ST Engineering
Electronics

DiskCrypt M100 (Enterprise)
Security Target

DiskCrypt M100 (Enterprise)
Security Target
Contents

Chapter 1 Security Target Introduction 4
1.1 Security Target Reference 4
1.2 TOE Reference Identification 4
1.3 TOE Overview 4
1.3.1 TOE Type 6
1.3.2 Non-TOE Hardware/Software and Firmware 7
1.4 TOE Description 7
1.4.1 Physical Scope of the TOE 7
1.4.2 Logical Scope of the TOE 8
Chapter 2 Conformance Claims 10
Chapter 3 Security Problem Definition 11
3.1 Asset 11
3.2 Threats 11
3.3 Organizational Security Policies 11
3.4 Assumptions 12
Chapter 4 Security Objectives 13
4.1 Security Objectives for the TOE 13
4.2 Security Objectives for the Operational Environment 13
4.3 Security Objective Rationale 14
Chapter 5 Extended components definition 16
Chaper 6 IT Security Requirements 17
6.1 Conventions 17
6.2 Security Functional Requirements 17
6.1.1 Class FIA: Identification and Authentication 17
6.1.2 Class FCS: Cryptographic support 18
6.1.2 Class FDP: User Data Protection 19
6.1.3 Class FMT: Security management 20

6.1.4 Class FPT: Protection of the TSF 21
6.3 Security Requirement Dependency Rationale 22
6.4 Security Requirements to Security Objective Mapping 24
6.5 Security Assurance Requirements 28
6.5.1 Rationale for Security Assurance Requirements 29
Chapter 7 TOE Summary Specification 30
7.1 SF1 – Identification and Authentication 30
7.2 SF2 – Cryptographic Support 30
7.3 SF3 – Security Management 31
7.4 SF4 – Protection of the TSF 31
7.5 TOE Summary SFR to TSF mapping 32

List of Illustrations

Table 1 - Assets protected by the TOE....11
Table 2 - Threat Statements....11
Table 3 - Assumptions....12
Table 4 - Security Objectives for the TOE....13
Table 5 - Security Objectives for the Operational Environment....14
Table 6 - Security Objective Rationale....15
Table 7 - Security Requirement Dependency Rationale....23
Table 8 - Security Requirements to Security Objective Mapping....25
Table 9 - Security Objective to SFR mapping Rationale....28
Table 10 - Assurance Components....29
Table 11 - SFR to Security Functions mapping....33

Chapter 1 Security Target Introduction

This document defines the security functionality of the target of evaluation (TOE) "DiskCrypt M100 (Enterprise)"

1.1 Security Target Reference

Security Target Reference:

DiskCrypt M100 (Enterprise) Security Target

Security Target Publication Date: 16 July 2018

Document Version: 2.0

1.2 TOE Reference Identification

TOE Reference:

DiskCrypt M100 (Enterprise)

ID: 9910-8000-1239

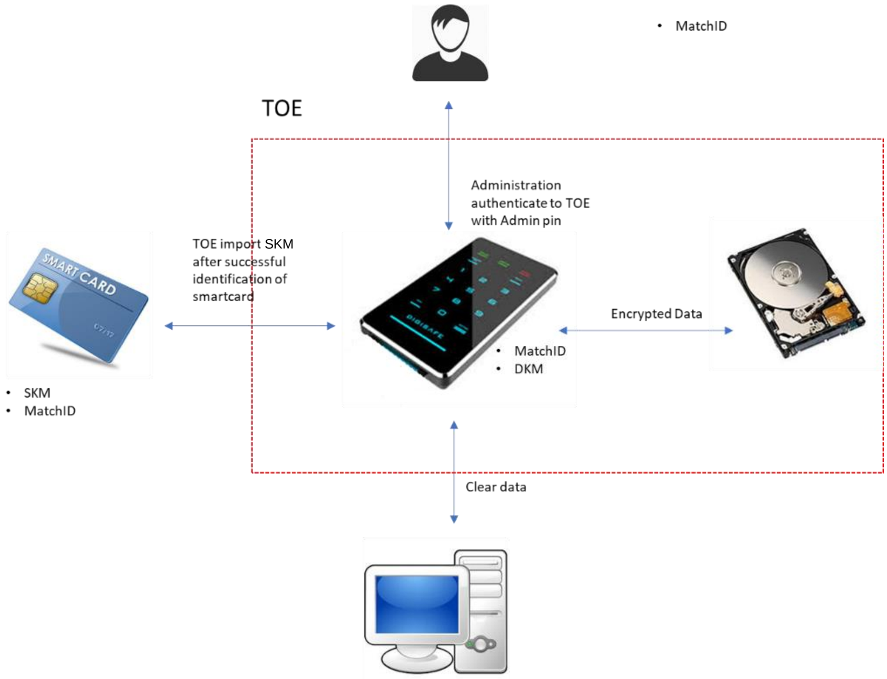
Ver: M253P15AO206

1.3 TOE Overview

The TOE is a portable USB encrypted storage device which provides a full disk encryption/decryption function for user data in the 2.5” SATA hard disk within the TOE.

The TOE interoperates with an authorized paired smartcard which stores the input keying material to the key derivation function for the Data Encryption Key (DEK). The smartcard and the PIN to the smartcard must be provided by the user before access to the user data is granted.

TOE Usage


• MatchID
TOE
Administration authenticate to TOE with Admin pin
TOE import SKM after successful identification of smartcard
SMART CARD
• SKM
• MatchID
Encrypted Data
• MatchID
• DKM
Clear data

The TOE has a built-in keypad and smartcard reader. It is powered via its USB interface (USB 3.0/2.0) by connecting it to a host machine. The TOE requires users to insert their authorized external smartcard and input his/her smartcard PIN via the integrated keypad of the TOE to authenticate to the smartcard. Upon successful user authentication to the smartcard, access to the user data is granted.

Security Features

The TOE employs hardware-based full disk encryption using the AES-256 XTS algorithm to encrypt all data in the hard disk.

The TOE performs full disk encryption using a Data Encryption key (DEK) derived from 2 separate keying materials. The first keying material (SKM – Smartcard Keying Material) is retrieved from the user smartcard. The second keying material (DKM – Device Keying Material) is injected into the TOE during device setup by the administrator.

The TOE ensures that the DEK, SKM, and Admin PIN are zeroized when no longer used.

The TOE is inbuilt with self-test mechanisms – Power-On-Self-Test (POST) and Known Answer Test (KAT). These self-tests mechanisms ensure the integrity and functionality of the TOE.

The TOE is designed with a screwless case enclosure whereby any tampering of the TOE to gain physical access to internal circuitry would be detectable by the user.

The TOE provides the following administrative functions:

1) Pairing of smartcard
2) DKM injection (during device setup)
3) Enable/disable smartcard lockout mode
4) Changing of Admin PIN

The TOE ensures that usage of the administrative functions requires the Administrator to authenticate to the TOE by inserting the paired smartcard and providing the Admin PIN. The TOE will disable the administrative function if there are eight consecutive Administrator authentication failures.

Prior to the issuance of the TOE and smartcard to the end-user, the TOE requires the Administrator to setup each TOE with its associated smartcards through the invocation of the above mentioned TOE administrative functions.

1.3.1 TOE Type

The TOE is a portable USB encrypted storage device which provides real time full disk encryption/decryption function for user data in the 2.5” SATA hard disk within the TOE.

1.3.2 Non-TOE Hardware/Software and Firmware

The following components described are hardware/software for supporting some of the TOE device functionality. These components are not part of the physical TOE for evaluation.

1. **DCM Smartcard** – Two types of smartcards are provided: Admin smartcard and User smartcard. The smartcards are PKCS #11 compliant. The Admin smartcard stores the DKM and the User smartcard stores the SKM. DKM and SKM are inputs to the key derivation function for the DEK. The smartcards are also used for identification.
2. **DiskCrypt Key Management Software (DMS) Verison 2.4** – The smartcards issued along with the DiskCrypt M100 are provisioned by the Administrator using the DiskCrypt Key Management software (DMS). The DMS is an external software application for enterprises to manage their own smartcards and SKM for usage with DiskCrypt M100.

   Administrators may refer to the DMS Guide for installation and operation guidance.
3. **AWP Manager Software Version 2.2** – AWP Manager is a software application used for performing cryptographic modification of smartcards issued with DiskCrypt. It communicates with the smartcards through a PKCS #11 module. It provides Administrators the means to perform PIN unblock and change the default PIN on the smartcards.
4. **Host Workstation** – The TOE requires a host system that provides an USB 2.0/3.0 interface supporting the USB mass storage device class.

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The physical scope of the TOE is defined by the enclosure and hardware components which provide the cryptographic function, authentication mechanism, interfaces for authentication, LED indicators and hard disk. It does not include the smartcard.

The scope of delivery (of the TOE) is listed as follow:

No.	Delivery Items	Version	Type	Part of TOE
1	DiskCrypt M100	ID: 9910-8000-1239 Ver: M253P15AO206	Hardware	Yes
2	DCM Smartcards (User and Admin)	Oberthur ID-One Cosmo v7-n	Hardware	No
3	USB 3.0 cable	-	Hardware	No
4	DiskCrypt M100 User Manual	Issue A	Hard-copy Document	Yes
5	2.5 inch SATA hard disk	-	Hardware	Yes
6	DMS Software	Version 2.4	Software Application	No

7	AWP Manager Software	Version 4.6	Software Application	No
8	DiskCrypt M100 Administrator Guide	Version 1.0.0	Soft copy Document (*.pdf)	Yes
9	DiskCrypt Key Management Software Guide	Version 1.0.0	Soft copy Document (*.pdf)	No
10	AWP Manager Guide	Version 1.0.0	Soft copy Document (*.pdf)	No

Items 6-10 (software deliverables and soft copy documents) are burnt into a CD and along with the other items from 1-5, are packaged in a box and delivered via either:

- In-house delivery – for Local delivery (Singapore)
- Trusted courier – for Overseas delivery

The TOE is shipped with a default factory configuration.

1.4.2 Logical Scope of the TOE

The TOE provides the core security functionalities in the following areas.

Identification

The TOE requires the user to be identified before either access to the administrative functions can be granted or user data can be decrypted.

Authentication

The TOE requires the Administrator to be authenticated before they are allowed to administer the TOE using the administrative functions available in the TOE.

Administrators shall present the paired Admin smartcard and input the correct Admin PIN via the integrated keypad, authenticating to the TOE. During Administrator authentication, a hash of the input Admin PIN is computed and compared with the stored hash value. Upon successful authentication, the administrative function selected will be successfully invoked. The Admin PIN is zeroized upon completion of usage.

Cryptographic Support

User data sent from the host machine via the USB interface will be encrypted and stored in the Hard disk. Similarly, all data retrieved from the encrypted storage will be decrypted and sent to the host machine. Data encryption is performed using the DEK (AES-256 XTS algorithm) to provide user data confidentiality.

The DEK is derived from 2 separate keying materials. The first keying material (SKM – Smartcard Keying Material) is retrieved from the user smartcard. The second keying material (DKM – Device Keying Material) is injected into the TOE during device setup by the administrator.

The TOE performs Hashing to verify integrity of TSF data (TOE application, configuration data, DKM and Admin PIN) during POST. The Admin PIN is stored as a hash within the TOE during device setup.

The TOE performs zeroization of TSF data (SKM and DEK) when no longer required.

Administrative Management

The TOE provides the following administrative functions:

1) Injection of DKM into the TOE during device setup
2) Pairing a User smartcard with the TOE
3) Change Admin Pin
4) Enable/disable the Smartcard Lockout mode
   This function controls the behavior of TOE when the smartcard is removed (after user authentication). The Smartcard Lockout mode is enabled by default: In this mode, DEK is zeroized from internal RAM memory upon removal of smartcard. The TOE requires users to re-authenticate to the smartcard should the user wish to access the user data again. If Smartcard Lockout mode is disabled, users may continue to access the encrypted user data even after smartcard removal.

Protection of TSF

The TOE implements the Power-On Self-Test (POST) of the Micro Controller Unit (MCU) during initial startup to ensure the integrity and functionality. Separately, the TOE implements a Known Answer Test of the cryptographic module upon the cryptographic module’s startup to ensure correct operation.

The TOE performs zeroization of the Admin PIN.

The TOE is built with a tamper evident casing where any physical tampering to access the internal circuitry can be detected.

Chapter 2 Conformance Claims

The following conformance claims are made for the TOE and ST:

CCv3.1 Rev.5 conformant. The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 5.

Part 2 conformant. The ST is Common Criteria Part 2 conformant.

Part 3 conformant. The ST is Common Criteria Part 3 conformant.

Package conformant. The ST is package conformant to the package Evaluation Assurance Level EAL2.

Protection Profile conformant. The ST claims conformance to the following Protection Profiles: **None.**

Chapter 3 Security Problem Definition

3.1 Asset

The TOE is concerned with the protection of the following assets enumerated in the table below.

Identifier	Asset statement
AST.DATA	Confidential plaintext user data stored in or processed by the TOE.
AST.TSF_DATA	MatchID, DEK, SKM, DKM, Admin PIN and configuration data of the TOE.

Table 1 - Assets protected by the TOE

3.2 Threats

Threats enumerated in Table 3 are relevant to the TOE.

Identifier	Threat statement
T.LOGICAL_ ACC	An attacker compromises the confidentiality of AST.DATA or gain unauthorized access to AST.TSF_DATA by means of logical attack on the TOE through the available interfaces provided by the TOE.
T.PHYSICAL_ACC	An attacker compromises the confidentiality of AST.DATA or gain unauthorized access to AST.TSF_DATA by means of physical attack, bypassing the logical interfaces of the TOE.
T.MALFUNCTION	An attacker may use a malfunction of the TOE to deactivate, modify, or circumvent security functions of the TOE to enable attacks against the confidentiality of AST.DATA or gain unauthorized access to AST.TSF_DATA.

Table 2 - Threat Statements

3.3 Organizational Security Policies

No organizational security policy is defined for the TOE.

3.4 Assumptions

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

A.TRUSTED_USER	Users of the TOE are able to operate the TOE in a secure manner in accordance to the user guidance documentation.
A.ADMIN	Administrator of the TOE is trusted, trained, competent, and adheres to all guidance documentation provided.
A.SMARTCARD	DCM Smartcard provides appropriate protection for the SKM.

Table 3 – Assumptions

Chapter 4 Security Objectives

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

4.1Security Objectives for the TOE

Security objectives for the TOE are enumerated in the table below.

Identifier	Objective Statement
O.DATA_ACC	Access to user data is only granted to legitimate users.
O.ADMIN_ACC	Access to administrative functions and TSF data are only granted to legitimate administrators.
O.TOE_INTEGRITY	The security state of the TOE, including TSF data stored persistently on the TOE, is protected against unauthorized modification, and can only be altered by authorized and authenticated parties.
O.ENCRYPT	User data stored in the hard disk is encrypted, providing confidentiality protection in the event of physical and logical attacks on the TOE.
O.PHYSICAL	The TOE shall enable the user to detect any physical tampering that might compromise the TSF.

Table 4 - Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

Identifier	Objective Statement
OE.TRUSTED_USER	The TOE users must operate the TOE in accordance to the user guidance documentation.
OE.ADMIN	Administrator of the TOE must administer the TOE in accordance to the admin guidance documentation.
OE.SMARTCARD	The cryptographic smartcard used together with the TOE must conform to the following: • Secure Signature Creation device Protection Profile Type 2 v1.04, EAL 4+ • Secure Signature Creation device Protection Profile Type 3 v1.05, EAL 4+

Table 5 - Security Objectives for the Operational Environment

4.3 Security Objective Rationale

Threat/Assumption	Objective	Rationale
T.LOGICAL_ACC	O.DATA_ACC O.ADMIN_ACC O.ENCRYPT OE.SMARTCARD	O.DATA_ACC ensures that only identified users are allowed to access the user data. O.ADMIN_ACC ensures that only authorized administrators are allowed to access the TOE's administrative functions and TSF data. O.ENCRYPT ensures that user data are encrypted and prevents unauthorized access to user data. O.DATA_ACC, O.ADMIN_ACC, and O.ENCRYPT makes use of OE.SMARTCARD for user identification and storage of SKM.
T.PHYSICAL_ACC	O.PHYSICAL O.ENCRYPT	O.PHYSICAL ensures that the TOE enables the user to detect any physical tampering of the TOE that may compromise the TSF. O.ENCRYPT ensures that user data are encrypted prior to storage in the hard disk, hence preventing adversaries from compromising the confidentiality of user data in the event that the TOE (with hard disk) is physically compromised. O.ENCRYPT also ensures that secrets within the TOE, such as the Admin PIN and keying materials (SKM, DEK) are zeroized upon completion of usage.
T.MALFUNCTION	O.TOE_INTEGRITY	O.TOE_INTEGRITY requires the TOE to perform self-tests to ensure that TOE is functional and TSF data is not modified. In the event that self-test fails, the TOE shall preserve a secure state (non-operational).
A.TRUSTED_USER	OE.TRUSTED_USER	OE.TRUSTED_USER ensures that users practice proper usage procedures in accordance to the user guidance documentation.

A.ADMIN	OE.ADMIN	OE.ADMIN ensures that administrative personnel will administer the TOE in accordance to the admin guidance documentation.
A.SMARTCARD	OE.SMARTCARD	OE.SMARTCARD ensures that the DCM Smartcard is certified and therefore provides appropriate protection for the SKM.

Table 6 - Security Objective Rationale

Chapter 5 Extended components definition

There are no extended components applicable to the TOE, hence none of the requirements for the Extended Components Definition (ASE_ECD) are applicable to this ST.

Chaper 6 IT Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

6.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with ***bold italicized*** text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with *italicized* text;
- Iteration: Indicated by appending the iteration symbol.

  e.g. FCS_COP.1/AES, FCS_COP.1/Hash

6.2 Security Functional Requirements

6.1.1 Class FIA: Identification and Authentication

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

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

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 **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrator**.

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 ***the requirements where the PIN entered through the Keypad must be 8 digits in length.***

Application Note: Applicable to the authentication of Administrator.

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)*** unsuccessful authentication attempts occur related ***to the authentication of the Administrator.***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall ***disable all future access to Administrative functions of the TOE***.

6.1.2 Class FCS: Cryptographic support

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 **DEK** in accordance with a specified cryptographic key generation algorithm ***key derivation function*** and specified cryptographic key sizes **512 bits** that meet the following: ***None.***

Application Note: Applicable to FCS_COP.1/AES

FCS_CKM.4/MCU 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/MCU The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***7 rounds of zeroization*** that meets the following ***none.***

Application Note: Applicable to zeroization of DEK from MCU.

FCS_CKM.4.1/Crypto The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***writing zero to the specific memory location*** that meets the following ***none.***

Application Note*:* Applicable to zeroization of DEK from Cryptographic module.

FCS_COP.1/AES - 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/AES The TSF shall perform ***data encryption and decryption*** in accordance with a specified cryptographic algorithm ***AES 256 XTS mode*** and cryptographic key sizes ***512 bits*** that meet the following: ***IEEE P1619 Standard (2007).***

FCS_COP.1.1/Hash
The TSF shall perform ***cryptographic hashing*** in accordance with a specified cryptographic algorithm ***SHA-1*** and **message digest** sizes ***160 bits*** that meet the following: ***FIPS PUB 180-4, "Secure Hash Standard".***

Application note: SHA-1 used for Integrity check during POST and Admin PIN verification.

6.1.2 Class FDP: User Data Protection

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 *deallocation of the resource from* the following objects: ***Admin PIN, SKM.***

FDP_ACF.1 Security attribute-based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the ***role based SFP*** **to** objects based on the following:

Subjects	***All subjects acting on behalf of users***
Objects	***User data, SKM***
Security Attributes	***Role as defined in*** **FMT_SMR.1**

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

- ***Subject with role "Identified User" is allowed to encrypt and decrypt (based on FCS_COP.1/AES) user data.***
- ***Subject with role "Identified User" is allowed to import SKM into the TOE***

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***None***

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- ***POST Failure***
- ***KAT Failure***

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 The TSF shall enforce the ***role based SFP*** on**:**

Subjects	***All subjects acting on behalf of users***
Objects	***User data, SKM***
Operations	***Encryption & Decryption, Import***

6.1.3 Class FMT: Security management

FMT_SMR.1 Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles ***Unidentified User, Identified user, Administrators***

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

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:

1) ***Enable/disable the smartcard lockout mode.***

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable* the functions ***smartcard lockout mode*** to ***Administrator.***

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, modify* the ***Admin PIN, DKM, MatchID*** to ***Administrator***.

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the ***role based SFP*** to restrict the ability to *modify* the security attributes ***Role*** to ***None.***

Application note: Roles are pre-programmed into the TOE and not modifiable

FMT_MSA.3 Static attribute initialisation
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the ***role based SFP*** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***None*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4 Class FPT: Protection of the TSF

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: ***failure of self test as defined in FPT_TST.1)***

FPT_TST.1 TSF Testing
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up* to demonstrate the correct operation of ***the TSF.***

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of ***none.***

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of ***none***.

FPT_PHP.1 Passive detection of physical attack
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.3 Security Requirement Dependency Rationale

SFR	Dependency	Inclusion/Rationale for Non-inclusion
FIA_UID.2	No dependencies	-
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_SOS.1	No dependencies	-
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1/AES FCS_CKM.4/MCU, FCS_CKM.4/Crypto

	FCS_CKM.4	
FCS_CKM.4/MCU	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
FCS_CKM.4/Crypto	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4/MCU, FCS_CKM.4/Crypto
FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Keys are not required for hashing.
FDP_RIP.1	No dependencies	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_SMF.1	No dependencies	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FPT_FLS.1	No dependencies	-
FPT_TST.1	No dependencies	-
FPT_PHP.1	No dependencies	-

Table 7 - Security Requirement Dependency Rationale

6.4 Security Requirements to Security Objective Mapping

SFR	O.DATA_ACC	O.ADMIN_ACC	O.TOE_INTEGRITY	O.ENCRYPT	O.PHYSICAL
FIA_UID.2	X	X			
FIA_UAU.2		X			
FIA_SOS.1		X			
FIA_AFL.1		X			
FCS_CKM.1				X	
FCS_CKM.4/MCU				X	
FCS_CKM.4/Crypto				X	
FCS_COP.1/AES	X			X	
FCS_COP.1/Hash		X	X		
FDP_RIP.1	X	X			
FDP_ACF.1	X				
FDP_ACC.1	X				
FMT_SMR.1	X	X			
FMT_SMF.1		X			
FMT_MOF.1		X			
FMT_MTD.1		X			
FMT_MSA.1	X	X			
FMT_MSA.3		X			
FPT_FLS.1			X	X	

FPT_TST.1			X	X	
FPT_PHP.1			X		X

Table 8 - Security Requirements to Security Objective Mapping

The security objective to SFR mapping rationale is summarized in the table below.

Security objective	SFR Mapping	Rationale
O.DATA_ACC	FIA_UID.2	This requirement helps meet the objective by ensuring only the legitimate user is able to access the user data in the hard disk.
	FCS_COP.1/AES	This requirement helps meet the objective by ensuring that user data is encrypted in the hard disk and only accessible by the legitimate user.
	FDP_RIP.1	This requirement helps meet the objective by ensuring that SKM is zeroized from the TOE after use.
	FDP_ACF.1	This requirement helps meet the objective by ensuring that Subject with role "Identified User" is allowed to encrypt and decrypt (based on FCS_COP.1/AES) user data and import SKM into the TOE.
	FDP_ACC.1	
	FMT_SMR.1	This requirement helps meet the objective by ensuring only legitimate smartcards are able to access the user data.
	FMT_MSA.1	This requirement helps meet the objective by ensuring that no users are able to modify the security attribute: Role.
O.ADMIN_ACC	FIA_UID.2	This requirement helps meet the objective by ensuring that access to the TOE's administrative functions is granted only upon insertion of a paired smartcard.

	FIA_UAU.2	This requirement helps meet the objective by ensuring that only authenticated Administrators are able to access the TOE’s administrative functions.
	FIA_SOS.1	This requirement helps meet the objective by ensuring that the Admin PIN is 8 digits in length.
	FIA_AFL.1	This requirement helps meet the objective by ensuring that access to administrative functions will be made unavailable upon 8 unsuccessful authentication attempts.
	FCS_COP.1/Hash	This requirement helps meet the objective by ensuring that the Admin PIN is stored as a hash using SHA1.
	FDP_RIP.1	This requirement helps meet the objective by ensuring that Admin PIN is zeroized from TOE.
	FMT_MTD.1	This requirement helps meet the objective by ensuring that only the Administrator can access the TSF data on the TOE.
	FMT_SMF.1	This requirement helps meet the objective by providing administrative functions for the management of the TOE.
	FMT_SMR.1	This requirement helps meet the objective by ensuring only legitimate Administrators are able to access the administrative functions.
	FMT.MOF.1	This requirement helps meet the objective by ensuring only authenticated Administrators are able to access the administrative functions.
	FMT.MSA.1	This requirement helps meet the objective by ensuring that only legitimate administrators are able to modify the security attribute: Role.

	FMT.MSA.3	This requirement helps meet the objective by ensuring that no one shall be able to define initial restrictive values for the security attribute: Role.
O.TOE_INTEGRITY	FCS_COP.1/Hash	This requirement ensures the integrity of the TOE configuration through the use of SHA1 hash
	FPT_FLS.1	This requirement helps meet the objective by ensuring that TOE will enter a “halt” state with secret parameters zeroized when the integrity of the TOE is deemed compromised or at risk (e.g. POST failure).
	FPT_TST.1	This requirement helps meet the objective by ensuring that TOE will self-tests to ensure that the TOE is able to operate correctly and that the integrity of internal of application data and TSF data stored persistently in the TOE is intact.
	FPT_PHP.1	This requirement helps meet the objective by ensuring that the TOE provides the user with the capability to determine if physical tampering that leads to the compromise of the TOE has occurred.
O.ENCRYPT	FCS_CKM.1	This requirement provides the key derivation function for the encryption key that is utilised in FCS_COP.1/AES.
	FCS.CKM.4/MCU	This requirement helps meet the objective by ensuring that the DEK is zeroized from the MCU memory. E.g. upon removal of smartcard when lockout mode is enable. This is to minimize any possible compromise of the DEK.
	FCS_CKM.4/Crypto	This requirement helps meet the objective by ensuring that the DEK is zeroized from the Cryptographic Module memory. E.g. upon removal of smartcard when lockout mode is enable. This is to minimize any possible compromise of the DEK.

	FCS_COP.1/AES	This requirement helps meet the objective by ensuring that all user data are encrypted using AES-256 XTS algorithm.
	FPT_FLS.1	This requirement helps meet the objective by ensuring that in the event of malfunction of the Cryptographic module which performs the full disk encryption, the TOE will enter a "halt" state with secret parameters zeroized when integrity of device is deemed compromised or at risk (e.g. KAT failure).
	FPT_TST.1	This requirement helps meet the objective by ensuring that the cryptographic function of the TOE which performs the full disk encryption is functional and unaltered.
O.PHYSICAL	FPT_PHP.1	This requirement helps meet the objective by ensuring that the TOE provides unambiguous detection of any tampering on the external casing of the TOE.

Table 9 - Security Objective to SFR mapping Rationale

6.5 Security Assurance Requirements

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.

The assurance components are summarised in the table below.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage

	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 10 - Assurance Components

6.5.1 Rationale for Security Assurance Requirements

The evaluation assurance package selected for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). EAL2 was chosen to provide a low to moderate level of assurance that is consistent with commercial products of this sort. The chosen assurance level is appropriate with the threats defined for the environment (limited interface and access to the TOE).

Chapter 7 TOE Summary Specification

This section summarizes the Security Functions of the TOE (TSF) - a high-level description of how the TOE implements the claimed security functional requirements.

7.1 SF1 – Identification and Authentication

The default state upon power up of the TOE provides access only to the identification and authentication mechanism.

Identification

Each smartcard is paired to a TOE by a “MatchID”. The MatchID is required for both User and Administrator access. The MatchID of the smartcard is verified against the MatchID stored in the TOE.

Users are first required to insert a paired smartcard containing the correct SKM. Upon successful identification of the smartcard (MatchID), the SKM will be allowed to be imported by the TOE allowing decryption of the data (Master Boot Record, file allocation table, etc) to enable access to the user data in the encrypted hard disk. In the event that an unpaired smartcard is inserted, no access to the decryption/encryption function is allowed.

Authentication

Administrators, similarly, are required to insert a paired smartcard and authenticate successfully to the TOE to successfully invoke any Admin function (modification of: Admin PIN, lockout mode - DKM, MatchID) of the TOE. The administrator is required to enter a 8-digit PIN to authenticate to the TOE. The TOE maintains a counter of the number of failed consecutive Admin authentication attempts. All access to administrative functions will be blocked after 8 consecutive wrong PIN entries. In the event, that an unpaired smartcard is inserted, only access to the Admin functions: initialize smartcard shall be allowed upon successful authentication.

The TOE is also designed with a “lockout mode” feature. If lockout mode is enabled, the TOE automatically enters into an unauthenticated state whenever the smartcard is removed. This would require users to re-perform the authentication process to gain user access.

This TSF is mapped to the following SFRs: FIA_UID.2, FIA_UAU.2, FIA_AFL.1, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FIA_SOS.1

7.2 SF2 – Cryptographic Support

The TOE provides cryptographic function such as symmetric data encryption/decryption and integrity verification using secure hashing.

The SKM retrieved from the inserted smartcard and the DKM that is stored in the TOE are used as inputs to a key derivation function to generate the DEK. The DEK is then loaded into the cryptographic module of the TOE where the MBR or file allocation table will be decrypted and sent to the host PC; thereafter user may access the encrypted hard disk of the TOE.

The TOE's cryptographic module utilizes the DEK to perform real time data encryption and decryption when data is transferred from host machine to encrypted hard disk and vice versa. Encryption and decryption of user data is performed in accordance to the cryptographic algorithm AES-256 XTS mode.

This TSF is mapped to the following SFRs: FCS_COP.1/AES, FCS_COP.1/Hash, FCS_CKM.1

7.3 SF3 – Security Management

The TOE shall provide the following administrative functions to the Administrator:

1) Pairing of legitimate smartcard to TOE
2) Enable/disable the smartcard lockout mode.
3) Change of Admin PIN.
4) DKM injection (device setup)

Option 1 enables the Administrator to pair a smartcard with a TOE using the smartcard's MatchID attribute. The smartcard's MatchID is stored in the TOE.

Option 2 enables the Administrator to enable/disable the lockout mode (enabled by default). When lockout mode is enabled, the TOE will enter into an unauthenticated state whenever the smartcard is removed from the TOE.

Option 3 enables the Administrator to change the Admin PIN. The Admin PIN must be 8 digits in length and will be stored as a hash (SHA1) within the TOE.

Option 4 enables the Administrator to inject the DKM (from the Administrator smartcard) into the TOE during device setup.

The TOE enters into a "halt" state upon the successful invocation of each of the four administrative functions. The Administrator is required to authenticate again should they want to invoke any of the administrative function again.

This TSF is mapped to the following SFRs: FIA_UID.2, FIA_UAU.2, FIA_SOS.1, FCS_COP.1/Hash, FMT_SMR.1, FMT_SMF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FDP_ACC.1, FDP_ACF.1

7.4 SF4 – Protection of the TSF

The TOE is designed with protection and detection mechanisms to prevent and detect possible malfunction or compromised TSF/TSF data.

After the DEK is derived from the SKM and DKM, the TOE transfers the DEK to the cryptographic module and performs the zeroization of the SKM and the DEK from the MCU's memory.

The TOE performs zeroization of the Admin PIN upon completion of usage.

The "lockout mode" feature forces the TOE to automatically enter into an unauthenticated state whenever the smartcard is removed from the TOE. When the TOE enters into an unauthenticated state, the DEK stored in the internal RAM of the cryptographic chip will be zeroized.

The TOE performs a POST upon every power up to perform integrity checks on the MCU, a critical subsystem of the TOE. In the event of any POST failure, the TOE will enter a "halt" state. POST includes the following tests:

1) LED Display Test
2) Memory Read/Write Test (includes MCU's internal RAM)
3) ROM (EEPROM) Integrity Check
4) SHA-1 Hash Check

The cryptographic module conducts a Known Answer Test whenever it is enabled. The TOE performs zeroization of all parameters (e.g. DEK) upon failure of the KAT.

In the event of failure of any of the above self-tests, the TOE enters into a "halt" and secure state, and the "ERROR" LED will be lighted up. In this state, the TOE is non-operational.

The TOE is also housed in a tamper evident casing where any physical tampering to the TOE can be visually detected.

This TSF is mapped to the following SFRs: FCS_CKM.4/MCU, FCS_CKM.4/Crypto, FCS_COP.1/Hash, FDP_RIP.1, FPT_TST.1, FPT_FLS.1, FPT_PHP.1.

7.5 TOE Summary SFR to TSF mapping

SFR	Security Functions
FIA_UAU.2	SF1, SF3
FIA_UID.2	SF1, SF3
FIA_SOS.1	SF3
FIA_AFL.1	SF1
FCS_CKM.1	SF2
FCS_CKM.4/MCU	SF4
FCS_CKM.4/Crypto	SF4

FCS_COP.1/AES	SF2
FCS_COP.1/Hash	SF2, SF3, SF4
FDP_RIP.1	SF4
FDP_ACF.1	SF1, SF3
FDP_ACC.1	SF1, SF3
FMT_SMR.1	SF1, SF3
FMT_SMF.1	SF3
FMT.MOF.1	SF3
FMT.MSA.1	SF1, SF3
FMT.MSA.3	SF1, SF3
FMT_MTD.1	SF3
FPT_FLS.1	SF4
FPT_TST.1	SF4
FPT_PHP.1	SF4

Table 11 - SFR to Security Functions mapping