Biocryptodisk Encryptor Model SD302(Ver5.11-3.03), SD302CR(Ver5.11-5.03), ST302(Ver5.11-1.00), and ST302B(Ver5.11-1.00) with Remote Token Management Systemv1.00Security Target

(Version 0.7)

29 December, 2014

Table of Contents

Version History

Version No	Reason To Change	Release Date
0.1	Initial draft	26 Sept 2013
0.2	Second draft	11 Oct 2013
0.3	Third draft	08 Nov 2013
0.4	fourth draft	23 Dec 2013
0.5	fifth draft	30 Dec 2013
0.6	sixth draft	30 June 2014

Approvals

Name	Role	Date
0.7	Seventh draft	29 December 2014

1 Security Target Introduction

This section presents the following information:

- Identifies the Security Target (ST) and Target of Evaluation (TOE);
- Defines the terminology and acronyms used in the ST,
- Defines TOE overview and TOE description.

1.1 ST Reference and TOE Reference

ST Title:	Biocryptodisk Encryptor Model SD302(Ver5.11-3.03), SD302CR(Ver5.11-5.03), ST302(Ver5.11-1.00), and ST302B(Ver5.11-1.00) with Remote Token Management System v1.00 Security Target
ST Version:	V 0.7
TOE Identification	Biocryptodisk Encryptor Model SD302 (Ver5.11-3.03), SD302CR(Ver5.11-5.03), ST302(Ver5.11-1.00), and ST302B(Ver5.11-1.00) with Remote Token Management System v1.00
CC Identification	Common Criteria for Information Technology Security Evaluations, version 3.1 R4
Keywords	

1.2 Terminology & Acronyms

1.2.1 Terminology

The following terminology is used in this Security Target:

AES: Advanced Encryption Standard (AES) is a symmetric-key encryption defined in Federal Information Processing Standard (FIPS) Publication 197. The standard comprises three block ciphers, AES-128, AES-192 and AES-256.

AES CBC Mode: The CBC-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES) algorithm. (The acronym CBC stands for Cipher Block Chaining)

AES XTS Mode The XTS-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES) algorithm. (The acronym XTS stands for the **X**EX **T**weak able Block Cipher with Cipher-text**S**tealing)

Elliptic Curve Cryptography (P-256, P-384): is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Specified inFIPS186-3.

ECDSA P-256/P-384: Elliptic Curve Digital Signature Algorithm; specified in ANS X9.62. Curve P-256 and P-384 are used.

ECIES P-256: Elliptic Curve Integrated Encryption Scheme. Curve P-256 is used.

KDF: Key Derivation Function; specified in ANSI X9.63

RNG: Random Number Generator; specified in ANSI X9.31

SHA-2 (SHA-256/SHA-384): Secure Hash Algorithm; specified in FIPS 180-3

HMAC (SHA-256):The Keyed-Hash Message Authentication Code in FIPS PUB 198

Hash_DRBG(SHA256): Deterministic Random Bit Generator in NIST SP 800-90A

Bulk Encryption: Encryption of bulk data

Key pair:A public key and its corresponding private key

Cryptanalysis: A methodology used by threat agents in order to break the cryptographic protection of the TOE.

Cryptographic Operation: Encryption and decryption operations inside the TOE with Asymmetric and Symmetric algorithm.

Encryption Key: The 256-bit AES key used by the TOE for encryption process.

Non-Volatile Memory: The memory portion developed with flash technology inside the integrated circuit.

Random Key Generation: 256-bit AES key generated by random number generation (RNG) compliant with ANSI X9.31 which is seeding with USB channel frame number.

Host System: The system on which the TOE is plugged and used. (desktop pc, laptop pc, testing equipment .etc)

Authorized User: Owner of the TOE.TOE recognizes the Authorized User by valid password.

Retry Number: Number of consecutive failed authentication attempts which is incremented each time when a failure occurs and reset each time when an authentication is successful.

File System: A method for storing files in any kind of mass storage device. (etc. FAT32, NTFS, EXT3)

Small Computer System Interface: SCSI is a set of standards for physically connecting and transferring data between computers and peripheral devices.

Mass Storage Device Driver: A type of device driver which supports the interface with all kind of USB flash drives and USB external hard drives

Logical Unit Number: Number of logical device interface in a single physical channel.

Encryptor: Biocryptodisk Token Model of SD302, SD302CR, ST302, ST302B (hardware)

SSD: is a data storage device using integrated circuit assemblies as memory to store data persistently

HDD: is a data storage device used for storing and retrieving digital information using rapidly rotating disks (platters) coated with magnetic material.

- SD302/SD302CR models of encrypted drive with hardware file en-/decryption
- ST302/ST302B models of encrypted drive based on SSD and HDD

AES Mass Storage Controller: a crypto controller which has a hardware AES en-/decryption engine and support high speed hardware AES en-/decryption of mass storage data

Cryptographic Controller:a controller capable of performing asymmetric and symmetric en-/decryption by its firmware and is able to store critical security parameter securely

1.2.2 Encryptor: Include Hardware and Firmware of TOE Acronyms

AES	Advanced Encryption Standard
CC	Common Criteria
SCSI	Small Computer System Interface
TOE	Target of Evaluation
ST	Security Target
SFR	Security Functional Requirements
SAR	Security Assurance Requirements
EAL	Evaluation Assurance Level
MSD	Mass Storage Device
LUN	Logical Unit Number
FIPS	Federal Information Processing Standard
USB	Universal Serial Bus
HSM	Hardware Security Module
CSP	Critical Security Parameter

1.3 TOE Overview

1.3.1 Usage and Major Security Features of the TOE

The TOE can be divided into two categories, one is hardware which represented by Biocryptodisk Encryptor and software which represented by Remote Token Management System (RTM System).

Biocryptodisk Encryptor is a USB portable hardware cryptographic module. It has an on-the-fly AES 256-bit hardware en-/decryption engine on board which have capability of en/decrypting files from any computer detected storage such as USB external drive, network attached drive and virtual drives. It is truly driverless and zero footprint. In addition, it has an on board encrypted storage.

The data stored in ST302 series of Biocryptodisk Encryptor is in AES 256 bit XTS mode; whereas, the data stored SD302 series of Biocryptodisk Encryptor is in AES 256 bit CBC mode.

Remote Token Management System (RTM System) is combination of two main application, one is RTMManager which helps to remotely manage and control the Biocryptodisk Encryptor, another one is BCDLogin which helps to perform login/logout, change password and hardware file en-/decryption.

The main feature of RTM System is managing the Biocryptodisk Encryptor over network which have ability to perform the functionality of disable Encryptor, enable Encryptor, destroy Encryptor, and monitoring the diary activities of the Biocryptodisk Encryptor remotely. All of the communication over network is encrypted by SSL protocol.

The second feature of RTM System is have ability to perform hardware file en-/decryption with key strength up to AES-256. Each of keys is represented by file extension in order to make it easier to use and recognized. The AES/IV keys are stored as a group profile, named as Encryption Profile, each of Encryption Profile are includes up to 5 differences of set AES/IV keys and its corresponding file extension. The Encryption Profile is selected and imported to the Biocryptodisk Encryptor during enrolment process by administrator. The imported AES keys are never exposed and exported to outside from Biocryptodisk Encryptor. The Encryption Profile is generated and centralized control by an administrator of corporation in order to allow the authorized workers who have Biocryptodisk Encryptor to en-/decrypt the confidential documents from computer detected storage such as virtual drives. The activities of en-/decrypting process from Biocryptodisk Encryptor will be recorded and upload to server.

The third feature of RTM System is hardware file en-/decryption with non-managed setup. This feature is special designed for Non-Managed Encryptor. The supported application is mainly focus on BCDLogin Application which has ability to perform the functionality of login/logout, change password, EP management and hardware file en-decryption. The user of Non-Managed Encryptor is able to use the EP management tool to generate one/multiple Encryption Profile and import it to Non-Managed Encryptor. The user may later use the imported keys to en-decrypt files anytime anywhere.

Biocryptodisk Encryptor is delivered to customer in two types of models which are

1) Master Encryptor (with RTMManager +BCDLogin Applications)
2) Non-Managed Encryptor (with BCDLogin Application)

The Master Encryptor has ability to enrol/initialize the Non-Managed Encryptor to become Managed Encryptor by using RTM Manager Application. Once the Non-Managed Encryptor is converted to Managed Encryptor, it is unable to change back to Non-Managed Encryptor.

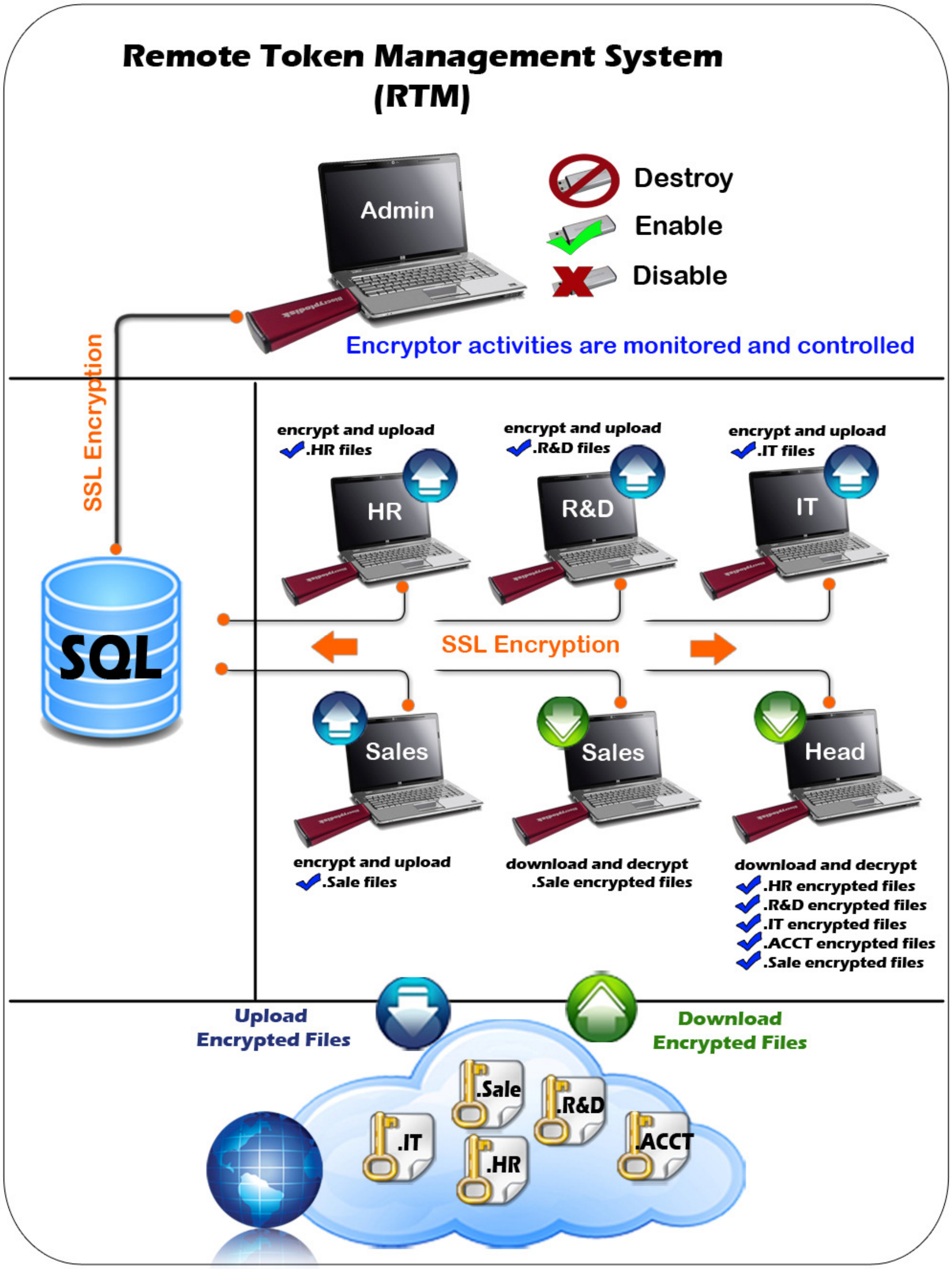


Figure 1: RTM System VS Biocryptodisk Encryptor

1.3.2 Type of Biocryptodisk Encryptor

Biocryptodisk Encryptor consists of 2major series namely:

SD Series

- SD302 – USB2.0 portable encrypted drive with hardware file en-/decryption
- SD302CR – USB2.0 portable encrypted drive with hardware file en-/decryption and smart card reader

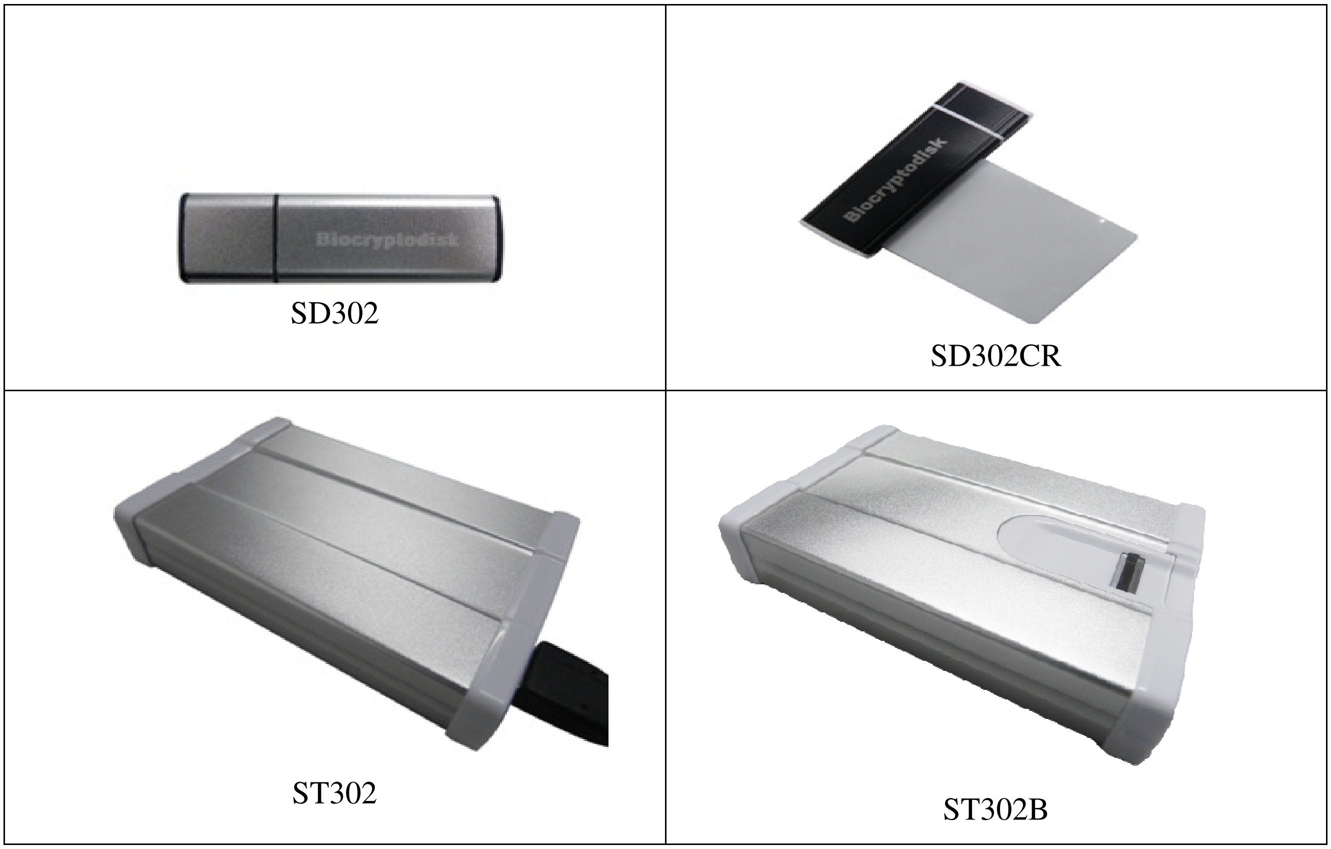
ST Series

- ST302 – USB3.0 portable encrypted HDD/SSD
- ST302B – USB3.0 portable encrypted HDD/SSD with biometric

Biocryptodisk Encryptor is categorized into three types

- Master Encryptor
- Non-Managed Encryptor
- Managed Encryptor

Only SD series can be configured as Master Encryptor.



SD302

SD302CR

ST302

ST302B

Figure 1: Biocryptodisk Encryptor Model

Biocryptodisk Encryptor is performed as 2 factor authentication (password + Encryptor)

Biocryptodisk Encryptor is splitted into 2 partitions, which are CDFS drive and encrypted drive. The size of the CDFS drive is pre-defined to 32MB, while the size of the encrypted drive is based on the series of Biocryptodisk Encryptor.

1.3.3 Supported Applications along with Biocryptodisk Encryptor

The BCDLogin Application will be burned into Biocryptodisk Encryptor's CDFS drive.

The RTM Manager Application is only supported for Master Encryptor which is stored in Encryptor's encrypted drive before shipped to customer.

1.3.4 Security Assurance

The TOE is designed to minimize threats to an organization by providing secure management and reporting capabilities. The TOE is using state of the art encryption technology to secure communication data as well as mass storage data. The Encryptor is a hardware cryptographic module implemented with the following cryptographic algorithms on board:

a) Elliptic Curve Cryptography (P-256, P-384):(FIPS186-3)
   Elliptic Curve Digital Signature Algorithm(ECDSA P-256/P-384)
   Elliptic Curve Integrated Encryption Scheme (ECIES P-256)
b) PKI Key Pair (P-256, P384) Generation
c) Key Derivation Function (KDF)(ANSI X9.63)
d) Random Number Generator (RNG)(ANSI X9.31)
e) V-Seed Generator for RNG(HASH_DRBG SP 800-90)
f) SHA-2 series of hash functions.(SHA-256/SHA-384)
g) AES with 256-bit key mode Encrypt/Decrypt (FIPS197)
h) HMAC-SHA256

The Encryptor on board random number generator has passed the test of NIST SP800-22 Rev 1a "A Statistical Test Suite for Random Number Generators for Cryptographic Applications".

The communication between RTM System and the Encryptor is secured by AES session key generated through the random number exchanged protected by the algorithms above. The RTM System communication with SQL server is secured by SSL as well as AES encryption.

The RTMManager in the Master Encryptor allow system administrator to manage the Encryptor remotely anytime anywhere over the internet. The security for updating Encryptor activities isprovided by SSL and AES encryption. The security for destroy, disable and enable Encryptor involves SSL, AES and PKI based on P-256 ECIES. The Encryptor application is operating in Microsoft Windows Operating system only.

The SD series Encryptor are able to performed high speed on-the-fly AES files encryption/decryption on board the Encryptor if they are pre-configure with AES Encryption key. The SD series Encryptor can be configured up to 5 AES encryption keys. Each AES Encryption key is represented by a file extension. The file extension scheme enable organization wide file sharing as well as information control. Junior employee may have only an encryption key inside his Encryptor and thus have limited sharing to company secret. The Encryptor encryption and decryption activities can be controlled and monitored by the RTMManager.

1.4 Initial State of TOE

Initially, the Encryptorcan be assumed in 2conditions which are

- User purchases the Non-Managed Encryptor for the first time
- User purchases the Master Encryptor for the first time

Non-Managed Encryptor

At initial state, Encryptor is shipped from factory as Non-Managed Encryptor. It can function as password protected encrypted drive. BCDLogin.exe is burned into Encryptor’s CDFS drive which provides functions of login/logout and self-managed Encryption Profile to implement on-the-fly AES file en-/decryption. As first time login to encrypted drive, the application will enforce the user to change their encrypted drive’s password.

Master Encryptor

At initial state, the Master Encryptor is shipped from factory. The Master Encryptor cannot be assigned by other Master Encryptor except Biocryptodisk Sdn.Bhd. It can be performed as Non-Managed Encryptor and supported full functionality of RTMManager Application. In addition, it has ability to initial/enroll the Non-Managed Encryptor to become as Managed Encryptor.

1.5 Configuring the TOE

For Server side:

The server has to be setup with Windows Server 2008 R2and Microsoft SQL Server 2012 Express Version. The Microsoft SQL Server 2012 Express Version must be setup with SSL encryption.

1.6 Activate State of TOE- Normal Usage

For RTM Manager Application:

The RTM Manager is used to implement the following functions which

- Enroll Non-Managed Encryptor to be a Managed Encryptor locally
- Enable Managed Encryptor remotely
- Disable Managed Encryptor remotely
- Generate and modify Encryption Profile
- Destroy Managed Encryptor remotely
- Maintain Administrator Privileges
- Export events-log from server database
- Maintain the offline log on number for Managed Encryptor locally
- Password of Managed Encryptor can be reset locally only with the present of Master Encryptor which is used to enroll the specific Managed Encryptor.

For BCDLogin Application:

The functionality of BCDLogin Application is as table below:

Series	Type	Functionality
SD302/SD302CR	Master	• Login/logout • Change password • RTM Manager • Hardware file en-/decryption
SD302/SD302CR	Non-Managed	• Login/logout • Change password • Encryption Profile Management • Hardware file en-/decryption
SD302/SD302CR	Managed	• Login/logout • Change password • Hardware file en-decryption • Upload activities of Encryptor to server • Remote enable, disable and destroy

ST302/ST302B	Non-Managed	• Login/logout • Change password • Delete all fingerprint
ST302/ST302B	Managed	• Login/logout • Change password • Upload activities of Encryptor to server • Remote enable, disable and destroy

1.7 TOE Type

TOE is an integrated system that includes hardware, firmware and software modules which can be categorized as a data protection product with management capability.

1.7.1 Required Non-TOE hardware/software/firmware

TOE should be configured before the usage in a host system with the following minimum configuration:

Server Center

Windows OS Recommended: Windows Server 2008 R2

Requirements:

- Processor: minimum: 1G (x86 processor) or 1.4GHz (x64 processor)
- Memory: minimum: 512MB RAM, recommended :2GB RAM or greater
- Available Disk Space: minimum 10GB, recommended: 40GB or greater
- Display and peripherals: High-resolution monitor, keyboard, mouse

SQL Server Software Recommended: Microsoft SQL Server 2012 Express Version

Requirements:

- Supported OS: Windows 7, Windows Server 2008 R2, Windows Server 2008 Service Pack 2, Windows Vista Service Pack 2
- Memory: minimum of 512MB of RAM (2GB or more is recommended)
- 2.2GB of available hard disk space
- Must installed either .NET 3.5 SP1 or .NET 4

RTM System

1) RTM Manager
   Requirements:
   - Windows OS Recommended: Windows XP SP2, Windows Vista, Windows 7, Windows 8.(running in Admin Account)
   - Installed CA Certificate which is exported from Server Center for SSL Encryption

- Internet Connection

2) BCDLogin (Managed Encryptor)

   Requirements:
   - Windows OS Recommended: Windows XP SP2, Windows Vista, Windows 7, Windows 8
   - Installed CA Certificate which is exported from Server Center for SSL Encryption
   - Internet Connection

3) BCDLogin(Non-Managed Encryptor/ Master Encryptor)
   - Windows OS Recommended: Windows XP SP2, Windows Vista, Windows 7, Windows 8

1.7.2 TOE DESCRIPTION

The TOE is an eco system which is created to secure organizations' mobile intellectual properties anytime anywhere in the world. Biocryptodisk Encryptor stores organizations' information in the password protected encrypted drive. In additional, SD series of Encryptor has ability to perform hardware file en-decryption which is useful to secure confidential data. Biocryptodisk Encryptor has support up to 5 set of hardware file en-decryption keys. Appropriate user authentication is performed using password validation. If the password enter is incorrect after 10 attempts, Data Encryption Key (DEK) will change and all data in encrypted drive cannot be recovered.

1.7.3 Capability of TOE

i. **Master Encryptor (SD302, SD302CR)**

- Encrypted drive with password protected
- Able to login/logout and change password of encrypted drive
- Self destructafter10 failed login attempts
- Enforced to change password as first time login
- Perform hardware files en-/decryption
- Able to generate Encryption Profile for Managed Encryptor and personal use
- Enroll/manage Managed Encryptor
- Reset Managed Encryptor's encrypted drive password
- Monitor activities of Managed Encryptor

ii. **Non-Managed Encryptor (SD302/SD302CR)**

- Encrypted drive with password protected
- Able to login/logout and change password of encrypted drive
- Self destruct after 10 failed login attempts
- Enforced to change password as first time login
- Self-generate Encryption Profile for personal use
- Perform hardware files en-/decryption with self generate Encryption Profile

iii. Non-Managed Encryptor (ST302/ST302B)

- Encrypted drive with password/biometric protected
- Able to login/logout and change password of encrypted drive
- Self destruct after 10 failed login attempts
- Enforced to change password as first time login
- Delete fingerprint for ST302B only

iv. Managed Encryptor (SD302/SD302CR)

- Encrypted drive with password protected
- Able to login/logout and change password of encrypted drive
- Self destruct after 10 failed login attempts
- Enforced to register as first time login
- User set encrypted drive's password during registration
- Upload the activities of Encryptor to server
- Perform hardware files en-/decryption with Encryption Profile which is generated/imported by Master Encryptor

v. Managed Encryptor (ST302/ST302B)

- Encrypted drive with password/biometric protected
- Able to login/logout and change password of encrypted drive
- Self destruct after 10 failed login attempts
- Enforced to register as first time login
- User set encrypted drive's password during registration
- Upload the activities of Encryptor to server

1.8 PHYSICAL SCOPE

Biocryptodisk Encryptor consists of hardware and firmware module

Firmware module consists of HSM Ver5.11, SD Ver3.03, SD Ver5.03 and ST Ver1.00

Feature Model	Cryptography Processor	AES Mass Storage Controller	Size	Managed	USB	Smart Card Reader	Bulk En/Decryption	Biometric Authentication
SD302-M	HSM (Ver5.11)	SD (Ver3.03)	8-32GB	YES	USB 2.0	No	Yes	No
SD302	HSM (Ver5.11)	SD (Ver3.03)	8-32GB	NO	USB 2.0	No	Yes	No
SD302CR-M	HSM (Ver5.11)	SD (Ver5.03)	8-32GB	YES	USB 2.0	Yes	Yes	No

SD302CR	HSM (Ver5.11)	SD (Ver5.03)	8-32GB	NO	USB 2.0	Yes	Yes	No
ST302-M	HSM (Ver5.11)	ST (Ver1.00)	500GB -4TB	YES	USB 3.0	No	No	No
ST302	HSM (Ver5.11)	ST (Ver1.00)	500GB -4TB	NO	USB 3.0	No	No	No
ST302B	HSM (Ver5.11)	ST (Ver1.00)	500GB -4TB	NO	USB 3.0	No	No	Yes
ST302B-M	HSM (Ver5.11)	ST (Ver1.00)	500GB -4TB	Yes	USB 3.0	No	No	Yes

1.9 LOGICAL SCOPE

The TOE includes:

Database:

1) RTM System
- Store the Encryptor device information
- Store the privilege management roles for each of administrator
- Store the audit record

Audit:

1) RTM System
- Generate audit records of auditable events
- Administrator is able to read the audit records
- Audit records are selectable

Cryptographic support:

1) Encryptor
- Key generation for Key Pair, Digital Signature and Random Number Generation (RNG)
- Data encryption/decryption using drive sector based encryption/decryption
- Key destruction
- Key hashing

2) RTM System
- USB channel encryption/decryption between RTM System and Encryptor

User Data Protection:

1) Encryptor:

- User accessible function based on privilege given by Administrator
- Ensure that the network communication between is encrypted by SSL. However, the SSL is not enforced by the TOE but by the environment.

2) RTM System:

- The accessibility of specific functionality from RTMManager Application is based on the admin privilege level.

Identification and Authentication:

1) Encryptor:
    - User must enter the valid password to access the encrypted drive and cryptographic services.
    - The password must be 8 to 16 characters in length and must contain at least a number, an alphabet and a symbol.
    - For Model ST302B, an alternative fingerprint authentication can be used to access the encrypted drive and cryptographic services.

2) RTM System
    - The user must provide valid username and password for connecting to SQL server.
    - Database username and password are part of the scope.

Management:

RTM System for Managed Encryptor to control and monitor the Managed Encryptor locally and remotely:

- Manage offline login number
- Manage Encryption Profile
- Monitor Encryptor's activities
- Reset Encryptor's password
- Remote enable/disable/destroy Encryptor

Testing:

During the start-up of Encryptor, the following self tests are conducted;

- SHA256 KAT
- AES CBC-Encrypt/Decrypt KAT
- P256 PKI Key Pair Generation KAT
- Data integrity of Critical Security Parameter

Encryptor will preserve secure state on several failure events.

Critical security parameter are encrypted and stored in cryptographic module. It is replicated in two memory spaces in the cryptographic module (Bank 1 and Bank 2). CRC checking on integrity of each bank is executed. The CSP is consistent when replicated between parts of the TOE and protected from modification.

Trusted path:

- Encrypt communication session between RTM System and Encryptor. Establish secure channel with the RTM System. The communication session is protected by P256 ECIES and AES-256 session key.

2 CONFORMANCE CLAIM

The conformance claims regarding to the TOE are stated in the following sub-sections.

2.1CC Conformance Claim

This TOE and ST are consistent with the following specifications:

CC conformant	The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 4.
Part 2 conformant	The ST is Common Criteria Part 2 extended
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+ Augmented with ALC_FLR.1.
Protection Profile conformance	None

2.1.1 Conformance Rationale

The assurance level of EAL2+ is considered to be most appropriate for this type of TOE since it is intended to defend against attacks that can be made given the assumptions, and the threats defined in Chapter 3.

3 SECURITY PROBLEM DEFINITION

3.1Assumption

The assumptions are made to ensure the security of the TOE and its deployed IT environment.

Table 1: Assumptions

A.PHY	The TOE and its environment are physically secured and managed by authorized TOE Administrator.
A.ADMIN	Authorized TOE Administrators is non-hostile, assigned by organization and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.
A.BACKUP	The TOE environment will provide data backups on user data and TOE data such as audit logs.
A.STORAGE	The TOE environment will provide sufficient storage for TOE operational environments.
A.TIMESTAMP	The TOE environment will provide reliable time stamps to enable the TOE to timestamp audit records.
A.IDLE	The TOE environment must be protected during idle.
A.NETSECURE	The TOE environment will provide secure channel for network communication between Host and Server.

3.2Threats

Assets that are protected by the TOE are sensitive data, stored in the TOE or the TOE environment.

Threat agents are entities that can adversely act on the assets. The threat agents identified is an unauthorized person, an authorized user (a person that has been successfully authenticated and authorized to use TOE) or unauthorized external entities.

Threats may be addressed either by the TOE or by its IT environment.

Table 2: Threats

T.DATA	An unauthorized person may successfully accesses or disclosed the User data, TOE data and TOE Configurations.
T.AUDIT	An unauthorized person or authorized user specifically Administrator may intentionally or unintentionally perform malicious actions undetected.
T.EAVESDROP	An unauthorized person may eavesdrop the communication between Encryptor- RTM (Host) and RTM-SQL Server.
T.BRUTEFORCE	An unauthorized person may brute force the TOE authentication to obtain unauthorized access to TOE.
T.SESSIONHIJACK	An unauthorized person may use Administrator idle session to obtain unauthorized access to TOE.
T.CONFIG	An unauthorized person may read, modify, or destroy TOE data.
T.INTEGRITY	An unauthorized person may compromise the confidentiality of User data and TSF data in transitand/or in the Encryptor.The TOE may be compromised in the aspects of logical (data tampering – by renaming the filename or changing some file in the memory card SD) and physically (tampering with the circuit board or changing the SD card), in which, changing the integrity of the TOE.

3.3Organizational Security Policies

The Organizational Security Policies (OSP) is imposed by an organization to secure the TOE and its environment.

Table 3: Organizational Security Policy

P.ROLE	Only authorized person assigned by the organization manage the Master Encryptor.

4 Security Objectives

Security objectives are formed to address the security problem definition defined in earlier section. The security implementation in TOE and its IT environment will meet these objectives.

4.1Security Objectives for the TOE

The security objectives for the TOE as following:

Table 4: Security Objectives for the TOE

O.DATA	The TOE shall ensure that only authorized person can accesses or disclosed the User data, TOE data and TOE Configurations.
O.AUDIT	The TOE shall record the security events generated by TOE and prevent the audit records from intentionally or unintentionally deletion which may destroy evidence of adverse events executed.
O.EAVESDROP	The TOE shall prevent unauthorized person to eavesdrop and interpret the communication between Encryptor-RTM (Host) and RTM-SQL Server.
O.BRUTEFORCE	The TOE shall prevent unauthorized person to brute force the TOE authentication to obtain unauthorized access to TOE.
O.CONFIG	The TOE shall prevent unauthorized person to read, modify, or destroy TOE configuration data. Only Administrator is authorized to read and modify the TOE configuration data.
O.INTEGRITY	The TOE shall prevent unauthorized person to compromise the confidentialityof User data and TSF data in transit and/or in the Encryptor.The TOE may be compromised in the aspects of logical (data tampering – by renaming the filename or changing some file in the memory card SD) and physically (tampering with the circuit board or changing the SD card), in which, changing the integrity of the TOE.

4.2Security Objectives for the Operational Environment

The security objectives for the TOE operational and IT environment as following:

Table 5: Security Objectives for the Operational Environment

OE.PHY	The TOE and its environment shall be physically secured and managed by authorized TOE Administrator.

OE.ADMIN	Authorized TOE Administrator shall be non-hostile, assigned by organization and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.
OE.BACKUP	The TOE environment shall provide data backups for encryption profile and audit logs.
OE.STORAGE	The TOE environment shall provide sufficient storage for TOE operational environments.
OE.TIMESTAMP	The TOE environment shall provide reliable time stamps to enable the TOE to timestamp audit records.
OE.IDLE	The TOE environment shall be secured during idle.
OE.NETSECURE	The TOE environment shall provide secure channel for network communication between Host and Server.

5 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE. These requirements are presented following the conventions identified in Section Conventions.

5.1 Extended Security Functional Requirement (SFR)

Table 6: Extended SFR Component

Extended Component	Extended Component Name	Rationale
Class FAU : Security Audit		
FAU_GEN.3	Simplified Audit Data Generation	FAU class contains families of functional requirements that are related to monitor security-relevant events, and act as a deterrent against security violations. This component is a member of FAU_GEN, an existing CC Part 2 family. This extended requirement for the FAU class has been included in this ST because TSF audit function does not log start and stop of auditing function; hence FAU_GEN.1.1 (a) is not applicable. This component is also created to

		simplify the requirement of FAU_GEN.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.3 Simplified Audit Data Generation

Hierarchical No other component

Dependencies FPT_STM.1 Reliable time stamps

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:

[**assignment: defined auditable events**].

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event

b) [**assignment: other information about the event**].

5.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

6 TOE Security Functional Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 Conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to the statement of security functional requirements. Following are the operations and the document conventions as used within this ST to depict their application:

Assignment The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows[**assignment**].

Selection The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

Refinement The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

Iteration The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing an acronym at the end of the component identifier as follows: FCS_COP.1(A) Cryptographic operation (Hashing).

6.2 Security Functional Requirements

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Table 7: Security Functional Requirements

Component	Component Name
Class FAU: Security Audit	
FAU_GEN.3	Simplified Audit Data Generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
Class FCS: Cryptographic support	
FCS_CKM.1 (A)	Cryptographic key generation (Key Pair)
FCS_CKM.1 (B)	Cryptographic key generation (Digital Signature)
FCS_CKM.1 (C)	Cryptographic key generation (Random Number Generator)
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1 (A)	Cryptographic operation (Data Encryption/Decryption)
FCS_COP.1 (B)	Cryptographic operation (Hashing)
FCS_COP.1 (C)	Cryptographic operation (USB Channel Encryption/Decryption)
FCS_COP.1 (D)	Cryptographic operation (Digital Signature)
Class FDP : User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Class FIA : Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_UID.2	User Identification Before Any Action
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.5	Multiple authentication mechanisms

FIA_AFL.1	Authentication failure handling
FIA_SOS.1	Verification of secrets
Class FMT : Security Management	
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
Class FPT: Protection of the TSF	
FPT_TST.1	TSF testing
FPT_FLS.1	Failure with preservation of secure state
Class FTP: Trusted Paths/Channels	
FTP_TRP.1	Trusted path

6.2.1 Class FAU: Security Audit

6.2.1.1 FAU_GEN.3 Simplified Audit Data Generation

Hierarchical No other components.

Dependencies FPT_STM.1 Reliable time stamps

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:[**assignment:**

a) **Administrator Management**

b) **Encryption Profile**

c) **Token Enrollment**

d) **Token Management**

e) **Client Register**

f) **Client Logon**

g) **Client Encrypt**

h) **Client Decrypt**

i) Other]

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

[**assignment:**

a) Owner name (User)

b) Event Type

c) Event Details

d) Timestamp

e) PC Name

f) PC User

g) PC Serial Number

h) IP Address]

Application notes None

6.2.1.2 FAU_SAR.1 Audit review

Hierarchical No other components.

Dependencies FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**assignment: Administrator**] with the capability to read [**assignment: all audit log data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application notes None

6.2.1.3 FAU_SAR.3 Selectable audit review

Hierarchical No other components.

Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**assignment: select and search**] of audit data based on [**assignment:**

a) Owner name (User)

b) Event Type

Application notes None

6.2.2 Class FCS: Cryptographic support

6.2.2.1 FCS_CKM.1(A)Cryptographic key generation (Key Pair)

Hierarchical 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(A).1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment: ECIES**

which includes[

Generate Private Key by using

1) **V-Seed Generator for RNG (HASH_DRBG SP 800-90)**
2) **Random Number Generator (RNG)(ANSI X9.31)**
3) **Key Derivation Function (KDF)(ANSI X9.63)**

And

The Public Key is derived from the Private Key]

] and specified cryptographic key sizes [**assignment: 256-bits/384-bits**] that meet the following: [**assignment: FIPS 186-3**].

Application notes ECIES 256-bit is applicable for HSM Ver5.11 and RTM System

ECIES 384-bit is applicable for HSM Ver5.11

Key pair generation for :

a) AES session key to establish secure communication between host and Encryptor

b) Enrollment of User(Managed-Encryptor) where will be used during destroy, enable logon or disable logon remotely

Table A: FCS_CKM.1(A)

TOE Series	**Operation**	**Algorithm**	**Refer**
SD302/SD302CR	Has an on-the-fly AES 256-bit with CBC mode hardware en-/decryption engine Refer TOE	Symmetric encryption for generating 32-byte AES-key only, not for keypair.	FCS_COP.1 (A)

	Summary Specification for further details		
ST302/ST302B	Has an on-the-fly AES 256-bit with XTS mode hardware en-/decryption engine Refer TOE Summary Specification for further details	Symmetric encryption for generating 32-byte AES-key only, not for keypair.	FCS_COP.1 (A)

6.2.2.2 FCS_CKM.1(B) Cryptographic key generation (Digital Signature)

Hierarchical 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(B).1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment: ECDSA**

which includes[

Generate Private Key by using

4) **V-Seed Generator for RNG (HASH_DRBG SP 800-90)**
5) **Random Number Generator (RNG)(ANSI X9.31)**
6) **Key Derivation Function (KDF)(ANSI X9.63)**

And

The Public Key is derived from the Private Key]

] and specified cryptographic key sizes [**assignment: 256-bits/384-bits**] that meet the following: [**assignment: FIPS 186-3**].

Application notes **ECDSA** 256-bit is applicable for HSM Ver5.11 and RTM System

ECDSA 384-bit is applicable for HSM Ver5.11

6.2.2.3 FCS_CKM.1(C) Cryptographic key generation (Random Number Generator)

Hierarchical 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(C).1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment: Random Number Generator (RNG)**] and specified cryptographic key sizes [**assignment: 256-bits**] that meets the following: [**assignment: none**].

Application notes Key generation for hardware file en-/decryption

Key generation for encrypted drive

RNG passed the test of NIST SP800-22 Rev1a

6.2.2.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical No other components.

Dependencies [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**assignment: overwriting random data after 10 times wrong login password or manual initialize by Administrator**] that meets the following: [**assignment: none**].

Application notes Critical Security Parameter (Data Encryption Key, PKI Keypair, AES Key, RTM Data for Managed Encryptor(Offline Login Number, Encryptor Current Status, Server Authentication for Bulk Enc/Dec))

The CSP will be destructed after 10-times wrong login password or manual initialize by Administrator.

6.2.2.5 FCS_COP.1 (A) Cryptographic operation (Data Encryption/Decryption)

Hierarchical 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(A).1 The TSF shall perform [**assignment: data encryption and decryption**] in accordance with a specified cryptographic algorithm [**assignment: AES**] and cryptographic key sizes [**256-bits**] that meet the following: [**assignment: FIPS PUB 197**].

Application notes a) Data encryption/decryption is sector based encryption/decryption for encrypted drive.

b) Hardware bulk encryption/decryption which applicable for SD series only.

SD302/SD302CR has an on-the-fly AES 256-bit with CBC mode hardware en-/decryption engine.

ST302/ST302B has an on-the-fly AES 256-bit with XTS mode hardware en-/decryption engine.

6.2.2.6 FCS_COP.1 (B) Cryptographic operation (Hashing)

Hierarchical 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(B).1 The TSF shall perform [**assignment: key hashing**] in accordance with a specified cryptographic algorithm [**assignment: SHA-256 and SHA-384]** and cryptographic key sizes [**assignment: none**] that meet the following: [**assignment: FIPS PUB 180-2**].

Application notes SHA256-bits is applicable for HSM Ver5.11 and RTM System

SHA384-bit is applicable for HSM Ver5.11

SHA256-bits will be called during Reset Password of Managed Encryptor to verify signature of Master Encryptor

6.2.2.7 FCS_COP.1 (C) Cryptographic operation (USB Channel Encryption/Decryption)

Hierarchical 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(C).1 The TSF shall perform [**assignment: USB channel encryption and decryption between RTM System (host) and Encryptor**] in accordance with a specified cryptographic algorithm [**assignment: AES**] and cryptographic key sizes [**assignment: 256-bits**] that meet the following: [**assignment: FIPS PUB 197**].

Application notes The USB channel between RTM System (host) and Encryptor is protected by AES session key and P256 ECIES.

6.2.2.8 FCS_COP.1 (D) Cryptographic operation (Digital Signature)

Hierarchical 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(D).1 The TSF shall perform [**assignment: digital signing and digital signature verification**] in accordance with a specified cryptographic algorithm [**assignment: ECDSA**] and cryptographic key sizes [**256-bits/384-bits**] that meet the following: [**assignment: FIPS 186-3**].

Application notes **Only ECDSA** 256-bit is currently applicable for digital signing and signatureverification process in RTM System

ECDSA 384-bit is applicable for future use as this feature is applicable to be implement upon request

a) Verify the Master Encryptor during password reset of Managed Encryptor.

6.2.3 Class FDP: User Data Protection

6.2.3.1 FDP_ACC.1 Subset access control

Hierarchical No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**assignment: Access Control Policy**] on [**assignment:**

a) subjects: all authorized users

b) objects:

- **Token Management**
- **Token Enrollment**
- **Administrator Management**
- **EP Management**
- **Events Log**

- **SQL Connection**

c) operations: all operations on the identified objects by subjects].

Application notes None

6.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical No other components.

Dependencies FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [**assignment:Access Control Policy**] to objects based on the following: [**assignment:**

a) **subject attributes: username, password, fingerprint, permission**
b) **object attributes: as listed in FDP_ACF1.2**].

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

a) **Encryptor**

- **File encryption and decryption**
- **Establish USB Secure channel from Encryptor to RTM System**
- **Modify login password**
- **Reset password-only has the verified digital signature from specific master Encryptor**
- **Disable, enable and destroy-only has the verified shared code that decrypted by Managed Encryptor's private key**

b) **RTMManager (Master Encryptor)**

Administrator able to add & modify permissions in Administrator Management to User which are:

- **(P1) Enrollment/Reset – Only has the permission to enroll Encryptor device and reset password of Managed Encryptor's encrypted drive.**
- **(P2)Disenrollment – Only has the permission to disenrollment the Encryptor device.**
- **(P3)Destroy Token – Only has the permission to destroy the Encryptor device.**
- **(P4)Enable/Disable Token – Only has the permission to enable and disable the Encryptor device.**
- **(P5)Maintain EP – Only has the permission to create,delete and modify Encryption Profile.**
- **(P6)Maintain AdministratorPrivileges– Only has the permission to add newanddeleteuserto the server.**

c) **BCDLogin (Managed Encryptor)**

- **User is enforced do a registration as first time login**

d) **BCDLogin (Non-Managed Encryptor/Master Encryptor)**
- **User is enforced to change password as first time login**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**assignment:none**].

Application notes None

6.2.4 Class FIA: Identification and Authentication

6.2.4.1 FIA_ATD.1 User attribute definition

Hierarchical No other components.

Dependencies No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment:**

a) **Administrator(Master Encryptor)**
- **Username(SQL database account)**
- **Password(encrypted drive and SQL database account)**
- **Permission**
- **Encryptor[refer to Terminology & Acronyms on page 7]**

b) **User(Managed Encryptor)**
- **Username(SQL database account)**
- **Password(encrypted drive and SQL database account)**
- **Encryptor[refer to Terminology & Acronyms on page 7]**
- **Biometric Fingerprint(alternative)**]

C) **User(Non-Managed Encryptor)**
- **Password(encrypted drive)**
- **Encryptor[refer to Terminology & Acronyms on page 7]**
- **Biometric Fingerprint(alternative)**]

Application notes Biometric Identification and authentication for model ST302B only

6.2.4.2 FIA_UID.2 User identification before any action

Hierarchical	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.
Application notes	Applicable for Managed Encryptor

6.2.4.3 FIA_UAU.2 User authentication before any action

Hierarchical	FIA_UAU.1 Timing of authentication
Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Application notes	Applicable to Non-Managed and Managed Encryptor, User authentication is 2 factor authentication(Password/Fingerprint + Encryptor)

6.2.4.4 FIA_UAU.5Multiple authentication mechanisms

Hierarchical No other components.

Dependencies No dependencies.

FIA_UAU.5.1 The TSF shall provide **[assignment:**

a) Password
b) Fingerprint

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **[assignment:**

a) Password to access encrypted drive and cryptographic services
b) Password or Fingerprint to access encrypted drive and cryptographic services
].

Application notes Applicable to Model ST302BNon-Managed and Managed Encryptor.

6.2.4.5 FIA_AFL.1 Authentication failure handling

Hierarchical No other components.

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*selection:*[*assignment:*10 ***pre-configured***]] unsuccessful authentication attempts occur related to [**assignment: login to Encryptor**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***selection:met***], the TSF shall [**assignment: destroy the data and CSP in the Encryptor**].

Application notes None

6.2.4.6 FIA_SOS.1 Verification of secrets

Hierarchical No other components.

Dependencies No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment: at least a number, an alphabets and a symbol of 8-16characters or fingerprint**].

Application notes There is an alternative biometric verification method for model ST302B only.

6.2.5 Class FMT: Security Management

6.2.5.1 FMT_MTD.1 Management of TSF data

Hierarchical 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 [***selection:add, modify, delete, export[assignment: none]***] the [**assignment:**

Table B: FMT_MTD.1

No	Management Functions	Add	Modify	Delete	Export

1	Token Management	No action	modify the Encryptor current status (remote action:[destroy, disable logon,enable logon], reset password)	Delete the enrolled Encryptor data from database	No Action
2	Token Enrollment	Add new Encryptor data to database	No action	No action	No action
3	Administrator Privilege Management	Add new database administrator account with selected privilege permission	No action	Delete administrator account (except:[sa account, current login SQL Database Account])from database	No action
4	EP Management	Add new bulk encryption key(represented by file extension), store the encryption keys to a EP, each of EP can store up to 5 encryption key	Modify bulk encryption key (copy/paste encryption key from another EP) of existing EP	Delete bulk encryption key of existing EP	No action
5	Events Logs	No action	No action	No action	Export searched audit data from database

to [**assignment: Administrator**].

Application None

Note

6.2.5.2 FMT_SMF.1 Specification of Management Functions

Hierarchical No other components.

Dependencies No dependencies.

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

a) Token Management

b) Token Enrollment

c) Administrator Management

d) EP Management

e) Events Log

].

Application Note None

6.2.5.3 FMT_SMR.1 Security roles

Hierarchical No other components.

Dependencies FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**assignment: Administrator,User(Managed Encryptor), User(Non-Managed Encryptor**].

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

Application Note None

6.2.5.4 FMT_MSA.1 Management of security attributes

Hierarchical 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 [**assignment: Access Control Policy**] to restrict the ability to [***selection: change_default, add, modify, delete, enroll[assignment: none]***] the security attributes [**assignment:**

Table C: FMT_MSA.1

Users[Security Attributes]	**Change_default**	**Add**	**Modify**	**Delete**	**Enroll**
Administrator with maintain administrator privilege[Username (SQL Database Account)]	**No action**	**Add new username when create new SQL database account**	**No action**	**Delete username when delete a SQL database account**	**No action**
Administrator[Password (Encrypted Drive)]	**Force change the default password for the first time login**	**No action**	**Change the current password to new password**	**No action**	**No action**
Administrator with maintain administrator privilege [Password(SQL Database Account)	**No action**	**Add new password when create new SQL database account**	**No action**	**Delete password when delete a SQL database account**	**No action**
Administrator with maintain administrator privilege [Permission]	**No action**	**Add permission to SQL database**	**No action**	**Delete permission when delete the SQL database account**	**No action**

		account when generate a new SQL database account			
User (Managed Encryptor)[Username (SQL Database Account]	**No action**	**No action**	**No action**	**No action**	**No action**
User (Managed Encryptor)[Password(SQL Database Account)]	**No action**	**No action**	**No action**	**No action**	**No action**
User (Managed Encryptor)[Password(Encrypted Drive)]	**Force change the default password for the first time login**	**No action**	**Change the current password to new password**	**No action**	**No action**
User (Managed Encryptor)[Biometric Fingerprint(Alternative)]	**No action**	**No action**	**No action**	**Delete the enrolled fingerprints witheithermeet condition of[1. authenticated by enrolled fingerprint** **2. Re-enrolled by Administrator with RTM Manager software]**	**Enroll 4 differences of fingerprints**
User (Non-Managed Encryptor)[Password(Encrypted Drive)]	**Force change the default password**	**No action**	**Change the current passw**	**No action**	**No action**

	for the first time login		**ord to new passw ord**		
User (Non-Managed Encryptor)[Biometric Fingerprint(Alternative)]	**No action**	**No action**	**No action**	**Delete the enrolled fingerprints with either meet condition of[1. provide correct Encrypted Drive login password** **2. authenticated by enrolled fingerprint**	**Enroll 4 differences of fingerprints**

] to [**assignment: Administrator, User(Managed Encryptor), User(Non-Managed Encryptor**].

Application Note None

6.2.5.5 *FMT_MSA.3 Static attribute initialisation*

Hierarchical 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 [**assignment: Access Control Policy**] to provide [***selection: restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**assignment: Administrator, User**] to specify alternative initial values to override the default values when an object or information is created.

Application Note Administrator and user can modify/change their default password. (user is force to change the default password)

6.2.6 Class FPT: Protection of the TSF

6.2.6.1 FPT_TST.1 TSF testing

Hierarchical No other components.

Dependencies No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [***selection: during initial start-up[assignment: none]***] to demonstrate the correct operation of [***selection: [assignment:***

- ***SHA256 KAT***
- ***AES CBC-Encrypt/DecryptKAT***
- ***P256 Key Pair generationKAT***
- ***Data Integrity of Critical Security Parameter]***

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [***selection: [assignment: Critical Security Parameter (Data Encryption Key, PKI Keypair, AES Key, RTM Data for Managed Encryptor(Offline Login Number, Encryptor Current Status, Server Authentication for Bulk Enc/Dec))]***].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [***selection: TSF***].

Application Note The self test will be executed when Encryptor is plugged in to the PC USB Port

User is forced to change the default password when the integrity of CSP is failed to verify.

6.2.6.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical No other components.

Dependencies No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**assignment: list of types of failures in the TSF**

a) **Self Test fail**
b) **Critical Security Parameter corrupted**
c) **Hardware Failure(Physical tampering)]**

Application Note When SelfTest fail, Encryptor's drive [CDFS,encrypted drive] would not be shown on PC

When CSP is corrupted, the user is forced to change default password

In the event of the TOE hardware failure, the data reside in the TOE storage memory (SD) unable to access.

Hardware failure in term of physical tampering are required physical inspection (visual)

6.2.7 Class FTP: Trusted Paths/Channels

6.2.7.1 FTP_TRP.1 Trusted path

Hierarchical No other components.

Dependencies No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***selection: local***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***selection: modification, disclosure[assignment: none]***].

FTP_TRP.1.2 The TSF shall permit [***selection: the TSF***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***selection: before initial user authentication,*** **[assignment: USB channel encryption and decryption between RTM (host) and Encryptor]**].

Application Note None

6.3Security Assurance Requirements

This ST claims compliance to the assurance requirements from the CC EAL2+ assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

Table 8: Security Assurance Requirements for 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.1 Basic flaw remediation
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

7 TOE Summary Specifications

TOE addressed the security functional requirements as following:

7.1 Audit

Audit module in RTM System will generate audit records for selected security events. The security events that will be audited are:

a) AdministratorManagement
b) Encryption Profile
c) Token Enrollment
d) Token Management
e) Client Register

f) Client Logon
g) Client Encrypt
h) Client Decrypt
i) Other

Each audited events will be recorded along with:

a) Owner name(User)

b) Event Type

c) Event Details

d) Timestamp

e) PC Name

f) PC User

g) PC Serial Number

h) IP Address

Reliable date and time of event will be provided by the operating system. This covers FAU_GEN.3.

Audit records are able to be viewed and interpret directly by TOE Administrator. This covers FAU_SAR.1.

TOE Administrator is able to select and search audit records based on:

a) Owner name(User)

b) Event Type

This covers FAU_SAR.3.

7.2 Cryptographic support

1) Encryptor

Key pair generation is generated using ECIES with 256-bits/384-bits key sizes are for:

a) AES session key to establish secure communication between host and Encryptor
b) Destroy, enable or disable Encryptor remotely

SD302/SD302CR has an on-the-fly AES 256-bit with CBC mode hardware en-/decryption engine.

ST302/ST302B has an on-the-fly AES 256-bit with XTS mode hardware en-/decryption engine.

This covers FCS_CKM.1(A).

Key generation for Digital Signature is using ECDSA with 256-bits/384-bits for:

a) Verify the Master Encryptor during password reset of Managed Encryptor

ECDSA 256-bit is applicable for HSM Ver5.11 and RTM System.

ECDSA 384-bit is applicable for HSM Ver5.11.

This covers FCS_CKM.1(B) and FCS_COP.1(D).

Key generation using Random Number Generation (RNG) with 256-bits key sizes are for:

a) Key generation for hardware file en-/decryption
b) Key generation for encrypted drive

This covers FCS_CKM.1(C).

Keys shall be destroyed after 10 wrong login passwords of manual initialization by Administrator. This covers FCS_CKM.4.

Data encryption/decryption using drive sector based encryption/decryption using AES with 256-bits key sizes. It provides data protection and confidentiality of user data by encrypting the data on-the-fly. Critical Security Parameter (CSP) (Data Encryption Key, PKI keypair, Bulk AES key, and RTM data) are stored encrypted in cryptographic module. The data integrity of CSP is verified before used. Hardware file encryption and decryption service for data stream is provided by TOE. The Bulk AES key is generated by the Master Encryptor's RNG. The Encryptor can store up to 5 Bulk AES key.The Managed Encryptor's current status will be encrypted with a self generated AES key before stored into database.SD302/SD302CR has an on-the-fly AES 256-bit with CBC mode hardware en-/decryption engine.ST302/ST302B has an on-the-fly AES 256-bit with XTS mode hardware en-/decryption engine.

This covers FCS_COP.1(A).

Key hashing is using SHA-2 series with key size 256-bits and 384-bits. This covers FCS_COP.1(B).

2) RTM System

USB communication channel between RTM System and Encryptoris encrypted. Communication channel encryption/decryption is using AES with 256-bits key size.The USB vendor specific command is protected by the AES session key. This covers FCS_COP.1(C).

7.3 User Data Protection

Access Control Policy covers all authorized users access to perform all operations on the objects as following:

- Token Management
- Token Enrollment
- Administrator Management
- EP Management
- Events Log
- SQL Connection

a) Encryptor

User who successfully authenticated using username and password (with or without fingerprint) is able to perform:

- File encryption and decryption
- Establish USB secure channel between Encryptor and RTM System
- Modify login password
- Reset password-only has the verified digital signature from specific master Encryptor
- Disable, enable and destroy-only has the verified shared code that decrypted by Managed Encryptor's private key

b) RTMManager (Master Encryptor)

Administrator is able to add & modify permissions in Database Login User to User which are:

- (P1) Enrollment/Reset – Only has the permission to enroll Encryptor device and reset password of Managed Encryptor's encrypted drive.
- (P2)Disenrollment – Only has the permission to disenrollment the Encryptor device.
- (P3)Destroy Token – Only has the permission to destroy the Encryptor device.
- (P4)Enable/Disable Token – Only has the permission to enable and disable the Encryptor device.
- (P5)Maintain EP – Only has the permission to create,delete and modify Encryption Profile.
- (P6)MaintainAdministratorPrivileges– Only has the permission to add new, delete user and alter existing user permission to the server.

c) BCDLogin (Managed Encryptor)

User is enforcedtodo a registration as first time login.

d) BCDLogin (Non-Managed Encryptor/Master Encryptor)

User is enforced to change password as first time login.

This covers FDP_ACC.1 and FDP_ACF.1.

7.4 Identification and Authentication

1) Encryptor:
   - User must enter the valid password to access the encrypted drive and cryptographic services.This covers FIA_ATD.1, FIA_UID.2 and FIA_UAU.2.
   - The password must be 8 to 16 characters in length and must contain at least a number, an alphabet and a symbol.For Model ST302B, an alternative fingerprint authentication can be used to access the encrypted drive and cryptographic services. This covers FIA_SOS.1 and FIA_UAU.5.
   - Only 10 unsuccessful attempts allowed to login to Encryptor before the data and CSP in the Encryptor is destroyed.This covers FIA_AFL.1.

2) RTM System
   - The user must provide valid username and password for connecting to SQL server.This covers FIA_ATD.1, FIA_UID.2 and FIA_UAU.2.

7.5 Management

The TOE has 2 roles defined in the Access Control Policy. The roles are User and Administrator. Administrator role is able to:

- Change default password for first time login.
- Add new username, new password, and permission when generate new SQL database account.
- Modify the current password.
- Delete username, password, and permission when delete the SQL Database account.

User role is able to;

- Change default password for first time login.
- Modify the current password.
- Delete the enrolled fingerprint.
- Enrol 4 different fingerprints.

This covers FMT_SMR.1 and FMT_MSA.1.

RTM System for Managed Encryptor is to control and monitor the Managed Encryptor locally and remotely:

- Manage offline login number
- Manage Encryption Profile
- Monitor Encryptor's activities
- Reset Encryptor's password
- Remote enable/disable/destroy Encryptor

Administrator is able to manage from RTMManager:

- Token Management
    - Modify the Encryptor current status.
    - Delete the enrolled Encryptor from database.
- Token Enrollment
    - Add new Encryptor data to database.
- Administrator Management
    - Add new database administrator account.
    - Delete administrator account.
- EP Management
    - Add new bulk encryption key.
    - Modify bulk encryption key.
    - Delete bulk encryption key.
- Events Log
    - Export audit data.

This covers FMT_MTD.1 and FMT_SMF.1.

The Access Control Policy implements restrictive default values at the initial TOE start up or TOE initial execution. There will be a default Administrator account with default password for first time access by Administrator. No other user account is allowed to access the TOE for first time use. Administrator and User are able to change the initial values of password to a new password after successfully authenticate in TOE. This covers FMT_MSA.3.

7.6 Testing

During the start-up of Encryptor, the following self tests are conducted;

- SHA256 KAT
- AES CBC-Encrypt/Decrypt KAT
- P256 PKI Key Pair Generation KAT
- Data integrity of Critical Security Parameter

The integrity of Critical Security Parameter (Data Encryption Key, PKI Keypair, AES Key, RTM Data for Managed Encryptor(Offline Login Number, Encryptor Current Status, Server Authentication for Bulk Encryption/Decryption) is checked during self test.

Critical security parameter are encrypted and stored in cryptographic module. It is replicated in two memory spaces in the cryptographic module (Bank 1 and Bank 2). CRC checking on integrity of each bank is executed. When the TOE is plugged in to the PC USB Port, CSP Bank 1 data integrity checking is executed. If CRC checking success, proceed with running the TOE. Otherwise, CSP Bank 2 integrity is checked. If CSP Bank 2 data integrity success, CSP of Bank 2 is used. Otherwise, CSP of both banks are initialized.

The CSP is consistent when replicated between parts of the TOE and protected from modification.

The self test will be executed when Encryptor is plugged into the PC USB Port. User is forced to change the default password when the integrity of CSP is failed to verify. This covers FPT_TST.1, FIA_UAU.2 and FIA_UID.2.

Encryptor will preserve secure state if Self Test fail and Critical Security Parameter corrupted. When Self Test fail, Encryptor’s drive [CDFS,encrypted drive] would not be shown on PC. When CSP is corrupted, the user is forced to change default password.In the event of the TOE hardware failure, the data reside in the TOE storage memory (SD) unable to access.This covers FPT_FLS.1.

7.7 Trusted path

USB communication session between RTM System and Encryptor is encrypted. Communication session is protected by P256 ECIES and AES-256 session key. This covers FTP_TRP.1.

8 Rationale

8.1 Protection Profile Conformance Claim Rationale

ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

8.2 Security Objectives Rationale

This section explains how threat, assumptions and OSP are related to each other. The following tables show threat, assumptions and organizational policy being mapped to security objectives.

8.2.1 Rationale for Security Objectives Mapped to Threats

Table 9: Rationale for Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.DATA	O.DATA	The security objective counters threat because it concerns with the prevention of unauthorised access to the TOE or security functions without being granted permission. It also concerns on unauthorized access event that is not detected by the TOE.
T.AUDIT	O.AUDIT	The security objectives counters threat because it concerns with TOE recording the security events performed by authorized or unauthorized person.
T.EAVESDROP	O.EAVESDROP	The security objective counters threat because TOE shall prevent unauthorized person to eavesdrop and interpret the communication between Encryptor- RTM (Host) and RTM-SQL Server.
T.BRUTEFORCE	O.BRUTEFORCE	The security objective counters threat because TOE shall prevent unauthorized person to brute force the TOE authentication to obtain unauthorized access to

		TOE.
T.SESSIONHIJACK	OE. IDLE	The security objective counters threat because TOE environment shall prevent unauthorized person using user's idle session to obtain unauthorized access to TOE.
T.CONFIG	O.CONFIG	The security objective counters threat because TOE shall prevent unauthorized person to read, modify, or destroy TOE configuration data. Only Administrator is authorized to read and modify the TOE configuration data.
T.INTEGRITY	O.INTEGRITY	The security objective counters threat because TOE shall prevent unauthorized person to compromise the confidentiality of User data and TSF data in transit and/or in the Encryptor. The TOE may be compromised in the aspects of logical (data tampering – by renaming the filename or changing some file in the memory card SD) and physically (tampering with the circuit board or changing the SD card), in which, changing the integrity of the TOE.

8.2.2 Rationale for Security Objectives Mapped to OSP

Table 10: Rationale for Security Objectives Mapped to OSP

OSP	Security Objectives	Rationale
P.ROLE	OE.ADMIN	The security objective counters OSP because the TOE Administrator is assigned by organization and trusted to be non-hostile and will follow guidance documentation in handling the TOE.

8.2.3 Rationale for Security Objectives Mapped to Assumptions

Table 11: Rationale for Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.PHY	OE.PHY	The security objective counters assumption because TOE and its environment shall be physically secured and managed by authorized TOE Administrator.
A.ADMIN	OE.ADMIN	The security objective counters assumption because authorized TOE Administrator shall be non-hostile, assigned by organization and follows guidance documentation accordingly; however,

		TOE Administrators is not free from human error and mistakes.
A.BACKUP	OE.BACKUP	The security objective counters assumption because TOE environment shall provide data backups on user data and TOE data such as encryption profile and audit logs.Data backup for Managed Encryptor is performed by admin. Data backup for Non-Managed Encryptor is performed by user.
A.STORAGE	OE.STORAGE	The security objective counters assumption because TOE environment shall provide sufficient storage for TOE operational environments.
A.TIMESTAMP	OE.TIMESTAMP	The security objective counters assumption because TOE environment shall provide reliable time stamps to enable the TOE to timestamp audit records.
A.IDLE	OE.IDLE	The security objective counters assumption because TOE environment shall be protected during idles with password protection or other secure mechanism.
A.NETSECURE	OE.NETSECURE	The security objective counters assumption because TOE environment shall provide secure channel for network communication between Host and Server.

8.3 Extended Security Functional Requirement Rationale

Refer Section Extended Security Functional Requirement (SFR) for the rationale.

8.4 Extended Security Assurance Requirement Rationale

Not applicable since there is no extended Security Assurance Requirement declared in ST.

8.5 Security Functional Requirements Rationale

This section provides the rationale of using SFRs to meet the security objectives for the TOE and justify the SFRs dependencies that have been satisfied or not satisfied.

8.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Table 12: Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.DATA	FDP_ACC.1	This SFR specify that TOE is enforcing Access Control Policy on all entity who tries to access the TOE. Only authorised User and Administrator able to access, interpret or modify the User data or TOE configurations. It traces back to this objective.
	FDP_ACF.1	This SFR specify that each user will be given access and functionalities based on certain user attributes. User or Administrator is able to access TOE based on several controls. It traces back to this objective.
	FIA_UAU.2	This SFR specify that User or Administrator must be successfully authenticated or provide their correct username before being allowed to do any action to TOE or User data. Only selftest is allowed before user is identified. It traces back to this objective.
	FIA_UID.2	This SFR specify that User or Administrator must be successfully identified or provide their correct password before being allowed to do any action to TOE or User data. Only self test is allowed before user is identified. It traces back to this objective.
	FIA_ATD.1	This SFR specify that User or Administrator shall have several security attributes tied to each user account. The security attributes are username, password/fingerprint and permission. These security attributes will determine the TOE access for each user to perform the encryption and decryption of User data. It traces back to this objective.
	FIA_SOS.1	This SFR specify that password criteria and fingerprint that user needs to provide to be authenticated to TOE. It traces back to this objective.
	FCS_CKM.1(A)	This SFR specify that the key pair is generated using ECIES with 256-bits/384-bits key sizes. The key will be used in AES session communication between RTM (Host) and Encryptor. It traces back to this objective.
	FCS_CKM.1(B)	This SFR specify that key generation for digital signature is generated using ECDSA with 256-bits/384-bits key sizes. The key will be used for verification of Master

		Encryptorduring password reset of Managed Encryptor and firmware update. It traces back to this objective.
	FCS_CKM.1(C)	This SFR specify that key generation using RNG with 256-bits key size. The key will be used for drive encryption/decryption and file encryption/decryption. It traces back to this objective.
	FCS_CKM.4	This SFR specify that cryptographic keys will be destroyed after 10 wrong login passwords from unauthorized or authorized person or manual initialize by Administrator. It traces back to this objective.
	FCS_COP.1(A)	This SFR specify that drive/file encryption/decryption using AES with 256-bits key size. Only authorized User can interpret the data for his or her usage. It traces back to this objective.
	FCS_COP.1(B)	This SFR specify that keys are hashed using SHA-2 series with 256-bits and 384-bits key sizes. It traces back to this objective.
	FCS_COP.1(C)	This SFR specify that USB channel encryption and decryption between RTM System (host) and Encryptor is using AES with 256-bits key size. It traces back to this objective.
	FCS_COP.1(D)	This SFR specify that digital signing and digital signature verification are using ECDSA with 256-bits/384-bits key size that meets FIPS 186-3. It traces back to this objective.
O.EAVESDROP	FTP_TRP.1	This SFR specify that secure communication between USB channel between RTM (host) and Encryptor. It traces back to this objective.
	FCS_COP.1(C)	This SFR specify that USB channel encryption and decryption between RTM System (host) and Encryptor is using AES with 256-bits key size. It traces back to this objective.
O.AUDIT	FAU_GEN.3	This SFR specify that selected security events will be audited and recorded. It traces back to this objective.
	FAU_SAR.1	This SFR specify that all audit records are able to be viewed and interpret directly by TOE Administrator. It traces back to this objective.
	FAU_SAR.3	This SFR specify that audit records able to be selected and selected by Administrator based on audit records information. It traces back to this objective.

O.BRUTEFORCE	FIA_AFL.1	This SFR specify that TOE provides mechanism to detect and temporarily stop unsuccessful authentication attempt to TOE. When the pre-configured 10 unsuccessful authentication attempts occur at TOE, the TOE shall destroy the data and CSP in Encryptor. This mechanism mitigates brute force attack. It traces back to this objective.
	FIA_SOS.1	This SFR specify that password criteria and fingerprint that user needs to provide to be authenticated to TOE. It traces back to this objective.
	FIA_UAU.5	This SFR specify that TOE provides multiple authentication mechanism using password and fingerprint. This mechanism mitigates brute force attack. It traces back to this objective.
O.CONFIG	FMT_MTD.1	This SFR specify Administrator is able to manage user and TOE configurations. It traces back to this objective.
	FMT_SMF.1	This SFR specify Administrator is able to manage user and TOE configurations. Only Administrator can change default, modify, delete and add/enrol user and TOE configuration data. It traces back to this objective.
	FMT_SMR.1	This SFR specify 2 roles defined in the Access Control Policy. The roles are User and Administrator. User role is prevented from accessing the Administrator's function and only able to manage the User data resides in the storage. It traces back to this objective.
	FMT_MSA.1	This SFR specify that only Administrator role is able to change default, modify, delete and add/enrol user or TOE configurations at TOE. It traces back to this objective.
	FMT_MSA.3	This SFR specify Access Control Policy implements restrictive default values at the initial TOE start up or TOE initial execution. There will be a default Administrator account with default password for first time access by Administrator. Administrator should then change the initial values of password to a new password after successfully authenticate as Administrator. User can also change their default password after first time login. It traces back to this objective.
O.INTEGRITY	FPT_FLS.1	This SFR specify that TOE preserve a secure state when self test fail, CSP is corrupted or hardware failure. It traces back to this objective.
	FPT_TST.1	This SFR specify that TOE will run self tests to ensure operation of TOE is not being tampered and

		confidentiality of data is preserve. It traces back to this objective.

8.5.2 SFR Dependency Rationale

The following table provides a demonstration that all SFRs dependencies included in the ST have been satisfied or justification is provided for not meeting the dependencies.

Table 13: SFR Dependencies

SFR	Dependency	Dependency Met?	Justification
FAU_GEN.3	FPT_STM.1	No	FPT_STM.1 Reliable timestamp is provided by the TOE environment (Server operating system) as specified in A.TIMESTAMP. The TOE environment will provide reliable time stamps to enable the TOE to timestamp audit records.
FAU_SAR.1	FAU_GEN.1	No	FAU_GEN.1 is satisfied by using FAU_GEN.3. Refer Section 5 for more details.
FAU_SAR.3	FAU_SAR.1	Yes	-
FCS_CKM.1 (A)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Yes. FCS_COP.1(A) and FCS_CKM.4	-
FCS_CKM.1 (B)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Yes. FCS_COP.1(D) and FCS_CKM.4	-
FCS_CKM.1 (C)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Yes. FCS_COP.1(C) and FCS_CKM.4	-
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes	-
FCS_COP.1 (A)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes	-

	FCS_CKM.4		
FCS_COP.1 (B)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes No	Since the operation for FCS_COP.1 (B) need keys to be hashed, so, key generations are required first for keys to exist FCS_COP.1(B) is used for SHA-2 algorithm. SHA-2 is a keyless operation. So there is no need to manage key operations like generate (FCS_CKM.1), destruct (FCS_CKM.4), or import (FDP_ITC.1 or FDP_ITC.2).
FCS_COP.1 (C)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes	-
FCS_COP.1 (D)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes	-
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes	-
FIA_ATD.1	-	-	-
FIA_UID.2	-	-	-
FIA_UAU.2	FIA_UID.2	Yes	-
FIA_AFL.1	FIA_UAU.2	Yes	-
FIA_SOS.1	-	-	-
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_SMF.1	-	-	-
FMT_SMR.1	FIA_UID.2	Yes	-

FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes	-
FPT_TST.1	-	-	-
FPT_FLS.1	-	-	-
FTP_TRP.1	-	-	-

8.6 Security Assurance Requirements Rationale

EAL2 was chosen to provide a basic assurance. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the TOE will have undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of basic.