DIGITTRADE High Security HS256 S3
(external encrypted HDD/SSD)
Version 1.0

Security Target (ST)
Version 1.10

DIGITTRADE GmbH

18.09.2017

Revision History

Version	Date	Changes	Reasons	Author
1.0	05.11.2015		Erstellung	A. Gimbut, DIGITTRADE GmbH
1.1	23.02.2016	Updating references and labels	Review	A. Gimbut, DIGITTRADE GmbH
1.2	24.02.2016	Insert footnote	Review	A. Gimbut, DIGITTRADE GmbH
1.3	08.04.2016	Update documentation	Review	A. Gimbut, DIGITTRADE GmbH
1.4	30.06.2016	Update documentation	Review	A. Gimbut, DIGITTRADE GmbH
1.5	27.01.2017	Update documentation	Review	A. Gimbut, DIGITTRADE GmbH
1.6	31.01.2017	Update documentation	Review	A. Gimbut, DIGITTRADE GmbH
1.7	17.03.2017	Update documentation	Review	A. Gimbut, DIGITTRADE GmbH
1.8	03.04.2017	Update documentation	Review	A. Gimbut, DIGITTRADE GmbH
1.9	24.04.2017	Update user manual Version	Review	A. Gimbut, DIGITTRADE GmbH
1.10	18.09.2017	Add “User Manual important notice”	Review	A. Gimbut, DIGITTRADE GmbH

Status: final	Owner of process and document: Leonid Gimbut, DIGITTRADE	Datum: 18.09.2017
		Version: 1.10

Inhaltsverzeichnis

Index of Tables

Illustration Index

Bibliography

CC: Common Criteria for Information Technology Security Evaluation Version 3.1R4, September 2012

PP: German Federal Office for Information Security, Protection Profile for Portable Storage Media (PSMPP), Common Criteria Protection Profile, BSI-CC-PP-0081-2012, Version 1.0

XTS: National Institute of Standards and Technology, „ Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication SP800-38E“, 2010

AES: National Institute of Standards and Technology, „Advanced Encryption Standard (AES), FIPS PUB 197“, 26. November 2001

TR: Bundesamt für Sicherheit in der Informationstechnik, „BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, BSI TR-02102, Version 2013.02, 09.01.2013

1 Security target introduction

1 This document defines the security functionality of the target of evaluation (TOE) “DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD), Version 1.0” as a security target (ST) that is conformant to common criteria [CC] and the protection profile [PP].

2 Changes of the [PP] made by the ST author are marked in blue fonts.

1.1 Security target reference

3	Title	DIGITTRADE GmbH, “DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD), Version 1.0, Security Target (ST)”
4	Version	1.10
5	Published	2017-09-18
6	Author	DIGITTRADE GmbH
7	TOE	DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD), Version 1.0
8	EAL	EAL2
9	Keywords	portable storage, portable memory, mobile storage, storage device, HDD, SSD, encrypted, memory stick, USB memory, USB key, flash drive, portable hard drive, two-factor authentication
10	CC Version	3.1R4

1.2 TOE overview

1.2.1 TOE Type

11 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 Usage and major security features of the TOE

12 The Target of Evaluation (TOE) is the portable storage device “DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD)”, which is connectable to a host system via USB.

13 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, as well as in the event of logical or physical attacks. Therefore the TOE provides the following security functions:

- full disc hardware encryption using AES (256 bit, XTS mode);
- two-factor authentication (key on the smart card and knowing the smart card PIN);

- administration of the encryption key

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

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

16 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.

17 The smart card PIN and the encryption key are stored securely on a smart card.

18 The TOE provides a keypad, onto which the user can enter his PIN.

19 The encryption key is generated and stored securely on a smart cards from NXP with JCOP v2.4.2 R3, certified by NSCIB-CC-13-37761-CR2.

20 For encryption and decryption of the data, the encryption key will be transmitted to the crypto module of the USB-to-Sata Bridge inside of the “DIGITTRADE High Security HS256 S3”. Upon completion of usage, the encryption key will be deleted securely on the storage device.

21 The authorized user possesses the authentication data, e.g. encryption key on the smart card in combination with the smart card PIN.

22 Using the smart card and the smart card PIN, the user is able to generate and change the encryption key. If necessary, he can also destroy the encryption key by generating a new key. After generating a new encryption key on the smart card, the encrypted data on the storage device will only be accessible with the previous, matching encryption key.

23 The initialization is defined as the process of allowing the device to use a smart card with a different encryption key as the smart card that had been used before. After initialization of a new smart card, the data on the storage device will be encrypted with the new encryption key, so that the previous data won’t be readable anymore. The old smart card will not be accepted by the device until this smart card has been initialized to the device again.

24 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.

25 The protected data will be locked in case of disconnection of TOE and host if additionally the power supply is disconnected. E.g. if the TOE got a separate power supply by an additional USB-AC Adapter trough an USB-Y Cable then it will be still unlocked after disconnection of TOE and Host.

26 The protected data will be locked in case of disconnection of smart card and storage device, if the lock-out mode is activated. In order to use the TOE in certified mode the Lock-out mode must be activated.

27 The TOE provides a secure state when a failure occurs. This failures can be 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.

28 Extended Package – Extended Authentication PSMPP-EA is realized in the form of a two-factor authentication by key on the smart card and smart card PIN entry on the Keypad of the HS256 S3.

29 The TOE provides physical self-protection in the form of sealing encapsulation of the security enforcing components. Apart from making it difficult for attackers to directly access electronic components, this provides tamper evidence for the device. The security relevant components (e.g. USB-to-Sata Bridge and controller) are sealed by an epoxy sealing. Additionally a warranty label is installed at the opening area of the enclosure.

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

31 Overall the TOE implements the following key security features:

- Confidentiality protection of user data by encryption
- Protection of TSF data

32 **Use cases of the DIGITTRADE HS256 S3**

Besides common use cases of secure storage media, like the transport of confidential data between two host systems using a storage device, the transport of the working environment of a user, the backup and the storage of confidential keys or digital certificates, the HS256 S3 provides additional use cases. As the encryption key is stored externally on the smart card and because of other security features of the HS256 S3, a wide variety of use cases arises.

Attention should be paid to the fact that the TOE with evaluation assurance level EAL2 is resistant to attacks performed by an attacker possessing basic attack potential.

- Secure and cost-effective data transport:
    - The encryption key will be stored on two different smart cards, which are accessible by two different persons. The storage device "DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD)" with confidential data can be sent via not especially secured communication ways, e.g. by mail in a security bag.
    - Both, the sender and the recipient have to ensure with each data transport, that they will be able to identify manipulations to the

HS256 S3. It must be paid attention, if the used security bags are unbroken. The same applies to all other transportation possibilities by the HS256 S3.

  - Additional security offers the use of multiple smart cards with different encryption keys, which are stored at the sender and the recipient. The smart cards with different encryption keys will be used in a certain order or according to prior agreement for the encryption and decryption of the data.

- Separation of storage device and authentication data:
  - The access to the data can be regulated in a way, that it will be only possible by bringing together of e.g. three persons. Person X possesses the storage device, person Y possesses the smart card (with key) and person Z knows the smart card PIN. These three persons get together only for the data transfer at the receiving center and separate afterwards again. Person X, Y and Z separately, are not able to access the data.
- Use of few storage devices at a wide circle of customers:
  - Each data recipient receives a smart card with its own encryption key. The data sender keeps a copy of the smart cards with the encryption keys of the particular recipients. For the data transport each available HS256 S3 can be used. Prior to this the required smart card will be initialized. The quantity of the storage devices can be reduced significantly.
- Use of few storage devices in field work and government agencies:
  - Each employee receives a smart card with his own encryption key. For the work outside of the company the employee can receive any available HS256 S3 that had been initialized for the employee before. The employee stores his data with his own encryption key. After use the HS256 S3 will be initialized with a new smart card for the next user.

1.2.3 Non-TOE hardware/software and firmware

33 The TOE needs a host system that provides an USB 2.0/3.0 interface that includes support for USB mass-storage class.

1.3 TOE boundary

34 The physical TOE boundary is defined by the host interface and the Authenticcation interface. Physically the TOE consists of the complete storage device including Java Card Applet and smart card.

1.4 TOE description

35 The scope of delivery is listed in table 1:

delivery item	type	Part of TOE
portable storage device “DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD)”, Version 1.0 With internal 2.5” SATA HDD or SSD drive (with 512 byte external sector size) from Samsung (preferred), Seagate, Western Digital, Toshiba or Hitachi. The following capacities are available: 120GB SSD, 160GB HDD, 250GB SSD, 320GB HDD, 500GB HDD/SSD, 640GB HDD, 750GB HDD/SSD, 1TB HDD/SSD, 1,5TB HDD/SSD, 2TB HDD/SSD, 4TB HDD/SSD.	hardware	Yes, TOE device
two smart cards NXP J2E081_M64 R3 with JCOP v2.4.2 R3, certified by NSCIB-CC-13-37761-CR2, loaded with DIGITTRADE HS256 S3 Java Card Applet version 1.1.0	hardware	Yes, TOE smart card
Guidance “DIGITTRADE High Security HS256 S3 – User Manual“, version 1.8 Printed version is inside the packaging box. Digital version can be downloaded at: http://www.digittrade.de/cms/support-center/download-center/?did=83 To validate the originality and integrity of the user manual the SHA-512 hash of the downloaded file must be equal to this value: 5aff4ca83276cdb572842ec131de0fb7a0f7a2bdb192e858a800238c1075c2d3233a90cfb537afcbcdbb2f36d9eb21f8e3707781e06696e2711cd9ee25f8a3e0	documentation	Yes, TOE guidance Only the digital version of the user manual is part of the evaluation.

User Manual important notice	documentation	Yes, TOE guidance
USB-Cable	accessory	No
Hard case	accessory	No
Security Bag	packaging	No

Table 1: TOE's scope of delivery

36 The scope of delivery of additional smart cards:

delivery item	type	Part of TOE
ordered quantity of smart cards NXP J2E081_M64 R3 with JCOP v2.4.2 R3, certified by NSCIB-CC-13-37761-CR2, loaded with DIGITTRADE HS256 S3 Java Card Applet version 1.1.0	hardware	Yes, TOE smart card
Security Bag	packaging	No

Table 2: TOE's scope of delivery of additional smart cards

37 The storage device HS256 S3 is composed as follows:

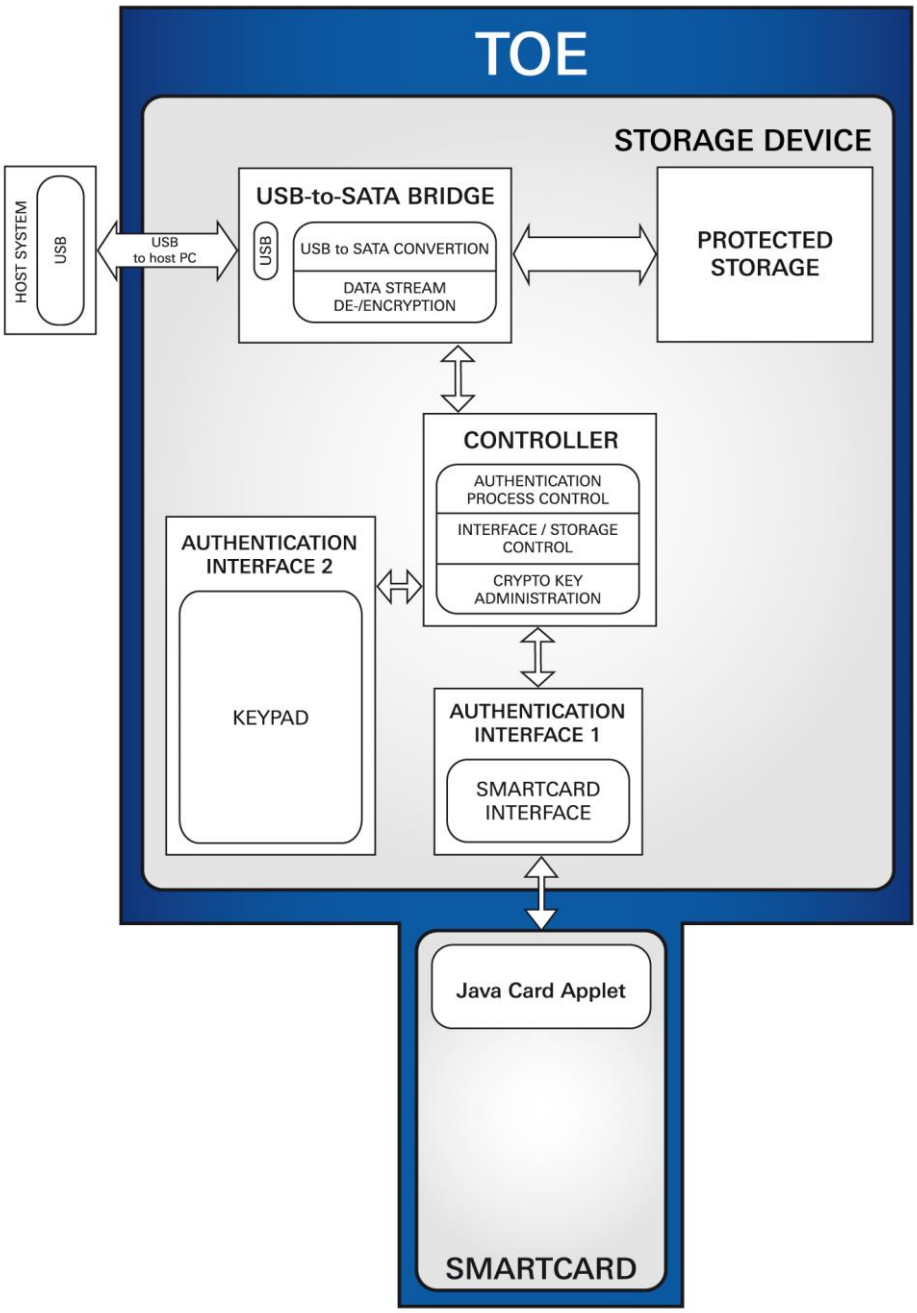
- Controller: regulates the data flow within the TOE and to the host system via USB interface. The controller controls access to the protected storage of the storage device and allows the administration of the encryption key. Only after successful authentication the controller establishes a connection to the protected storage. The firmware of the controller is listed in table 1 as type firmware.
- USB-to-Sata Bridge: allows the connection between the storage device and the host system via USB. It is also used for the encryption and decryption processes of the storage device. Due to the implemented crypto module the encryption and decryption processes take completely place inside of the storage device. In the deactivated state the crypto module includes no encryption key. The encryption key will be loaded into the crypto module for the encryption and decryption after successful authentication. The encryption key will be deleted off the crypto module, if the storage device will be disconnected from the power or the smart card removed off the storage device. The encryption key will be deleted actively off the crypto module of the storage device by triggered flip flops.
- Protected storage: this covers the complete HDD/SDD storage of the TOE. It contains the confidential data of the user and is therefore protected by the security functions of the TOE. The user is only granted access to the protected storage after successful authentication.

- Remark: The TOE does not contain a public storage area
- Authentication interface 1 (smart card interface): allows the communication between the smart card and the storage device.
- Authentication interface 2 (Keypad): Consists of 14 keys and serves for the entry of commands and digits that are necessary for the authentication and operation of the storage device.

38 Java Card Applet and smart card:

- The DIGITTRADE HS256 S3 Java Card Applet that is installed on a Java-based Smartcard from NXP with JCOP v2.4.2 R3 that is certified by NSCIB-CC-13-37761-CR2, serves together for the generation, the secure storage and the administration of the encryption key and smart card PIN.

39 Drawing 1 shows the structure of the TOE.



Drawing 1: TOE structure

40 The TOE guarantees the confidentiality of the data in the protected storage by four different security mechanisms:

- access control
- user authentication
- encryption
- administration of the ecnryption key

41 Access control: The controller of the storage device establishes a connection to the protected storage only after prior successful authentication by the user by smart card and PIN entry at the keypad. Access trials without successful authentication will be blocked by the storage device. For the authentication the TOE consists of two authentication interfaces: one smart card interface for the communication of the storage with the smart card and one keypad for the PIN entry.

42 User authentication:

- For the authentication it is necessary that the smart card will be inserted into the storage device and the appropriate 8-digit smart card PIN will be entered on the keypad of the TOE. On the smart card is the encryption key stored, which will be transmitted to the crypto module of the USB-to-Sata Bridge after successful PIN entry and will be stored temporarily inside of the crypto module of the USB-to-Sata Bridge for the encryption and decryption.
- After the smart card PIN had been entered 8 times incorrectly, the encryption key on the smart card will be destroyed and will not be available anymore. Additionally, the smart card will be terminated by the Java Card Applet.
- For the operation it is necessary that the smart card remains inserted in the storage device.
- The encryption key on the storage device will be deleted and the access to the data interrupted, if the storage device is disconnected from the power or the smart card is removed off the storage device. The encryption key will be deleted actively off the crypto module of the USB-to-Sata Bridge of the storage device by triggered flip flops.
- The authentication by the user only needs to be done once per session.
- The smart card PIN can be changed by the user. Only 8-digit PINs are accepted.
- When choosing the smart card PIN, trivial PINs should be excluded (e.g. ascending, descending or user related PINs)

43 Encryption: the third security mechanism of the TOE is the encryption of the data in the protected storage. The encryption ensures the confidentiality of the data especially in case of physical attacks to the HDD or SSD storage. All data and the separate sectors are encrypted by the integrated crypto module of the USB-to-Sata Bridge in real-time by an AES 256-bit (Advanced Encryption Standard) encryption key in XTS mode (XEX-based tweaked-codebook mode with ciphertext stealing). Multiple theft and differential crypto analysis of the device are explicitly not part of the Common Criteria evaluation.

44 Administration of the encryption key: by using this fourth security mechanism, with the aid of the TOE and the smart card PIN the user is able to generate, change or destroy the encryption key. Furthermore, with the aid of the smart card PIN the user is able to copy the encryption key onto another smart card.

- The encryption key will be generated and stored securely on an authorized and certified smart card by the user. For the generation of the encryption key the smart card requires the correct user authentication. The PIN at delivery is: 1-2-3-4-5-6-7-8. The user has to change the smartcard PIN before the first usage.
- The access to the encryption key is only allowed after correct entry of the 8-digit smart card PIN (user authentication). After the smart card PIN had been entered 8 times incorrectly, the encryption key on the smart card will be destroyed by generation of a new encryption key and will be not available anymore. Additionally, the smart card will be terminated by the Java Card Applet.
- After the generation of the encryption key, the smart card needs to be initialized for the use with the storage device.
- After the initialization, the protected storage will be formatted, whereby the encrypted storage will be created.
- The user is able to copy the encryption key from one smart card (smart card PIN is necessary) onto another. For that purpose the encryption key of one smart card first will be transmitted into the storage device and afterwards copied onto the other smart card, after the access to the other smart card had been authorized by entering the appropriate 8-digit smart card PIN (user authentication).
- The user is able to change the encryption key of a smart card by new generation (generation of a new key) at any time. Afterwards the initialization of this smart card on the storage device is necessary for the use. The access to the old data will only be limited possible with a smart card with the old encryption key in the context of data recovery.
- The user is able to destroy the encryption key on the smart card irreversibly by new generation. The access to data will only be possible with a different smart card with the appropriate encryption key.
- Furthermore, the encryption key can be destroyed on the smart card, if the smart card PIN had been entered 8 times incorrectly by generation of a new encryption key. The smart card will be terminated by the Java Card Applet.
- For the complete destruction of the encryption key, a new encryption key can be generated on the smart card. Thereby the old encryption key will be destroyed by the overwriting with the new encryption key by the Java Card Applet with random values from the smart cards RNG (Random Number Generator). In this context the storage device needs to be overwritten completely with random bits, by what any still available encryption keys on other smart cards will be useless.

- The Random numbers for the encryption key generation are provided by the RNG of the smart card. This RNG generates random numbers according to DRG.3 of AIS 20/31.[1]
- The encryption key will be deleted, if the storage device is disconnected from the power or the smart card is removed off the storage device. The encryption key will be deleted actively off the crypto module of the USB-to-Sata Bridge of the storage device by triggered flip flops.
- For the administration of the encryption key no software, no additional hardware and no host system is necessary.

45 A major feature of the TOE is the fact that the security functions are completely implemented within the TOE itself (see drawing 1). This means that the TOE is independent of the host system's configuration as long as an USB interface is available and accessible through the host's operating system. 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 storage.

46 The controller regulates the four security mechanisms: access control, user authentication, encryption and administration of the encryption key.

- The authentication mechanism is realized by the Java Card Applet and the PIN entry at the keypad of the storage device. Therefore the storage device transmits the entered PIN to the Java Card Applet. The PIN is verified by using a corresponding mechanism provided by the smart card and the encryption key is transmitted with the aid of the controller to the crypto module of the USB-to-Sata Bridge inside of the storage device, in case of the correct authentication data.
- If the authentication is successful, the controller establishes a logical connection to the protected storage and the data will be en-/decrypted.
- The controller enables also the administration of the encryption key: It enables generation, changing, copying and destruction of the encryption key as well as the initialization of a new smart card on the storage device.

47 The TOE is designed to be user-friendly. Apart from the authentication required at the outset, working with the TOE is not different from 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.

48 The encryption and decryption processes are performed transparently in the background for the user. After successful authentication only the data, which is needed for the action will be decrypted and transmitted to the host system.

[1] NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3, Security Target Lite, Rev. 00.02 – 13.08.2014, NSCIB-CC-13-37761-CR2,

49 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 storage 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 reactivated. The user must be re-authenticated in order to regain access to the protected storage.

50 The following functions are only available in combination with the device PIN. The device PIN is not part of the authentication data in the context of the Common Criteria evaluation:

- At delivery the device PIN is: 8-7-6-5-4-3-2-1. The user has to change the device PIN. Only 8-digit PINs are accepted.
- To initialize a smart card with a different encryption key on the storage device the user only need the TOE and the device PIN.
- With the aid of the smart card PIN and the device PIN the user is able to copy the encryption key onto another smart card.
- The Lock-out mode can be de-/ activated, using the device PIN.

51 The following features and use cases are outside the scope of the Common Criteria evaluation:

- The authentication data can be split among two persons. Authentication data 1 (person 1): encryption key on the smart card and smart card PIN. Authentication data 2 (Person 2): device PIN. If only the device PIN is known, the protected data will not be accessible.
- In special use cases it can be necessary that the smart card needs to be removed out of the storage device after successful authentication. E.g., if the security environment does not allow that the smart card remains inside of the storage device or if multiple storage devices are operated with one smart card. Therefore the lock-out mode can be deactivated and activated at any time (device PIN is necessary).
- Operation of several storage devices with only one smart card. The storage devices will be initialized with one smart card. Thereby larger data volumes can be sent at the same time or one after another. The recipient can access all storage devices with the same smart card.
- The TOE provides physical self-protection in the form of sealing encapsulation. The security relevant components (e.g. USB-to-Sata bridge and controller) are secured against physical manipulation trials by an epoxy sealing.
- Additionally, a warranty label is placed on the opening area of the enclosure.

2 Conformance Claims

52 The following sections describe the conformance claims.

2.1 CC conformance claim

53 This ST is [CC] Part 2 extended and Part 3 conformant.

2.2 PP claim

54 This ST claims conformance to [PP].

2.3 Package claim

55 This ST is conformant to an Evaluation Assurance Level of EAL2.

56 This ST claims also conformance to Extended Package “Extended Authentication PSMPP-EA” Version 1.0 that is defined in [PP]: “Extended Authentication PSMPP-EA” conformant.

2.4 Conformance Rationale

57 The TOE Type of this ST claims conformance to the TOE type of the Protection Profile [PP] by being identical.

58 The protection profile [PP] postulates “demonstrable conformance“. This security target realizes the demonstrable conformance as follows:

- The security problem definition is identical to the protection profile [PP].
- The security objectives of the TOE are identical to the protection profile [PP] with the following amendment: O.AuthAccess is originated from the extended package PSMPP-EA. The rationale is identical to [PP].
- The security requirements are identical to the protection profile [PP] with the following amendment: FIA_UAU.5-EA is originated from the extended package PSMPP-EA. The rationale is identical to [PP]. Furthermore operations have been performed and are marked.
- OE.AuthProt of PP is removed because the TOE provides its own authentication interface and does not rely on the host for authentication. Therefore the Security Objectives coverage in Chapter 4.3.1 has been changed.
- The roles in Chapter 3.2 are identical to the protection profile [PP] with the following amendment: Usage of smart card for Authorized TOE user.
- The FIA_UAU.5.1 of the PP has been modified by removing “one of” to define more precisely that it is necessary to have m1 as well as m2 at the same time to get access to the user data.

- The FMT_SMF.1.1 b) of the PP has been modified to be generalized.

59 The following Table 3: Realization of the application notes demonstrates the realization of the application notes of the protection profile [PP] in this ST.

No.	Ref.	Application Note	Implementation
1	1.2.3	The TSF data could be for example stored within a HSM (High Security Module) or in an encrypted form on the device.	is implemented
2	4.2	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.	Remark
3	4.3.1	Threats arising from repeated theft and differential crypto analysis of the device are explicitly not considered.	Remark
4	5.2	The ST author may remove OE.AuthProt if the TOE provides its own authentication interface and does not rely on the host for authentication.	OE.AuthProt of PP is removed because the TOE provides its own authentication interface and does not rely on the host for authentication.
5	6.1.5	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	The TOE contains a smart card.
6	FIA_ UAU.6	The re-authentication shall use the same authentication mechanism as the initial authentication.	Is implemented

No.	Ref.	Application Note	Implementation
7	FIA_ AFL.1	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.	8 failed attempts are evaluated to be enough, cf. chap. 7.
8	FIA_ AFL.1	Implementing this requirement may render the device unusable. It is up to the ST author to decide whether this is 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.	The security measure is appropriate, cf. chap. 7.
9	FCS_ CKM.1	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.	The used cryptographic algorithm is recommended by BSI, cf. [TR].
10	FCS_ CKM.1	The TOE will generate a new encryption key when ~~it is initialized or~~ a new key generation is explicitly requested.	remark
11	FCS_ CKM.4	Should the endorsed standards referenced in FCS_CKM.1 mandate key destruction methods, those are to be applied here. Please contact the certification body for the list of endorsed standards.	not applicable: FCS_CKM.1 do not refer to a key destruction method

No.	Ref.	Application Note	Implementation
12	FCS_ CKM.4	A typical scenario for key destruction would be the ~~re-initialization~~ re-generation of the encryption key for the device. If data wiping is included in the security functionality of the TOE, this could be implemented by key deletion.	New generation of the cryptographic key destroys the old one. For the use of the generated encryption key on the storage device, the smart card needs to be initialized on the storage device. Afterwards the complete storage device needs to be overwritten with random bits, by what any still available encryption keys on other smart cards will be useless. According to the assurance level EAL2 this will be done by the user. The user will be guided by user documentation.
13	FCS_ CKM.4	If a TOE user suspects the TOE to be compromised, he should completely wipe it, not just reset it by deleting the key.	remark
14	FCS_ COP.1	Please contact the certification body for the list of endorsed standards.	The used cryptographic algorithm is recommended by BSI, cf. [TR].

No.	Ref.	Application Note	Implementation
15	FMT_SMF.1	Further management functions can be specified by an ST author.	Further management functions are not necessary.
16	FMT_SMF.1	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.	remark: Keys need to be deleted on all smartcards that contain those keys. deleting data storage will be done by organisational measures
17	FDP_RIP.1	Deallocation in the context of this PP is defined as logical or physical termination of the host connection.	remark: Logical termination of the host connection is realised by removing the smartcard from the hard drive. Physical termination of the host connections is realized by removing all physical connections to the hard drive including power supply.
18	FPT_FLS.1	The details of the secure state are defined in O.FailSafe.	remark
19	FPT_FLS.1	The integrity of the storage data on the device is not in the scope of the PP.	remark

No.	Ref.	Application Note	Implementation
20	FPT_FLS.1	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.	remark
21	FPT_SDC.1	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.	The TOE contains a smart card.
22	8.5.1	When using this extended package, O.AuthAccess-EA replaces O.AuthAccess from the base PP	is realized
23	8.5.1	The remainder of the rationale is to be taken from the base PP.	is realized
24	FIA_UAU.5	The authentication methods used have to consist of at least one cryptographic token and a second method.	two-factor authentication (key on smart card and knowledge of PIN) is implemented with a smart card as cryptographic token
25	FIA_UAU.5	The weaker of the two methods has to satisfy FIA_SOS.1 from the base PP.	is implemented

Table 3: Realization of the application notes

3 Security Problem Definition

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

3.1 Assets

61 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 (Authentication data is defined as key on the smart card and smart card PIN) and cryptographic key material used for the encryption of the user data.

3.2 Roles

62 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

63 **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 (change smart card PIN, change cryptographic key on the smart card).
- Has no read access to TSF data.
- Is allowed to administrate the smart card in the following ways: generation, re-generation and destruction of the cryptographic key on the smart card.
- Is allowed to copy the cryptographic key of one smart card onto another

64 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 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.

3.3 Threats

65 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.

66 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 portable storage medium.
- Can gain possession of the TOE relatively easily since the TOE has a compact form.
- Does not hold the authentication data.

3.3.1 Threats countered by the TOE

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

68 **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.

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

70 **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 Threats arising from repeated theft and differential crypto analysis of the device are explicitly not considered.

3.3.2 Threats countered by the TOE environment

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

3.4 Organizational Security Policies

72 This security target does not specify any organizational security policies.

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

3.5 Assumptions

74 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.

75 **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.

4 Security Objectives

4.1 Security Objectives for the TOE

76	**O.ProtectTSF**	The TOE must provide protection for TSF data so that authentication data and cryptographic key material are protected from access.
77	**O.AuthAccess-EA**	The TOE must provide a **two-factor** authentication mechanism to allow only authenticated users access to the protected storage area.[2]
78	**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.
79	**O.AuthChange**	Only authenticated users are allowed to change the authentication data.
80	**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.

4.2 Security Objectives for the Operational Environment

81	**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.
82	**OE.AuthConf**	The TOE users must keep their authentication data confidential.
83	**[…]**	

[2] Taken from Extended Package PSMPP-EA [PP].

4.3 Security Objectives Rationale

4.3.1 Security Objectives coverage

Objective	Threat	Assumption
O.ProtectTSF	T.LogicalAccess, T.PhysicalAccess	
O.AuthAccess-EA[2]	T.LogicalAccess (from the base PP)	
O.Encrypt	T.PhysicalAccess	
O.AuthChange	T.AuthChange	
O.FailSafe	T.Disruption	
OE.TrustWS		A.TrustedWS
OE.AuthConf	T.LogicalAccess	
[…]	[…]	

Table 4: Objectives tracing to threats and assumptions

4.3.2 Security Objectives sufficiency

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

85 **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[2]. 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 […]. This security objective for the environment is necessary to ensure a secure usage of the authentication mechanism.

86 **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.

87 **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.

88 **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.

89 **A.TrustedWS**

The assumption of a trusted workstation is supported 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.

5 Extended Components Definition

5.1 FPT_SDC Trusted storage of TSF data

90 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.

5.1.1 Family Behavior FPT_SDC

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

5.1.2 Component Leveling FPT_SDC.1

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

5.1.3 Management FPT_SDC.1

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

94 There are no management activities foreseen.

5.1.4 Audit FPT_SDC.1

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

96 There are no actions defined to be auditable.

5.1.5 FPT_SDC.1 Trusted storage of TSF data

97 Hierarchical to: No other components.

98 Dependencies: No dependencies.

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

5.1.6 Rationale

100 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.

6 Security Requirements

6.1 Security Functional Requirements

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

102 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.

103 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 by the ST author are *italicized*; in addition, a footnote will show the original text from CC, Part 2.

104 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 by the ST author are *italicized*; in addition, a footnote will show the original text from CC, Part 2. 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*.

6.1.1 Identification and Authentication (FIA)

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

106 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.5-EA Multiple authentication mechanisms[2]

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: *smartcard*[3] and m2: *PIN*[4,5] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the success of both authentication mechanisms[6].

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[7].

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[8].

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 *8 (eight)*[9] unsuccessful authentication attempts occur related to the authentication of the user[10].

[3] *[selection: smartcard, [assignment: other cryptographic token]]*

[4] *[selection: password, PIN, biometric authentication, [assignment: other authentication mechanism]]*

[5] [assignment: list of multiple authentication mechanisms]

[6] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

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

[8] [assignment: a defined quality metric]

FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[11], the TSF shall disable access to the protected storage area[12].

6.1.2 Cryptographic Operation (FCS)

107 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 *for AES keys by requesting random numbers from the RNG provided by the Smartcard*[13] and specified cryptographic key sizes *2x 256 Bit*[14] that meet the following: *[AES]*[15].
Application note:	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

---

[9] *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]*

[10] [assignment: list of authentication events]

[11] [selection: met, surpassed]

[12] [assignment: list of actions]

[13] [assignment: cryptographic key generation algorithm]

[14] [assignment: cryptographic key sizes]

[15] [assignment: list of Endorsed standards]

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 *over-write with new generated key*[16] that meets the following: *none*[17].
Application Note:	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*[18] in accordance with a specified cryptographic algorithm *AES in XTS-Mode*[19] and cryptographic key sizes *2x 256 Bit*[20] that meet the following: *[AES] and [XTS]*[21].

6.1.3 Management Functions (FMT)

108 The TOE supports management functions for the role of the authenticated user to alter authentication data or to generate the encryption key.

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

[16] *[assignment: cryptographic key destruction method]*

[17] *[assignment: list of **Endorsed** standards]*

[18] [assignment: list of cryptographic operations]

[19] *[assignment: cryptographic algorithm]*

[20] *[assignment: cryptographic key sizes]*

[21] *[assignment: list of **Endorsed** standards]*

b) ~~initialization of the device by~~ *explicit* generation of the encryption key and deletion of any previous keys[22]

Application Note: Deletion of the previous keys on all smartcards containing those keys will render old encrypted data on the device useless.

6.1.4 User Data Protection (FDP)

109 User data is 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[23] the following objects: plaintext user and TSF data[24].

Application Note: Deallocation in the context of this ST is defined as logical or physical termination of the host connection. The logical termination is defined by removing the smartcard from the hard drive. The physical termination is defined as removing all physical connections to the hard drive, including power supply.

6.1.5 Protection of TSF Data (FPT)

110 The TOE is expected to handle disruptions in a fail-secure way, removing any access in case of failures. It will not allow direct physical access to the physical storage of protected data and TSF data.

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[25].

[22] [assignment: list of management functions to be provided by the TSF]

[23] [selection: allocation of the resource to, deallocation of the resource from]

[24] [assignment: list of objects]

[25] [assignment: list of types of failures in the TSF]

Application Note:	The details of the secure state are defined in O.FailSafe.
Application Note:	The integrity of the storage data on the device is not in the scope of the ST.
Application Note:	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.

FPT_SDC.1 Trusted storage of TSF data

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_SDC.1	The TSF must provide secure storage for authentication data and cryptographic key material.

6.2 Security Assurance Requirements

111 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.

6.3 Security requirements rationale

6.3.1 Rationale for Security Functional Requirements

Internal Consistency of Requirements

112 The mutual support and internal consistency of the components selected for this security target is described in this section.

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

6.3.1.1 Authentication

114 Users accessing the protected storage area shall be authenticated with a two-factor mechanism before being allowed access to the protected storage area (FIA_UAU.5-EA).[2] The TOE shall provide the capability to lock access after too many unsuccessful authentication attempts.

115 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 requirements on residual information protection (FDP_RIP.1) ensure that no residual TOE data is available.

6.3.1.2 Cryptographic Support

116 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.

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

6.3.1.3 Management Functions

118 The TOE shall enable authenticated users to modify the security attributes used for authentication and to generate the encryption key.

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

6.3.1.4 Protection of TSF Data

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

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

6.3.2 Security Requirements Coverage

SFR	O.Protect TSF	O.Auth-Ac-cess-EA	O.En-crypt	O.Auth-Change	O.Fail-Safe
FIA_UAU.2		X			
FIA_UAU.5-EA[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 5: SFR objective tracing

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

123 **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.

124 **O.AuthAccess-EA**[2] 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.

125 **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.

126 **O.AuthChange** Management of the authentication data is modeled by FMT_SMF.1 and supported by FIA_UAU.6.

127 **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.

Security Requirements Dependency Analysis

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

SFR	Dependencies identified in [CC]	Resolved in ST / Rationale for unresolved dependencies
FIA_UAU.2	FIA_UID.1	Not resolved as the TOE does no need user IDs. Only authentication is required.
FIA_UAU.5-EA[2]	none	N/A
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 6: SFR dependency resolution

6.3.3 Rationale for Security Assurance Requirements

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

7 TOE summary specification

7.1 TOE security functionality

130 The TOE offers the following security functions to realize the security requirements.

7.1.1 SF1 „Access control“

131 Access control for access to the cryptographic key is realized by the security function SF1:

- The user enters the 8-digit smart card PIN at the storage device. The 8-digit PIN consists of digits between 0 and 9.
- The storage device transmits this PIN via ISO 7816 command to the Java Card Applet. The PIN is verified by using a corresponding mechanism provided by the smart card, i.e. the smart card replies to the Java Card Applet with an error code, if the PIN was wrong and with a confirmation code if the PIN was correct.
- If the PIN was correct, the smart card will be activated.
- The Java Card Applet sends a confirmation code to the storage device.

132 Afterwards the smart card stays in the authorized state until the session will be terminated by removing of the smart card or disconnection of the power.

133 If access is granted the user will get an acoustical feedback from the TOE and the TOE will be available as a storage media on the Host system. Furthermore the “Status”-LED of the TOE is enlighten in red or green color according to the setting of the lock-out mode. If access is denied the user will get an acoustical feedback and the “Error”-LED starts blinking in red color.

134 Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below one in 1,000,000.

135 If the smart card PIN had been entered 8 times incorrectly, the encryption key on the smart card will be destroyed and the smart card will be terminated by the Java Card Applet.

136 The initial smart card PIN is “1-2-3-4-5-6-7-8”. The user is able to change the PINs, cf. SF2. The user has to change the smartcard PIN before the first usage.

137 The utilized smart card PIN is stored securely on the individual smart card.

7.1.2 SF2 „Change PIN“

138 It is possible to change the authentication data smart card PIN on the smart card by the security function SF2:

139 SF2 is realized as follows:

- The user enters on the keypad of the storage device the command for the changing of the PIN and the 8-digit smart card PIN.

- The storage device transmits this command and the PIN via ISO 7816 command to the smart card. The smart card replies with an error code, if the PIN was wrong and with a confirmation code if the PIN was correct.
- If the smart card PIN was correct, the smart card allows the input of a new smart card PIN:

  The user enters the new smart card PIN twice.

  The portable storage device verifies, if the PIN consists of 8 digits and if the two PINs are identical. Otherwise the smart card rejects the process with an error code.

  The storage device transmits the appropriate ISO 7816 commands to the smart card.

140 If the smart card PIN had been entered 8 times incorrectly, the encryption key on the smart card will be destroyed and the smart card will be terminated by the Java Card Applet.

7.1.3 SF3 „Key generation and key destruction"

141 The cryptographic key needs to be generated initially on the smart card (user responsibility) after access is granted with SF1. Therefor the cryptographic key generation algorithm RNG of the certified smart card is used with cryptographic key size of 2x 256 Bit and AES [AES]. This RNG generates random numbers according to DRG.3 of AIS 20/31. For key generation the portable storage device transfers an ISO 7816 command to the smart card. The encryption key is stored securely on the smart card.

142 For the destruction of the encryption key on the smart card, a new key will be generated. By the generation of a new encryption key, the old encryption key will be destroyed by overwriting with the new encryption key. Therefore SF1 has to be executed.

143 For the use of the generated encryption key on the storage device, the smart card needs to be initialized on the storage device. (user responsibility)

144 Afterwards the complete storage device needs to be overwritten with random bits, by what any still available encryption keys on other smart cards will be useless. According to the assurance level EAL2 this will be done by the user. The user will be guided by user documentation.

145 The encryption key on the storage device will deleted, if the storage device is disconnected from the power or the smart card is removed off the storage device if the lock-out mode is activated. The encryption key will be deleted actively off the crypto module of the USB-to-Sata Bridge of the storage device by triggered flip flops. The lock-out mode can be deactivated, but in order to use the TOE in certified mode the Lock-out mode must be activated.

146 Deallocation in the context of this ST is defined as logical termination of the host connection by removing the smartcard from the hard drive. Physical termination of the host connections is defined as removing all physical connections to the hard drive, including power supply. If the logical or the physical

connection between the TOE and the host system being lost, the TOE ensures that the data in the storage 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 regain access to the protected storage.

147 Administration of the encryption key: with the aid of the TOE and the smart card PIN the user is able to generate, change or destroy the encryption key. Furthermore, with the aid of the smart card PIN the user is able to copy the encryption key onto another smart card.

7.1.4 SF4 „Encryption and decryption“

148 The TOE provides encryption mechanisms and realized thereby the protected storage. For encryption and decryption the TOE uses the cryptographic algorithm:

- AES in XTS mode with 2x 256 Bit keys according to [AES, XTS].
- As the XTS mode requires 2x 256 bit keys the controller provides a 512-bit key value form the smartcard which is split into Key_1 and Key_2. The LBA (Local Block Addressing) of the HDD / SSD is used as the data unit number and is used with Key_2 for the tweak generation. The encryption of the data is done by AES and Key_1 in conjunction with the tweak.

149 For the encryption and decryption the AES keys are used, which had been transmitted by the smart card.

7.1.5 SF5 „Secure state“

150 The TOE preserves a secure state and provides re-authentication of the user when the following types of failures occur:

- abnormal abort of the TSF
- system crash in the host,
- power failure,
- unintentional physical disconnection or
- other disruption to the connection.

7.2 TOE summary specification rationale

151 In table 7 and 8 is demonstrated that the prior defined TOE security functions are suitable to fulfill the security functional requirements:

security requirements	security functions
FIA_UAU.2	SF1, SF2, SF3
FIA_UAU.5-EA[2]	SF1
FIA_UAU.6	SF2, SF3
FIA_SOS.1	SF2, SF1

security requirements	security functions
FIA_AFL.1	SF1, SF2, SF3
FCS_CKM.1	SF3
FCS_CKM.4	SF3
FCS_COP.1	SF4
FMT_SMF.1	SF2, SF3
FDP_RIP.1	SF3
FPT_FLS.1	SF5
FPT_SDC.1	SF1, SF3

Table 7: Mapping from security requirements to security functions

security functions	security requirements
SF1	FIA_UAU.2, FIA_UAU.5-EA, FIA_AFL.1, FIA_SOS.1, FPT_SDC.1
SF2	FIA_SOS.1, FMT_SMF.1, FIA_AFL.1, FIA_UAU.2, FIA_UAU.6,
SF3	FCS_CKM.1, FCS_CKM.4, FIA_UAU.2, FIA_UAU.6, FIA_AFL.1, FDP_RIP.1, FMT_SMF.1, FPT_SDC.1
SF4	FCS_COP.1
SF5	FPT_FLS.1

Table 8: Mapping from security functions to security requirements