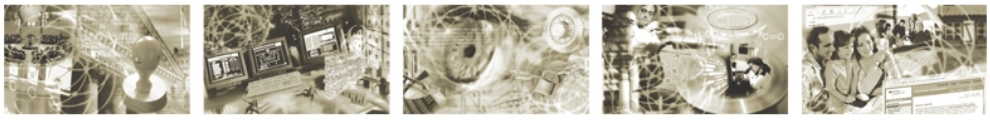
Federal Office
for Information Security



Protection Profile for Portable Storage Media (PSMPP)

Common Criteria

Common Criteria Protection Profile

BSI-CC-PP-0081-2012

Version 1.0

German Federal Office for Information Security
PO Box 20 03 63
D-53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: http://www.bsi.bund.de

Table of Contents

Index of Tables

Illustration Index

Bibliography

CC: Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009

Revision History

Version	Date	Author	Changes
1.0	2012-07-32	Andreas Siegert, atsec	Initial Release

1 Protection Profile Introduction

1 This document defines the minimum security functionality expected to be provided by a portable storage device with a physical host connection that uses cryptographic means to protect the stored user data.

2 Unlike most other protection profiles, the Protection Profile for Portable Storage Media (PSMPP) is structured into a "base" part and an (optional) "extended package part". This structure was chosen to maximize adaptability for different operational environments and different operational requirements.

3 Extended packages allow a flexible adjustment to specific requirements like stronger authentication functionality without the need to set up completely new protection profiles.

1.1 Protection Profile Reference

4	Title	Protection Profile for Portable Storage Media (PSMPP)
5	PP ID	BSI-CC-PP-0081-2012
6	Version	1.0
7	Published	2012-07-31
8	Sponsor	German Federal Office for Information Security
9	Author	Andreas Siegert, atsec information security GmbH
10	TOE	Portable storage media with physical host connection
11	EAL	EAL2
12	Keywords	portable storage, portable memory, mobile storage, memory stick, USB memory, USB key, flash drive, portable hard drive
13	CC Version	3.1R3

1.2 TOE Overview

1.2.1 TOE Type

14 The TOE is a portable, self contained storage device with a physical host connection providing encrypted storage of user data and strong authentication to unlock access to the encrypted user data.

1.2.2 Protection Profile Scope

15 This protection profile is targeted at portable storage media that is easily lost or stolen and it describes the security functions needed to protect the confidentiality of the data of a stolen or lost device.

16 There is no requirement for access control beyond the protected storage, so

specific file systems and their access control mechanisms are not included.

17 Although write protection of the device is not part of the requirements of the PP, the PP does not preclude write protection of the device as an additional security mechanism. For example, write protection would allow to use the device in potentially hostile environments where a risk of data modification or introduction of malware exists.

18 Although a public storage area on the device is not part of the requirements of the PP, the PP does not preclude the implementation of a read-only public storage on the device that can be used to store supplemental code, for example a password entry program.

1.2.3 Usage and major security features of the TOE

19 This protection profile considers all portable storage devices which can be physically connected to a host system. Predominant examples would be USB attached memory sticks or FireWire attached disk drives.

20 The TOE is a physically attached storage device such as an USB stick or a portable hard drive with a physical connection. The exact details of the connection are not specified in this protection profile as this PP aims to be usable for all access controlled physically attached storage devices.

21 The encrypted user data in the protected storage area of the portable storage medium must not be accessible to unauthorized individuals in case the medium is lost, misplaced or stolen. To this end, this protection profile defines a basic set of security requirements intended to maintain the confidentiality of the user data in the protected storage area by cryptographic means to counter logical or physical attacks.

22 The default power-up state of the device provides only access to the authentication mechanism.

23 A key aspect of the user-friendly IT security offered by a portable storage device is that the security functions are completely implemented within the storage device itself. This enables using a PP-compliant mobile data storage device with a wide range of host systems since it is not subject to supporting software requirements.

24 One single authentication process is enough to unlock the access to the encrypted user data on the storage device and make it accessible to the user. After successful authentication, the storage medium provides its security service transparently without any further access control requirements on the device.

25 The TSF data, i.e. authentication data and the cryptographic key material used need to be stored securely within the TOE.

Application note (1) The TSF data could be for example stored within a HSM (High Security Module) or in an encrypted form on the device.

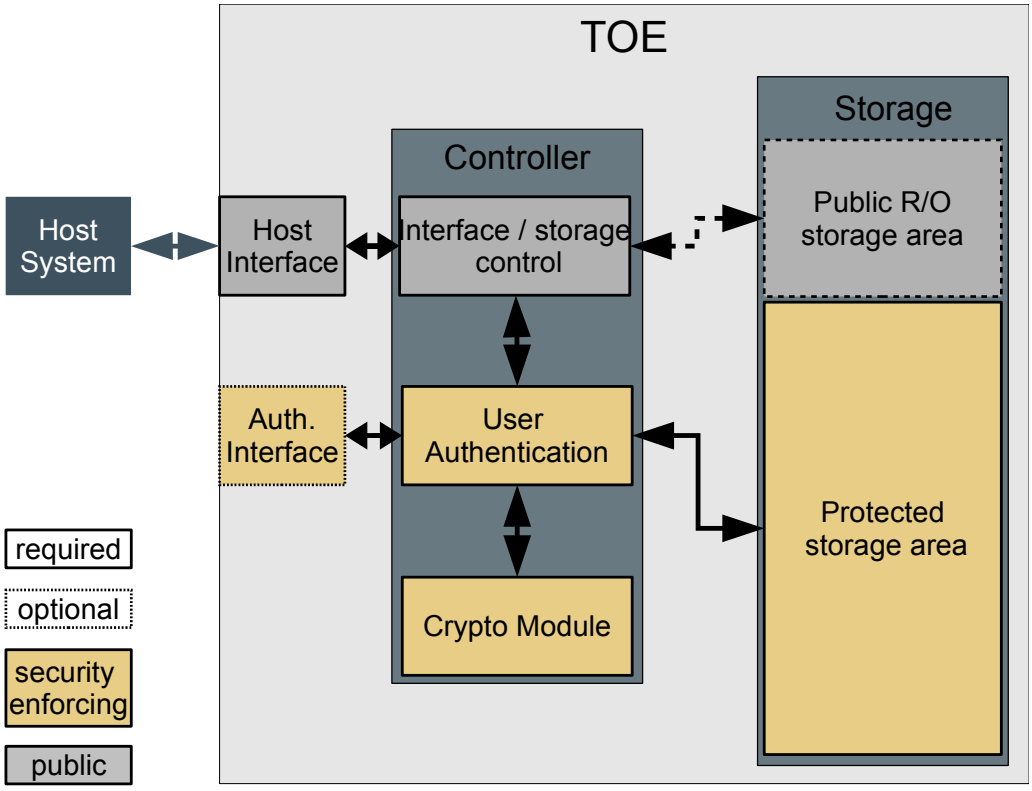
26 The TOE has to ensure the confidentiality of user and TSF data in case that the TOE is separated from the host either logically due to a failure (e.g. abnormal system end or power failure) or inadvertently physically in particular even if the separation happens during a read or write access.
Other logical changes like putting the host into a sleep or hibernation state can trigger locking as well at the discretion of the ST author.

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

28 Manufacturers may, at their own discretion, enhance the security provided by products which conform to this protection profile by adding extra security functions if these extra security functions do not contradict the descriptions in the PP. 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.

29 The operational environment of the TOE is quite diverse. Portable storage devices can be used nearly anywhere where they can be connected to a host computer via the standard interfaces like USB, FireWire or Thunderbolt.

30 Drawing 1: TOE Structure shows the basic structure of the TOE for which this protection profile is written.



Drawing 1: TOE Structure

31 The TOE has at least one external interface to the host system. Besides this it may implement an optional local authentication interface or rely on the host to provide the UI for obtaining the authentication data.

32 The main parts of the TOE are the controller (implements the interface to the storage area, the user authentication and the cryptographic functionalities) and the protected storage area.

33 The TOE may implement an optional public storage area that is read-only for the TOE user.

34 The producer of a TOE should use internal sealing encapsulation, e.g. with casting resin, of the security relevant components. This sealing encapsulation may impede physical attacks.

35 Note: As such an impeding mechanism is not measurable, it is not possible to certify it against the CC.

36 Overall the TOE implements the following key security features:

– Confidentiality protection of user data by encryption

– Protection of TSF data

1.2.4 Non-TOE hardware, software and firmware

37 This PP does not mandate a specific environment or dedicated host software.

1.3 TOE boundary

38 The physical TOE boundary is defined by the host interface and the optional authentication interface. Physically the TOE consists of the complete storage device.

2 PSMPP Framework

39 The PSMPP allows the definition of functional extensions that can be optionally claimed by an ST in addition to the PSMPP base. As such, the PSMPP defines the following components:

– The PSMPP base specifies the conformance claim, security problem definition, security objectives, and security functional requirements that are to be implemented by all portable storage media. The PSMPP base is mandatory and defines the common denominator for all portable storage media claiming conformance with the PSMPP.

– An PSMPP extended package specifies the security problem definition, security objectives, and security functional requirements for mechanisms that may be implemented in addition to the PSMPP base. Usually, an PSMPP extended package defines an extension that is either desired or implemented by several portable storage media devices. However, the functionality specified in an PSMPP extended package is not commonly found among portable storage media. PSMPP extended packages can optionally be added to the PSMPP base functionality when writing an ST. The ST author may choose from the set of PSMPP extended packages when deriving an ST. To avoid fragmentation of security functionality into PSMPP extended packages that are too small to be practical, an PSMPP extended package shall define a set of functional requirements that address one or more general security problems.

40 The PSMPP is defined as an extensible framework. The current set of PSMPP extended packages can be enhanced with newly-developed or updated PSMPP extended packages. Those will then be part of a re-evaluation and re-certification of the PSMPP base. Therefore, this framework invites anybody interested in specifying an aspect of portable storage media to author an PSMPP extended package and commit it to the BSI, where the PSMPP is managed. Using this approach, there will always be a valid set of PSMPP base and extended packages, which are compliant to each other. Dependencies on other PSMPP extended packages can be specified.

2.1 Mandatory information given by the ST

41 The following information must be given as part of the ST derived from the PSMPP.

2.1.1 Conformance claim

42 When specifying conformance to the PSMPP, the ST must specify any PSMPP extended packages to which the ST claims conformance to.

2.1.2 SFR reference with PSMPP extended package reference

43 When specifying the SFRs as part of the ST, a reference to the PSMPP base or

PSMPP extended package abbreviation must be given in order to facilitate a direct mapping of the SFR, specifically considering iterations.

44 This requirement shall support ST authors and evaluators to ensure that no SFR from the PSMPP base or an PSMPP extended package the ST claims conformance to is left uncovered.

2.2 Mandatory information given by PSMPP extended packages

45 The following information must be given for each PSMPP extended package to allow the extended package to be embedded into the framework of the PSMPP.

2.2.1 Extended package identification

46 The following information must be given to identify an PSMPP extended package:

– Extended package name in narrative English

– Abbreviation of the extended package name to allow easy and unambiguous reference to the extended package

– Version of the extended package

– Owner of the extended package; that is, who is in charge of performing authoritative changes

2.2.2 Extended package composition rules

47 To specify how the PSMPP extended package can be used together with other PSMPP extended packages, the following information must be provided:

– A list of dependent PSMPP extended packages with their respective minimum versions.

– A list of disallowed PSMPP extended packages with their respective minimum versions.

48 Note that the extended package must not exclude the PSMPP base or any portion of it; however, the extended package may specify a minimum version of the PSMPP base that is required for the respective extended package.

49 If an existing extended package must be changed to accommodate another extended package (the “current” extended package), the author of the current extended package is requested to approach the owner of the existing extended package to agree on the required modifications.

2.2.3 Specification of PSMPP extended packages

50 The PSMPP extended packages may define many aspects as an addition to the PSMPP base. Specification includes the following information:

- Package introduction
- Dependencies on other PSMPP extended packages
- Security problem definition
- Security objectives
- Security functional requirements: For the sake of better readability, the author uses the following notation to indicate SFRs belonging to an extended package: The SFR name is augmented by a hyphen “-” and the identifying abbreviation of the extended package.
- Refinements to security assurance requirements. Note that specification of higher or extended security assurance requirements is not allowed; the entire PSMPP is intended to be covered by the mutual recognition agreement (CCRA), and the PSMPP base shall ensure this.

2.3 Specification restricted to the PSMPP base

51 The PSMPP base exclusively defines the following properties:

- Conformance claims to other protection profiles
- Conformance type (either strict or demonstrable)
- Conformance claim to the EAL including any augmentation

52 An PSMPP extended package may define refinements to assurance components. Refinements may provide guidance on how to satisfy the assurance requirements specifically for the SFRs in the extended package. However, one of the core intentions for PSMPP is to keep the protection profile and all its modules covered under the mutual recognition agreement. Therefore, no PSMPP extended package shall add an SAR or modify the level of an SAR.

3 Conformance Claims

53 The following sections describe the conformance claims of the Protection Profile for Portable Storage Media (PSMPP).

3.1 Conformance with CC parts 2 and 3

54 PSMPP is [CC] Part 2 extended and Part 3 conformant.

3.2 Conformance with Packages

55 The PP mandates an Evaluation Assurance Level of EAL2 for product evaluations.

3.3 Conformance with other Protection Profiles

56 This PP claims no conformance with other protection profiles.

3.4 Conformance Statement

57 This PP requires demonstrable-PP conformance by any ST or PP claiming conformance to this PP.

4 Security Problem Definition

58 This chapter describes the purpose of the device in terms of the assets to be protected and the threats to be countered.

4.1 Assets

59 Assets to be protected are:

– User data: The encrypted data in the protected storage area of the portable storage device.

– TSF data: Authentication data used to authenticate the authorized user and cryptographic key material used for the encryption of the user data .

4.2 Roles

60 There is only one role defined for the device, the authorized user, a user who successfully authenticates against the device. Non-authenticated users trying to access the assets (protected data) are considered threat agents.

61 **Authorized TOE User**

– Has successfully authenticated with the TOE.
This implies that he holds the authentication data.

– Is allowed to access the TOE's protected storage area, in which the confidential user data is stored.

– Is allowed to modify the authentication data after successful re-authentication.

– Has no read access to TSF data.

62 Every non-authorized user is not in the above role, which means:

– Is not authenticated with the TOE.

– Must not access the protected storage area of the TOE.

– Must not access authentication data or cryptographic key material used to access the protected storage area.

Application note (2) Both the authorized and the unauthorized user can be the same individual, only distinguished by being authenticated or not. Any individual can hold only one of these roles at any time.

4.3 Threats

63 Threat agents emerge from the group of external entities not authorized to access the assets (protected data). Threat agents are typically characterized by a number of factors, such as expertise, available resources, and motivation, with motivation being linked directly to the value of the assets at stake. The TOE protects against intentional and unintentional breach of TOE security by attackers possessing a basic attack potential.

64 Threat agents satisfy one or more of the following:

– May attempt to access assets they are not authorized to either by masquerading as an authorized entity or by attempting to use TSF services without proper authorization.

– Wishes to access user data, authentication data or cryptographic key material in the portable storage medium's storage.

– Can obtain a portable storage medium of the same type. Can try out both logical and physical attacks on this portable storage medium to prepare for attacking the TOE.

– Can gain possession of the TOE relatively easily since the TOE has a compact form.

– Does not hold the authentication data.

4.3.1 Threats Countered by the TOE

65 **T.LogicalAccess** A threat agent can access the user data, authentication data or cryptographic key material on the TOE using the exported TOE interfaces.

66 **T.PhysicalAccess** A threat agent can access the TOE's storage by means of a physical attack, bypassing the exported TOE interfaces to obtain user data, authentication data or cryptographic key material.

67 **T.AuthChange** A threat agent modifies the authentication data.

68 **T.Disruption** A threat agent can access data intended to be protected but remaining unprotected due to a failure interrupting the correct operation of the TOE.

Application note (3) Threats arising from repeated theft and differential crypto analysis of the device are explicitly not considered.

4.3.2 Threats Countered by the TOE Environment

69 There are no threats to be countered by the TOE environment.

4.4 Organizational Security Policies

70 This protection profile does not specify any organizational security policies.

71 All motivation for the IT security functionality is derived from the threats to be countered.

4.5 Assumptions

72 This section lists the security-related assumptions for the environment in which the TOE is to be used. It can be considered a set of rules for the TOE operator.

73 **A.TrustedWS** Once the authorized user has unlocked the protected storage area, i.e. he has authenticated to the TOE, there are no unauthorized attempts to access the TOE from the host system or any connected networks. This assumption also covers the transfer of malware onto the TOE.

5 Security Objectives

5.1 Security Objectives for the TOE

74	**O.ProtectTSF**	The TOE must provide protection for TSF data so that authentication data and cryptographic key material are protected from access.
75	**O.AuthAccess**	The TOE must provide a strong authentication mechanism to allow only authenticated users access to the protected storage area.
76	**O.Encrypt**	The TOE encrypts all data stored in the protected storage area of the TOE. The encryption specifically protects confidentiality in the event of physical attacks on the TOE.
77	**O.AuthChange**	Only authenticated users are allowed to change the authentication data.
78	**O.FailSafe**	The TOE reverts to a stable and consistent state following a disruption. Reverting to a safe state implies that the device will be in a locked state so that neither the protected storage area nor the TSF data will be accessible in clear text after a failure. Successful authentication is required again to unlock the device.

5.2 Security Objectives for the Operational Environment

79	**OE.TrustedWS**	The host system must ensure proper protection of all data retrieved from the protected storage area of the TOE and must ensure no malware is transferred to the TOE.
80	**OE.AuthConf**	The TOE users must keep their authentication data confidential.
81	**OE.AuthProt**	If the host provides the user interface for the authentication mechanism, the host shall protect the authentication data against misuse.
	Application note (4)	The ST author may remove OE.AuthProt if the TOE provides its own authentication interface and does not rely on the host for authentication.

5.3 Security Objectives Rationale

5.3.1 Security Objectives Coverage

Objective	Threat	Assumption
O.ProtectTSF	T.LogicalAccess, T.PhysicalAccess	
O.AuthAccess	T.LogicalAccess	
O.Encrypt	T.PhysicalAccess	
O.AuthChange	T.AuthChange	
O.FailSafe	T.Disruption	
OE.TrustedWS		A.TrustedWS
OE.AuthConf	T.LogicalAccess	
OE.AuthProt	T.LogicalAccess	

Table 1: Objectives tracing to threats and assumptions

5.3.2 Security Objectives Sufficiency

82 The following rationale describes how the objectives counter the threats and meet the assumptions:

83 **T.LogicalAccess**

The threat of unauthenticated logical access to the protected storage area is countered by O.AuthAccess ensuring that only authenticated access is possible. The threat of unauthenticated logical or physical access to TSF data is countered by O.ProtectTSF ensuring the TSF protection.
OE.AuthConf ensures that the user keeps his authentication data confidential and OE.AuthProt ensures that host protects the authentication data in the case that the host is used for the authentication interface. Both security objectives for the environment are necessary to ensure a secure usage of the authentication mechanism.

84 **T.PhysicalAccess**

The threat of physical access to the protected data is countered by O.Encrypt ensuring that the data is not accessible without the proper decryption key. A physical attack on the TOE may lead to the disclosure of the encrypted data in the protected storage of the TOE. For O.Encrypt to be sufficient, the encryption algorithms and key lengths need to be strong enough. The threat of physical access to TSF data is countered by O.ProtectTSF that explicitly protects the TSF data.

85 **T.AuthChange**

The threat of unauthorized modification of authentication information

is countered by O.AuthChange which ensures that only the already authenticated user can change authentication data.

86 **T.Disruption**

The threat of service disruption causing unauthenticated access to the protected data is countered by O.FailSafe ensuring that:
no protected data will be accessible in clear text after a failure and
a re-authentication is needed after interruptions.

87 **A.TrustedWS**

The assumption of a trusted workstation is supported by the objective for the environment (OE.TrustedWS) that the host system ensures proper protection of all data retrieved from the protected storage area of the TOE and protection against the storage of malware on the TOE.

6 Extended Components Definition

6.1 FPT_SDC Trusted storage of TSF data

88 FPT_SDC.1 Trusted storage of TSF data requires that stored TSF data, namely authentication data and cryptographic key material, is securely stored to prevent disclosure of the TSF data.

6.1.1 Family Behavior FPT_SDC

89 This family defines protection requirements for stored authentication data and cryptographic key material that is used to enable the secure function of the device.

6.1.2 Component Leveling FPT_SDC.1

90 FPT_SDC.1 is not hierarchical to any other component within the FPT_SDC family.

6.1.3 Management FPT_SDC.1

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

92 There are no management activities foreseen.

6.1.4 Audit FPT_SDC.1

93 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

94 There are no actions defined to be auditable.

6.1.5 FPT_SDC.1 Trusted storage of TSF data

95 Hierarchical to: No other components.

96 Dependencies: No dependencies.

FPT_SDC.1.1 The TSF must provide secure storage for authentication data and cryptographic key material.

Application note (5) It is up to the developer what mechanisms are employed to ensure protection of the authentication data and cryptographic key material. It could be a HSM, a smart card, encrypted storage or other forms of protection that ensures that neither keys nor authentication data are accessible.

6.1.6 Rationale

97 This extended SFR is required to have an explicit requirement for the protection of the TSF data which otherwise would not have a defined requirements as this type of protection is usually ensured with the architecture of the TOE and not modeled with CC provided SFRs.

7 Security Requirements

7.1 Security Functional Requirements

98 The following formatting conventions are used to identify operations (refinements, selections and assignments) that have been performed in this PP:

99 The **refinement** operation is used to add detail to a requirement and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed words are ~~crossed out~~. If a refinement is added as a separate paragraph to an SFR instead of modifying its wording, this paragraph starts with the word **Refinement:** in bold text.

100 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections by the PP author are denoted as underlined text; in addition, a footnote will show the original text from CC, Part 2. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are *italicised*.

101 The **assignment** operation is used to assign a specific value to an unspecified parameter such as the length of a password. Assignments by the PP author are denoted as underlined text; in addition, a footnote will show the original text from CC, Part 2. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are *italicised*. In some cases the assignment made by the PP authors defines a selection or assignment to be performed by the ST author. Thus this text is underlined and *italicised like this*.

7.1.1 Identification and Authentication (FIA)

102 The TOE must provide at least a basic authentication mechanism that is strong enough to satisfy the requirements of FIA_SOS.1.

103 Access to the protected data is only granted after the authentication data has been successfully provided. Successful authentication establishes a context in which the protected data can be accessed. The context is destroyed in case of disconnects of the TOE and the host and during device failures.

FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication.
Dependencies:	FIA_UID.1 Timing of identification
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.

FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions change of the authentication data[1].
Application note (6)	The re-authentication shall use the same authentication mechanism as the initial authentication.

FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet a) For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000; b) Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metric[2].

FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]* unsuccessful authentication attempts occur related to the authentication of the user[3].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[4], the TSF shall disable access to the protected storage area[5].
Application note (7)	The thresholds need to be defined to be reasonable for the intended operational environment and the type of blocking implemented. If the blocking is implemented by key destruction, therefore rendering the stored data completely inaccessible, higher thresholds are appropriate than for an environment where an administrator can unblock the device.
Application note (8)	Implementing this requirement may render the device unusable. It is up to the ST author to decide whether this is

1 [assignment: list of conditions under which re-authentication is required]
2 [assignment: a defined quality metric]
3 [assignment: list of authentication events]
4 [selection: met, surpassed]
5 [assignment: list of actions]

acceptable for the intended use of the TOE. If a mechanism is implemented that allows resetting of the failed authentication counter, then the associated security issues need to be addressed and modeled in the ST.

7.1.2 Cryptographic Operation (FCS)

104 The TOE protects data via cryptographic means. The exact implementation is governed by national or international cryptographic regulations that have to be specified in the ST.

FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[assignment: cryptographic key generation algorithm]*[6] and specified cryptographic key sizes *[assignment: cryptographic key sizes]*[7] that meet the following: *[assignment: list of **Endorsed** standards]*[8].
Application note (9)	Please contact the certification body for the list of endorsed standards. The list of endorsed standards shall provide appropriate cryptographic algorithms, modes of operation and key lengths, appropriate key generation algorithms and random number generators.
Application note (10)	The TOE will generate a new encryption key when it is initialized or a new key generation is explicitly requested.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
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.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[assignment: cryptographic key destruction method]*[9] that meets the following: *[assignment: list of **Endorsed** standards]*[10].
Application note (11)	Should the endorsed standards referenced in FCS_CKM.1

6 [assignment: cryptographic key generation algorithm]
7 [assignment: cryptographic key sizes]
8 [assignment: list of standards]
9 [assignment: cryptographic key destruction method]
10 [assignment: list of standards]

mandate key destruction methods, those are to be applied here. Please contact the certification body for the list of endorsed standards.

Application note (12) A typical scenario for key destruction would be the re-initialization of the device. If data wiping is included in the security functionality of the TOE, this could be implemented by key deletion.

Application note (13) If a TOE user suspects the TOE to be compromised, he should completely wipe it, not just reset it by deleting the key.

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform *encryption and decryption of data when writing to / reading from the protected storage area of the storage device*[11] in accordance with a specified cryptographic algorithm *[assignment: cryptographic algorithm]*[12] and cryptographic key sizes *[assignment: cryptographic key sizes]*[13] that meet the following: *[assignment: list of Endorsed standards]*[14].

Application note (14) Please contact the certification body for the list of endorsed standards.

7.1.3 Management Functions (FMT)

105 The TOE supports management functions for the role of the authenticated user to alter authentication data or initialize the device.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) modification of the authentication data
b) initialization of the device by generation of the encryption key and deletion of any previous keys [15].

Application note (15) Further management functions can be specified by an ST

11 [assignment: list of cryptographic operations]
12 [assignment: cryptographic algorithm]
13 [assignment: cryptographic key sizes]
14 [assignment: list of standards]
15 [assignment: list of management functions to be provided by the TSF]

author.

Application note (16) Deletion of the previous keys will render old encrypted data on the device useless. For added security, a device may choose to also delete the data storage.

7.1.4 User Data Protection (FDP)

106 Plaintext user data and TSF data are only accessible in the unlocked state of the TOE. The TOE is expected to ensure that no residual information is accessible in the locked state.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **physical or logical** deallocation of the resource from[16] the following objects: plaintext user and TSF data[17].

Application note (17) Deallocation in the context of this PP is defined as logical or physical termination of the host connection.

7.1.5 Protection of TSF Data (FPT)

107 The TOE is expected to protect TSF data and to handle disruptions in a fail-secure way, removing any access in case of failures.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: abnormal abort of the TSF[18].

Application note (18) The details of the secure state are defined in O.FailSafe.

Application note (19) The integrity of the storage data on the device is not in the scope of the PP.

Application note (20) Failures in the sense of this SFR are failures in the environment of the TOE, e.g. a system crash in the host, a power failure or an unintentional physical disconnection or other failures that result in a failure in the TSF, i.e. an abnormal abort of the TSF, e.g. an abort of a read or write operation.

16 [selection: allocation of the resource to, deallocation of the resource from]
17 [assignment: list of objects]
18 [assignment: list of types of failures in the TSF]

FPT_SDC.1 Trusted storage of TSF data

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_SDC.1.1	The TSF must provide secure storage for authentication data and cryptographic key material.
Application note (21)	It is up to the developer what mechanisms are employed to ensure protection for the authentication data and cryptographic key material. It could be a HSM, a smart card or other forms of protection that ensures that neither keys nor authentication data are accessible.

7.2 Rationale for Security Functional Requirements

7.2.1 Internal Consistency of Requirements

108 The mutual support and internal consistency of the components selected for this protection profile is described in this section.

109 The following rationale demonstrates the internal consistency of the functional requirements.

7.2.1.1 Authentication

110 Users accessing the protected storage area shall be authenticated before being allowed access to the protected storage area. The TOE shall provide the capability to lock access after too many unsuccessful authentication attempts.

111 This is enforced via the requirement to authenticate before use (FIA_UAU.2), the requirements on the quality of the authentication factor (FIA_SOS.1) and the protection of the authentication mechanism via FIA_AFL1. The requirement to revert to a secure state (FPT_FLS.1) supports this. The requirement on residual information protection (FDP_RIP.1) ensures that no plain-text user and TSF data is available.

7.2.1.2 Cryptographic Support

112 The TOE shall provide a cryptographically-protected storage based on cryptographic algorithms, modes of operation and key lengths that are endorsed by the national scheme.

113 This is enforced by the requirement to encrypt the TSF data (FCS_COP.1), supported by FCS_CKM.1 and FCS_CKM.4

7.2.1.3 Management Functions

114 The TOE shall enable authenticated users to modify the security attributes used for authentication and to initialize the device.

115 Management of the authentication data is specified via FMT_SMF.1 and supported by FIA_UAU.6.

7.2.1.4 Protection of TSF Data

116 The TOE shall revert to a secure state in case of communication failures. This is implemented via FPT_FLS.1

117 The TOE shall protect TSF data. This is implemented via FPT_SDC.1 and FDP_RIP.1

7.2.2 Security Requirements Coverage

SFR	O.ProtectTSF	O.AuthAccess	O.Encrypt	O.AuthChange	O.FailSafe
FIA_UAU.2		X			
FIA_UAU.6				X	
FIA_SOS.1		X			
FIA_AFL.1		X			
FCS_CKM.1			X		
FCS_CKM.4			X		
FCS_COP.1			X		
FDP_RIP.1	X	X			X
FMT_SMF.1				X	
FPT_FLS.1					X
FPT_SDC.1	X				

Table 2: SFR objective tracing

118 The objectives are met by the SFRs in the following way:

119 **O.ProtectTSF** Unauthorized access to TSF data is prevented by FPT_SDC.1 which requires secure storage for authentication data and cryptographic key material and FDP_RIP.1 that ensures no residual data is accessible. For access to authentication data see O.AuthChange below.

120 **O.AuthAccess** Access to the protected storage area is only granted after authentication which is modeled via FIA_UAU.2 and FIA_SOS.1. FIA_AFL.1 ensures that authentication attempts can not continue indefinitely, thereby blocking brute force attacks. FDP_RIP.1 ensures residual user data is not available in the locked state.

121 **O.Encrypt** Encryption of data in the protected storage area is

		implemented via the cryptographic protection modeled in FCS_CKM.1, FCS_CKM.4, FCS_COP.1.
122	**O.AuthChange**	Management of the authentication data is modeled by FMT_SMF.1 and supported by FIA_UAU.6.
123	**O.FailSafe**	The requirement to fail safe is modeled by FDP_RIP.1 which protects residual data and FPT_FLS.1 which requires the TOE to fail to a safe state.

7.2.3 Security Requirements Dependency Analysis

124 The following table shows how the dependencies of the SFRs are met.

SFR	Dependencies identified in [CC]	Resolved in PP / Rationale for unresolved dependencies
FIA_UAU.2	FIA_UID.1	Not resolved as the TOE does not need user IDs. Only authentication is required.
FIA_UAU.6	none	N/A
FIA_SOS.1	none	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_RIP.1	none	N/A
FMT_SMF.1	none	N/A
FPT_FLS.1	none	N/A
FPT_SDC.1	none	N/A

Table 3: SFR dependency resolution

7.3 Security Assurance Requirements

125 The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components, as specified in [CC] part 3. No operations are applied to the assurance components.

7.4 Rationale for Security Assurance Requirements

126 The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

8 Extended Package – Extended Authentication PSMPP-EA

127 This PSMPP extended package specifies mechanisms and interfaces for extended authentication mechanisms for portable storage media, for example smartcard based authentication.

8.1 PSMPP Extended Package Identification

128 Title PSMPP Extended Package – Extended Authentication

129 Abbreviation: PSMPP-EA

130 Version 1.0

131 Owner German Federal Office for Information Security

132 Published 2012-07-31

133 Sponsor German Federal Office for Information Security

134 Author Andreas Siegert, atsec information security GmbH

135 Keywords two factor authentication

136 CC Version 3.1R3

8.2 Extended Package overview

137 The base PP defined in previous chapters only requires a user authentication without specific requirements for the authentication mechanism. This extended package augments the base PP to include two factor authentication mechanisms like smart cards.

8.3 Conformance Claims

8.3.1 Conformance with CC Parts 2 and 3

138 This extended package does not augment the conformance claim of the base protection profile specified in chapter 3.

8.3.2 Extended Package Composition Rules

139 This extended package does not depend on other extended packages.

140 This package can only be claimed together with the base package, in the version defined in chapter 1.1.

8.4 Security Problem Definition

141 The security problem definition of the extended package is consistent with the security problem definition of the base. This extended package does not define any additional threats, assumptions or organizational security policies.

8.5 Security Objectives

8.5.1 Security Objectives for the TOE

142 The objective O.AuthAccess from the base PP is strengthened to specify two-factor authentication instead of just strong authentication. It is replaced as follows:

143 **O.AuthAccess-EA** The TOE must provide a **two-factor** authentication mechanism to allow only authenticated users access to the protected storage area.

Application note (22) When using this extended package, O.AuthAccess-EA replaces O.AuthAccess from the base PP.

8.5.2 Security Objectives for the Operational Environment

144 This extended package does not define any additional objectives for the operational environment.

8.5.3 Security Objectives Rationale

8.5.3.1 Security Objectives Coverage

Objective	Threat
O.AuthAccess-EA	T.LogicalAccess (from the base PP)

Table 4: Objectives tracing to threats and assumptions

8.5.3.2 Security Objectives Sufficiency

145 The following rationale describes how the objectives counter the threats and meet the assumptions:

146 **T.LogicalAccess** The threat of unauthenticated logical access to the protected storage area is countered by O.AuthAccess-EA ensuring that only authenticated access is possible.

Application note (23) The remainder of the rationale is to be taken from the base PP.

8.6 Security Functional Requirements

8.6.1 Identification and Authentication (FIA)

147 The TOE must provide strong authentication via a token based or two factor mechanism.

FIA_UAU.5-EA Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide one of each of the following authentication mechanisms: m1: [*selection: smartcard, [assignment: other cryptographic token]]* and m2: *[selection: password, PIN, biometric authentication, [assignment: other authentication mechanism]]* [19] to support user authentication.
Application note (24)	The authentication methods used have to consist of at least one cryptographic token and a second method.
Application note (25)	The weaker of the two methods has to satisfy FIA_SOS.1 from the base PP.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the success of both authentication mechanisms[20].

8.6.2 Rationale for Security Functional Requirements

148 This section provides the rationale for the internal consistency and completeness of the security functional requirements defined in this extended package.

8.6.2.1 Internal Consistency of Requirements

149 The mutual support and internal consistency of the components selected for this extended package is described in this section.

150 The following rationale demonstrates the internal consistency of the functional requirements.

8.6.2.1.1 Authentication

151 Users accessing the protected storage area shall be authenticated with a two-factor mechanism before being allowed access to the protected storage area.

19 [assignment: list of multiple authentication mechanisms]
20 [assignment: rules describing how the multiple authentication mechanisms provide authentication]

8.6.2.2 Security Requirements Coverage

152 Chapter 7.2.2 is extended as follows:

SFR	O.AuthAccess-EA
FIA_UAU.5-EA	X

Table 5: Extended Package - SFR objective tracing

153 The objective is met by the SFRs in the following way:

154 **O.AuthAccess-EA** Access to the protected storage area is only granted after authentication which is modeled via FIA_UAU.2, FIA_UAU.5-EA, FIA_AFL.1 and FIA_SOS.1. FDP_RIP.1 ensures residual user data is not available in the locked state.

8.6.2.3 Security Requirements Dependency Analysis

155 Chapter 7.2.3 is extended as follows:

SFR	Dependencies identified in [CC]	Resolved in PP / Rationale for unresolved dependencies
FIA_UAU.5-EA	none	N/A

Table 6: Extended Package - SFR dependency resolution