide means to protect the computer when the authorised user is temporarily absent without the need to switch it off. This is realised by screen blanking and keyboard / mouse lock which is either TSF-initiated (automatic; Component TSF-initiated Session Locking, FTA_SSL.1) or caused by the user's action (user-initiated; Component User-initiated Locking, FTA_SSL.2).

- Before the system returns to normal operation, the user must authenticate himself (Re-authenticating; component Re-authenticating, FIA_UAU.6). Note that function Timing of authentication (FIA_UAU.1) is included for the sake of completeness only. There is no need to include the function Timing of identification (FIA_UID.1) because the users are either not identified (standard user administration) or identification is inseparable linked up with the authentication process (extended user administration).

The components describing functional requirements selected from Part 2 of the Common Criteria are contained in Section 3.9.5 (Annex E: Functional Components for <RF5>).

3.5.1..6 Further Functions of *SafeGuard Easy* (informative only)

SGE supports some more functions for the convenience of secure operation and administration of PCs. **The following functions** are included into some or all product versions, but **are not part of the evaluated functions of the TOE**.

Device Encryption

Besides hard disk and floppy disk encryption, SGE in version <P1>, <P2> and <P3> is able to encrypt other storage devices like BERNOULLI drives, ZIP drives, PCMCIA fixed disks etc. The encryption algorithms available are the same as for the hard disk encryption. Like for the floppy disk encryption, the system administrator can determine for each user, if he is allowed to switch on and switch off the device encryption.

Auto Log On

The product versions <P2> and <P3> allow the pass through of the user name and the password from SGE to Windows 95 respectively Windows 98. This mechanism is called "Auto Log On" or "Single Sign On". The user has to logon only once and his identity and authorisation is passed to the Windows 95/98 logon. This option can be switched on and off in the system administration.

Twin Boot Option

SGE in the versions <P1>, <P2> and <P3> can be installed with the Twin Boot option (but confer <A1>). With this option there exist two primary boot partitions, one encrypted and one in plain text. Before PBA is started, a simple boot manager offers the two partitions to be booted from. Only when the encrypted partition is selected, the PBA is performed and the encryption functions are enabled. During the session, the user has no access to any plain text partition, except when a special option switch is set by the system administrator.

When the plain text partition is booted, no encryption/decryption is invoked.

TOE Assurance Requirements

The *TOE security assurance requirements* are identical with those defined by the *Evaluation Assurance Level 3 (EAL3)*. These are:

Documents for Configuration management (Class ACM)

CM Capabilities (Component ACM_CAP.3)

CM Scope (Component ACM_SCP.1)

Documents for Delivery and operation (Class ADO)

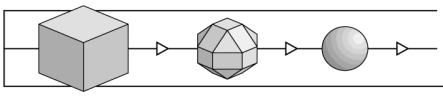
Delivery (Component ADO_DEL.1)

Installation, generation, and start-up (Component ADO_IGS.1)

Documents for Development (Class ADV)

Functional Specification (Component ADV_FSP.1)

High-Level Design (Component ADV_HLD.2)



Representation Correspondence (Component ADV_RCR.1)

Guidance documents (Class AGD)

Administrator Guidance (Component AGD_ADM.1)

User guidance (Component AGD_USR.1)

Documents for Life cycle support (Class ALC)

Development Security (Component ALC_DVS.1)

Documents for Tests (Class ATE)

Coverage (Component ATE_COV.2)

Depth (Component ATE_DPT.1)

Functional Tests (Component ATE_FUN.1)

Independent Testing (Component ATE_IND.2)

Documents for Vulnerability assessment (Class AVA)

Misuse (Component AVA_MSU.1)

Strength of TOE Security Functions (Component AVA_SOF.1)

Vulnerability Analysis (Component AVA_VLA.1)

The *assurance requirements* are to give evidence that the security functions of the TOE work correctly.

3.5.2 Security Requirements for the IT Environment

There are the following *Security Requirements for the IT Environment*:

<RE1> Product <P4> only

Unauthorised individuals <S2> shall not be able to read the screen contents <O3> or to start a process <O4>. This attempt is expected to be performed when the PC is running (the operating system is loaded), but the screen is darkened, the mouse / keyboard is locked, and the authorised user is temporarily absent <M3>. The product <P4> for Windows NT does not cover <T4> by its own security functions.

The automatic or user initiated function „screen blanking and keyboard / mouse lock including re-authentication“ must be provided by the operating system

Windows NT. The mechanism provided by the operating system is considered strong enough not to break the strength of mechanisms for the TOE.

<RE2> Untrusted software shall not be placed on the PC's hard disk designed to attack (disclose or modify) the TOE software or its TSF data <O6>. Such programs will be executed by the authorised user (Trojan horse), unnoticed (virus), or accidentally (both). In this case the TOE will miss to provide the security defined above.

Solution: The users are instructed to use appropriate tools to scan for such untrusted software and to remove it.

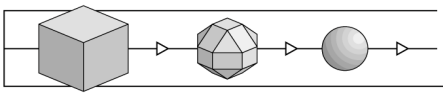
<RE3> Software which does not use the respective Application Programming Interface of the OS platform for disk access shall not be placed on the PC's hard disk or executed while the computer is operated. In addition, parts of the hard disk(s) shall not be shared with other users of this LAN. If this is not guaranteed by the environment, the TOE will miss to provide the security defined above.

Solution: The users are instructed to use appropriate means to look for such „bad" software and to remove it. The same holds for „bad" connections.

This *Security Requirement for the IT Environment* responses to the following security problem defined in form of a *Security Objective*:

	Requirements	Solution or example, resp.
<G4>b	<RE1> Screen Blanking and Keyboard / Mouse Lock (similar to <RF5>)	Windows NT screen saver
<G5>	non-IT: refer to remark below	(organisational: follow instructions)
<G6>	<RE2> IT related: ensure that no untrusted software brought into the system, it shall be detected and removed	(virus scanners)
<G7>	<RE3> IT related: ensure that no software is used which bypasses TSFs, do not share devices with other users of a LAN	(organisational: do not use „bad" software and „bad" connections)

Note that there is no *Security Requirement* for the *IT Environment* for the *Security Objective* <G5>. For <G5> users must follow the instructions to keep the password secret. This is an organisational measure.



In case of the product <P4> the security must be provided by the Windows NT screen saver in a similar way like <RF5> to response to the *Security Objective* <G4>b.

Regarding the *Security Objectives* <G6> and <G7> the *IT Environment* must have specific characteristics as indicated above. To ensure this users shall follow the instructions and may additionally use other IT products to respond to those objectives.

3.6 TOE Summary Specification

The chapter *TOE Summary Specification* is organised as follows: *TOE Security Functions*, *Assurance Measures*.

3.6.1 TOE Security Functions

The *TOE Security Functions* are described now. In addition, it is shown how these functions satisfy the *TOE security functional requirements*.

TOE security functional requirements	TOE Security Functions
Pre-Boot Authentication (PBA) <RF2>	Pre-Boot Authentication (PBA) <F1>
Protection of Data on Hard Disks <RF3>	Protection of Data on Hard Disk Partitions <F2>
Protection of Data on Floppy Disks <RF4>	Protection of Data on Floppy Disks <F3>
Screen Blanking and Keyboard / Mouse Lock <RF5>	Screen Blanking and Keyboard / Mouse Lock <F4>
Installation and Secure Administration <RF1>	Installation and Secure Administration <F5>

When the computer is started (before the operating system is booted) the user is prompted to input his password (logon). If the user has successfully been authenticated by the function *Pre-Boot Authentication (PBA) <F1>* other functions of the TOE are invoked: The function *Protection of Data on Hard Disk Partitions <F2>* ensures that all user data on the hard disk are encrypted. Even if the hard disk is removed an attacker cannot perform any substantial access to these data. The function *Protection of Data on Floppy Disks <F3>* ensures that all user data on the floppy disks are encrypted. Hence, an attacker cannot perform any substantial access to these data. The function *Screen Blanking and Keyboard / Mouse Lock <F4>* ensures that unauthorised individuals are not able to read the screen contents or to start a process when the authorised user is temporarily absent. Note that for product <P4> this function must be supported by the IT environment. All these security functions use TSF data which are encrypted when the computer is switched off. After successful authentication the PBA provides all TSF data needed to the other security functions.

When the installation and administration program is started the user is prompted to input his password (logon). Only authorised users can perform administrative opera-

tions. The function *Installation and Secure* Administration <F5> ensures that only the authorised persons can (i) deinstall SGE (disable the security functions) or (ii) change TSF data.

As a result, the *TOE Security Functions* exactly map to the requirements derived above. Now the IT security functions are defined in an informal style to a level of detail necessary for understanding their intent.

All security functions have a strength[8]. The claimed rating of the minimum strength of security functions is *SOF-medium*.

Pre-Boot Authentication (PBA) <F1>

Under the extended user administration, SGE works with different user names and with different passwords to identify and authenticate a user. Under the standard user administration only the entry of a valid password is required to perform an authentication.

PBA means, the system has to be provided with a valid user name (for extended user administration only) and password before the PC is booting from hard disk. This password is used to calculate the keys for the on-line device encryption of the hard disk (see chapter <F2>). The encryption key cannot be calculated without knowledge of a valid password. The password is entered via keyboard, when a login mask is displayed on the screen. Alternatively to entering the password it can be provided by Challenge Response Login.

Under extended user administration, the system checks also, if the entered password belongs to the user name entered.

Protection of Data on Hard Disk Partitions <F2>

The partitions of the installed hard disk(s) (up to four disks) of a PC <O1> can be held encrypted by SGE. The keys necessary to encrypt these data are provided by the security function <F1> only if the user has been authenticated successfully. Hence, the security function <F2> ensures that data provided by authorised users are protected when being stored on the hard disk.

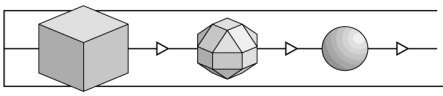
The used encryption algorithm can be selected from the range of available system algorithms (DES or IDEA)[9]. The key for the encryption is defined by the system administrator during installation; alternatively it can be selected by a random key generator, when the administrator selects this.

All write and read accesses to the encrypted hard disk partitions are maintained by one of the encryption handlers (INT 13h handler or 32-bit disk access device driver) depending on the state of the system. On a write access, the data is encrypted; on a read access, the data is decrypted.

---

8 although some underlying mechanisms are neither probabilistic nor permutational

9 Note that due to <A1> BLOWFISH, STEALTH and XOR must not be used.



[Installation, changes and de-installation: Encryption state changes of any partition are defined by using the SGE administration program. As a result of such a change initial encryption or complete decryption of the affected partitions is automatically invoked by SGE. If the initial encryption or complete decryption is interrupted, it continues automatically after booting the PC again. A user logon is not permitted unless the partition(s) is / are completely encrypted, except for <P4> where this task is performed by a background process, which is started after user logon. Note that the evaluation pertains the installed TOE with settings which correspond to <A1>.]

Protection of Data on Floppy Disks <F3>

All floppy disks can be read and written encrypted by SGE. The keys necessary to encrypt these data are provided by the security function <F1> only if the user has been authenticated successfully. Hence, the security function <F3> ensures that data provided by authorised users are protected when being stored on floppy disks. The algorithm used for floppy disk encryption can be selected out of the available algorithms (see above) during installation. The key for floppy disk encryption is defined by the system administrator during installation.

The encryption of floppy disks can be switched on and off by a special program. The right to use this program can be assigned to any user by the administrator.

An encrypted floppy disk is only readable on a workstation with an identical floppy algorithm and floppy key.

There is no initial encryption of a floppy disk, but before using a floppy disk for encrypted operation, it has to be formatted with the floppy encryption activated.

Screen Blanking and Keyboard / Mouse Lock <F4>

To prevent other persons from access to screen, keyboard and mouse during the absence of a user, these output and input devices can be locked. This function is not provided in <P4>.

This function is initiated by a special user action or automatically by the system after a definable period of time without user interaction. The user has different methods available to invoke the lock function: pressing a special key combination (under DOS only) or clicking on a special icon (under Windows 3.x, Windows 95 and Windows 98).

While the lock function is active, the screen is darkened. All input from the mouse and the keyboard is captured by the lock program and is not processed by the desktop or any application program. Background processes (under Windows) keep on running, but are thus temporarily disconnected from their input. Process output cannot be seen, because the screen is darkened.

When, with active lock function, the user presses any key on the keyboard or moves or clicks with the mouse (as far as a mouse driver is active), a login dialogue box appears. The user is prompted to enter his user password. The lock program checks the pass-

word and, if the password is correct, the screen contents are restored and keyboard and mouse inputs are sent to the processes from now on. If the password is incorrect, the user can input the password again. Only the user logged in during PBA can unlock the screen / keyboard lock.

Installation and Secure Administration <F5>

The system administration data include all installation and maintenance parameters of the TOE: users, passwords, encrypted devices and partitions, encryption keys, screen / keyboard lock parameters and the rights of the user(s) to modify these parameters.

Special administration programs give the ability to change these parameters. The administration data is stored in the real mode kernel on the hard disk. To prevent unauthorised users from access or modification of the administration data, it is protected by encryption mechanisms. Only the access with a correct password will enable the system to decrypt the administration data and set the parameters into effect.

3.6.2 Assurance Measures

The TOE does not provide any measure or mechanism to satisfy the assurance requirements. Assurance is guaranteed by the development process and by the users observing the corresponding directions. The latter are described in manuals which are evaluated together with the TOE (Guidance documents; Class AGD). The measures taken in the development process will be evaluated according to other assurance requirements of EAL3.

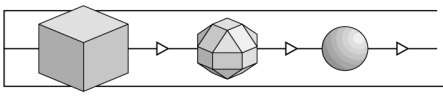
The *TOE Assurance Requirements* (section 0) cover all aspects to ensure that the security functions provided by the TOE are actually able to response to the security problems defined in form of *TOE Security Objectives* (section 3.4.1). The assurance requirements are exactly those defined for the Evaluation Assurance Level 3. There is no need to specify assurance measures: At Utimaco a sophisticated Quality Management System is in place. The development is organised to comply with essential requirements defined by widely accepted standards. The sites are protected by physical and organisational measures. The assessment of all these measures is the subject of the evaluation.

3.7 PP Claims

This Security Target does not make any claim that the TOE conforms with the requirements of a *Protection Profile*. As a result, sections „*PP Reference*“, „*PP Refinement*“ and „*PP Additions*“ are omitted.

3.8 Rationale

The chapter *Rationale* is organised as follows: *Security Objectives Rationale*, *Security Requirements Rationale*, *TOE Summary Specification Rationale*, *PP Claims Rationale*.



The purpose of the ST rationale is to demonstrate that a complete, coherent and internally consistent set of security objectives, security requirements, IT security functions and assurance measures have been proposed to satisfy the identified security problem.

3.8.1 Security Objectives Rationale

It shall be demonstrated that the *Security Objectives* (chapter 3.4) are appropriate referring to the aspects of the *Security Environment* (chapter 3.3).

The stated *Security Objectives* (chapter 3.4) address all of the identified *Threats* (section 3.3.2). Since the Security Objectives of the TOE are only derived from the threats together with assumptions (section 3.3.1), no *Organisational Security Policies* must be taken into considerations (section 3.3.3).

The list of *Threats* is complete provided that it is actually no problem that users may perform administrative operations. The corresponding *Assumption* is described as <A3>.

Taking this into consideration, there is a bi-directional mapping between *Security Objectives* and *Threats* only.

Note that the *Assumptions* <A1> and <A2> contain fundamental statements that could be formulated as *Security Objectives for Environment*. But there is little to be gained from that. In addition, the Common Criteria do not require security requirements for the non-IT environment to be a formal part of the Security Target. As a consequence, it has been decided to include the corresponding statements as *Assumptions*. Although no *Security Objective* addresses these issues, the instructions contained in the assumptions just mentioned must be followed by the users: The TOE and its security functions must be properly installed, administrated and used. The corresponding instructions are described as assumption <A1> and <A2>. Otherwise there is no basis for the TOE to provide security.

Taking this into consideration, each threat is addressed by one security objective, and each security objective addresses one threat:

	<G1>	<G2>	<G3>	<G4>a	<G4>b	<G5>	<G6>	<G7>
<T1>	×							
<T2>		×						
<T3>			×					
<T4>a				×				
<T4>b					×			
<T5>						×		
<T6>							×	
<T7>								×

The wording of the *Security Objectives* on the one hand (chapter 3.4) and of the *Threats* on the other (section 3.3.2) is very similar. The description of the *Security Objectives* contain additional information to indicate how the security problem (*Threat*) is addressed by the TOE. This information („solution“) provide sufficient detail to argue that the objectives provide for effective countermeasures to the threats.

3.8.2 Security Requirements Rationale

It shall be demonstrated that the set of *Security Requirements* (TOE and environment, chapter 3.5) is suitable to meet and traceable to the *Security Objectives* (chapter 3.4).

TOE Functional Requirements

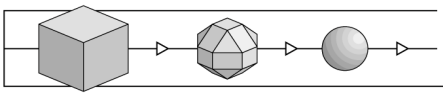
The *TOE Functional Requirements* (section 0) response to the security problems defined in form of *TOE Security Objectives* (section 3.4.1) as follows:

	<RF1>	<RF2>	<RF3>	<RF4>	<RF5>
<G1>		×	×		
<G2>		×		×	
<G3>	×				
<G4>a					×

The goal to protect user data on the hard disk <G1> is primarily addressed by the functional requirement *Protection of Data on Hard Disks <RF3>*. The latter is basically realised by the function *Export of user data without security attributes (FDP_ETC.1)* which ensures that all data written onto the hard disk is encrypted. The functional requirement *Pre-Boot Authentication (PBA) <RF2>* supports this by providing the key needed only if the user has been authorised before. This requirement is met by the function *User authentication before any action (FIA_UAU.2)*.

The goal to protect user data on protected floppy disks <G2> is primarily addressed by the functional requirement *Protection of Data on Floppy Disks <RF4>*. The latter is basically realised by the function *Export of user data without security attributes (FDP_ETC.1)* which ensures that all data written onto a floppy disk is encrypted. The functional requirement *Pre-Boot Authentication (PBA) <RF2>* supports this by providing the key needed only if the user has been authorised before. This requirement is met by the function *User authentication before any action (FIA_UAU.2)*.

The goal to protect the administration <G3> (changing the protection status of the TOE or modifying other TSF data) is addressed by the functional requirement *Installation and Secure Administration <RF1>*. The latter is basically realised by the function *User authentication before any action (FIA_UAU.2)*. Only authorised users may have access to administrative functions and the corresponding TSF data.



The goal to protect the data displayed on the screen and to prevent unauthorised access to user data when the authorised user is temporarily absent <G4> is addressed by the functional requirement *Screen Blanking and Keyboard / Mouse Lock <RF5>*. The latter is basically realised by the function *TSF-initiated Session Locking (FTA_SSL.1)* and *User-initiated Locking (FTA_SSL.2)*, respectively. Unlocking requires the user to be re-authenticated. This requirement is met by the function *Re-authenticating (FIA_UAU.6)*. This is valid only for the products <P1>, <P2> and <P3>. In case of product <P4> the functional requirements must be met by the IT environment (see below).

Information on dependencies of functional components (whether they are satisfied) is given above (refer to section 0 and the corresponding appendices in chapter 3.9).

Security Requirements for the IT Environment

The *Security Requirement for the IT Environment* (section 3.5.2) responses to the security problem defined in form of *Security Objectives for Environment* (section 3.4.2) as follows.

	Requirements	Solution or example, resp.
<G4>b	<RE1> Screen Blanking and Keyboard / Mouse Lock (similar to <RF5>)	Windows NT screen saver
<G5>	non-IT: refer to remark below	(organisational: follow instructions)
<G6>	<RE2> IT related: ensure that no untrusted software brought into the system, it shall be detected and removed	(virus scanners)
<G7>	<RE3> IT related: ensure that no software is used which bypasses TSFs, do not share devices with other users of a LAN	(organisational: do not use „bad“ software and „bad“ connections)

For the product <P4> the functional requirements have to be met by the IT environment (Windows NT screen saver). For description and arguments regarding <G4>b refer to <G4>a above.

Note that there is no *Security Requirements for the IT Environment* for the *Security Objective* <G5>. For <G5> users must follow the instructions to keep the password secret. This is an organisational measure.

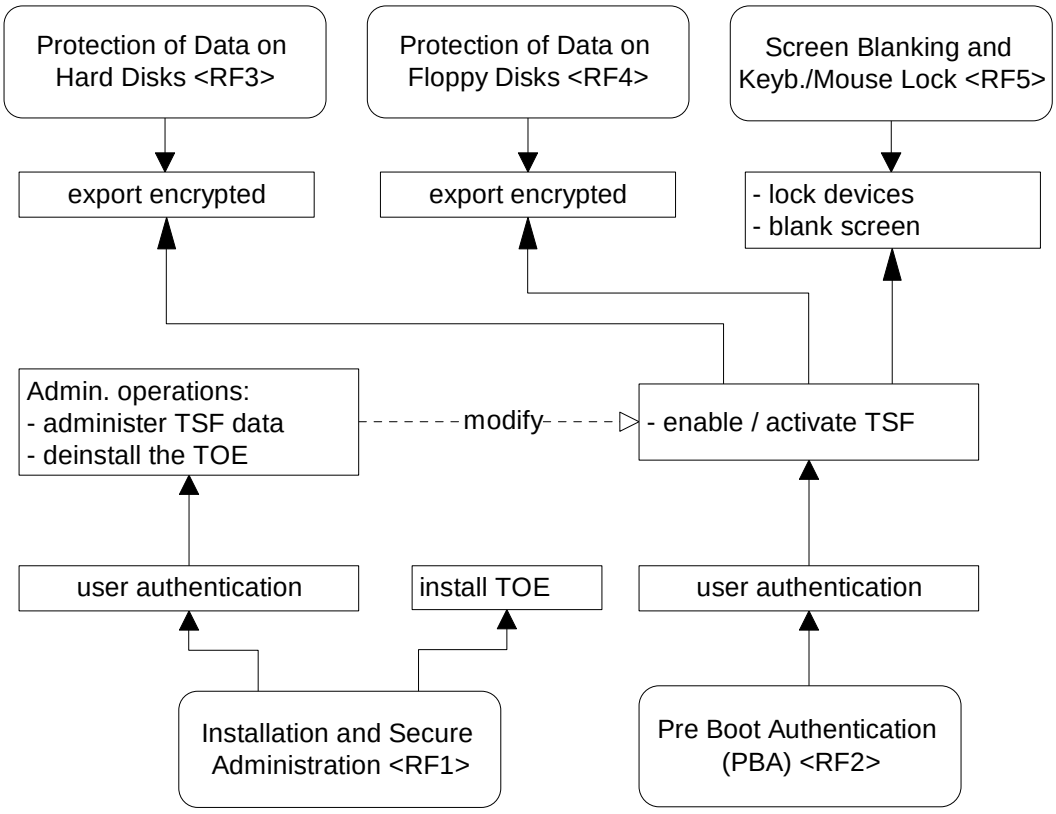
In case of the product <P4> the security must be provided by the Windows NT screen saver in a similar way like <RF5> to response to the *Security Objective* <G4>b.

Regarding the *Security Objectives* <G6> and <G7> the *IT Environment* must have specific characteristics as indicated above. To ensure this users shall follow the instructions and may additionally use other IT products to respond to those objectives.

Consistency of Security Requirements

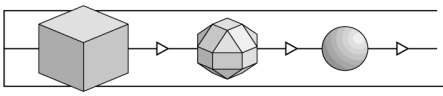
It shall further be demonstrated that the set of security requirements together forms a mutually supportive and internally consistent whole.

The figure below shows that the functional security requirements are mutually supportive and internally consistent.



The main goal of using the TOE is to protect user data stored on hard disks (<RF3>), to protect user data on protected floppy disks (<RF4>), and to protect the computer when the authorised user is temporarily absent (<RF5>). Basically, this is achieved by export functions and by screen blanking and keyboard / mouse locking. This requires users to be authenticated (<RF2>). Otherwise user data are not provided to the user. All security functions must be installed once and enabled. They use TSF data when being active. It is ensured that only authorised users can modify or deinstall the TSF (<RF1>).

In case of the product <P4> the *Security Objective* <G4>b replaces <G4>a. The IT environment provides security in a similar way as the TOE. So, the *TOE Functional Requirement* <RF5> is replaced by the *Security Requirement for the IT Environment* <RE1>. Hence, the consistency is shown even for product <P4>.



The TOE does not provide any measure or mechanism to protect itself. Therefore, the *Security Requirement for the IT Environment* <RE2> is necessary to ensure that the TOE is not modified and its TSF data are not disclosed. Otherwise the TOE will miss to provide the security defined above.

The *Security Requirement for the IT Environment* <RE3> is necessary to ensure that data which are exchanged with the hard disk or floppy disks are actually treated by the TSFs as required by the *TOE Functional Requirement* <RF3> and <RF4>.

Assurance Requirements and Strength of Security Functions

The *TOE Assurance Requirements* (section 0) cover all aspects to ensure that the security functions provided by the TOE are actually able to response to the security problems defined in form of *TOE Security Objectives* (section 3.4.1). The assurance requirements are exactly those defined for the Evaluation Assurance Level 3. So, there is no need to further demonstrate that these requirements are useful and suitable.

The claimed rating of the minimum strength of security functions for the configuration of the TOE mentioned in section 3.3.1 („Assumptions“) is *SOF-medium*. These requirements match with the background of identified threats (expertise and available resources; section 3.3.2) on the one hand and to the security environment and the scope of the security problem (refer to section 3.3.1) on the other. From the requirements of the environment the *Security Objectives* were derived very straightforward (see section 3.8.1). So, it is argued that the claimed rating of the minimum strength of security functions is also consistent with the *Security Objectives*. All security functions base upon mechanisms which have a strength. Basically, these mechanisms are (i) user authentication and (ii) encryption using secret keys. The right password used for user authentication allows to recover the key for the encryption / decryption mechanism.

3.8.3 TOE Summary Specification Rationale

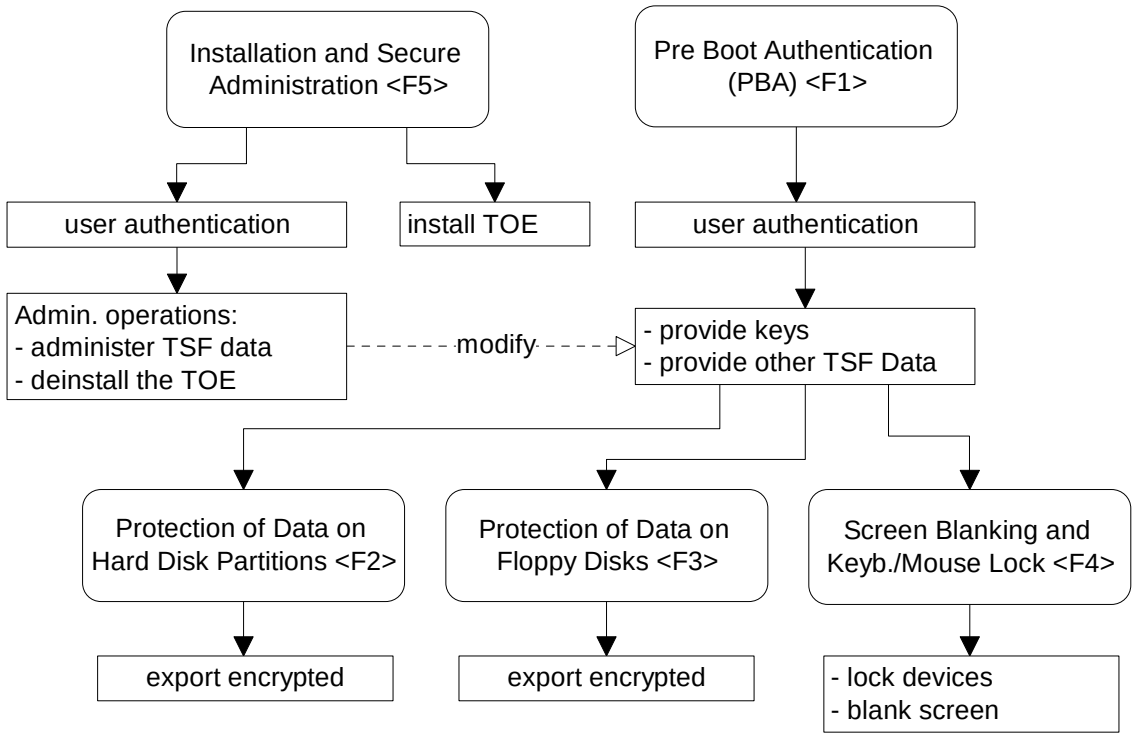
It has been shown above (section 3.6.1) that the *TOE Security Functions* are suitable to meet the TOE security requirements.

Consistency of Security Functions

The figure below shows that the set of security functions work together so as to satisfy the TOE security requirements.

The security functions <F1> though <F3> are connected together by the fact, that Protection of Data on Hard Disk Partitions <F2> and Protection of Data on Floppy Disks <F3> are only enabled to work whenever Pre-Boot Authentication (PBA) <F1> is passed. Only if correct authentication during PBA has been performed, the real mode kernel and afterwards the filter driver are loaded with the correct keys for fixed disk and floppy disk encryption. The function Screen Blanking and Keyboard / Mouse Lock <F4> uses the real mode kernel loaded by <F1> to check the password before the lock is released. This assures, that always the correct password is required for release of the screen lock. The security function Installation and Secure Administration <F5> supports all

other security functions. Administrative operations can be performed by authorised individuals only.

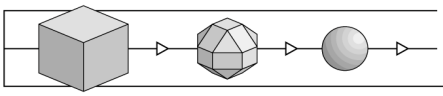


Satisfaction of Functional Requirements

Each of the security functions addresses the respective security requirement (its counterpart having a similar name, refer to the table below). Hence, the set of functional requirements are satisfied.

	<F1>	<F2>	<F3>	<F4>	<F5>
<RF1>					×
<RF2>	×				
<RF3>		×			
<RF4>			×		
<RF5>				×	

The functional requirements were selected from Part 2 of the Common Criteria to form the security behaviour described in form of security function <Fx>. The components are contained in chapter 3.9. In this chapter it is also shown that all dependencies are either satisfied or evidence is given that a non-satisfaction of a dependency is appropriate. This supports the argumentation that the security requirements are mutually supportive and internally consistent.



TOE Assurance Requirements

The *TOE Assurance Requirements* (section 0) cover all aspects to ensure that the security functions provided by the TOE are actually able to response to the security problems defined in form of *TOE Security Objectives* (section 3.4.1). The assurance requirements are exactly those defined for the Evaluation Assurance Level 3. There is no need to specify assurance measures: At Utimaco a sophisticated Quality Management System is in place. The development is organised to comply with essential requirements defined by widely accepted standards. The sites are protected by physical and organisational measures. The assessment of all these measures is the subject of the evaluation.

The TOE does not provide any measure or mechanism to satisfy the assurance requirements. Assurance is guaranteed by the development process and by the users observing the corresponding directions. The latter are described in manuals which are evaluated together with the TOE (Guidance documents; Class AGD). The measures taken in the development process will be evaluated according to other assurance requirements of EAL3.

Strength of Security Functions

The claimed rating of the minimum strength of security functions is *SOF-medium*. These requirements match with the background of identified threats (expertise and available resources) on the one hand and to the security environment and the scope of the security problem (refer to section 3.3.1) on the other. All security functions base upon mechanisms which have a strength. Basically, these mechanisms are (i) user authentication and (ii) encryption using secret keys. The right password used for user authentication allows to recover the key for the encryption/decryption mechanism. The function *Screen Blanking and Keyboard/Mouse Lock <F4>* itself has no strength, but the authentication mechanism is used to unlock the user's interface.

3.8.4 PP Claims Rationale

This Security Target does not make any claim that the TOE conforms with the requirements of a *Protection Profile*. As a result the chapter *PP Claims Rationale* is omitted.

3.9 Annexes

3.9.1 Annex A: Functional Components for <RF1>

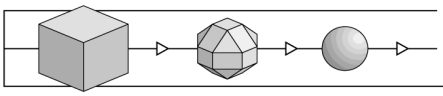
Only „authorised individuals (users)“ may perform administrative operations (SFP2).

FIA_UAU.2 User authentication before any action

FIA_UAU.2	User authentication before any action, requires that users authenticate themselves before any action will be allowed by the TSF.
Management:	FIA_UAU.2 The following actions could be considered for the management functions in FMT: a) management of the authentication data by an administrator; b) management of the authentication data by the user associated with this data.
Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of Identification Actually, before user authentication users may backup, restore or repair of the system kernel of SGE. But these are not TSF-mediated actions. In addition, before the actual user authentication takes place there may be challenge response password transfer. But this action is regarded as being a part of the user authentication itself. Note: that there is no need to include the function *Timing of identification (FIA_UID.1)* because the users are either not identified (standard user administration) or identification is inseparable linked up with the authentication process (extended user administration).

FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1	Management of Security Functions Behaviour allows the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable.
Management:	FMT_MOF.1



The following actions could be considered for the management functions in FMT Management:

a) managing the group of roles that can interact with the functions in the TSF;

Hierarchical to: no other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [deinstall SGE (disable the security functions) or modify the behaviour of the security functions (refer to the list given in section 3.5.1..1)][10] to [authorised users][11].

Dependencies: FMT_SMR.1 Security Roles

FMT_MTD.1 Management of TSF Data

FMT_MTD.1 Management of TSF Data allows authorised users to manage TSF data.

Management: FMT_MTD.1

The following actions could be considered for the management functions in FMT Management:

a) managing the group of roles that can interact with the TSF data.

Hierarchical to: no other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [modify or add][12] [a password][13] to [authorised users][14]. [In case of the extended user administration accounts can also be deleted.]

Dependencies: FMT_SMR.1 Security Roles

Note: that due to assumption <A3> there is actually only one role. Therefore, there is no need to add the function *Security Roles (FMT_SMR.1)*. Nevertheless, the TOE is able to recognise the roles „user“ and „administrator“ by checking passwords. Refer to section 3.3.3.

---

10 [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions]

11 [assignment: the authorised identified roles]

12 [selection: change_default, query, modify, delete, clear, [assignment: other operations]

13 the [assignment: list of TSF data]

14 [assignment: the authorised identified roles]

3.9.2 Annex B: Functional Components for <RF2>

Only authorised users may start / boot the operating system from an encrypted device (especially from the hard disk) to use the computer (SFP3). This requirement must be fulfilled to support SFP1.

FIA_UAU.2 User authentication before any action

FIA_UAU.2 User authentication before any action, requires that users authenticate themselves before any action will be allowed by the TSF.

Management: FIA_UAU.2

The following actions could be considered for the management functions in FMT:

a) management of the authentication data by an administrator;

b) management of the authentication data by the user associated with this data.

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of Identification

Note: that there is no need to include the function *Timing of identification (FIA_UID.1)* because the users are either not identified (standard user administration) or identification is inseparable linked up with the authentication process (extended user administration).

FMT_MTD.1 Management of TSF Data

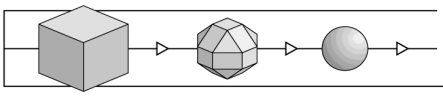
FMT_MTD.1 Management of TSF Data allows authorised users to manage TSF data.

Management: FMT_MTD.1

The following actions could be considered for the management functions in FMT Management:

a) managing the group of roles that can interact with the TSF data.

Hierarchical to: no other components.



FMT_MTD.1.1 The TSF shall restrict the ability to [modify][15] [a password][16] to [authorised users][17].

Dependencies: FMT_SMR.1 Security Roles

Note: that due to assumption <A3> there is actually only one role. Therefore, there is no need to add the function *Security Roles (FMT_SMR.1)*. Nevertheless, the TOE is able to recognise the roles „user“ and „administrator“ by checking passwords. Refer to section 3.3.3.

3.9.3 Annex C: Functional Components for <RF3>

Only authorised users may access user data on the hard disk protected by the TOE. This means, access to user data is controlled (access control, SFP5).

The *Common Criteria* distinguish between *inter-TSF transfer* and *transfer outside TSF control*. The *inter-TSF transfer* is defined for a distributed TOE where the TOE communicates with a remote trusted IT product. Exchange of data is called *transfer outside TSF control* if there is no TSF (or its characteristics are unknown) on the remote IT product.

In the case of TOE the hard disk can be regarded as external IT products. User data which are written onto hard disk are actually brought outside the *TSF Scope of Control (TSC)* since these encrypted user data are not under control of any TSF (but protected using the TOE) when the computer is switched off (refer to <T1> with <M1>). Hence, appropriate export and import functions are used to describe the behaviour of SGE.

FDP_ACC.1 Subset Access Control (Policy)

FDP_ACC.1 Subset Access Control requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.

Management: for FDP_ACC.1 and FDP_ACC.2

There are no management activities foreseen for this component.

Hierarchical to: no other components.

FDP_ACC.1.1 The TSF shall enforce the [above SFP 1][18] [whenever user data stored on the hard disk are accessed][19].

---

15 [selection: change_default, query, modify, delete, clear, [assignment: other operations]

16 the [assignment: list of TSF data]

17 [assignment: the authorised identified roles]

18 [assignment: access control SFP]

Dependencies: FDP_ACF.1 Security Attribute Based Access Control

Note: that there is no need to include the function *Security Attribute Based Access Control (FDP_ACF.1)* since the policy is actually enforced by the export / import functions.

FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1 Export of user data without security attributes requires that the TSF enforce the appropriate SFPs when exporting user data outside the TSF. User data that is exported by this function is exported without its associated security attributes.

Management: FDP_ETC.1

There are no management activities foreseen for this component.

Hierarchical to: No other components.

FDP_ETC.1.1 The TSF shall enforce the [above SFP 1][20] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1 Import of user data without security attributes requires that the security attributes correctly represent the user data and are supplied separately from the object.

Management: FDP_ITC.1, FDP_ITC.2

The following actions could be considered for the management functions in FMT Management:

a) The modification of the additional control rules used for import.

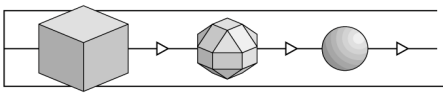
Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [above SFP 1][21] when importing user data, controlled under the SFP, from outside of the TSC.

---

19 on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

20 [assignment: access control SFP(s) and / or information flow control SFP(s)]



FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [not applicable: there are no rules][22].

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3 Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Management: FMT_MSA.3

The following actions could be considered for the management functions in FMT Management:

a) managing the group of roles that can specify initial values;

b) managing the permissive or restrictive setting of default values for a given access control SFP.

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [above SFP 1][23] to provide [restrictive][24] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [no roles][25] to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

FMT_MSA.1 Management of security attributes

---

21 [assignment: access control SFP and / or information flow control SFP]

22 [assignment: additional importation control rules]

23 [assignment: access control SFP, information flow control SFP]

24 [selection: restrictive, permissive, other property]

25 the [assignment: the authorised identified roles]

FMT_SMR.1 Security roles

Note: It is not necessary to include the functions *Management of security attributes (FMT_MSA.1)* and *Security roles (FMT_SMR.1)*. The management of other attributes needed for the present TSF is covered by the function *Installation and Secure Administration* <RF1> (see 3.5.1..1). The function *Pre-Boot Authentication (PBA)* <RF2> (see 3.5.1..2) provides the key. For its set-up and administration refer again to *Installation and Secure Administration* <RF1> (see 3.5.1..1).

3.9.4 Annex D: Functional Components for <RF4>

Only authorised users may access user data on floppy disks protected by the TOE. This means, access to user data is controlled (access control, SFP6).

The *Common Criteria* distinguish between *inter-TSF transfer* and *transfer outside TSF control*. The *inter-TSF transfer* is defined for a distributed TOE where the TOE communicates with a remote trusted IT product. Exchange of data is called *transfer outside TSF control* if there is no TSF (or its characteristics are unknown) on the remote IT product.

In the case of TOE the floppy disks can be regarded as external IT products. User data which are written onto floppy disks are actually brought outside the *TSF Scope of Control (TSC)* since these encrypted user data are not under control of any TSF (but protected using the TOE) when the computer is switched off (refer to <T2> with <M2>). Hence, appropriate export and import functions are used to describe the behaviour of SGE.

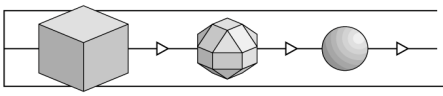
FDP_ACC.1 Subset Access Control (Policy)

FDP_ACC.1	Subset Access Control requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.
Management:	for FDP_ACC.1 and FDP_ACC.2 There are no management activities foreseen for this component.
Hierarchical to:	no other components.
FDP_ACC.1.1	The TSF shall enforce the [above SFP 1][26] [whenever user data stored on the protected floppy disks are accessed][27].
Dependencies:	FDP_ACF.1 Security Attribute Based Access Control

---

26 [assignment: access control SFP]

27 on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]



Note: there is no need to include the function *Security Attribute Based Access Control (FDP_ACF.1)* since the policy is actually enforced by the export / import functions.

FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1 Export of user data without security attributes requires that the TSF enforce the appropriate SFPs when exporting user data outside the TSF. User data that is exported by this function is exported without its associated security attributes.

Management: FDP_ETC.1

There are no management activities foreseen for this component.

Hierarchical to: No other components.

FDP_ETC.1.1 The TSF shall enforce the [above SFP 1][28] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1 Import of user data without security attributes requires that the security attributes correctly represent the user data and are supplied separately from the object.

Management: FDP_ITC.1, FDP_ITC.2

The following actions could be considered for the management functions in FMT Management:

a) The modification of the additional control rules used for import.

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [above SFP 1][29] when importing user data, controlled under the SFP, from outside of the TSC.

---

28 [assignment: access control SFP(s) and / or information flow control SFP(s)]

29 [assignment: access control SFP and / or information flow control SFP]

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [not applicable: there are no rules][30].

Dependencies:

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3 Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Management: FMT_MSA.3

The following actions could be considered for the management functions in FMT Management:

a) managing the group of roles that can specify initial values;

b) managing the permissive or restrictive setting of default values for a given access control SFP.

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [above SFP 1][31] to provide [restrictive][32] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [no roles][33] to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

FMT_MSA.1 Management of security attributes

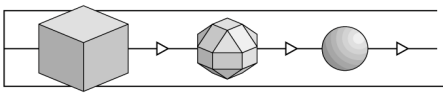
---

30 [assignment: additional importation control rules]

31 [assignment: access control SFP, information flow control SFP]

32 [selection: restrictive, permissive, other property]

33 the [assignment: the authorised identified roles]



FMT_SMR.1 Security roles

Note: It is not necessary to include the functions *Management of security attributes (FMT_MSA.1)* and *Security roles (FMT_SMR.1)*. The management of other attributes needed for the present TSF is covered by the function *Installation and Secure Administration* <RF1> (see 3.5.1..1). The function *Pre-Boot Authentication (PBA)* <RF2> (see 3.5.1..2) provides the key. For its set-up and administration refer again to *Installation and Secure Administration* <RF1> (see 3.5.1..1).

3.9.5 Annex E: Functional Components for <RF5>

The TOE shall provide means to protect the computer when the authorised user is temporarily absent without the need to switch it off (SFP4).

FTA_SSL.1 TSF-initiated Session Locking

FTA_SSL.1 TSF-initiated Session Locking includes system initiated locking of an interactive session after a specified period of user inactivity.

Management: FTA_SSL.1

The following actions could be considered for the management activities in FMT:

a) specification of the time of user inactivity after which lock-out occurs for an individual user;

b) specification of the default time of user inactivity after which lock-out occurs;

c) management of the events that should occur prior to unlocking the session.

Hierarchical to: no other components.

FTA_SSL.1.1 The TSF shall lock an interactive session after [after some time (length installable) of user inactivity][34] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access / display devices other than unlocking the session.

---

34 [assignment: time interval of user inactivity]

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [Re-authenticating (FIA_UAU.6, see below)][35].

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.2 User-initiated Locking

FTA_SSL.2 User-initiated Locking provides capabilities for the user to lock and unlock the user's own interactive sessions.

Management: FTA_SSL.2

The following actions could be considered for the management activities in FMT:

a) management of the events that should occur prior to unlocking the session.

Hierarchical to: no other components.

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [Re-authenticating (FIA_UAU.6, see below)][36].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.1 Timing of authentication

FIA_UAU.1 Timing of authentication, allows a user to perform certain actions prior to the authentication of the user's identity.

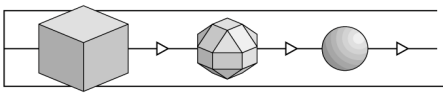
Management: FIA_UAU.1

The following actions could be considered for the management functions in FMT:

---

35 [assignment: events to occur]

36 [assignment: events to occur]



a) management of the authentication data by an administrator;

b) management of the authentication data by the associated user;

c) managing the list of actions that can be taken before the user is authenticated.

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [no TSF-mediated actions][37] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Note: that there is no need to include the function *Timing of identification (FIA_UID.1)* because the users are either not identified (standard user administration) or identification is inseparable linked up with the authentication process (extended user administration).

FIA_UAU.6 Re-authenticating

FIA_UAU.6 Re-authenticating, requires the ability to specify events for which the user needs to be re-authenticated.

Management: FIA_UAU.6

The following actions could be considered for the management functions in FMT:

a) if an authorised administrator could request re-authentication, the management includes a re-authentication request.

Hierarchical to: no other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [that the user requests to restore the screen contents and to unlock keyboard / mouse. If the user has successfully been authenticated, the screen contents is restored and the keyboard / mouse is unlocked to operate the computer][38].

Dependencies: No dependencies.

---

37 [assignment: list of TSF mediated actions]

38 [assignment: list of conditions under which re-authentication is required]

4 Remarks and Recommendations concerning the Certified Object

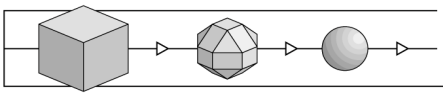
24 The statements given in chapter 2 are to be considered as the outcome of the evaluation.

25 The Certification Body has the following additional information and recommendations for the user:

- It is highly recommended to contact the sponsor for further guidance if it is intended to use the certified products on laptops or notebooks. This recommendation is based on the corresponding statement in the Security Target: „SGE provides special mechanisms for working with the suspend operation on different laptop or notebook computers. However, a correct functionality together with the suspend operation cannot be guaranteed for every transportable computer model.“

- Due to the fact that PCs can be used in peer-to-peer LANs, users should observe the following statement in the Security Target: „Security is also inactive, when the secured PC is included in a peer-to-peer LAN and parts of its hard disk(s) are accessible to other users within this LAN.

- As far as the installation / configuration process is concerned, users should observe the following statement in the Security Target: „The system can be installed by using a predefined configuration file. In this case the configuration file contains the settings, with which SGE has to be installed and a system administrator is not required for installation. This feature must not be used, when the certified operation of SGE is required.”



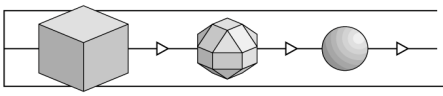
(This page is intentionally left blank.)

5 Annex

5.1 Glossary

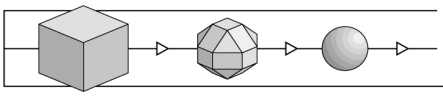
This glossary provides descriptions of the expressions used in this brochure, but does not guarantee their completeness or general validity. The term *security* here is always used in the context of information technology.

Accreditation	– A process to confirm that an evaluation facility complies with the requirements stipulated by the DIN EN 45001 standard. Accreditation is performed by an *accreditation body.* Accreditations from bodies represented in the German Accreditation Council (DAR) are generally recognised. – Result of an accreditation procedure.
Availability	Classical security objective: Data should always be available to authorised persons, i.e. this data should neither be made inaccessible by unauthorised persons nor be rendered unavailable due to technical defects.
Certificate	Summary representation of a certification result, issued by the certification body.
Certification	Independent confirmation of the correctness of an evaluation. This term is also used to describe the overall process consisting of evaluation, monitoring and subsequent issue of certificates and certification reports.
Certification body	An organisation which performs certifications (see also „Trust Centre“ for a second meaning).
Certification ID	Code designating a certification process.
Certification report	Report on the object, procedures and results of certification; this report is issued by the certification body.
Certification scheme	A summary of all principles, regulations and procedures applied by a certification body.
Certifier	Employee at a certification body authorised to carry out certification and to monitor evaluations.
Common Criteria	Security criteria derived from the US Orange Book / Federal Criteria, European ITSEC and Canadian CTCPEC, and intended to form an internationally accepted security evaluation standard.
Confidentiality	Classical security objective: Data should only be accessible to authorised persons.



Confirmation Body	Body that issues security confirmations in accordance with SiG and SigV for technical components (suitability) and trust centres (implementation of security concepts)
DebisZERT	Name of the debis IT Security Services Certification Scheme.
Digital Signature Act - SigG	§3 of legislation on Information and Communications Services Act (IuKDG).
Digital Signature Ordinance – SigV	Official regulations concerning the implementation of the German Digital Signature Act, having the force of law.
EN 45000	A series of European standards applicable, in particular, to evaluation facilities and certification bodies.
Evaluation	Assessment of an (IT) product, system or service against published IT security criteria or IT security standards.
Evaluation facility	The organisational unit which performs evaluations.
Evaluation level	Refer to „Security level“.
Evaluation report	Report on a single aspect of an evaluation (see Individual evaluation report) or evaluation technical report (ETR).
Evaluation technical report	Final report written by an evaluation facility on the procedure and results of an evaluation (abbreviated as „ETR“ in the ITSEC context).
Evaluator	Person in charge of an evaluation at an evaluation facility.
Individual evaluation report	Report written by an evaluation facility on individual evaluation aspects as part of an evaluation.
Initial certification	The first certification of an (IT) product, system or service.
Integrity	Classical security objective: Only authorised persons should be capable of modifying data.
IT component	A discrete part of an IT product or IT system, well distinguished from other parts.
IT product	Software and / or hardware which can be procured from a supplier (manufacturer, distributor).
IT service	A service depending on the support by IT products and / or IT systems.
IT system	– An inherently functional combination of IT products. – (ITSEC:) A real installation of IT products with a known operational environment.

ITSEC	Information Technology Security Evaluation Criteria: European de facto standard for the evaluation of IT products and IT systems.
ITSEM	Information Technology Security Evaluation Manual. This manual on ITSEC applies in particular to evaluation processes.
Licence (personal)	Confirmation of a personal qualification (in the context of debisZERT here).
Licence agreement	An agreement between an evaluation facility and a certification body specifying procedures and responsibilities for evaluation and certification.
Licensing	Evaluation of organisation and qualification of an evaluation facility with respect to an intended licence agreement (to become a CLEF).
Manufacturer's laboratory	An organisational unit belonging to the manufacturer of a product /system or the supplier of a service, charged with performing evaluation of that product, system or service.
Milestone plan	A project schedule for the implementation of evaluation and certification processes.
Monitoring	Procedure implemented by the certification body in order to check whether an evaluation is performed correctly (compliance with criteria, use of standard processes and appraisal techniques etc.).
Pre-certification	Confirmation of the results of a preliminary investigation of a product-specific or process-specific security standard or a security-related tool (with a view to later certification).
Problem report	Report sent by an evaluation facility to the certification body and concerning special problems during evaluation, e. g. concerning the interpretation of IT security criteria.
Process ID	ID designating a certification or confirmation process within debisZERT.
Re-certification	Renewed certification of a previously certified object due to a new version following modification; re-certification might also be required after a change of tools, production / delivery processes and security criteria.
Recognition (agreement)	Declaration and confirmation (of the equivalence of certificates and licences).



Regulatory Authority for Telecommunications and Posts	The authority responsible in accordance with §66 of the German Telecommunications Act (TKG).
Right of disposal	In this case: Authorisation to allow all inspections of a product, system or service as part of evaluation and certification.
Security certificate	Refer to „Certificate“.
Security confirmation	In debisZERT: A legally binding confirmation of security features extending beyond the scope of a certificate, e. g. a confirmation according to SigG / SigV.
Security criteria	Normative document that may contain technical requirements for products, systems and services, but at least describes the evaluation of such requirements.
Security function	Function of an IT product or IT system for counteracting certain threats.
Security level	Many security criteria (e.g. ITSEC, CC) define a metric to indicate various levels of security relating to different requirements for the object to be certified and the degree of detail needed during evaluation.
Security specification	Security-related functional requirements for products, systems and services.
Security standards	A joint expression encompassing security criteria and security specifications.
Service type	Particular type of service (DLB) offered by debisZERT.
Sponsor	A natural or legal person who (in this case) issues an order for certification or evaluation, and who must possess a sufficient right of disposal for the object to be certified or evaluated, respectively.
System accreditation	Procedure of accepting an IT system or IT service for usage (considered here from the perspective of adequate security) in a specific environment and/or application.
Trust centre	A centre which confirms the relationship between signature keys and persons by means of electronic certificates - such a centre is termed „certification body“ in the Digital Signature Act.
ZKA criteria	Security criteria used by the central credit committee (ZKA) in Germany

5.2 References

/A00/ Lizenzierungsschema, debisZERT, Version 1.1, 16.12.98

[Licensing Scheme]

/ALG/ Anhang zu „Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98 im Bundesanzeiger Nr. 31 v. 14.02.98“, http://www.regtp.de/Fachinfo/Digitalsign/start.htm

[Annex to „Official Announcement concerning the Digital Signature according to the Digital Signature Act and Signature Ordinance by February 9, 1998 published in Bundesanzeiger No. 31, February 14, 1998“]

/BSIG/ Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG), BGBl. I. vom 17. Dezember 1990, Seite 2834 ff.

[Act on the Establishment of the German Information Security Agency, BGBl. I. from 17th December 1990, Page 2834]

/CC/ Common Criteria for Information Technology Security Evaluation, CCIB-98-026, CCIB-98-027, CCIB-98-027A, CCIB-98-028, Version 2.0, Mai 1998

/EBA/ Kriterien für die sicherheitstechnische Bewertung und Konstruktion von CIR-Netzkomponenten, Eisenbahn-Bundesamt, Version 1.0 vom 8.2.94

[Criteria for Security-Related Evaluation and Construction of CIR Network Components, Federal Railway Office, version 1.0 from 8.2.94]

/ITSEC/ Information Technology Security Evaluation Criteria (ITSEC), Version 1.2 (1991), ISBN 92-826-3004-8

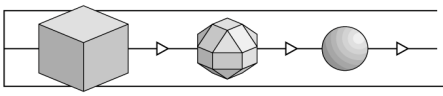
/ITSEM/ Information Technology Security Evaluation Manual (ITSEM), Version 1.0 (1993), ISBN 92-826-7087-2

/IuKDG/ Gesetz zur Regelung der Rahmenbedingungen für Informations- and Kommunikationsdienste (Informations- and Kommunikationsdienste-Gesetz - IuKDG), BGBl. I. vom 28. Juli 1997, Seite 1872 ff.

[Information and Communication Services Act, BGBl. I. from 28th July 1997, Page 1872]

/JIL/ Joint Interpretation Library, Version 1.04, December 1997

/Mkat12/ Maßnahmenkatalog nach §12 Abs. 2, Regulierungsbehörde für Telekommunikation und Post,
http://www.RegTp.de/Fachinfo/Digitalsign/start.htm



[Catalogue of Security Measures in accordance with §12 Abs. 2, Regulatory Authority for Telecommunications and Posts]

/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6, Regulierungsbehörde für Telekommunikation und Post,
http://www.RegTp.de/Fachinfo/Digitalsign/start.htm

[Catalogue of Security Measures in accordance with §16 Abs. 6, Regulatory Authority for Telecommunications and Posts]

/SigG/ Article 3 of /IuKDG/

/SIGV/ Verordnung zur digitalen Signatur (Signaturverordnung - SigV), BGBl. I. vom 27.10.1997, Seite 2498 ff.

[Digital Signature Ordinance, BGBl. I. from 27th October 1997, Page 2498 ff.]

/TKG/ Telekommunikationsgesetz (TKG), BGBl. I. vom 25.7.1996, Seite 1120

[Telecommunications Act, BGBl. I. from 25.7.1996, Page 1120]

/V01/ Certificates in accordance with ITSEC/CC, Service type 1, debisZERT, Version 1.4E, 16.12.98

/V02/ Confirmations for Products in accordance with the German Digital Signature Act, Service type 2, debisZERT, Version 1.4E, 16.12.98

/V04/ Certificates recognised by the BSI, Service type 4, debisZERT, Version 1.4E, 16.12.98

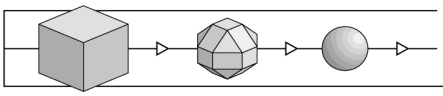
/Z01/ Certification Scheme, debis IT Security Services, Version 1.4E, 16.12.98

/Z02/ Certified IT Products, Systems and Services, debisZERT, Version 1.1E dated 16.12.98 (consecutively numbered issues)

5.3 Abbreviations

AA	Work instructions
AIS	Request for an interpretation of security criteria
BSI	Bundesamt für Sicherheit in der Informationstechnik [German Information Security Agency]
BSIG	Act on the Establishment of the BSI
CC	Common Criteria for Information Technology Security Evaluation
CLEF	Commercially licenced evaluation facility (under debisZERT) (cf. ITSEF)

CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]
DBAG	Deutsche Bahn AG [German Railways AG]
debisZERT	Certification Scheme of debis IT Security Services
DEKITZ	Deutsche Akkreditierungsstelle für Informations- und Telekommmunikations-technik [German Accreditation Body for Information and Telecommunication Technology]
DLB	Service type
EBA	Eisenbahn-Bundesamt [Federal German Railway Office]
ETR	Evaluation Technical Report
IT	Information technology
ITSEC	IT Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	IT Security Evaluation Manual
IuKDG	German Information and Communication Services Act
LG	Management Board
RegTP	Regulierungsbehörde für Telekommunikation und Post [Regulatory Authority for Telecommunications and Posts]
SigG	German Digital Signature Act
SigV	German Digital Signature Ordinance
TKG	German Telecommunications Act
TOE	Target of Evaluation
ZKA	Zentraler Kreditausschuß [German Central Credit Committee]
ZL	Head of the Certification Body
ZZ	Person in charge of a certification procedure (responsible certifier)



(This page is intentionally left blank.)

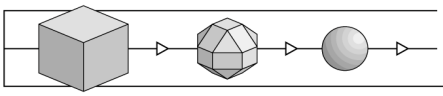
6 Re-Certification

26 When a certified object has been modified, a re-certification can be performed in accordance with the rules of debisZERT. The annexes to this chapter 6 (ordered by date of issuance) describe the type of modification, the new product version and the certification status.

27 If current findings in the field of IT security affect the security of a certified object, a technical annex to this certification report can be issued.

28 Re-certification and new technical annexes will be announced in the brochure /Z02/, also published on WWW.

29 The annexes are numbered consecutively.



End of initial version of the certification report.