CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

C054 Certification Report

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

File name: ISCB-5-RPT-C054-CR-v1
Version: v1
Date of document: 11 March 2015
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme®

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C054 Certification Report

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

11 March 2015
ISCB Department

CyberSecurity Malaysia
Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Copyright Statement

Registered office:
Level 5, Sapura@Mines
No 7, Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated **19 March 2015**, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	5 March 2015	All	Initial draft
v1	11 March 2015	vii-viii, 1, 2, 8, 10, 11, 12, 19 and 20	Update scope, architectural design, adding pictures in TOE module and explanation on SAMM.

Executive Summary

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 (Ver1.00) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation.

The TOE is consists of two categories as follows:

a) Hardware: Biocryptodsik Encryptor **(Not SAMM Accredited)**;
b) Software: Remote Token Management System (RTM System).

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

Meanwhile for the Remote Token Management System (RTM System) is a combination of two main applications which are RTM Manager and BCDLogin. RTM Manager is used to remotely manage and control the Biocryptodisk Encryptor while BCDLogin is used to perform login/logout; change password and hardware file en–decryption.

Disclaimer: Tests marked **"Not SAMM Accredited"** in this report is not included in the SAMM Accreditation Schedule of MySEF laboratory.

Note: **SAMM** is Malaysian Laboratory Accreditation Scheme.

The TOE scope of evaluation covers various major security functions described as below:

a) **Audit** – The TOE (Biocryptodisk Encryptor) is designed to minimize threats to an organization by providing secure management and reporting capabilities. The TOE provides Audit module in RTM System which will generate audit records for the selected security events such as administrator management, encryption profile, token enrolment, token management, client register, client logon, client encrypt, client decrypt and others. Each audited events will be recorded along with owner's name (user), event type, event details, timestamp, PC Name, PC user, PC serial number and IP address.

b) **Cryptographic Support** – TOE has cryptographic support module that can generate the keypair generation by using ECIES with 256–bits/384–bits key sizes; generate key for Digital Signature by using ECDSA with 256–bits/384–bits, and generate key using Random Number Generation (RNG) with 256–bits key sizes. Besides key generation, it also have USB communication channel between RTM system and Encryptor is encrypted. Communication channel encryption/decryption is using AES with 256-bits key size and the USB vendor specific command is protected by the AES session key.

c) **User Data Protection** - TOE has an access control policy that covers all authorized users access to perform all operations such as Token Management, Token Enrolment, Administrator Management, etc.
d) **Identification and Authentication** - TOE allows an authorized user to access the encrypted drive and cryptographic services; and access RTM System to connect with SQL server by entering the valid username and password.
e) **Management** -TOE has two roles defined in the Access Control Policy which is administrator and user. 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.
f) **Testing** - TOE enforces Testing module for self-tests during the start-up of Encryptor and preserve secure state on several failure events in order to maintain the integrity of the data and protect from any modification.
g) **Trusted Path** - TOE enforces USB communication session between RTM System and Encryptor under Trusted Path module which is protected by P256 ECIES and AES-256 session key.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies the following:

i) Assumptions made during the evaluation,
ii) The intended environment for Biocryptodisk Encryptor Model and Remote Token Management System platform,
iii) The security requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements.

Prospective consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of TOE platform to the Common Criteria (CC) evaluation assurance level EAL2+ Augmented with ALC_FLR.1. The report confirms that the product has met the target assurance level of EAL2+ Augmented with ALC_FLR.1 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification

(MyCC) Scheme (Ref [4]). The evaluation was performed by CyberSecurity Malaysia MySEF and was completed on 27 February 2015.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL2+ Augmented with ALC_FLR.1. The product Certificate, Certification Report and Security Target will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Biocryptodisk Encryptor Model and Remote Token Management System meet their requirements. It is recommended that a potential user of TOE to refer to the Security Target (Ref [6]) and this Certification report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

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

3 Biocryptodisk Encryptor is a USB portable hardware cryptographic module. It has an on-the-fly AES 256-bit hardware encryption/decryption engine on board which have the capability of encrypting/decrypting files from any computer detected storage such as USB external drive, network attached drive and virtual drives. It is truly driveless and zero footprint in which TOE does not require any client software to be installed or configured on a user's system. Moreover, it also have an on board encrypted storage. The data stored in ST302 series is in AES 256 bit XTS mode; whereas the data stored in SD302 series is in AES 256 bit CBC mode.

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

5 The details of the modules can be referred in section 1.3 of the ST (Ref [6]).

6 The major security functions that implemented by the TOE are as below

a) **Audit** – The TOE (Biocryptodisk Encryptor) is designed to minimize threats to an organization by providing secure management and reporting capabilities. The TOE provides Audit module in RTM System which will generate audit records for the selected security events such as administrator management, encryption profile, token enrolment, token management, client register, client logon, client encrypt, client decrypt and others. Each audited events will be recorded along with owner's name (user), event type, event details, timestamp, PC Name, PC user, PC serial number and IP address. Audit record is selected and searched based on Qwner name (User) and Event Type.

b) **Cryptographic Support** – TOE has cryptographic support module that can generate the keypair generation by using ECIES with 256-bits/384-bits key sizes; generate key for Digital Signature by using ECDSA with 256-bits/384-bits, and generate key using Random Number Generation (RNG) with 256-bits key sizes. Besides key generation, it also have USB communication channel between RTM system and Encryptor which is encrypted. Communication channel encryption/decryption is using AES with 256-bits key size and the USB vendor specific command is protected by the AES session key.

c) **User Data Protection** – TOE has an access control policy that covers all authorized users access to perform all operations on Token Management, Token Enrolment, Administrator Management, EP Management, Events Log and SQL Connection.

d) **Identification and Authentication** – TOE allows an authorized user to access the encrypted drive and cryptographic services; and access RTM System to connect with SQL server by entering the valid username and password.

e) **Management** -TOE has two roles defined in the Access Control Policy which is administrator and user. 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.

f) **Testing** – TOE enforces Testing module for self-tests during the start-up of Encryptor and preserve secure state on several failure events in order to maintain the integrity of the Critical Security Parameter (CSP) data and protect from any modification.

g) **Trusted Path** – TOE enforces USB communication session between RTM System and Encryptor under Trusted Path module which is protected by P256 ECIES and AES-256 session key.

7 Biocryptodisk Encryptor consists of 2 major Series namely SD Series and ST Series. SD series has two models which are SD302 and SD302CR while ST series has ST302 and ST302B. It also has categorized into three types which are Master Encryptor, Non-Managed Encryptor and Managed Encryptor. Noted that only SD series can be configured as Master Encryptor. Biocryptodisk Encryptor is performed as two factor authentication (password + encryptor) and splitted into 2 partitions, which are CDFS drive and encrypted drive. The size of CDFS drive is pre-defined to 32MB, while the size of the encrypted drive is based on the series of Biocryptodisk Encryptor.

8 The server side of the TOE is configured in Windows Server 2008 R2 and Microsoft SQL Server 2012 Express Version. The Microsoft SQL Server 2012 Express Version must be setup with SSL encryption.

1.2 TOE Identification

9 The details of the TOE are identified in Table 1 below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C054
TOE Name	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
TOE Version	Biocryptodisk Encryptor Model SD302(Ver5.11-Biocryptodisk Encryptor Model SD302(Ver5.11-3.03), SD302CR(Ver5.11-5.03), ST302(Ver5.11-1.00), and ST302B0.7(Ver5.11-1.00) with Remote Token Management System v1.00
Security Target 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
Security Target Version	0.7
Security Target Date	29 December 2014
Assurance Level	Evaluation Assurance Level 2+ (EAL2+) Augmented with ALC_FLR.1
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL2+ Augmented with ALC_FLR.1

Sponsor and Developer	Biocryptodisk Sdn Bhd 27B, Jalan Sutera Tanjung 8/3, Taman Sutera Utama, 81300 Skudai, Johor MALAYSIA
Evaluation Facility	Cybersecurity Malaysia MySEF

1.3 Security Policy

10 The organisational security policy is imposed by an organization to secure the TOE and its environment where only authorized person has been assigned by the organization to manage the Master Encryptor.

1.4 TOE Architecture

11 TOE Architectural Design has been describes into subsystems in the below table:

Table 2: TOE Architectural Design

TOE Design	Description
Identification and Authentication Subsystem	TOE can be categorized into 3 kinds of mechanism • **TOE Administrator (Master Encryptor + BCDLogin Application + RTMManager Application)** Master Encryptor has to access the encrypted drive, by providing correct password with using provided BCDLogin application. After logged in to encrypted drive, by using RTMManager application, TOE Administrator able connect to SQL Server Database by providing correct hostname, port number SQL account username and SQL account password. If the combination of SQL account username and password is true, this subsystem will pass the result to User Data Protection Subsystem to obtain the role of administrator. Once role is obtained, TOE Administrator will be redirected to RTMManager administrator interface. • **TOE User(Managed Encryptor + BCDLogin application)** Managed Encryptor has to provide correct password or Biometric Fingerprint (alternative) to unlock the encrypted drive. TOE User is enforced do a registration as first time login by providing owner name and password. Password is used to unlock encrypted drive while owner name will

	be saved as record in SQL Server Database. By using the pre-defined SQL account username and password, Managed Encryptor able connects to SQL Server Database. If the combination of SQL account username and password is true, this subsystem will pass the result to User Data Protection Subsystem to obtain the role of user. Once role is obtained, TOE User will be redirected to BCDLogin user interface. • **TOE User(Non-Managed Encryptor + BCDLogin application)** Non-Managed Encryptor has to provide correct password or Biometric Fingerprint (alternative) to unlock the encrypted drive. If the password is true, this subsystem will pass the result to User Data Protection Subsystem to obtain the role of user. Once role is obtained, TOE User will be redirected to BCDLogin user interface. TOE provides mechanism to detect and temporarily stop unsuccessful authentication attempt to TOE. When the pre-configured 10 unsuccessful authentication attempts occur at BCDLogin application of TOE, data for the user account will be erased/destroyed and TOE will be terminated. User need to inform Administrator to reactivate the TOE.
User Data Protection Subsystem	The User Data Protection Subsystem has the capabilities of enforcing Access Control Policy on all entity who tries to access the TOE. Only authorised User or Administrator able to access, interpret or modify the User data or TOE configurations. Administrator and Users (for non-managed SD302 series only) are able to generate key for himself/herself which will be stored in Encryption Profile. Each user will be given access and functionalities based on certain user attributes. User or Administrator is able to access TOE based on following controls: • If user is assigned with Administrator role and authenticated successfully, the user can access the Identification & Authentication, Security Management, Cryptographic Protection, Access Control and Audit Log Subsystems; • If user is assigned with User role and authenticated

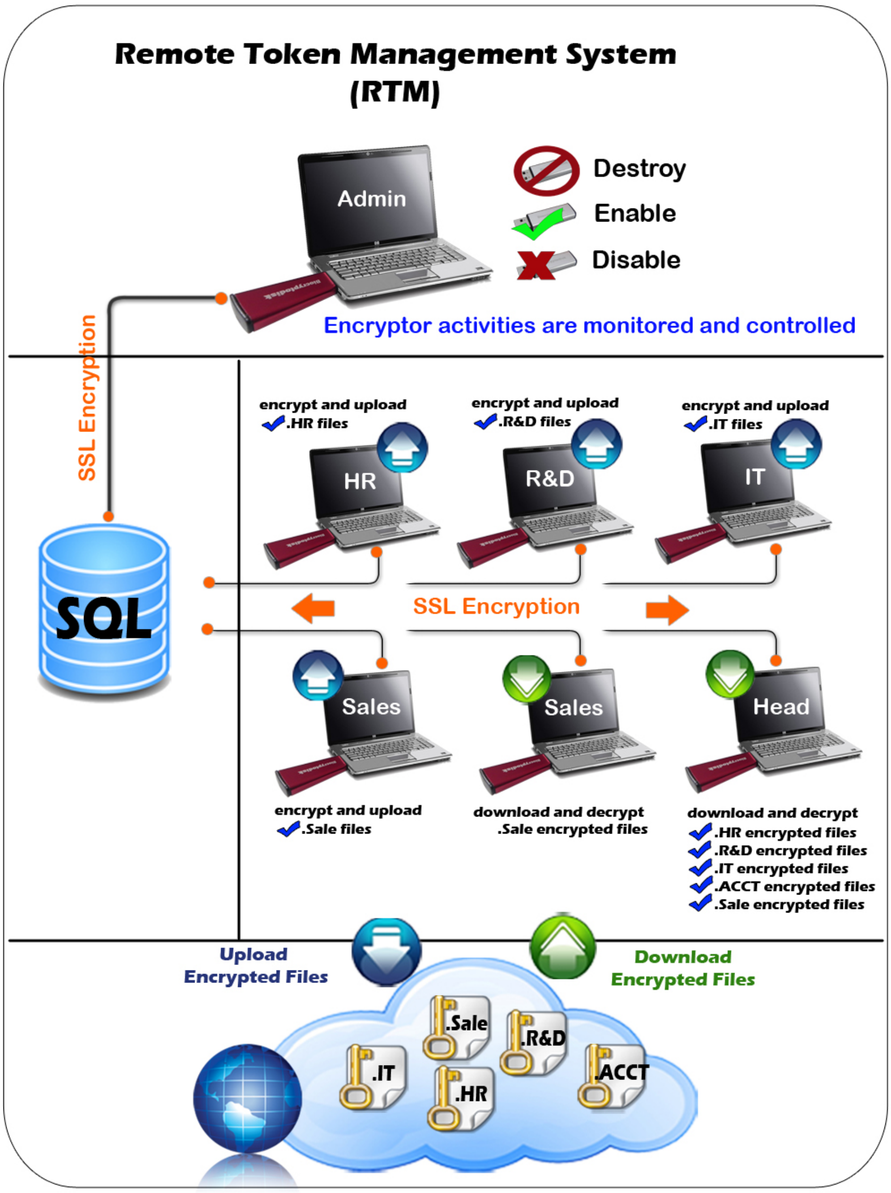
	successfully, the user can encrypt and decrypt data using the PKI key in Cryptographic Protection Subsystem; • If user is assigned with User role and authenticated successfully, the user can access modify password function in Security Management Subsystem. • User that is allowed to access Identification & Authentication Subsystem is successfully authenticated.
Cryptographic Protection Subsystem	Cryptographic Protection Subsystem implements key generation, data encryption/decryption and key hashing functions. Key generation for hardware bulk encrypt/decrypt and encrypted drive are based on random number generator (RNG) 256-bit of key sizes. Key hashing is using SHA-2 series(SHA-256, SHA-384). The key pair which use for AES session key to establish secure communication between host and Encryptor and destroy, enable or disable Encryptor remotely, is generated by ECIES with 256-bits/384-bits key sizes.Key generation for Digital Signature is using ECDSA with 256-bits/384-bits and use to verify the Master Encryptor during password reset of Managed Encryptor. Data encryption/decryption using drive sector based encryption/decryption is using AES with 256-bits key sizes. It provides data protection and confidentiality of user data by encrypting the data on the fly. SD Series has an on-the-fly AES 256-bit with CBC mode hardware en-/decryption engine, ST Series has an on-the-fly AES 256-bit with XTS mode hardware en-/decryption engine. 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 in Encryption Profile (EP). The Managed Encryptor's current status will be encrypted with a self-generated AES key before stored into database. Only an Administrator and non-managed SD302 series User can self-create/manage the key for Encryption Profile. The other Encryptor model's user will have to get the Encryption Profile from Administrator during enrolment process for

	encrypt/decrypt process. The key destruction is initialized by an Administrator manually or after 10 time's wrong login password.
Security Management Subsystem	Security Management Subsystem defined 2 roles in the Access Control Policy. The roles are User and Administrator. Administrator role is able to change default, modify, destroy and enrol user or TOE configurations. User role is able to manage bulk encrypt/decrypt user data, change his/her own password. TOE functionalities can be managed through TOE interface by TOE Administrator. Administrator is able to manage user and TOE configurations on RTM Manager such as: a) Token Enrolment b) Token Management c) Events Log d) Encryption Profile (EP) Management e) SQL Connection f) Administrator Management The Access Control Policy implements restrictive default values at the initial TOE start up or TOE initial execution. There will be a default password for first time access to encrypted drive by Administrator and User. Administrator and User are able to change the initial values of password to a new password after successfully authenticated in TOE.
Audit Log Subsystem	The Audit Log Subsystem will generate audit records for selected security events. The security events that will be audited are Administration Management, Encryption Profile, Token Enrolment, Token Management, Client Register, Client Logon, Client Encrypt, and Client Decrypt. Each audited events will be recorded along with Owner name, Event Type, Event Details, Timestamp, PC Name, PC User, PC Serial Number, and IP Address. Reliable date and time of event will be provided by the operating system. Audit records are able to be viewed and interpret directly by TOE Administrator. All audit records cannot be edited and deleted. TOE Administrator is able to search log records based on Owner name and Event Type which will highlight the records

	that contain the key string. By default, the audit records are sorted by date.
Testing Subsystem	During the start-up of Encryptor, a self-test is conducted using SHA256 KAT, AES CBC-Encrypt/Decrypt KAT, and P256 PKI Key Pair Generation KAT. 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 (Bank1 and Bank2). When the TOE is plugged into 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, 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 before user authentication. Encryptor will preserve secure state if Self-Test fail and Critical Security Parameter corrupted.
Trusted Path Subsystem	USB communication session between RTM System and Encryptor is encrypted. Communication session is protected by P256 ECIES and AES-256 session key.

12 The following figure 1 shows the subsystems that constructs the TOE*:*

Figure 1: Subsystem that constructs the TOE



13 The following Table 3 describes the capability of the TOE:

Table 3: The capability of the TOE

TOE Module	Description
Master Encryptor	• Encrypted drive with password protected

(SD302, SD302CR) 	• 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
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

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
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

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

1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communication security in accordance with administrator guidance that is supplied with the product.

15 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The TOE has divided into two categories which is Biocryptodisk Encryptor (represent for hardware) and Remote Token Management System (represent for software). The Biocryptodisk Encryptor is a USB portable hardware cryptographic module which has an on-the-fly AES 256-bit hardware encryption/decryption engine on board which have capability of encrypting/decrypting files from any computer detected storage while 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 TOE operates depending on the medium storage, which contains the TOE files such as installer executable and supporting hardware required by the TOE to operate. Other components of TOE which includes the hardware appliance, operating system, medium storage specified in Section 1.7.1 of the Security Target (Ref [6]) are not part of TOE scope.

16 Potential consumers of the TOE are advised that some functions and services of the overall product may not have been evaluated as part of the evaluation activity. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

17 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the Biocryptodisk Encryptor and Remote Token Management System platform as defined in subsequent sections and in the Security Target (Ref [6]).

1.6.1 Usage assumptions

18 The following specific conditions are required to ensure the security of the TOE in term of TOE Usage:

a) The TOE administrator is not careless, wilfully negligent or hostile and complies with administrator documentation.

b) The authorised user will keeps their passwords secret and not write them down or disclose them to any other system or user.

1.6.2 Environment assumptions

19 The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed:

a) The TOE and its environment are physically secured and managed by authorized TOE Administrator.

b) Authorized TOE Administrator is non–hostile, assigned by organisation and follows guidance documentation accordingly; however, TOE Administrator is not free from human error and mistakes.

c) The TOE environment will provide data backups on user data and TOE data such as audit logs.

d) The TOE environment will provide sufficient storage for TOE operational environments.

e) The TOE environment will provide reliable time stamps to enable the TOE to timestamp audit records

f) The TOE environment must be protected during idle.

g) The TOE environment will provide secure channel for network communication between Host and Server.

1.7 Evaluated Configuration

20 This section describes the configurations of the TOE that are included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative and operational user guidance (Ref [25]).

1.8 Delivery Procedures

21 Basically there are several methods applied in delivering the Biocryptodisk Encryptor to Biocryptodisk respected customer. Firstly, the customer will purchase the product and complete the payment. Once payment is confirmed and legal documentations have been completed, Biocryptodisk personnel can proceed with preparing and delivering the product.

22 Then, Biocryptodisk personnel will make the necessary preparation by preparing manual in softcopy such as Admin Manual, Managed Encryptor Manual SD302/SD302CR, Non-Managed Encryptor Manual Model SD302/SD302CR, Managed Encryptor Manual ST302/ST302B, Non-Managed Encryptor Manual Model ST302/ST302CR and; SSL and Server Configuration Manual. Biocryptodisk Encryptor appliance will be labelled with Biocryptodisk identification and serial number; and apply security tape at Biocryptodisk Encryptor casing in order to avoid the product being tampered during distribution to customer. The product will be ship to customer by Courier Services.

23 Lastly, once customer has received the package of product; they are required to acknowledge received items receipt at the courier person.

1.9 Documentation

24 To ensure continued secure usage of the product, it is important that the TOE is used in accordance with the guidance documentation.

25 The following guidance documentation is used by the developer's authorised personnel and administrator as guidance to ensure secure installation and operation of the product:

a) Admin Manual Rev1.0

b) SSL and Server Configuration Manual Rev1.1

c) Managed Encrytor Manual Model SD302_SD302CR Rev1.0

d) Managed Encryptor Manual Model ST302_ST302B Rev1.0

e) Non-Managed Encryptor Manual Model SD302_SD302CR Rev1.0

f) Non-Managed Encryptor Manual Model ST302_ST302B Rev1.0

2 Evaluation

26 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2+ (EAL2+) Augmented ALC_FLR.1. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

27 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

28 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

29 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of TOE during distribution to the consumer.

2.1.2 Development

30 The evaluators analysed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

31 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

32 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

33 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

34 Testing at EAL2+ Augmented ALC_FLR.1 consists of assessing developer tests, independent function test, and performing penetration tests. The TOE testing was conducted by evaluators from CyberSecurity Malaysia MySEF and Tubitak Bilgem Center of Research for Advanced Technologies of Informatics and Information Security from Turkey (accredited by TURKAK- Turkish Accreditation Agency). The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

35 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

36 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

37 At EAL2+ Augmented ALC_FLR.1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a sample of the developer's test plan, and creating test cases that augmented the developer tests.

38 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent test developed and performed by the evaluators to verify the TOE functionality as follow:

Table 4: Independent Functional Testing

TEST TITLE	DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
Test Group A Test Group E Test Group F Test Group G Test Group H Test Group I Test Group J	This tests comprises a series of test cases on TOE security functions of how TOE control access and privilege for each user.	User Data Protection	Connect to System (RTM Manager) Master Encryptor Verification Connect to Database Engine Maintain Database Login Account Maintain Encryption Profile (EP) Enrol ST/SD Encryptor Initialize ST/SD Encryptor Reset Password Enable Logon, Disable Logon and Destroy Logon Update Enrol Setting ST/SD Encryptor Delete Enrolled ST/SD Encryptor Data from Database Maintains Events Log Connect SQL Thread Online Login Offline Login Non-Managed/Master Encryptor Activity Register ST/SD Encryptor Encryption/Decryption Data	**PASS**. Result as expected
Test Group A Test Group B Test Group Y Test Group Z	This tests comprises a series of test cases on TOE security functions on how TOE validate the	Identification and Authentication	Connect to System (RTM Manager) Master Encryptor Verification Connect to Database Engine Maintain Database Login Account Maintain Encryption Profile (EP) Enrol ST/SD Encryptor Initialize ST/SD Encryptor	**PASS**. Result as expected

	password and match it with user account		Reset Password Enable Logon, Disable Logon and Destroy Logon Update Enrol Setting ST/SD Encryptor Delete Enrolled ST/SD Encryptor Data from Database Maintains Events Log Connect SQL Thread Online Login Offline Login Non-Managed/Master Encryptor Activity Register ST/SD Encryptor Encryption/Decryption Data	
Test Group A Test Group C Test Group E Test Group F Test Group G Test Group H Test Group I Test Group J	This tests comprises a series of test cases on TOE security functions of how TOE maintains the security protection for user's data, Encryption profile, token management, enrolment management, log management, administrator management, and a connection to the server.	Security Management	Encryption/Decryption Data Maintain Database Login Account Maintain Encryption Profile (EP) Enrol ST/SD Encryptor Initialize ST/SD Encryptor Reset Password Enable Logon, Disable Logon and Destroy Logon Non-Managed/Master Encryptor Activity	**PASS**. Result as expected
Test Group B Test Group C Test Group D Test Group G Test Group I Test Group L Test Group M Test Group N	This tests comprises a series of test cases on TOE security functions of how TOE validate the Encryption Extension with encrypted/decrypted file and the cryptographic support needed	Cryptographic Support	Register ST/SD Encryptor Online Login Connect SQL Thread Maintains Events Log Maintain Database Login Account Maintain Encryption Profile (EP) Enrol ST/SD Encryptor Initialize ST/SD Encryptor Reset Password Enable Logon, Disable Logon and Destroy Logon Update Enrol Setting ST/SD Encryptor	**PASS**. Result as expected

Test Group O Test Group P Test Group Q Test Group R Test Group S Test Group T Test Group U Test Group Y Test Group Z	for the encryption/decryption process.		Delete Enrolled ST/SD Encryptor Data from Database	
Test Group J	This tests comprises a series of test cases on TOE security functions of how TOE record the event activities and how the event log is managed	Security Audit	Connect to System (RTM Manager) Master Encryptor Verification	**PASS**. Result as expected
Test Group V Test Group W Test Group X	This tests comprises a series of test cases on TOE security functions of how TOE protect the user's data	Protection of the TSF	Connect to System (RTM Manager) Master Encryptor Verification Connect to Database Engine Maintain Database Login Account Enrol ST/SD Encryptor Maintain Encryption Profile (EP) Initialize ST/SD Encryptor Maintains Events Log Connect SQL Thread Online Login Offline Login Non-Managed/Master Encryptor Activity Register ST/SD Encryptor Encryption/Decryption Data	**PASS**. Result as expected
Test Group E Test Group K	This tests comprises a series of test cases on TOE security functions of how TOE maintain the connection with the server and	Trusted Paths/Channel	Connect to System (RTM Manager) Master Encryptor Verification Connect to Database Engine Maintain Database Login Account Maintain Encryption Profile (EP) Enrol ST/SD Encryptor Initialize ST/SD Encryptor Reset Password Enable Logon, Disable Logon and	**PASS**. Result as expected

	the communication between RTM (host) and Encryptor		Destroy Logon Update Enrol Setting ST/SD Encryptor Delete Enrolled ST/SD Encryptor Data from Database Maintains Events Log Connect SQL Thread Online Login Offline Login Non-Managed/Master Encryptor Activity Register ST/SD Encryptor Encryption/Decryption Data	

39 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

40 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design and security architecture description.

41 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);
b) Specialist technical expertise required (specialised expertise);
c) Knowledge of the TOE design and operation (knowledge of the TOE);
d) Window of opportunity; and
e) IT hardware/software or other requirement required for exploitation.

42 The penetration tests that has been conducted by CyberSecurity Malaysia MySEF focus on:

a) USB Sniffing;
b) Invisible Data Transfer;
c) Open Encrypted File;
d) Brute Force;
e) Key Logging

43 Moreover, CyberSecurity Malaysia MySEF has appointed a subcontractor from Tubitak Bilgem Center of Research for Advanced Technologies of Informatics and Information Security from Turkey in order to conduct the penetration test on Hardware Security Module (HSM). Tubitak Bilgem Common Criteria Test Center is accredited by the Turkish Accreditation Agency (TURKAK) within the standard of ISO 17025. Some of the penetration test that has been focused by Tubitak are as below:

a) Software Penetration Testing:
   - Man-in-the-middle attack

- Software Perturbation
- Transit User Data Integrity Analysis
- Stored User Data Integrity Analysis

b) Power Analysis

c) Power Line Perturbation Analysis **(Not SAMM Accredited)**

44 The results of the penetration testing note that a number of additional vulnerabilities exist that are dependent on an attacker having access to the end-user host computer. Therefore, it is important for the user to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

45 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

46 Justification for the testing performed by Tubitak Lab as below:

a) The evaluation assurance scope of work is EAL2+ with augmented ALC_FLR.1. In which, did not compliment to any AVA_VAN requirements of higher level testing (more than EAL2). Therefore, it is concluded that the testing for Perturbation Attacks is outside the scope of AVA_VAN EAL2 requirements.

b) Note that, Perturbation Attacks are performed towards Smart Card Technologies and relevant hardware, in which, requires details documentations of CC evaluation leveraging towards the same requirements of EAL4 and above. Furthermore, the testing were performed based on supporting document relevant to CC guidance for Smart Card Evaluation and Smart Card Attack Potential Calculation.

3 Result of the Evaluation

47 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of the TOE performed by the CyberSecurity Malaysia MySEF.

48 CyberSecurity Malaysia MySEF found that TOE upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL2+ Augmented ALC_FLR.1.

49 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

50 EAL2+ Augmented ALC_FLR.1 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

51 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

52 EAL2+ Augmented ALC_FLR.1 also provides assurance through use of a configuration management system, evidence of secure delivery procedures and flaw remediation.

3.2 Recommendation

53 In addition to ensure secure usage of the product, below are additional recommendations for TOE users. Please note that, the opinions and interpretations expressed herein are outside the scope of SAMM accreditation:

a) The administrators and users of the TOE should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

b) Users are not allowed to share their external USB drive to others. If the product has been missing or stolen, the user needs to inform the personnel for further action.

c) The underlying operating system, database and active directory servers are patched and hardened to protect against known vulnerabilities and security configuration issues.

d) It is advice to change default password of supporting software or application which integrated with the TOE.

Annex A References

1.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] 2014-12-29-Encryptor-ST-0.7, Security Target, version 0.7, 29 December 2014.

[7] MySEF-3-EXE-E033-ETR-v1, Evaluation Technical Report, version 1, 27 February 2015.

1.2 Terminology

A.2.1 Acronym

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
SAMM	Skim Akreditasi Makmal Malaysia (Malaysian Laboratory Accreditation Scheme)
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---