Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

for

USB Storage Media

Common Criteria

BSI-PP-0025

Version 1.4, 27.03.06

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

Disclaimer: This report is the English translation of the document “Common Criteria Schutzprofil für USB-Datenträger, BSI-PP-0025-2006, Version 1.4, 19. April 2006”. In cases of doubt the German version shall prevail.

Remarks and Comments related to this Protection Profiles should be addressed to:

CONTACT ADDRESS:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
D-53133 Bonn, Deutschland
Tel +49 228 9582-0
Fax +49 228 9582-5400
Email bsi@bsi.bund.de

Contents

1 Introduction

1.1 PP identification

1	Title:	Protection Profile for USB Storage Media BSI-PP-0025
2	Version:	1.4
3	Publishing date:	27.03.2006
4	Sponsoring organisation:	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), Bonn
5	Applicant:	Fachhochschule Bonn-Rhein-Sieg (Bonn-Rhine-Sieg University of Applied Sciences), St. Augustin
6	Author:	Thomas Gilles
7	TOE:	USB storage media
8	EAL:	EAL2+
9	Search terms:	USB storage medium (media), USB stick, USB memory, USB hard drive, USB key drive, USB flash drive
10	CC version used for: development	2.1 Incorporates all of the final interpretations published as of 27.03.2006

1.2 PP overview

11 This protection profile considers all mass storage media which can be connected to the USB interface. Such devices are referred to as USB storage media.

12 The confidential data in the memory area of a USB storage medium must not fall into the hands of unauthorised persons if the USB medium is lost, misplaced or stolen. Furthermore, unauthorised persons must not be able to delete or manipulate confidential data on the storage medium. To this end, this protection profile defines a basic set of security requirements intended to maintain the confidentiality of the data in the event of logical or physical attacks. The requirements also define how data integrity is to be maintained in the event of a failure.

13 A key aspect of the user-friendly IT security offered by a USB storage medium is that the security functions are completely implemented within the storage medium itself. This makes it possible to use a PP-compliant USB data storage medium in a number of host systems since the latter are not subject to software requirements.

14 One single authentication process is enough to create a link to the confidential data. After authentication, the storage medium provides its security service transparently.

15 The protection profile only specifies hardware assumptions if they are absolutely essential. This makes a wide range of technical solutions possible.

16 Manufacturers may, at their own discretion, enhance the security provided by products which conform to this protection profile by adding extra security functions. The PP contains some points of guidance on this issue in the form of application notes. The enhancements can be specified in the Security Targets (STs), which are the basis upon which a product is certified.

1.3 PP organisation

17 The protection profile (PP) primarily consists of

- the TOE description,
- the TOE security environment,
- the security objectives,
- the IT security requirements and
- the rationale.

18 The TOE description (Section 2) provides general information on the Target of Evaluation (TOE), such as the intended use and the assets requiring protection. The description is necessary in order to be able to understand the security requirements. It is important to note that a PP usually describes a category of products of the same type rather than a specific implementation.

19 The TOE security environment (Section 3) describes assumptions concerning the obligations for the environment in which the TOE is to be used. This section can be considered a set of rules for the TOE operator. The sub-sections on threats and organisational security policies detail the threats to be countered by the TOE and the relevant laws to which it has to adhere.

20 The security objectives (Section 4) give a product-independent explanation of how the TOE addresses the identified threats and complies with the organisational security policies. In addition, the security objective behind each assumption concerning TOE use is also explained.

21 The IT security requirements (Section 5) describe the security functional requirements pertaining to the TOE and its environment, and define the security assurance requirements. The requirements are specified using the semi-formal language predefined in the Common Criteria.

22 The rationale (Section 6) demonstrates that the protection profile is a complete and cohesive set of IT security requirements and that a conformant TOE fully meets the security objectives.

23 A protection profile which complies with the Common Criteria meets certain requirements concerning form, specification and structure. The most important CC abbreviations and terms are explained in Sub-sections 1.4 and 1.5.

24 To make the protection profile’s content easier to understand, application notes have been included. They contain information which is not included in the evaluation of the protection profile and is only intended as commentary. The application notes also include information concerning possible security functions which could increase security beyond the requirements of this protection profile.

1.4 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
FSP	Functional Specifications
FSUD	Funktionale Sicherheitspolitik USB-Datenträger (Security Functional Policy for USB Storage Media)
HLD	High Level Design
PP	Protection Profile
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
USB	Universal Serial Bus

1.5 Glossary of terms

Authentication attribute	Attribute required to unprotect the protected data. Can be, for example, a password, a smart card or a biometric attribute.
User	Holds the authentication attribute required to unprotect his/her protected data.
Data trace	Data, such as temporary files or log data, which remains on the host system after the TOE has been disconnected and which may make it possible to draw conclusions about confidential data in the TOE's memory.
Target of Evaluation	This term is taken from the CC and refers to the IT product/component/system whose compliance with all of the security requirements is to be evaluated. In this protection profile, the TOE is a USB storage medium.
Unprotect	Access to the data in the protected memory, permitted by means of successful authentication.
Recycle-bin function	If the user deletes a file, the host operating system moves it to a central folder on the hard disk rather than actually deleting it.
Malware	Malicious software such as viruses, worms or Trojans, which pose a potential risk to the confidentiality and integrity of the TOE data requiring protection.

Security functions	TOE security functions (TSFs) are the part of the TOE responsible for enforcing the security policy.
Memory	The part of the TOE which is used to store digital data and information. The security functions can be implemented within this memory.
Session	Period between the unprotecting of the TOE and disconnection.
Universal Serial Bus (USB)	A bus system used to connect a computer to external USB peripherals for the purpose of data exchange.
Host system	A computer with a USB interface to which the TOE is connected. The user accesses the TOE data via the computer system.
Access	The possibility to read, write or modify data on the TOE.

2 TOE description

25 In addition to a description of the Target of Evaluation (TOE), this section contains general information on the TOE, such as its intended use and the assets requiring protection.

2.1 Product type

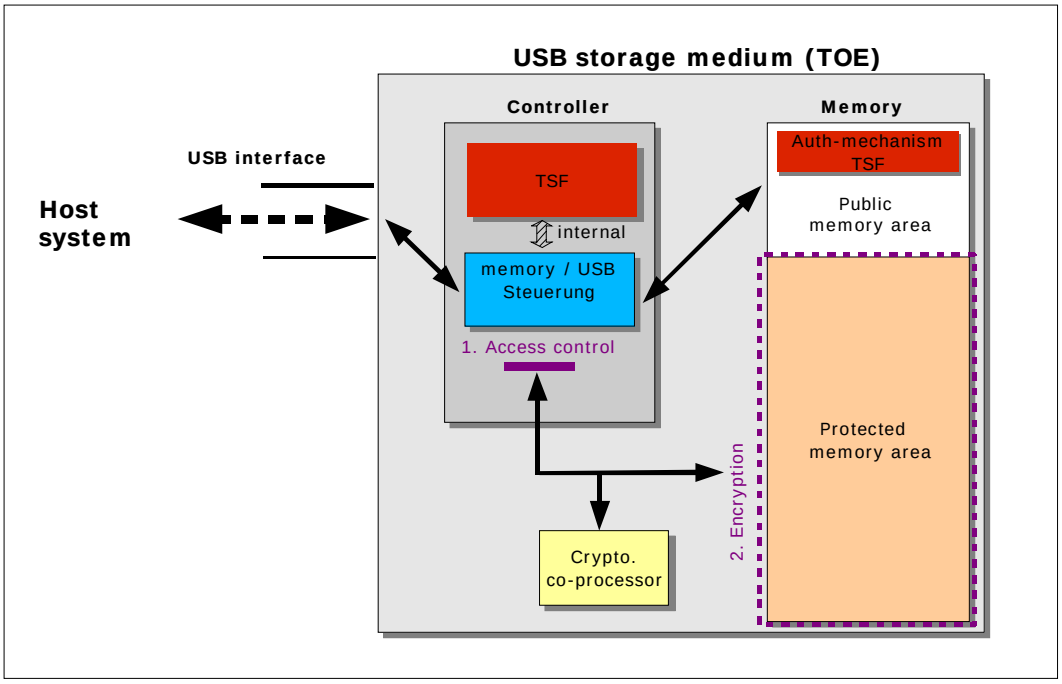
26 In this protection profile, the term “Target of Evaluation” (TOE) refers to storage media which have integrated security functionality and are intended to be connected to host systems’ USB interfaces.

> ***Application note 1***
> *It is assumed that the interface is a USB interface because such an interface facilitates automatic identification of USB peripherals during operation, without software having to be installed. This makes it possible to encapsulate the security functions in the TOE itself.*

27 The protection profile only specifies hardware assumptions if they are absolutely essential. This makes a wide range of technical solutions possible.

> ***Application note 2***
> *There are numerous different types of storage medium which can be connected to the USB interface. The storage media have different memory technologies, capacities, access speeds and service lives. These criteria are not relevant in the context of a protection profile.*

Figure 1 General structure of the TOE



28 Figure 1 shows the general structure of a USB storage medium with integrated security functionality. The components relevant to the security service are defined as follows:

- Controller: Controls the flow of information within the TOE and, via the USB interface, to the host system. It controls access to the TOE's memory areas, creating a connection to the protected memory area only if authentication is successful.
- Memory: The memory contains the TOE's data. It is divided into two areas, i.e.:
  - public memory: this area can be accessed without authentication. The data in it is not encrypted. The public area can be used to supply the user with a program with which to enter the authentication attribute (see Fig. 1). If the program used to transmit the authentication data to the controller is in the public area, that part of the public area must be considered a TSF and be write-protected.

    If the public area does not contain any security functions, it does not have to be in the TOE's memory structure. Otherwise, this memory area can be used to store data which does not require protection and which can be accessed without authentication; and

  - protected area: this area contains the user's confidential data and is thus protected by the TOE's security functions. The user is only granted access to the protected memory after successful authentication.

  Application note 3
  The public area is only relevant for the context dealt with here if it contains the authentication mechanism. Requirements concerning confidential storage of data only relate to the protected area. The protected memory area can encompass the entire TOE memory.

- Cryptographic co-processor: Used to execute the encryption/decryption processes in the TOE. The cryptographic co-processor means that the encryption/decryption processes can run completely in the actual TOE. The cryptographic co-processor can be implemented as an independent element or in the TOE's controller. If the former is the case, the co-processor does not contain the complete cryptographic key needed for decryption.

29

Application note 4
If the cryptographic co-processor contained the complete key, it would be possible to have the data decrypted by means of an unauthorised decryption command. Such a command could be generated by, for example, changing over the controller.

30 The TOE guarantees the confidentiality of the data in the protected area by means of two different security mechanisms, i.e.:

- access control and
- encryption.

31 Access control: The TOE's controller does not create a connection to the protected memory area until the user has been successfully authenticated. Access attempts without successful authentication are blocked at the TOE's hardware level.

32 Encryption: The TOE's second security mechanism is data encryption for the data in the protected memory area. Encryption secures data confidentiality specifically in the event of physical attacks on the memory.

33 A major feature of the TOE is the fact that the security functions are completely implemented within the TOE itself (see Figure 1). This means that the confidential data can be accessed via any host system. The TOE is independent of the host system's configuration. No preinstalled security software is required on the host system in order to operate the TOE. All that is needed is a USB interface and an interface-compatible operating system.

34 Once the TOE has been connected to the host system, the user has to be authenticated in order to access the data in the protected memory area. The controller handles the access-control and encryption security mechanisms. The authentication mechanism transmits the authentication attribute to the controller, which checks whether it is correct. If authentication is successful, the controller creates a logical connection to the protected memory area and the data is decrypted. The user only has to be authenticated once per session.

Application note 5
The protection profile does not stipulate any requirements regarding the technical implementation of the mechanism used to enter the authentication attribute. Authentication can be carried out, for example, by keying in the information or by means of a fingerprint scanner in the actual TOE. If the authentication attempt fails several times, the TOE should react by delaying its response. After a certain number of failed authentication attempts, the TOE's reaction could also be to destroy the confidential data since the attempts are probably linked to a penetration attack.

35 The TOE is designed to be user-friendly. Apart from the authentication required at the outset, working with the TOE is no different to working with an unsecured storage medium. Once authentication has been carried out, the user can access the TOE's file system via the host system.

36 The encryption processes run in the background and are transparent to the user. Successful authentication does not result in the entire contents of the protected memory area being decrypted. Only the actual data required for the action to be performed is decrypted and transferred to the host system.

37 If the logical connection is disrupted, e.g. due to a system crash, a power failure or the physical connection between the TOE and the host system being separated, the TOE ensures that the data in the memory remains encrypted and that the file system is not damaged. The TOE recovers to a stable and consistent state following a failure. All of its security mechanisms are re-activated. The user must be re-authenticated in order to re-gain access to the protected memory area.

Application note 6
A write-protect function in the TOE would also be of benefit to the user. Once activated (by means, for example, of a mechanical switch on the TOE housing), such a function could provide write protection for the data in the protected memory area. This function would counter any attacks from the host system on the integrity of the confidential data.

2.2 Definition of scope

38 The TOE dealt with in this protection profile is a storage medium with integrated security functionality. The following components are relevant for the evaluation: public memory area, protected memory area, controller, cryptographic co-processor and the USB interface.

39 The USB interface is the TOE's only external interface. Before being used, the TOE must be connected to a host system via the USB interface. The security service is entirely provided by the TOE itself. The TSFs are implemented in the TOE's controller but parts of them may be implemented in the public memory area. The host system does not fall within the scope of the evaluation.

40 The TOE is equipped with a cryptographic co-processor, which is used to execute the encryption/decryption processes. The cryptographic key *never* leaves the TOE.

41 The TOE cannot check whether data traces are left on the host system which make it possible to draw conclusions about the TOE's confidential data. Data traces occur when applications are used in conjunction with the TOE's data. In this context, the recycle-bin function can also pose a risk.

> ***Application note 7***
> *One of the points which this protection profile seeks to highlight is the issue of data traces. It is not possible to anticipate what data traces will be left on the host system, the TOE cannot control this factor. Consequently, the protection profile does not contain any requirements for the TOE in connection with data traces. The author recommends that functions be implemented within the TOE to remove the typical data traces on common operating systems, or that appropriate software be provided with the product. The risk could also be reduced by addressing the issue of data traces in the user manual.*

2.3 Technical flexibility

42 This protection profile is intended to cover the entire USB storage media product category. The requirements in this protection profile have been made as flexible as possible so that different technical implementations of USB storage media can be evaluated.

43 The following list contains the most important aspects with regard to implementation independence:

- authentication mechanism: there is no specification concerning the required type of authentication mechanism. Authentication can be carried out, for example, by means of a password or biometric data;
- memory structure: the choice of memory structure is discretionary apart from the requirement that there be a protected area. The memory can contain, for example, a public area;
- positioning of the cryptographic co-processor: the cryptographic co-processor can be implemented in the controller or as an independent element in the TOE;
- cryptographic algorithm: there is no specification concerning the required type of cryptographic algorithm. The specific cryptographic algorithm chosen is up to the manufacturer and thus the ST author; and
- cryptographic key: there is no specified requirement as to how the cryptographic key should be generated. One possible method, for example, is to generate it on the basis of the authentication attribute. Another possibility is for the key to be generated and integrated into the controller when the controller is produced.

2.4 Scenarios for TOE use

44 The example scenarios for the use of storage media set out below concentrate on the handling of confidential data. The scenarios illustrate typical cases in which the TOE should be used to protect confidential data.

45 Data transport

46 Data transport, i.e. transport of confidential data between host systems using a storage medium. Typical business scenarios in which confidential data has to be transported are project meetings, customer presentations and business trips. Confidential data is also often transported using storage media for private purposes, e.g. presentation of personal multi-media or submission of personal tax data.

47 Transporting the work environment (profile transport)

48 In addition to the user's confidential data, his or her work environment can be transported on a storage medium. When the storage medium is connected to a host system, the system's work environment adapts to the user's profile. The profile contains, for example, the user's wallpaper, icon arrangement and internet favourites.

49 The storage media have sufficient capacity to be able to transport complete, pre-configured applications such as Office packages, web browsers and e-mail clients. These applications are part of the work environment and are launched directly from the storage medium – no installation CD is required. This means that users have their usual work environment, with all of its applications, on the host system. Sometimes the work environment transported only includes the pre-configured applications.

50 Data back-ups

51 The term "data back-up" refers to the process of copying the confidential data residing on a host system onto a storage medium. The purpose of data back-ups is to provide protection against data loss caused, for example, by hardware damage, theft or accidental/intentional deletion. The storage medium contains a copy of the important and confidential data stored on the host system.

52 Keystore

53 The storage medium is used to store confidential keys or digital certificates. If a key is required, e.g. to encrypt an e-mail, the user connects the storage medium to the host system. The application uses the key from the storage media for the pending action. Afterwards, the user disconnects the storage media from the system and stores it in a safe place. Many asymmetric encryption procedures, such as PGP, recommend that the private key be stored on an external storage medium.

2.5 Types of data

54 The list below contains examples of data requiring protection.

55 **Business data**

- Presentations
- Business plans
- Back-ups (e.g. e-mail back-ups)
- Financial, personnel, customer, maintenance data
- Confidential e-mails
- Access data for the company network

56 **Private data**

- Passwords, PINs
- Letters, e-mails
- Confidential web access, e.g. for web banking
- Bank statements
- Address book, diary
- Personal multimedia (photos, videos, etc.)

57 **Software and keys**

- Programs
- Modules
- Algorithms
- Key data (PIN, passwords, PGP key chain)

3 TOE security environment

58 This section describes assumptions concerning the environment in which the Target of Evaluation is to be used. These assumptions therefore serve as operating requirements. In addition, all of the threats which the TOE has to counter are listed in this section.

3.1 Roles in the TOE

59 The roles and the related activities which have to be taken into account in the context of the Target of Evaluation are described below. (For a detailed list of permitted activities, please refer to the definition of the security functional policy in Section 5.1.1).

- Authorised user (S1)
  - Holds the authentication attribute required to access the TOE's protected memory area, in which the confidential data is stored.
  - Can modify the authentication attribute.

- Non-authorised user (S2)
  - Wishes to access S1's confidential data in the USB storage medium's memory (examples of confidential data are given in Section 2.5).
  - Does not have the authentication attribute to access the protected data.
  - Can obtain a USB storage medium of the same type. Can try out both logical and physical attacks on this USB storage medium.
  - Can gain possession of the TOE relatively easily since the TOE has a compact form.

3.2 Assumptions

60 This section lists the security obligations for the environment in which the Target of Evaluation is to be used and which is assumed to be implemented. It can be considered a set of rules for the TOE operator. For the sake of clarity, each assumption has been assigned a name beginning with the letter “A” (for “assumption”).

61 The justification for the assumptions is given in Section 6.3, Rationale, of this protection profile.

62 A.Ausspähen S1 ensures that his/her authentication attribute cannot be fraudulently obtained by, for example, someone else reading the password whilst it is being entered or reproducing the biometric authentication attribute.

Application note 8
It is virtually impossible for S1 to avoid leaving biometric traces (e.g. fingerprints) which can be used to reproduce his or her biometric authentication attribute. Assumption A.Ausspähen is intended to demonstrate that the possibility of reproducing a biometric authentication attribute is a potential risk.

63 A.Vertrau.WS Once S1 has unprotected the protected memory area,there are no unauthorised attempts to access the TOE from the host system or any connected networks.

64 A.Abwesend If S1 leaves the host system to which the unprotected TOE is connected, he/she takes appropriate measures to protect the data whilst absent. Appropriate measures could be, for example, locking the computer with the aid of the operating system or taking the TOE with them when they leave.

3.3 Threats

65 This section lists all of the threats as specific events which the TOE has to counter itself. For the sake of clarity, each threat has been assigned a name beginning with the letter “T” (for “threat”).

66 T.logZugriff Assuming that S2 gains possession of the TOE, he/she accesses the confidential data on the TOE. S2 gains logical access by, for example, connecting the TOE to the USB interface of a computer system.

67 T.phyZugriff Assuming that S2 gains possession of the TOE, he/she accesses the TOE’s memory by means of a physical attack. Such an attack could take the following form, for example: S2 removes the TOE’s memory and places it into another USB storage medium which he/she uses for the purpose of logical access to the memory.

68 T.AuthÄndern Assuming that S2 gains possession of the TOE, he/she sets a new authentication attribute, with the result that the data becomes unusable for S1.

69 T.Störung A failure (e.g. power failure or operating system error) stops the TOE operating correctly. As a result, confidential data remains unencrypted or the TOE’s file system is damaged.

3.4 Organisational security policies (OSPs)

70 The section on organisational security policies lists the relevant laws for which compliance must be enforced or supported by the TOE.

71 This protection profile does not specify any organisational security policies because all of the motivation to ensure IT security functionality is implicit in the form of the threats to be countered.

4 Security objectives

72 This section provides a product-independent description of how the TOE addresses the identified threats. For the sake of clarity, each security objective has been assigned a name beginning with the letter “O” (for “Objective”).

4.1 Security objectives for the TOE

73 O.logZugriff The TOE must provide a secure authentication mechanism via which only S1, following successful authentication, gains access to the protected data.

74 O.phyZugriff The TOE encrypts all of the data in the protected area of the TOE. The encryption specifically protects confidentiality in the event of physical attacks on the TOE.

75 O.AuthÄndern The TOE provides a function with which the authentication attribute can only be changed after S1 has successfully been authenticated.

76 O.Störung The TOE recovers to a stable and consistent state following a failure (e.g. power failure). The failure does not result in damage to the file system, nor to data remaining unencrypted in the TOE’s memory.

4.2 Security objectives for the IT environment

Application note 9
The IT environment is deemed to be the host system to which the TOE is connected during operation.

77 OE.Vertrau.WS Once the protected memory area has been unprotected, the TOE cannot protect itself against unauthorised access attempts from the host system. So there are no unauthorised attempts, e.g. by malware, to access the TOE via the host system and any networks connected to it.

78 OE.Abwesend Once the data has been unprotected, access to it is unrestricted while the TOE is still connected to the host system. This means that S1 has to take appropriate security measures for the duration of his/her absence from the host system in order to prevent S2 from accessing the unprotected data on the TOE.

4.3 Security objectives for the non-IT environment

79 OE.Ausspähen Since the TOE cannot recognise reproduced authentication attributes, S1 must ensure that it is not possible for others to see or reproduce his/her authentication attribute.

5 IT security requirements

80 This section contains security functional requirements for the TOE and security assurance requirements for the TOE and its environment.

81 The security functional requirements are defined in Section 5.1 “TOE security functional requirements”. They are taken from Part 2 of the CC, which contains a catalogue of security requirements in the form of semi-formal text components. Each component’s functionality, prerequisite for use and dependency on other security requirements are described there. The components can be adapted by means of defined operations.

82 The security assurance requirements are defined in Section 5.2 “TOE security assurance requirements”. They are taken from Part 3 of the CC and are intended as an aid in assessing how correctly a product has been implemented.

83 Font distinctions for operations

- The “assignment” and “selection” operations are shown in *italics.*
- The “refinement” operations are indicated by means of underlining.
- If the “assignment” and “selection” operations are not defined, the text in the square brackets is not formatted.

84 All of the text in the components listed in Section 5.1 which is neither in *italics* nor underlined is taken directly from the original text in Part 2 of the CC.

5.1 TOE security functional requirements

5.1.1 Definition of the security functional policy for USB storage media

85 Before listing the security functional requirements for the TOE, this section first defines the **security functional policy for USB storage media (FSUD),** as follows:

- permitted actions by the authorised user (S1):
  - use of the authentication mechanism,
  - reading/writing/modification of the data in the public and protected memory areas of the TOE (allow access),
  - re-authentication following a disruption in the connection between the host system and the TOE (e.g. due to physical disconnection, loss of power or an operating system error) and
  - modification of the authentication attribute;
- permitted actions by the non-authorised user (S2):
  - reading/writing/modification of the data in the public memory area (if there is one) and
  - use of the authentication mechanism.

5.1.2 TOE security functional requirements

86 This section presents the security functional requirements for the TOE.

Table 1 shows the functional requirements in this protection profile which are taken from Part 2 of the CC.

FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.6	Re-authenticating
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state

FPT_RCV.4	Function recovery

5.1.2.1 Cryptographic support (FCS)

87 FCS_CKM.1 Cryptographic key generation

88 Hierarchical to: No other components.

89 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

90 Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

91 FCS_CKM.4 Cryptographic key destruction

92 Hierarchical to: No other components.

93 FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

94 Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FMT_MSA.2 Secure security attributes

95 FCS_COP.1 Cryptographic operation

96 Hierarchical to: No other components.

97 FCS_COP.1.1 The TSF shall perform [assignment: *the encryption and decryption of the data in the TOE's protected memory area*] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

98 Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.1.2.2 Identification and authentication (FIA)

99 FIA_UAU.1 Timing of authentication

100 Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: *access to the public memory area*] on behalf of the user to be performed before the user is authenticated.

101 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.

102 Dependencies: FIA_UID.1 Timing of identification

Application note 10
If there is no public memory area, FIA_UAU.1 can be replaced by FIA_UAU.2.

Application note 11
Since the TOE concerned is a single-user system, identification is not necessary. There is only one authentication attribute, which allows access to the data in the protected memory area. It could also be possible to have a TOE on which several users each have their own memory area.

103 FIA_UAU.6 Re-authenticating

104 Hierarchical to: No other components.

105 FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *system crash, power failure, separation of the physical connection or another disruption to the connection*].

106 Dependencies: No dependencies

Application note 12
The assignment operation for the following functional component, FIA_SOS.1, is restricted to quality metrics which meet the SOF-medium requirements.

107 FIA_SOS.1 Verification of secrets

108 Hierarchical to: No other components.

109 FIA_SOS. 1 The TSF shall provide an authentication mechanism to verify that the authentication attribute meets [assignment: *a defined quality metric*].

Dependencies: No dependencies

5.1.2.3 User data protection (FDP)

110 **FDP_ACC.1 Subset access control**

111 Hierarchical to: No other components.

112 FDP_ACC.1.1 The TSF shall enforce the [assignment: *FSUD*] on [assignment: *S1's accessing of data in the TOE's protected memory area*].

113 Dependencies: FDP_ACF.1 Security attribute based access control.

Application note 13
If there is no public memory area, FDP_ACC.1 can be replaced by FDP_ACC.2.

114 **FDP_ACF.1 Security attribute based access control**

Application note 14
The text for component FDP_ACF.1.1 was adapted in line with Final Interpretation RI # 103.

115 Hierarchical to: No other components.

116 FDP_ACF.1.1 The TSF shall enforce the [assignment: *FSUD*] to objects based on the following: [assignment:

Subject	Object	Security attribute
S1	Protected memory area	Authentication attribute

],

117 FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- *permitted actions by the authorised user (S1):*
  - *use of the authentication mechanism,*
  - *reading/writing/modification of the data in the public and protected memory areas of the TOE (allow access),*
  - *re-authentication following a disruption in the connection between the host system and the TOE (e.g. due to physical disconnection, loss of power or an operating system error) and*
  - *modification of the authentication attribute;*
- *permitted actions by the non-authorised user (S2):*
  - *reading/writing/modification of the data in the public memory area (if there is one) and*
  - *use of the authentication mechanism.*

].

118 FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *no rules*].

119 FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: no rules]

120 Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.1.2.4 Security management (FMT)

121

Application note 15
The dependencies for the following component have been adapted in accordance with Final Interpretation RI # 65.

122 **FMT_MSA.1 Management of security attributes**

123 Hierarchical to: No other components.

124 FMT_MSA.1.1 The TSF shall enforce the [assignment: FSUD] to restrict the ability to [selection: *modify*, [assignment: *no other operations*]] the security attribute [assignment: *authentication attribute*] to [assignment: S1].

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Application note 16
The following functional component, FMT_SMF.1, is based on Final Interpretation RI # 65.

125 **FMT_SMF.1 Specification of Management Functions**

126 Hierarchical to: No other components.

127 FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *modification of the authentication attribute*]

128 Dependencies: No dependencies

129 FMT_SMR.1 Security roles

130 Hierarchical to: No other components.

131 FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *authorised user S1*].

132 FMT_SMR.1.2 The TSF shall be able to associate users with roles.

133 Dependencies: FIA_UID.1 Timing of identification

5.1.2.5 Protection of the TSF (FPT)

134 **FPT_FLS.1 Failure with preservation of secure state**

135 Hierarchical to: No other components.

136 FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *system crash, power failure, separation of the physical connection or another disruption to the connection*].

137 Dependencies: ADV_SPM.1 Informal TOE security policy model

138 **FPT_RCV.4 Function recovery**

139 Hierarchical to: No other components.

140 FPT_RCV.4.1 The TSF shall ensure that the [assignment: [*assignment*: *List of SF*] has the property that, *in the event of a system crash, power failure, separation of the physical connection or another failure*] the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

141 Dependencies: ADV_SPM.1 Informal TOE security policy model

5.1.2.6 Dependencies between security functional requirements

142 Table 2 shows the dependencies between the CC functional components selected for the TOE.

143 The functional components selected for this protection profile are numbered sequentially in the following table. If a component is dependent on another component, the latter is indicated in the third column. The fourth column shows the number of the component which fulfils the dependency.

Table 2: Dependencies between functional components

No.	Security functional requirements	Dependencies	Note
1	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	Fulfilled in 3
		FCS_CKM.4	Fulfilled in 2
		FMT_MSA.2	Not required (see 5.1.2.7): - the cryptographic key does not have any security attributes
2	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Fulfilled in 1
		FMT_MSA.2	Not required (see 5.1.2.7): - the cryptographic key does not have any security attributes
3	FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Fulfilled in 1
		FCS_CKM.4	Fulfilled in 2
		FMT_MSA.2	Not required (see 5.1.2.7): - the cryptographic key does not have any security attributes
4	FIA_UAU.1	FIA_UID.1	Not required (see 5.1.2.7): - the TOE does not distinguish

			between different users since it is only familiar with role S1. Consequently, identification is not required.
5	FIA_UAU.6		No dependencies
6	FIA_SOS.1		No dependencies
7	FDP_ACC.1	FDP_ACF.1	Fulfilled in 8
8	FDP_ACF.1	FDP_ACC.1	Fulfilled in 7
		FMT_MSA.3	Not required (see 5.1.2.7): - the TOE does not assign standard values to security attributes.
9	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Fulfilled in 7
		FMT_SMR.1	Fulfilled in 11
		FMT_SMF. 1	Fulfilled in 10
10	FMT_SMF.1		No dependencies
11	FMT_SMR.1	FIA_UID.1	Not required (see 5.1.2.7): - the TOE does not distinguish between different users since it is only familiar with role S1. Consequently, identification is not required.
12	FPT_FLS.1	ADV_SPM.1	Fulfilled by adapting the EAL (see Section 5.3)
13	FPT_RCV.4	ADV_SPM.1	Fulfilled by adapting the EAL (see Section 5.3)

5.1.2.7 Reasons for unfulfilled dependencies

This section explains the reasons for the unfulfilled dependencies between the functional components (see Table 2).

Re. 1, 2 and 3: Dependency FMT_MSA.2 is not necessary because the cryptographic key does not use any security attributes. No security attributes are required for the cryptographic key in order to implement security objective O.phyZugriff .

> ***Application note 17***
> *If a specific product is intended to have security attributes for the cryptographic key, the ST and functional component FMT_MSA.2 have to be adapted accordingly.*

Re. 8: Since the TOE does not assign standard values for security attributes, no dependency on FMT_MSA.3 is necessary. There is no need to assign standard values for security attributes in order to implement the O.logZugriff and O.authÄndern security objectives.

> ***Application note 18***
> *If a specific product is intended to have standard values for security attributes, the ST and functional component FMT_MSA.3 have to be adapted accordingly.*

Re. 4 and 11: The TOE only contains one role – the authorised user (S1). Consequently, a distinction between different roles based on identification, as required in FIA_UID.1, is not necessary. None of the defined security objectives requires identification in order to be implemented.

5.2 Requirements for the environment

144 The security objectives relating to the IT environment are covered by the following security requirements.

145 RE.Vertrau.WS The host system is able to prevent unauthorised accessing (e.g. by malware) of the TOE via the host system or any connected network.

146 RE.Abwesend The host system is able to block or disconnect logical access to the TOE at the request of S1.

5.3 TOE security assurance requirements

147 The security assurance requirements which the TOE has to meet are listed in the following table (Table 3: Actions required to achieve EAL2 plus ADV_SPM.1). They correspond to EAL 2 as defined in Part 3 of the Common Criteria.

Table 3: Actions required to achieve EAL2 plus ADV_SPM.1

EAL2 requirements		Developer actions
Configuration management	ACM_CAP.2	Gives TOE a unique reference name and ensures clear identification of the configuration parts in order to achieve better understanding of the TOE's composition.
Delivery and operation	ADO_DEL.1	The developer's delivery procedures are clearly defined and documented.
	ADO_IGS.1	Installation, generation and start-up procedures are dealt with in the documentation for the administrator.
Development	ADV_FSP.1	Functional specification of the TSF and its external interfaces in an informal style.
	ADV_HLD.1	Documentation of the TSF's main structural units (e.g. subsystems) and their functions.
	ADV_RCR.1	The various TSF descriptions (FSP and HLD in this specific case) must match.
	ADV_SPM.1	Proof that the TSF enforces the security policy.
Guidance documents	AGD_ADM.1	The developer must provide a system administrator's manual.
	AGD_USR.1	The developer must provide a user manual.
Tests	ATE_COV.1	Proof that the TSF has been tested against its functional specification.
	ATE_FUN.1	The TSF tests and the results have been documented.
	ATE_IND.2	The evaluator must conduct independent tests.
Vulnerability assessment	AVA_SOF.1	An analysis to ensure SOF "medium" has been carried out and documented for the SOF-relevant mechanisms (authentication mechanism).
	AVA_VLA.1	An analysis of all of the TOE's obvious vulnerabilities has been carried out and documented.

148 EAL 2 has been augmented to include component ADV_SPM.1 because of the dependencies of the following security functional requirements:

- FPT_FLS.1 Failure with preservation of secure state
- FPT_RCV.4 Function recovery

This has resulted in **EAL2+.**

5.4 Minimum strength of the TOE's security functions

149 The minimum strength of the TOE security functions implemented by probabilistic or permutation mechanisms (authentication mechanism) must reach **SOF-medium**.

6 Rationale

150 The rationale section of a protection profile is a type of quality-assurance measure by the profile's author. It analyses the preceding sections and examines whether the information in them is complete, appropriate and free of contradiction.

151 The rationale demonstrates that the protection profile is a complete and coherent set of IT security requirements and that a conformant TOE would fulfil the security needs effectively.

6.1 Security objectives rationale

152 Table 4 below shows the purpose of each security objective. It indicates which threats are countered and which assumptions are covered by the security objectives for the TOE and the security objectives for the environment.

Table 4: Relationship between security objectives and threats/assumptions

Security objective	Threat	Assumption
O.logZugriff	T.logZugriff	
O.phyZugriff	T.phyZugriff	
O.AuthÄndern	T.AuthÄndern	
O.Störung	T.Störung	
OE.Vertrau.WS	T.logZugriff T.AuthÄndern	A.Vertrau.WS
OE.Abwesend	T.logZugriff T.AuthÄndern	A.Abwesend
OE.Ausspähen	T.logZugriff T.AuthÄndern	A.Ausspähen

153 Table 4 illustrates that each threat and each assumption is addressed by at least one security objective and that each security objective addresses at least one threat or one assumption.

154 The following sections describe how the security objectives help counter the indicated threats and how the indicated assumptions are taken into account.

6.2 Countering of threats by the TOE

155 This section demonstrates for each threat that there is an adequate explanation as to why the assigned security objectives are suitable for countering it.

Table 5: Relationship between threats and security objectives

Threat	TOE security objective	Environment security objective
T.logZugriff	O.logZugriff	OE.Vertrau.WS OE.Abwesend OE.Ausspähen
T.phyZugriff	O.phyZugriff	
T.AuthÄndern	O.AuthÄndern	OE.Ausspähen OE.Abwesend OE.Vertrau.WS
T.Störung	O.Störung	

156 Explanation of the relationships in Table 5:

157 **T.logZugriff** Assuming that S2 gains possession of the TOE, he/she accesses the confidential data on the TOE. S2 gains logical access by, for example, connecting the TOE to the USB interface of a computer system.

- O.logZugriff addresses the compensation of threat T.logZugriff directly by requiring an access-control method which only grants access to the protected memory area to the authorised user (S1).
- OE.Abwesend provides additional support for measures to counter threat T.logZugriff by requiring S1 to take appropriate security measures for the duration of his/her absence from the host system in order to protect the TOE which has been unprotected.
- OE.Vertrau.WS provides additional support for measures to counter threat T.logZugriff by ruling out unauthorised access attempts from the host system and any networks connected to it, e.g. by malware.
- OE.Ausspähen provides additional support for measures to counter threat T.logZugriff by requiring S1 to ensure that it is not possible for others to see his/her authentication attribute while it is being entered or to reproduce it.

158 **T.phyZugriff** Assuming that S2 gains possession of the TOE, he/she accesses the TOE's memory by means of a physical attack. Such an attack could take the following form, for example: S2 removes the TOE's memory and places it into another USB storage medium which he/she uses for the purpose of logical access to the memory.

O.phyZugriff addresses the compensation of threat T.phyZugriff directly by requiring that the data in the protected memory area be encrypted.

159 **T.AuthÄndern** Assuming that S2 gains possession of the TOE, he/she sets a new authentication attribute, rendering the data unusable for S1.

O.AuthÄndern addresses the compensation of threat T.AuthÄndern directly by requiring that modification of the authentication attribute only be possible once S1 has been authenticated.

OE.Ausspähen provides additional support for measures to counter threat T.AuthÄndern by requiring S1 to ensure that it is not possible for others to see his/her authentication attribute while it is being entered or to reproduce it.

OE.Abwesend provides additional support for measures to counter threat T.AuthÄndern by requiring S1 to take appropriate security measures for the duration of his/her absence from the host system in order to protect the TOE which has been unprotected.

OE.Vertrau.WS provides additional support for measures to counter threat T.AuthÄndern by ruling out unauthorised access attempts from the host system and any networks connected to it, e.g. by malware.

160 **T.Störung** A failure (e.g. power failure or operating system error) stops the TOE operating correctly. As a result, confidential data remains unencrypted or the TOE's file system is damaged.

161

O.Störung addresses the compensation of threat T.Störung directly by requiring that the TOE recover to a stable and consistent state following a failure (e.g. power failure) without data remaining unencrypted or the file system being damaged.

6.3 Suitability to cover the assumptions

162 This section demonstrates for each assumption that there is an adequate explanation as to why the assigned environment security objective is suitable for covering it.

Table 6: Assumptions covered by security objectives

No.	Assumption	Security objective
1	A.Ausspähen	OE.Ausspähen
2	A.Vertrau.WS	OE.Vertrau.WS
3	A.Abwesend	OE.Abwesend

163 Explanation of the relationships in Table 6:

164 **A.Ausspähen** S1 ensures that his/her authentication attribute cannot be fraudulently obtained by, for example, someone else reading the password whilst it is being entered or reproducing the biometric authentication attribute.

OE.Ausspähen is the objective which implements the assumption. The assumption is necessary because the TOE cannot recognise reproduced authentication attributes.

165 **A.Vertrau.WS** Once S1 has unprotected the protected memory area, there are no unauthorised attempts to access the TOE from the host system or any connected networks.

OE.Vertrau.WS is the objective which implements the assumption. The assumption is necessary because the TOE cannot control access from the host system to the protected memory area once the protected area has been unprotected.

166 **A.Abwesend** If S1 leaves the host system to which the unprotected TOE is connected, he/she takes appropriate measures to protect the data whilst absent. Appropriate measures could be, for example, locking the computer with the aid of the operating system or taking the TOE with them when they leave.

OE.Abwesend is the objective which implements the assumption. The assumption is necessary because, once the protected memory area has been unprotected, the TOE cannot control whether S1 or S2 accesses the data.

6.4 Rationale for the TOE's security functional requirements

6.4.1 Rationale for the TOE's security functional requirements

167 The following table, Table 7, and the explanations relating to it show the relationship between the selected functional component and the TOE security objectives for each security functional requirement set out in this protection profile. They also illustrate how the components help meet the security objectives.

Table 7: Relationship between the TOE's security functional requirements and security objectives

No.	Component	Name	Security objective
1	FCS_CKM.1	Cryptographic key generation	O.phyZugriff
2	FCS_CKM.4	Cryptographic key destruction	O.phyZugriff
3	FCS_COP.1	Cryptographic operation	O.phyZugriff
4	FIA_UAU.1	Subset access control	O.logZugriff, O.AuthÄndern
5	FIA_UAU.6	Security attribute based access control	O.logZugriff, O.AuthÄndern
6	FIA_SOS.1	Verification of secrets	O.logZugriff, O.AuthÄndern
7	FDP_ACC.1	Timing of authentication	O.logZugriff, O.AuthÄndern
8	FDP_ACF.1	Re-authenticating	O.logZugriff, O.AuthÄndern
9	FMT_SMF.1	Management of security attributes	O.AuthÄndern
10	FMT_SMR.1	Specification of Management Functions	O.logZugriff, O.AuthÄndern
11	FMT_MSA.1	Security roles	O.AuthÄndern
12	FPT_FLS.1	Failure with preservation of secure state	O.Störung
13	FPT_RCV.4	Function recovery	O.Störung

168 Re. 1, 2 and 3: Components **FCS_CKM.1**, **FCS_CKM.4** and **FCS_COP.1** are necessary in order to encrypt the data in the protected memory area. As such, they address security objective **O.phyZugriff.** The cryptographic method and the key size must be defined in the above-mentioned components in the Security Targets (STs).

169 Re. 4: Component **FIA_UAU.1**, which requires user authentication before any TSF-mediated action, apart from access to the public memory area, addresses security objective **O.logZugriff** security objective, which specifies that logical access to the TOE must be controlled. The **O.AuthÄndern** objective is also only possible after authentication.

170 Re. 5: Component **FIA_UAU.6**, which requires re-authentication after any disruption to the connection, addresses security objectives **O.logZugriff** and **O.AuthÄndern**. It is not possible to avoid the access-control security mechanism by disrupting the connection.

171 Re. 6: Component **FIA_SOS.1** requires an authentication mechanism which ensures that the authentication attribute complies with SOF-medium. The SOF-medium authentication attribute addresses the **O.logZugriff** and **O.AuthÄndern** security objectives.

172 Re. 7: Component **FDP_ACC.1** requires subset access control and thus addresses security objectives **O.logZugriff** and **O.AuthÄndern** by requiring controlled access by S1 to the TOE's resources apart from its public memory area.

173 Re. 8: Component **FDP_ACF.1** requires certain rules for user-defined access control and thus addresses security objectives **O.logZugriff** and **O.AuthÄndern** by specifying controlled user access, implicitly governed by certain rules, to the TOE's resources and functions.

174 Re. 9: Component **FMT_SMF.1** requires a function for modifying the authentication attribute and thus addresses the **O.AuthÄndern** security objective.

175 Re. 10: Component **FMT_SMR.1** requires the role of authorised user (S1). This is necessary in order to be able to use authentication data for user-defined access control (see **FDP_ACF.1** and **FDP_ACC.1**). The component therefore supports the **O.logZugriff** and **O.AuthÄndern** security objectives.

176 Re. 11: Component **FMT_MSA.1** requires that management of the authentication attribute only be possible for the authorised user (S1). The component therefore addresses security objective **O.AuthÄndern**.

177 Re. 12: Component **FPT_FLS.1** requires the TSF to remain secure in the event of a failure (e.g. power failure). The component therefore addresses the **O.Störung** security objective.

178 Re. 13: Component **FPT_RCV.4** requires the TSF to ensure that, following a failure (e.g. power failure), the security function either completes successfully or recovers to a consistent and secure state. The component therefore addresses security objective **O.Störung**.

6.4.2 Relationship between security functional components and security objectives

179 The following table, **Table 8**, shows that at least one security functional component has been selected from Part 2 of the CC for each security objective, with the aim of supporting that security objective.

Table 8: Security objectives covered by functional components

Security objective	Selected component

O.logZugriff	FIA_UAU.1, FIA_UAU.6, FIA_SOS.1, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1
O.phyZugriff	FCS_CKM.1, FCS_CKM.4, FCS_COP.1
O.AuthÄndern	FIA_UAU.1, FIA_UAU.6, FIA_SOS.1, FDP_ACC.1,FDP_ACF.1, FMT_SMF.1, FMT_SMR.1
	FMT_MSA.1
O.Störung	FPT_FLS.1, FPT_RCV.4

180 The objective of restricting access to the TOE's confidential data to authorised users by means of access control (**O.logZugriff**) is achieved by means of the requirements that the user be authenticated before any action apart from accessing the public memory area (FIA_UAU.1) and that re-authentication be carried out in the event of a disrupted connection (FIA_UAU.6). The TSFs must include the role of authorised user (S1), which is implemented via (FMT_SMR.1). The operations which a user can perform depending on his/her authentication are determined by components (FDP_ACC.1,FDP_ACF.1). An authentication attribute with the appropriate strength must be selected in order to protect logical access (FIA_SOS.1).

181 The objective of using encryption to protect the memory in the event of a physical attack (**O.phyZugriff**) is implemented by components (FCS_CKM.1, FCS_CKM.4 and FCS_COP.1), which determine the procedure for encrypting/decrypting the data.

182 The objective of protecting the TOE against misuse of the "Modification of the authentication attribute" function by making it necessary for S1 to be authenticated (**O.AuthÄndern**) is primarily achieved by component (FMT_MSA.1). This requirement depends on how the authentication mechanism (FIA_UAU.1, FIA_UAU.6) and the subset access control (FDP_ACC.1,FDP_ACF.1 and FMT_SMR.1) are implemented. An authentication attribute with the appropriate strength must be selected in order to protect the "Modification of the authentication attribute" function (FIA_SOS.1).

183

184 The objective of protecting the TOE against misuse of the "Modification of the authentication attribute" function by making it necessary for S1 to be authenticated (**O.AuthÄndern**) requires a "Modification of the authentication attribute" function (FMT_SMF.1) to be in place. The aim is to restrict the use of this function to S1 (FMT_MSA.1). This will depend how the authentication

mechanism (FIA_UAU.1, FIA_UAU.6) and the subset access control (FDP_ACC.1,FDP_ACF.1 and FMT_SMR.1) are implemented.

185

186 The objective of ensuring that the TOE recovers to a consistent and stable state in the event of a failure and that the failure does not result in data remaining unencrypted or the file system being damaged (**O.Störung**) is implemented by components (FPT_FLS.1, FPT_RCV.4).

6.5 Rationale for the environment security requirements

6.5.1 Relationship between the environment security requirements and the security objectives for the IT environment

No.	Name	Security objective for the IT environment
1	RE.Vertrau.WS	OE.Vertrau.WS
2	RE.Abwesend	OE.Abwesend

187 Re. 1: Component “RE.Vertrau.WS” requires the host system to be able to prevent unauthorised accessing via the host system (e.g. by malware) or any connected network. This security requirement therefore addresses security objective OE.Vertrau.WS by ensuring that there are no unauthorised attempts to access the TOE from the host system or a connected network.

188 Re. 2: Component “RE.Abwesend” requires the host system to be able to enable S1 to block or disconnect logical access to the TOE. This security requirement thus addresses the OE.Abwesend security objective because S1 can block or disconnect logical access to the TOE for the duration of his/her absence.

6.6 Rationale for the TOE security assurance requirements

189 The security assurance requirements in line with the selected assurance level of **EAL 2+** are appropriate for the TOE because they are intended to guarantee a basic level of security. The TOE`s security service is intended to provide protection against logical and physical attacks.

190

191 The CC defines EAL 2 as meaning “structurally tested”.

192 EAL2 provides security assurance by requiring that the security functions be analysed using a functional and interface specification, guidance documents and the high-level TOE design in order to understand the security behaviour.

193 The analysis is backed up by independent testing of the TOE security functions, evidence that the development tests have been performed on the basis of the functional specification, selective, independent confirmation of the development-test results, analysis of the strength of functions and by evidence of a development search for obvious vulnerabilities (e.g. vulnerabilities which are general knowledge).

194 EAL2 also provides security assurance by means of a configuration directory for the TOE and evidence of the security of the delivery procedures.

195 In this protection profile, EAL 2 has been augmented to include component **ADV_SPM.1**, thus creating EAL2+. This component requires the developer to prove that the TSFs enforce a defined security policy. The augmentation is necessary in order to fulfil security objective O.Störung.

196 The required minimum strength of functions of **SOF-medium** has been chosen because the TOE security functions which are based on the authentication mechanism (implemented by FIA_SOS.1 and FIA_UAU.1) are supposed to be able to withstand moderate attack potential and thus to offer adequate protection against simple, intentional and direct attacks.

197 It is to be assumed that the attacker wishes to access the valuable data in the memory (examples of possible valuable data are given in Section 2.5). Furthermore, physical attacks on the TOE are possible. The attacker can obtain a USB storage medium of the same type as the TOE. He/she can try out both logical and physical attacks on that USB storage medium. Since the TOE is compact in size, it should be relatively easy for the attacker to gain possession of it. The TOE therefore has security functions to protect the confidential data both against logical and physical attacks.

198 The required SOF is thus in line with the threats to and the security objectives of the TOE and the environment in which it is used.

6.7 Final statement concerning the rationale for the IT requirements

199 The information provided by the rationale section with regard to the security objectives has shown that, taken together, the IT security requirements are suitable for covering all of the TOE's security objectives. None of the IT security requirements described conflicts with other IT security requirements.

200 The sum of the IT security requirements forms a mutually supporting and consistent whole.

7 References

[CC Part2] International Organization for Standardization, ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements, 1999.

[CC Part3] International Organization for Standardization, ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements, 1999.