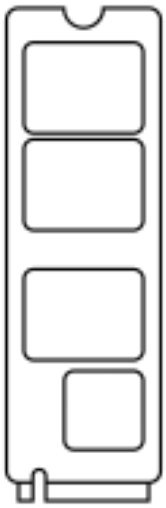

Flexxon X-PHY® AI Cyber Secure SSD Security Target

Date: 21 March 2022

Document version 1.2

Contents

1 ST Introduction (ASE_INT)

1.1 ST Reference

ST title	Flexxon X-Phy AI Cyber Secure SSD Security Target
Version	v 1.2
Author	Flexxon Pte Ltd
Date	21 March 2022

1.2 TOE Reference

TOE identification	X-PHY AI Cyber Secure SSD
Version	FAMP1.00

1.3 TOE Overview

1.3.1 TOE usage and major security features

The TOE is a solid-state drive (SSD) that protects its SSD data against ransomware and data cloning attacks; it is capable of detecting ransomwares and cloning wares of known behaviour.

Traditional malware detection methods require known signatures of ransomwares and cloning wares for effective malware detection. However, as these malwares becomes more sophisticated, malware authors use techniques such as polymorphism to change the signature of the malware objects as they spread from one machine to the next. As a result, this renders traditional signature-based detection methods ineffective.

The TOE advances the above method with its Artificial Intelligence (AI) implementation which analyses various attributes of ransomware and malicious data cloning behaviour. This allows the TOE to detect ransomwares and cloning wares of unknown signatures but known behaviour. Upon detection of such malicious behaviour[1], the TOE shall lock its SSD from further read/write access.

The following illustrates the TOE usage.

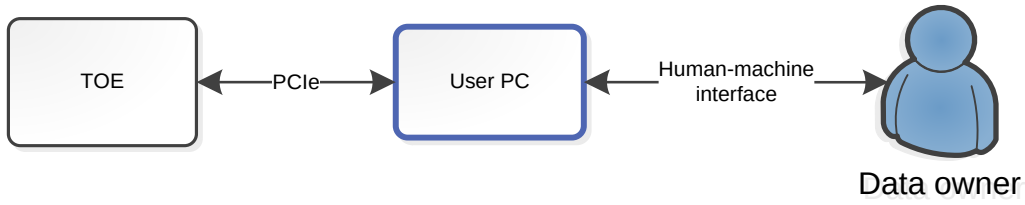

Figure 1: TOE usage during normal operation

[1] In a ransomware or cloning-ware attack, a user is expected to lose a maximum of 20% of total files before the TOE locks its SSD.

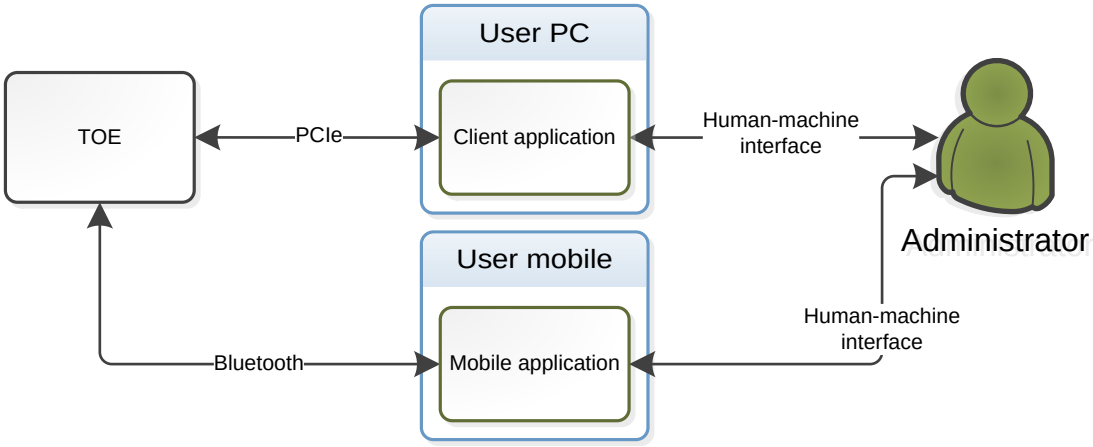

Figure 2: TOE usage during security management

The TOE also provides physical tamper detection/response by measuring physical properties of SSD disconnection. If the TOE detects any anomalies in those physical properties, the TOE shall either lock its SSD from further read/write access or purge its SSD data[2].

The TOE supports the following security functionalities

- Identification and authentication
- Security management
  - Management of identification and authentication data
  - Management subject security attributes
  - Management of SSD lock or unlock status
  - Enable or disable purge response to physical tamper
  - Enable or disable physical tamper sensors
- User data protection
  - Storage encryption and decryption
  - Information flow control
- Trusted path
- TSF protection
  - Physical tamper detection/response
  - Self-test
  - Inter-chip encryption/decryption

1.3.2 TOE Type

The TOE is a solid-state drive (SSD) that protects SSD data flow against all known ransomware and data cloning attacks.

1.3.3 Required non-TOE hardware/software/firmware

The table below states the hardware and software requirements to support TOE operations.

Hardware	Host interface
Laptop/Desktop PC	PCIe M Key, PCIe version Gen3
Mobile phone	Bluetooth version 5.0

[2] If TOE detects SSD disconnection, the TOE shall either lock its SSD from further read/write access or purge its SSD data.

Table 1: Hardware requirement

Software	
Laptop/Desktop OS	Windows 10/8
Mobile phone OS	Android, iOS
Authenticator application	Google/Microsoft authenticator

Table 2: Software requirements

1.3.3.1 Laptop/Desktop

During normal operation (Figure 1), the laptop/desktop is used by the data owner to read or write SSD data to the SSD within the TOE.

During security management (Figure 2), the laptop/desktop is used by the administrator to perform security management of the TOE.

1.3.3.2 Mobile phone

The mobile phone is used by the administrator to perform security management of the TOE via a mobile application. The mobile phone shall also contain a Google/Microsoft authenticator application that generates OTP. The OTP and user password are required for user identification and authentication prior access to TOE security management function.

1.4 TOE Description

1.4.1 Physical Scope

The TOE consists of all hardware and firmware components contained within a M.2 formfactor. Figure 3 provides an abstraction of the physical scope.

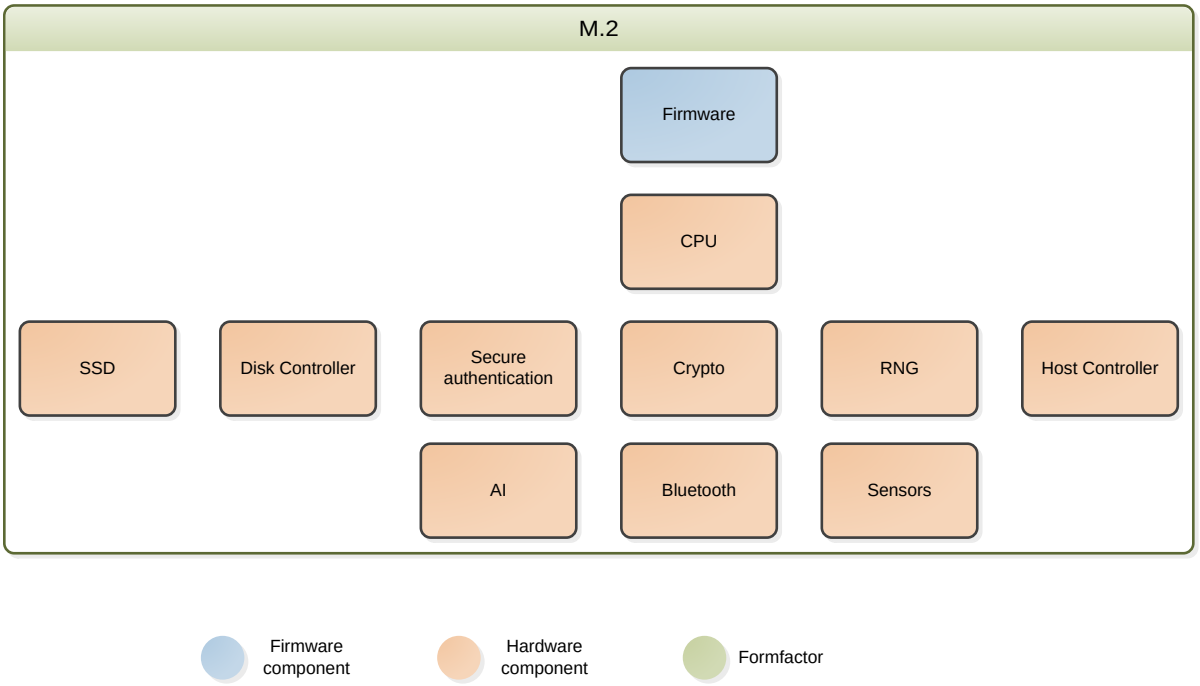

Figure 3: Physical scope of TOE

The table below lists the TOE deliverables and their corresponding delivery methods.

Items	Description	Format	Delivery method
TOE	FLEXXON X-PHY Cyber Secure SSD FAMP1.00	hardware	Courier
Preparative and operational user guidance	• X-PHY Quick Start Guide 24 Mar 22 • X-PHY User application Guide Windows 24 Nov 21 • X-PHY Bluetooth Application Guide Apple 24 Sep 21 • X-PHY Bluetooth Application Guide Android 24 Sep 21	PDF	Download from website

Table 3: TOE deliverables and delivery methods

1.4.2 Logical Scope

This section describes the logical security features of TOE.

1.4.2.1 Identification and authentication

The TOE performs identification and authentication of the administrator prior to allowing access to the TOE's security management functionality. The TOE authenticates the administrator using 2-Factor Authentication (2FA). The TOE performs 2FA using administrator's password and One-Time-Password (OTP).

On an administrator's desktop/laptop, a client application is run for the administrator to interact with the TOE's identification and authentication functionality. On a mobile phone, a mobile application is run for the same purpose i.e. for the administrator to interact with the TOE's identification and authentication functionality.

1.4.2.2 Security management

The TOE provides security management functionality to manage the following security function behaviour:

- Identification and authentication
  - Manage identification and authentication data
  - Management subject security attributes
- TSF protection
  - Management of users that gets informed about physical tamper
  - Management of SSD lock or unlock status
  - Enable or disable purge response to physical tamper.

1.4.2.3 User data protection

The TOE performs SSD data protection in two prongs during normal operation:

1. The TOE encrypts and decrypts user data stored in the SSD on-the-fly; SSD data confidentiality is protected at rest.
2. The TOE's AI analyses various attributes of user PC's read/write access to the TOE's SSD. Based on the behaviour of these attributes, the AI determines whether the user PC's read/write access behaviour is associated with that of a ransomware or data cloning attack. Once the TOE determines that the read/write access behaviour is associated with that of a ransomware or data cloning[3] attack, the TOE shall lock user PC's access to the SSD.

[3] In a ransomware or cloning-ware attack, a user is expected to lose a maximum of 20% of total files before the TOE locks its SSD.

1.4.2.4 Trusted path

The administrator performs TOE security management via the administrator's mobile phone. The TOE connects to the administrator's mobile phone via Bluetooth. To protect the confidentiality and integrity of administrator's identification/authentication data and other TOE Security Functionality (TSF) data being exchanged between the mobile phone and the TOE, the TOE establishes a trusted path between the TOE and the administrator.

1.4.2.5 TSF protection

The TOE provides TSF protection in the following areas:

1. Physically, the TOE provides physical tamper detection/response by measuring physical properties of SSD disconnection. If the TOE detects any anomalies in those physical properties, the TOE shall either lock its SSD from further read/write access or purge its user data.
2. Logically, TOE
    a. performs firmware integrity check using digital signature during initialisation and firmware update; this ensures the TSF integrity and authenticity is preserved in both scenarios.
    b. performs cryptographic Known-Answer-Test (KAT) during initialisation and operations to ensure the correctness of the cryptographic implementation.
    c. encrypts inter-chip communication to protect confidentiality of TSF data.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance

The Security Target and its TOE conforms with:

- Common Criteria Information Technology Security Evaluation Version 3.1, Revision 5
    - Part 2 extended
    - Part 3 conformant[CC3]

2.2 PP Conformance

The Security Target and its TOE does not conform to any Protection Profile (PP).

2.3 Package Conformance

The Security Target and its TOE conforms to Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2.

3 Security Problem Definition (ASE_SPD)

3.1 Introduction

This section shall define TOE's assets, subjects, external entities, and threat agent.

3.1.1 Assets

Name	Description	Type of protection
SSD data	Data stored in SSD	Information flow
Administrator's authentication data	Authentication data that is exchanged between the user and TOE to perform user authentication. The TOE performs user authentication prior to allowing user access to the TOE security management functions.	Confidentiality

Table 4: User data

Name	Description	Type of protection
Reference administrator's authentication data	Reference data used for TOE's authentication of user prior to allowing user access to the TOE security management functions.	Confidentiality and integrity
Reference read/write access attributes for determining ransomware and data cloning behaviour	TOE uses these attributes to determine ransomware and data cloning behaviour.	Confidentiality and integrity
Cryptographic keys	TOE uses these keys to perform cryptographic operations such as encryption and decryption.	Confidentiality and integrity
Threshold measurement values for physical properties of SSD disconnection	TOE uses these threshold values to determine whether a physical tamper has occurred.	Integrity
Purge enable value	TOE uses this value to determine the physical tamper response behaviour i.e. purge or lock.	Integrity
Lock status value	The TOE or user sets this value to lock or unlock access to the SSD.	Integrity
Physical tamper sensors enable values	TOE uses this value to determine the physical tamper sensors are enabled or disabled.	Integrity
Trusted path configuration settings	TOE uses these values to determine trusted path encryption/decryption algorithm and session timeout.	Integrity

Table 5: TSF data

3.1.2 Subjects

The subjects that the TOE can perceive are shown below. A TOE user is associated to one of these subjects.

Subjects	Description
Administrator	Subject that is authorised to perform TOE security management.
Data owner	Subject who owns the data stored in the SSD.
Threat agent	Subject that • performs ransomware or cloning-ware attacks on user data stored in the SSD. • physically tampers the TOE to access user data stored in the SSD.

Table 6: Subjects

3.1.3 External entities

External entity	Description
User PC	IT entity that the user uses to remotely[4] perform • security management on the TOE. • read and write on the TOE's SSD. This IT entity is untrusted.
User mobile	IT entity that the user uses to remotely perform security management on the TOE. This IT entity is to be endorsed by the TOE user's organisation to be secure and trusted.
Client application	IT entity that runs on the User PC so that user can remotely perform security management on the TOE.
Authenticator application	IT entity that generates OTP as part of user identification and authentication for access to TOE security management. This IT entity runs on the user mobile.
User	Human entity that uses the TOE a.k.a. TOE user.

Table 7: External entities

3.1.4 Threat agent

Threat agent	Description
Ransomware	Malicious IT entity that attempts to encrypt user data stored in SSD causing the user to lose his/her data.
Data-cloning ware	Malicious IT entity that attempts to exfiltrates user data stored in the SSD to an attacker.
Attacker	Any other unauthorised human or IT entity that • attempts to perform ransomware or cloning-ware attacks on user data stored in the SSD. • physically tampers the TOE to access user data stored in the SSD.

Table 8: Threat agent

3.1.5 Threat scenario

Figure 4 illustrates the three major threat scenarios that the TOE is designed to counter.

[4] Remote human users, meaning they interact indirectly with the TOE through another IT product (para 25 of [CC2]).

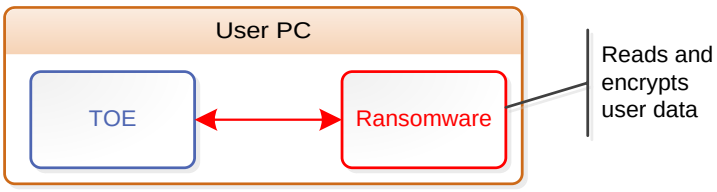

Figure 4: Threat scenario 1

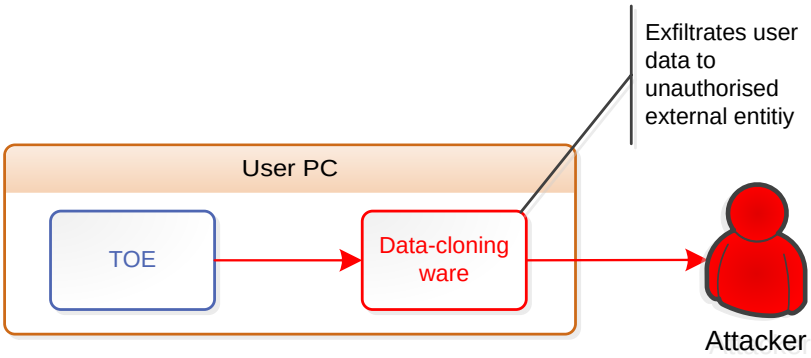

Figure 5: Threat scenario 2

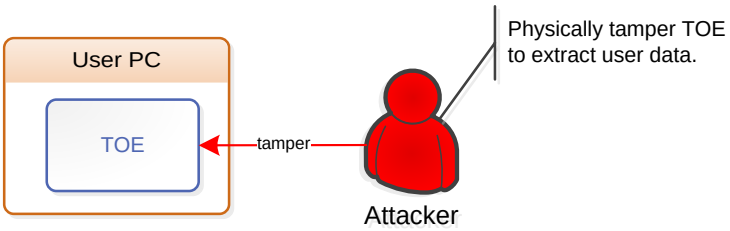

Figure 6: Threat scenario 3

3.2 Threats

Threat	Description
T.Ransomware	Ransomware attempts to encrypt user data stored in the TOE's SSD causing the user to lose his/her data.
T.DataCloningWare	Data-cloning ware attempts to clone user data stored in the TOE's SSD to attacker.
T.Tamper	Attacker attempts to tamper the TSF or TSF data (see Table 5) physically or logically to clone the SSD data.
T.Masquerade	Attacker masquerade as an Administrator via the Bluetooth interface to modify the TSF data (see Table 5).
T.BruteForce	Attacker attempts brute-force the administrator's authentication data to gain access to the TOE's security management function and modify the TSF data (see Table 5).

Table 9: Threats

3.3 Assumptions

Assumption	Description
A.Trusted_User	TOE users are well-trained to

	• operate the TOE securely in accordance with the operational guidance • setup the IT environment in accordance with the preparative guidance. TOE users are trusted i.e. does not harbour malicious intent.

A.PasswordPolicy	The client application shall ensure that the user password meets the below quality metric during user registration. After user registration, the reference password that meets the quality metric shall be stored in the TOE.
	• at least
	  ○ 1 uppercase
	  ○ 1 numeric digit
	  ○ 1 special character i.e.'!' '@', '#' and '$'
	  ○ 8 characters long
	• at most
	  ○ 15 characters long

A.User_mobile	The user mobile is secure and trusted.

Table 10: Assumptions

3.4 Organisation Security Policies (OSP)

None.

4 Security Objectives (ASE_OBJ)

This section identifies the security objectives for the TOE and the operational environment. Security objectives counters the identified threats, upholds the identified OSPs and fulfils the assumptions.

4.1 Security Objectives for the TOE

Security Objectives	Descriptions
O.InfoFlowControl	The TOE shall block information flow between its SSD and user PC when it detects ransomware and data-cloning ware behaviour.
O.Confidentiality	The TOE shall protect the confidentiality of user data stored in its SSD.
O.PhyTamper	The TOE shall detect physical tamper. When tamper is detected by TOE, the SSD will be locked or purged.
O.TrustedPath	The TOE shall establish and maintain trusted Bluetooth communication between the user and TOE.
O.2FA	The TOE shall enforce 2-FA during user authentication prior to allowing user access to its security management functionality.
O.IDnAuth	The TOE shall perform user authentication prior to allowing user access to its security management functionality. The TOE shall also set a limit on the number of failed authentications.
O.SelfTest	The TOE shall perform self-test during initialisation and operation.

Table 11: Security Objectives for TOE

4.2 Security Objectives for the Operational Environment

Security Objectives	Descriptions

OE.Trusted_User	The operational environment must ensure that
	• TOE users are well-trained to
	  ○ operate the TOE securely in accordance with the operational guidance
	  ○ setup the IT environment in accordance with the preparative guidance.
	• TOE users are trusted i.e. does not harbour malicious intent.

OE.User_mobile	The TOE user must ensure that the user mobile is secure and trusted.
OE.PasswordPolicy	The client application shall enforce password complexity policy for its user identification and authentication.

Table 12: Security Objectives for Operational Environment

4.3 Security Objective Rationale

4.3.1 Tracing between security objectives and security problem definition

Threats-OSPs-Assumptions / Security Objectives	O.InfoFlowControl	O.Confidentiality	O.PhyTamper	O.TrustedPath	O.2FA	O.IDnAuth	O.SelfTest	OE.Trusted_User	OE.PasswordPolicy	OE.User_mobile
T.Ransomware	X							X		
T.DataCloningWare	X							X		
T.Tamper		X	X				X			
T.Masquerade				X	X	X		X	X	X
T.BruteForce						X			X	
A.Trusted_user								X		
A.PasswordPolicy									X	
A.User_mobile										X

Table 13: Tracing between security objectives and SPD

4.3.2 Justification for tracing

This section explains the tracing illustrated in Table 13.

4.3.2.1 Threats-Security Objective Justification

T.Ransomware	Ransomware attempts to encrypt user data stored in the TOE's SSD causing the user to lose his/her data.
O.InfoFlowControl	diminishes the risk of SSD data from being encrypted by ransomware.
T.DataCloningWare	Data-cloning ware attempts to clone user data stored in the TOE's SSD to attacker.
O.InfoFlowControl	diminishes the risk of SSD data from being cloned by data-cloning ware.
T.Tamper	Attacker attempts to tamper the TOE or TSF data (see Table 5) physically or logically to access the SSD data.
O.PhyTamper	diminishes the risk of TSF being physically tampered.
O.Confidentiality	if physical tamper response is configured to lock, this mitigates the risk of compromising SSD data confidentiality.
O.SelfTest	diminishes the risk of TSF being logically tampered.
T.Masquerade	Attacker masquerade as an Administrator via the Bluetooth interface to modify the TSF data (see Table 5).

O.TrustedPath	protects the confidentiality of the communication channel, in turn, this diminishes the risk of the communication channel being tampered or monitored.
O.2FA	increases the difficulty of stealing the user login credentials, in turn, this directly diminishes the risk of attacker masquerading as an Administrator.
O.IDnAuth	ensures that only users with the correct user credentials can have access to the security management functionality, hence, directly diminishing the risk attacker masquerading as an Administrator.
OE.User_mobile	ensures the User mobile is trusted and secure; the User mobile faithfully executes the installed mobile application. In turn, diminishing the risk of the User mobile or mobile application bypassing or tampering TSF.
OE.Trusted_User	ensures that the users are well-trained and trusted; users faithfully install the legitimate client application or mobile application on the user PC or user mobile, respectively. In turn, this reduces the risk of loss of user credentials.
OE.PasswordPolicy	diminishes the risk of the user password being guessed or brute-forced.

T.BruteForce	Attacker attempts brute-force the administrator's authentication data to gain access to the TOE's security management function and modify the TSF data (see Table 5).
O.IDnAuth	limits the number of failed authentications; directly diminishes the risk of the user password being guessed or brute-forced.
OE.PasswordPolicy	diminishes the risk of the user password being guessed or brute-forced.

4.3.2.2 Assumptions-Security Objective Justification

A.Trusted_User	TOE users are well-trained and trusted
OE.Trusted_User	directly upholds the assumption.

A.PasswordPolicy	The client application shall ensure that the user password meets a set quality metric during user registration.
OE.PasswordPolicy	directly upholds the assumption.

A.User_mobile	The User mobile is to be endorsed by the organisation to be secure and trusted.
OE.User_mobile	directly upholds the assumption.

4.3.2.3 OSP-Security Objective Justification

None

5 Extended Components Definition

5.1 Definition of the Security Functional Component FDP_IFF.7

The following addition are made to “Information flow control (FDP_IFF)” in Common Criteria, Part 2 to describe the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy (FDP_IFC), which also specifies the scope of control of the policy. FDP_IFF.7 (Information flow metric) requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function and describes how security attributes are derived by the function. Additionally, it specifies quantity metric and quality metric for the degree of information flow enforcement. This kind of requirements lies beyond FDP_IFF.1 defined in Common Criteria, Part 2.

5.1.1 Family Behaviour

This family describes the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy (FDP_IFC), which also specifies the scope of control of the policy. It consists of two kinds of requirements: one addressing the common information flow function issues, and a second addressing illicit information flows (i.e. covert channels). This division arises because the issues concerning illicit information flows are, in some sense, orthogonal to the rest of an information flow control SFP. By their nature they circumvent the information flow control SFP resulting in a violation of the policy. As such, they require special functions to either limit or prevent their occurrence.

5.1.2 Component levelling

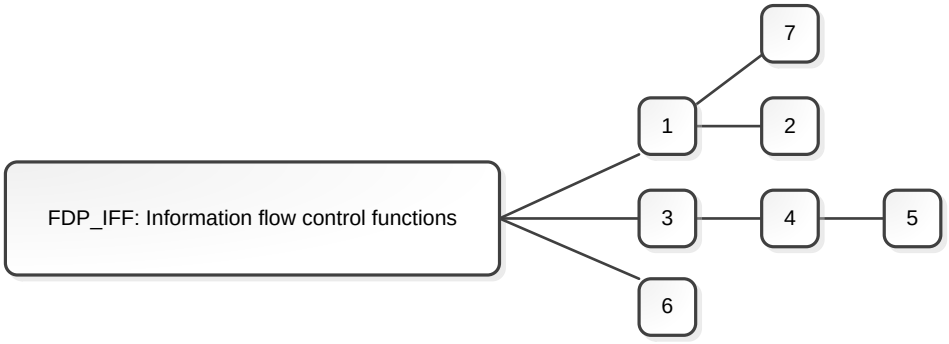

Figure 7: Component levelling

FDP_IFF.1 Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function and describes how security attributes are derived by the function.

FDP_IFF.2 Hierarchical security attributes, expands on the requirements of FDP_IFF.1 Simple security attributes by requiring that all information flow control SFPs in the set of SFRs use hierarchical security attributes that form a lattice (as defined in mathematics). FDP_IFF.2.6 is derived from the mathematical properties of a lattice. A lattice consists of a set of elements with an ordering relationship with the property defined in the first bullet, a least upper bound which is the unique element in the set that is greater or equal (in the ordering relationship) than any other element of the lattice, and a greatest lower bound, which is the unique element in the set that is smaller or equal than any other element of the lattice.

FDP_IFF.3 Limited illicit information flows, requires the SFP to cover illicit information flows, but not necessarily eliminate them.

FDP_IFF.4 Partial elimination of illicit information flows, requires the SFP to cover the elimination of some (but not necessarily all) illicit information flows.

FDP_IFF.5 No illicit information flows, requires SFP to cover the elimination of all illicit information flows.

FDP_IFF.6 Illicit information flow monitoring, requires the SFP to monitor illicit information flows for specified and maximum capacities.

FDP_IFF.7 Information flow metric, expands on the requirements of FDP_IFF.1 Simple security attributes by adding a quantity metric and a quality metric for the degree of information enforcement.

5.1.3 Management: FDP_IFF.7

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

a) Managing the attributes used to make explicit access based decisions.
b) Managing the quantity and quality metric

5.1.4 Audit: FDP_IFF.7

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

a) Minimal: Decisions to permit requested information flows.
b) Basic: All decisions on requests for information flow.
c) Detailed: The specific security attributes used in making an information flow enforcement decision.
d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).

FDP_IFF.7	**Information flow metric**	
	Hierarchical to:	FDP_IFF.1 Simple security attributes
	Dependencies:	FDP_IFC.1 Subset information flow control
		FMT_MSA.3 Static attribute initialisation
FDP_IFF.7.1	The TSF shall enforce the **[assignment: information flow control SFP]** based on the following types of subject and information security attributes: **[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]**.	
FDP_IFF.7.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].**	
FDP_IFF.7.3	The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.	
FDP_IFF.7.4	The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows].**	

FDP_IFF.7.5 The TSF shall explicitly deny an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly deny information flows]**.

FDP_IFF.7.6 The TSF shall enforce the information flow based on quantity metric of **[assignment: quantity metric over the defined quality metric]** and quality metric of **[assignment: quality metric over which the defined quantity metric is based on]**.

6 Security Requirements (ASE_REQ)

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Security functional requirements components are stated in section 5.1 Security Functional Requirements. Security assurance components stated in 5.2 Security Assurance Requirements are drawn from Common Criteria Part 3[CC3].

Operations for iteration, assignment, selection and refinement have been made. The following textual conventions are used in this chapter as part of every SFR:

- Iteration is represented by a slash ('/') followed by an identifier placed at the end of the component. For example, FDP_ACF.1/Signer.
- Assignment is represented by **bold text**.
- Selection is represented by *italic text*.
- Refinement is represented by underlined text.

6.1 Security Functional Requirements

6.1.1 Security management operation

The SFRs in this section are related to TOE usage during security management operation (Figure 2).

6.1.1.1 Identification and Authentication

6.1.1.1.1 FIA_ATD (User attribute definition)

FIA_ATD.1	**User attribute definition**
	Hierarchical to: No other components.
	Dependencies: No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: • **role** • **password** • **one-time password (OTP)**

Application note: There is only one role maintained for security management operation i.e. Administrator. Password and OTP are the administrator's authentication data. The administrator obtains his/her OTP from Google/Microsoft authenticator mobile app, which is out of TOE scope.

6.1.1.1.2 FIA_UAU (User authentication)

FIA_UAU.1	**Timing of authentication**
	Hierarchical to: FIA_UAU.1 Timing of authentication
	Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow • **Information flow control** • **SSD encryption and decryption** • **TSF protection** • **Trusted path** • **Password policy** on behalf of the user to be performed before the user is authenticated.

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

6.1.1.1.3 FIA_UID (User identification)

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow
- **Information flow control**
- **SSD encryption and decryption**
- **TSF protection**
- **Trusted path**
- **Password policy**

on behalf of the user to be performed before the user is identified.

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

6.1.1.1.4 FIA_USB (User-subject binding)

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **role**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **none**.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none**.

6.1.1.1.5 FIA_AFL (Authentication failures)

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 **5** unsuccessful authentication attempts occur related to **FIA_UAU.1**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall
1. **lock user access to security management.**
2. **request user to change password using OTP**.

Application notes: When unsuccessful authentication attempt is met, the client application will pop-up a message to request user to click the 'forget password'. The client application will prompt for authenticator OTP. User shall then enter the OTP that appears on the authenticator mobile application. After the client application successfully verifies the authenticator OTP, a new password dialog box will appear. The user will now input the new password as part of the TOE change password process.

6.1.1.2 Security Management

6.1.1.2.1 FMT_SMF (Specification of Management Functions)

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: **see 'Management function' column of Table 14**.

6.1.1.2.2 FMT_SMR (Security management roles)

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 **Administrator**.

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

6.1.1.2.3 FMT_MOF (Management of functions in TSF)

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 *see 'Action column of Table 14 the behaviour of* the functions **see 'Security function component being managed' column of Table 14** to **Administrator**.

Management functions	**Action**	**Security function component being managed**
Management of administrator's password	modify the behaviour of	FIA_UAU.2
Management of OTP authentication methods	modify the behaviour of	FIA_UAU.2
Change subject security attributes	modify the behaviour of	FIA_USB.1
Enable/Disable physical tamper sensors	disable, enable	FPT_PHP.1
Enable/Disable information flow control	disable, enable	FDP_IFC.1 and FDP_IFF.7

Table 14: Management of security function behaviour

6.1.1.2.4 FMT_MSA (Management of security attributes)

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 **Ransomware and Data-cloning ware SFP** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall not allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

Application notes: The security attributes that are used to enforce **Ransomware and Data-cloning ware SFP** are not configurable.

6.1.1.2.5 FMT_MTD (Management of TSF data)

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 **see 'Action' column of Table 15** the **see 'TSF data' column of Table 15** to **Administrator**.	

Action	TSF data
Modify	Reference administrator's authentication data i.e. password
View, Modify	Purge enable value
View, Modify	Lock status value
View, Modify	Physical tamper sensors enable values[5]

Table 15: Management of TSF data

6.1.1.3 Trusted Path

Trusted path is established over the Bluetooth and PCIe communication between the TOE and the mobile phone during security management operations.

6.1.1.3.1 FCS_COP (Cryptographic operations)

FCS_COP.1/TP_ENC	**Trusted path encryption/decryption 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.1 Cryptographic key generation]
FCS_COP.1.1/	The TSF shall perform **trusted path encryption and decryption** in accordance with a specified cryptographic algorithm **AES-CBC** and cryptographic key sizes **128 bits** that meet the following: **none**	

6.1.1.3.2 FCS_CKM (Cryptographic key management)

FCS_CKM.1/TP_ENC	**Trusted path encryption/decryption 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

[5] This includes sensors that detect SSD disconnection.

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH curve secp192r1(NIST 192-bit)** and specified cryptographic key sizes **192 bits** that meet the following: **RFC4492**

FCS_CKM.4/TP	**Trusted path key destruction**	
	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroization** that meets the following: **none**.	

6.1.1.3.3 FTP_TRP (Trusted Path)

FTP_TRP.1	**Trusted path**	
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure*.	
FTP_TRP.1.2	The TSF shall permit remote users to initiate communication via the trusted path.	
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *initial user authentication,* **security management**.	

6.1.1.3.4 FTA_SSL (Session locking and Termination)

FTA_SSL.3	**TSF-initiated termination**	
	Hierarchical to:	No other components.
		No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a **5 minutes of user inactivity**.	

FTA_SSL.4	**User-initiated termination**	
	Hierarchical to:	No other components.
		No dependencies.
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.	

6.1.3 Normal Operation

The SFRs in this section are related to TOE usage during normal operation (Figure 1).

6.1.3.1 Information Flow Control

6.1.3.1.1 FDP_IFC (Information flow control policy)

FDP_IFC.1 **Subset information flow control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attribute

FDP_IFC.1.1 The TSF shall enforce the **Ransomware and Data-cloning ware SFP** on **see Table 16**.

Subjects	threat agent, data owner
Information	SSD data
Operations	Read Write

Table 16: Subjects, information and operations.

6.1.3.1.2 FDP_IFF (Information flow functions)

FDP_IFF.7 **Information flow metric**

Hierarchical to: FDP_IFF.1 Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.7.1 The TSF shall enforce the **Ransomware and Data-cloning ware SFP** based on the following types of subject and information security attributes: **see Table 17**.

Subjects	Information	Security Attributes
Data owner, Threat agent	SSD data	Shannon entropy value, Frequency-Based Similarity Hashing, Magic number, platform type, File type, Type-Security-Platform (TSP), lookup table, Result values, Data image model, LBA content

Table 17: Security attributes

FDP_IFF.7.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **see Table 18**

Operations	Rules
Read/Write	If data image model of read and/or write activities complies to the reference data models, the TOE shall permit information flow,

	else the TOE shall lock access to the SSD.

Table 18: ransomware and data-cloning ware SFP rules

Application notes: Please refer to [PATENT1] and [PATENT2] for a summary of the methods of detecting data anomalies. As stated in [PATENT1] and [PATENT2], data image model is an aggregation of the security attributes stated in Table 17.

FDP_IFF.7.3	The TSF shall enforce the **none**.
FDP_IFF.7.4	The TSF shall explicitly authorise an information flow based on the following rules: **none**
FDP_IFF.7.5	The TSF shall explicitly deny an information flow based on the following rules: **none**.
FDP_IFF.7.6	The TSF shall permit an information flow based on quantity metric of **at least 80% user data** and quality metric of **a random set of user data within the quantity metric will be protected against modification**.

Application notes: FDP_IFF.7 applies to the detection of both ransomware and cloning-ware attacks.

Application notes: The user must maintain the files in the SSD in the following manner for the lock-up mechanism to be triggered

- minimum of 1000 files
- minimum of 10GB data
- mixed file size of at least 100kB.

6.1.3.2 SSD Encryption and Decryption

6.1.3.2.1 FCS_COP (Cryptographic operations)

FCS_COP.1/SSD **SSD encryption/decryption 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.1 Cryptographic key generation]

FCS_COP.1.1	The TSF shall perform **SSD encryption and decryption** in accordance with a specified cryptographic algorithm **AES-XTS** and cryptographic key sizes **512-bit** that meet the following: **none**.

Application notes: The TOE performs encryption and decryption of SSD data right after secure initialisation.

6.1.3.2.2 FCS_CKM (Cryptographic key management)

FCS_CKM.1/SSD **SSD 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 **none** and specified cryptographic key sizes **512-bit** that meet the following: **NIST SP800-90B**

Application note: The TOE implements TRNG that conforms to NIST SP800-90B.

FCS_CKM.4/SSD **SSD cryptographic key destruction**

	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroization** that meets the following: **none**.	

6.1.3.3 TSF Protection

6.1.3.3.1 FPT_PHP (TSF physical protection)

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.	

6.1.3.3.2 FPT_TST (TSF self-test)

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 • **FCS_COP.1/TP_ENC** • **FCS_CKM.1/TP_ENC** • **FCS_COP.1/SSD** • **FCS_CKM.1/SSD** • **FCS_COP.1/Inter-chip** • **FCS_CKM.1/Inter-chip**	
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***.	

6.1.3.3.3 FPT_FLS (Fail secure)

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 • **FCS_COP.1/TP_ENC** • **FCS_CKM.1/TP_ENC** • **FCS_COP.1/SSD** • **FCS_CKM.1/SSD** • **FCS_COP.1/Inter-chip** • **FCS_CKM.1/Inter-chip**	

Application notes: The TOE shall enter a halt state if any of the cryptographic self-tests has failed.

6.1.3.3.4 FPT_ITT (Internal TOE TSF data transfer)

FPT_ITT.1	**Basic internal TSF data transfer protection**	
	Hierarchical to:	No other components
	Dependencies:	No dependencies.
FPT_ITT.1.1	The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.	

Application note: The TOE encrypts the inter-chip communication to protect TSF data against disclosure.

6.1.3.3.5 FCS_COP (Cryptographic operations)

FCS_COP.1/Inter-chip	**Inter-chip encryption/decryption 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/Inter-chip	The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES-CBC** and cryptographic key sizes **128 bits** that meet the following: **none**.	

6.1.3.3.6 FCS_CKM (Cryptographic key management)

FCS_CKM.1/Inter-chip	**Inter-chip 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/Inter-chip	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH curve secp192r1 (NIST 192-bit)** and specified cryptographic key sizes **192 bits** that meet the following: **RFC4492**	

FCS_CKM.4/Inter-chip	**Inter-chip key destruction**	
	Hierarchical to:	No other components
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroization** that meets the following: **none**.	

6.2 Security Assurance Requirements

The assurance level for this TOE is EAL2.

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
	ALC_FLR.2 Flaw reporting 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 19: Assurance requirements for EAL2 + ALC_FLR.2

6.3 Security Requirement Rationale

6.3.1 Tracing between SFR and security objectives of TOE

SFR/Security Objectives	O.InfoFlowControl	O.Confidentiality	O.PhyTamper	O.TrustedPath	O.2FA	O.IDnAuth	O.SelfTest
Security management operations							
FIA_ATD.1					**x**	**x**	
FIA_UAU.1					**x**	**x**	
FIA_UID.1						**x**	
FIA_USB.1						**x**	
FIA_AFL.1						**x**	

FMT_SMF.1						x	
FMT_SMR.1						x	
FMT_MOF.1						x	
FMT_MSA.3	x						
FMT_MTD.1						x	
FCS_COP.1/TP_ENC				x			
FCS_CKM.1/TP_ENC				x			
FCS_CKM.4/TP				x			
FTP_TRP.1				x			
FTA_SSL.3				x			
FTA_SSL.4				x			
Normal operations							
FDP_IFC.1	x						
FDP_IFF.7	x						
FCS_COP.1/SSD		x					
FCS_CKM.1/SSD		x					
FCS_CKM.4/SSD		x					
FPT_PHP.1			x				
FPT_TST.1							x
FPT_FLS.1							x
FPT_ITT.1		x					
FCS_COP.1/Inter-chip		x					
FCS_CKM.1/Inter-chip		x					
FCS_CKM.4/Inter-chip		x					

Table 20: Tracing between SFR and security objectives of TOE

6.3.2 Justification for tracing

The following section provides justification for the tracing in Table 12.

O.InfoFlowControl	The TOE shall block information flow between its SSD and user PC when it detects ransomware and data-cloning ware behaviour.
FDP_IFC.1 and **FDP_IFF.7**	control the information flow in and out of the SSD according to a set of attribute-based rules.
FMT_MSA.3	defines the restrictive default values for security attributes that are used to enforce the **FDP_IFC.1** and **FDP_IFF.7**.

O.Confidentiality	The TOE shall protect the confidentiality of user data stored in its SSD.
FCS_COP.1/SSD	encrypts the SSD data, thereby protecting the confidentiality of SSD data.

FCS_CKM.1/SSD and **FCS_CKM.4/SSD**	ensures cryptographic keys are securely generated and destroyed after use, thus maintaining the confidentiality of SSD data.
FPT_ITT.1, FCS_COP.1/Inter-chip, FCS_CKM.1/Inter-chip and **FCS_CKM.4/Inter-chip**	protects the confidentiality of cryptographic keys exchanged during inter-chip communication.
O.PhyTamper	The TOE shall detect physical tamper. When tamper is detected by TOE, the SSD will be locked or purged.
FPT_PHP.1	ensures that physical tamper is detectable by the user. The user can detect physical tamper on the TOE, when he/she discovers that the TOE is locked or its SSD data has been purged.
O.TrustedPath	The TOE shall establish and maintain trusted Bluetooth communication between the user and TOE.
FCS_COP.1/TP_ENC	ensure that confidentiality of the Bluetooth communication is protected.
FCS_CKM.1/TP_ENC, and **FCS_CKM.4/TP**	ensure that the cryptographic keys are secure generated and destroyed after use, thereby maintaining the confidentiality of the Bluetooth communication.
FTP_TRP.1	provides a trusted path for user authentication and security management.
FTA_SSL.3 and **FTA_SSL.4**	provides user- and TSF initiated termination when the trusted path is no longer required, thus reducing risk of exposure of user and TSF data traversing over Bluetooth.
O.2FA	The TOE shall enforce 2-FA during user identification and authentication prior to allowing user access to its security management functionality.
FIA_ATD.1	maintains the security attributes required for user identification and authentication i.e. **FIA_UID.1** and **FIA_UAU.1,** respectively.
FIA_UAU.1	provides user authentication function.
O.IDnAuth	The TOE shall perform user authentication prior to allowing user access to its security management functionality. The TOE shall also set a limit on the number of failed authentications.
FIA_ATD.1	defines the user security attributes required for user identification and authentication.
FIA_UAU.1 and **FIA_UID.1**	provide user identification and authentication security function based on the user security attributes defined in **FIA_ATD.1**.
FIA_USB.1	provides user-subject binding after user authentication is successful.

FIA_AFL.1	controls the number of failed authentication attempts and define the TOE action when the number of attempts is met.
FMT_SMF.1	defines the security management functions offered by the TOE
FMT_SMR.1	defines security roles that can access the management functions defined in **FMT_SMF.1**.
FMT_MOF.1	defines the access control policy that governs access to management functions defined in **FMT_SMF.1** by security roles defined in **FMT_SMR.1**.
FMT_MTD.1	defines the access control policy to manage TSF data.

O.SelfTest	The TOE shall perform self-test during initialisation and operation.
FPT_TST.1	provides self-test on a subset of TSF to ensure the correct the operation of the TSF.
FPT_FLS.1	ensures the TSF maintains a secure state if the self-tests fail.

6.3.3 SFR Dependency Fulfilment

SFR	Dependencies	Fulfilment
Security management operations		
FIA_ATD.1	No dependencies.	Not applicable
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	No dependencies.	Not applicable
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FMT_SMF.1	No dependencies.	Not applicable
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	The security attributes for FDP_IFF.7 and FDP_IFC.1 are not configurable.
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FCS_COP.1/TP_ENC	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/TP_ENC
	FCS_CKM.4	FCS_CKM.4/TP
FCS_CKM.1/TP_ENC	[FCS_CKM.2, or FCS_COP.1]	FCS_COP.1/TP_ENC
	FCS_CKM.4	FCS_CKM.4/TP
FCS_CKM.4/TP	[FDP_ITC.1, or FDP_ITC.2, or	FCS_CKM.1/TP_ENC

	FCS_CKM.1]	
FTP_TRP.1	No dependencies.	Not applicable
FTA_SSL.3	No dependencies.	Not applicable
FTA_SSL.4	No dependencies.	Not applicable
Normal operations		
FDP_IFC.1	FDP_IFF.1	FDP_IFF.7 is hierarchical to FDP_IFF.1
FDP_IFF.7	FDP_IFC.1	FDP_IFC.1
	FMT_MSA.3	FMT_MSA.3
FCS_COP.1/SSD	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/SSD
	FCS_CKM.4	FCS_CKM.4/SSD
FCS_CKM.1/SSD	[FCS_CKM.2, or FCS_COP.1]	FCS_COP.1/SSD
	FCS_CKM.4	FCS_CKM.4/SSD
FCS_CKM.4/SSD	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/SSD
FPT_PHP.1	No dependencies.	Not applicable
FPT_TST.1	No dependencies.	Not applicable
FPT_FLS.1	No dependencies.	Not applicable
FPT_ITT.1	No dependencies.	Not applicable
FCS_COP.1/Inter-chip	[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.1/Inter-chip
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4/Inter-chip
FCS_CKM.1/Inter-chip	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]	FCS_COP.1/Inter-chip
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4/Inter-chip
FCS_CKM.4/Inter-chip	[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.1/Inter-chip

Table 21: SFR dependency fulfilment

6.3.4 Rationale for EAL2 + ALC_FLR.2

The assurance level for this protection profile is EAL2 + ALC_FLR.2. EAL2 + ALC_FLR.2 allows a developer to attain a reasonable assurance level without the need for highly specialized processes and practices. It is the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL2 is appropriate for commercial products that can be applied to basic security functions.

7 TOE Summary Specification (ASE_TSS)

7.1 Security management operation

This section describes a summary of how the TOE achieves the SFRs during security management operations.

7.1.1 Identification and Authentication

TOE performs user identification and authentication only when user accesses the TOE's security management functions. The TOE maintains only one role i.e. administrator when user access its security management function.

FIA_ATD.1 User attribute definition	The TOE maintains the following attributes to belonging to the user These attributes are required as part of user identification and authentication. • password • role • one-time password (OTP**)**
FIA_UAU.1 Timing of authentication **FIA_UID.1 Timing of identification**	The TOE enforces the following security functions on behalf of the user before user is identified and authenticated. The TOE performs user identification and authentication only user needs to access its security management functions. • Information flow control • SSD encryption and decryption • TSF protection • Trusted path • Password policy
FIA_USB.1 User-subject binding	When the TOE has successfully identified and authenticated the user, the TOE shall associate the email ID with the administrator role.
FIA_AFL.1 Authentication failure handling	When the TOE detects 5 has met, the TOE shall 1. lock user access to security management. 2. request user to change password using OTP.

Table 22: TSS related to Identification and Authentication

7.1.2 Security Management

FMT_SMF.1 Specification of Management Functions	The TOE implements the following management functions: • Management of administrator's password • Management of 2-FA authentication methods • Change subject security attributes • Enable/Disable physical tamper sensors • Enable/Disable information flow control
FMT_SMR.1 Security roles	The TOE implements only one security role i.e. administrator to manage the TSF.
FMT_MOF.1 Management of security functions behaviour	The TOE specifies the following SFRs that can be managed by the administrator: • FIA_UAU.1 • FIA_UID.1 • FIA_USB.1 • FMT_SMR.1 • FPT_PHP.1 • FDP_IFC.1 and FDP_IFF.7

FMT_MSA.3 Static attribute initialisation	The TOE does not allow alternative initial values for security attributes that are used to enforce the Ransomware and Data-cloning ware SFP.
FMT_MTD.1 Management of TSF data	The TOE restricts the ability to manage the following TSF data to the administrator: • Reference administrator's authentication data i.e. password • Purge enable value • Lock status value • Physical tamper sensors enable values

Table 23: TSS related to security management

7.1.3 Trusted Path

The TOE communicates with the user mobile via Bluetooth and user PC via PCIe over a trusted path. The trusted path is used for initial user authentication and security management.

FCS_COP.1/TP_ENC Trusted path encryption/decryption operation	The TOE implements AES-128 to protect the Bluetooth and PCIe communication against disclosure during security management.
FCS_CKM.1/TP_ENC Trusted path encryption/decryption key generation	The TOE implements ECDH curve secp192r1 (NIST 192-bit) for encryption/decryption key generation.
FCS_CKM.4/TP Trusted path key destruction	The TOE implements zeroization for destruction of keys related to the trusted path. This further preserves the confidentiality of the Bluetooth communication.
FTP_TRP.1 Trusted path	The TOE establishes a trusted path between the TOE and the user mobile to protect the Bluetooth communication against disclosure and modification.
FTA_SSL.3 TSF-initiated termination	The TOE allows user-initiated termination of user's own interactive session via the user mobile.
FTA_SSL.4 User-initiated termination	The TOE implements termination of an interactive session after 5 minutes.

Table: TSS related to trusted path

7.2 Normal operations

7.2.1 Information Flow Control

FDP_IFC.1 Subset information flow control	The TOE shall enforce the Ransomware and Data-cloning ware SFP on the subjects '*Data owner*' and '*Threat agent*', information '*SSD data*' and over read and write operations The TOE SFP shall be based on the following attributes-based rules: If data image model of read and/or write activities deviates from reference data models, the TOE shall lock access to the SSD.
FDP_IFF.7 Information flow metric	

Table 24: TSS related to information flow control

7.2.2 SSD encryption and decryption

FCS_COP.1/SSD SSD encryption/decryption operation	The TOE implements AES-256 to protect the SSD data against disclosure.

FCS_CKM.1/SSD SSD cryptographic key generation	The TOE implements SM4 algorithm for key generation of SSD data encryption/decryption.
FCS_CKM.4/SSD SSD cryptographic key destruction	The TOE implements zeroization for destruction of keys related to the SSD data encryption/decryption. This further preserves the confidentiality and integrity of the Bluetooth communication.

Table 25: TSS related to storage encryption and decryption

7.2.3 TSF Protection

FPT_PHP.1 Passive detection of physical attack	The TOE monitors SSD disconnection for physical tamper.
FPT_TST.1 TSF testing	The TOE performs self-tests during initial start-up to demonstrate correct operations of • FCS_COP.1/TP_ENC • FCS_CKM.1/TP_ENC • FCS_COP.1/SSD • FCS_CKM.1/SSD • FCS_COP.1/Inter-chip • FCS_CKM.1/Inter-chip • FDP_IFC.1 • FDP_IFF.7
FPT_FLS.1 Failure with preservation of secure state	The TOE will halt when any one of the self-tests related to the following SFRs fails. • FCS_COP.1/TP_ENC • FCS_CKM.1/TP_ENC • FCS_COP.1/SSD • FCS_CKM.1/SSD • FCS_COP.1/Inter-chip • FCS_CKM.1/Inter-chip
FPT_ITT.1 Basic internal TSF data transfer protection	The TOE encrypts the inter-chip communication to protect TSF data being exchanged between the chips against disclosure.
FCS_COP.1/Inter-chip Inter-chip encryption/decryption operation	The TOE implements AES-128 to protect the TSF data against disclosure during inter-chip communication.
FCS_CKM.1/Inter-chip Inter-chip key generation	The TOE implements ECDH curve secp192r1 (NIST 192-bit) for key generation of inter-chip communication.
FCS_CKM.4/Inter-chip Inter-chip key destruction	The TOE implements zeroization for destruction of keys related to the inter-chip encryption/decryption. This further preserves the confidentiality and integrity of the inter-chip communication.

Table 26: TSS related to TSF protection

8 References

[CC1] Common Criteria Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5

[CC2] Common Criteria Information Technology Security Evaluation, Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5

[CC3] Common Criteria Information Technology Security Evaluation, Part 3: assurance components, April 2017, Version 3.1, Revision 5

[PATENT1] System And Method For Detecting Data Anomalies By Analysing Morphologies Of Known And/Or Unknown Cybersecurity Threats, 2020

[PATENT2] Module And Method For Detecting Malicious Activities In A Storage Device, 2020

9 Glossary

Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.
Digital signature	A non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.
Firmware	The programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Hardware: the physical equipment used to process programs and data in a CIMC.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Security policy	A precise specification of the security rules under which a CIMC shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.
Software	The programs and associated data that can be dynamically written and modified.
Target of Evaluation (TOE)	An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

10 Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IT	Information Technology
OS	Operating System

SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification