MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C123 Certification Report

YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure

File name: ISCB-3-RPT-C123-CR-v1
Version: v1
Date of document: 10 FEBRUARY 2022
Document classification : PUBLIC

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

CyberSecurity Malaysia
(726630-U)

T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C123 Certification Report

YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure

10 FEBRUARY 2022

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C123 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C123-CR-v1
ISSUE:	v1
DATE:	10 FEBRUARY 2022
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 201601006881 (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, 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 17 Feb 2022, 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).

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 using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	21 January 2022	All	Initial draft
d2	31 January 2022	References	Review by Scheme Manager
v1	10 February 2022	All	Final version

Executive Summary

The Target of Evaluation (TOE) is YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure. The TOE can be categorised as a data protection product and the YOUTech 256 Cipher with Secret Key Infrastructure (YOUTECH256SKI) ecosystem consists of two major components which is YOUTech 256 SKI Token (YOUTECH256SKIT) and YOUTech 256 SKI Cipher System (YOUTECH256SKICS).

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional 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 the evaluated configuration, 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 the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by CyberSecurity Malaysia MySEF and the evaluation was completed on 25 January 2022

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure meets their requirements. It is recommended that a potential user of the TOE 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

1 YOUTech 256 Cipher with Secret Key Infrastructure (YOUTECH256SKI) is the product designed and developed by You Tech Solutions Sdn Bhd. This product was developed with the main purpose to secure all types of data/information integrity, ownership, to restore data privacy and prevent data/information from being compromised.

2 YOUTECH256SKI consists of several components which are YOUTECH256SKIT and YOUTECH256SKICS. YOUTECH256SKI offers end users to encrypt their files with AES 256-bit encryption algorithm which is a FIPS approved cryptographic algorithm standard. SHA-2 512 bits hashing algorithm is used to hash the private key for private key exchange. Files in the protected folder require YOUTECH256SKIT to decrypt and the files will automatically encrypt by YOUTECH256SKICS once YOUTECH256SKIT is unplugged form the computer / laptop. Public Key Cryptography (PKC) also known as asymmetric encryption is being used by YOUTECH256SKI.

3 The TOE includes the following security functions:

- User Data Protection
- Identification & Authentication
- Cryptographic Support
- Security Audit

1.2 TOE Identification

4 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	C123
TOE Name	YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure
TOE Version	YOUTech 256AKI which consists of: • YOUTech256SKI Token (v2.5) • YOUTech256SKI Cipher System (v9.78 build 504)

Security Target Title	YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure Security Target
Security Target Version	V1.0
Security Target Date	27 November 2021
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC v3.1 Conformant (Revision 5) CC Part 2 Conformant CC Part 3 Conformant
Sponsor	YOUTech Sdn Bhd 51-1, Lorong Perda Utama 3, Taman Prominence, 14000 Bukit Mertajam, Penang
Developer	YOUTech Sdn Bhd 51-1, Lorong Perda Utama 3, Taman Prominence, 14000 Bukit Mertajam, Penang
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

5 The organisational security policy is defined based on the use of the TOE.

Table 2: Organisational Security Policy

OSPs	Statements
P.ROLE	Only authorized user assigned by the organization have access to the TOE and TOE environment.

1.4 TOE Architecture

6 The TOE includes both physical and logical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

7 The TOE consists of the following security functions identified in the Security Target (Ref [6]).

Table 3: TOE Logical Boundaries

User Data Protection	TOE offers end users to encrypt their files or data in Computer or Laptop with multifactor authentication capability. Files will be encrypted automatically by YOUTECH256SKICS once YOUTECH256SKIT had been removed from the Computer or Laptop. File will only be decrypted by YOUTECH256SKICS during presence of YOUTECH256SKIT with valid Username and Password is authenticated by YOUTECH256SKICS
Identification and Authentication	TOE requires user to connect their unique YOUTECH256SKIT for YOUTECH256SKICS to verify their token SKI key which is Hardware ID of YOUTECH256SKIT with YOUTECH256SKI PostgreSQL Database as first factor authentication. Then second factor authentication will be the username and password which are generated for each user. Users is only allowed to perform further action to view their protected files once both authentications had been successfully verified
Cryptographic Support	TOE offers end users to encrypt their files with AES 256-bit encryption algorithm which is a FIPS approved cryptographic algorithm standard. SHA-2 512 bits hashing algorithm is used to hash the private key for private key exchange. Files in the protected folder require YOUTECH256SKIT to decrypt and the files will automatically encrypt by YOUTECH256SKICS once YOUTECH256SKIT is unplugged form the computer /

	laptop. Public Key Cryptography (PKC) also known as asymmetric encryption is being used by YOUTECH256SKI.
Security Audit	TOE shall be able to generate audit record with reliable timestamp for several auditable events. Each event will be recorded with date and time, type of event, subject identity and outcome of the event. Furthermore, system logs that generated by YOUTECH256SKICS is protected from direct access to prevent system logs being tampered by the user. Additionally, another set of audit data will be stored at YOUTECH256SKI PostgreSQL Database which only manageable by YOUTECH256SKI Management Application which is not part of the evaluation scope.

1.4.2 Physical Boundaries

8 Product components included in the TOE are listed below. Figure 1 illustrates a representative diagram of the TOE in its evaluated configuration.

- YOUTECHSKIT – YOUTECH256SKI Token (Hardware) and
- YOUTECHSKICS – YOUTECH256SKI Cipher System (Software)

9 The TOE process flow includes the following:

- YOUTECH256SKIT is an embedded SKI which increases the security of the protected data by applying a complex algorithm to the keys used for encrypting data.
- YOUTECH256SKIT is the key for user to encrypt or decrypt the files that user would like to protect. Two factors authentication will be prompted to user when user connect the YOUTECH256SKIT to their computer/laptop.
- YOUTECH256SKICS will perform two factors authentication verification by comparing the username, password and unique identifier which embedded in microchip of YOUTECH256SKIT with YOUTECH256SKI PostgreSQL Database. Once successfully authenticated, the YOUTECH256SKICS will decrypt the files in the protected folder.
- Audit records with reliable timestamp will be generated by YOUTECH256SKICS and stored in PostgreSQL Database for audit purpose. Administrator is able to

login into YOUTECH256SKI Management Application to view the activity logs generated by the users for troubleshooting and user monitoring purpose.

- Audit logs that generated by YOUTECH256SKICS would be stored at Secure folder in user computer and protected from direct access by the user and log tampering thus logs can only be traced through YOUTECH256SKICS.
- YOUTECH256SKI Management Application is hosted at YOUTECH256SKI Third Party Verifier Server. This management application is used to manage the user account for YOUTECH256SKI users and their YOUTECH256SKIT SKI Key.

10 The supporting hardware and software for the TOE are as following:

- YOUTECH256SKI Third Party Verifier Server

YOUTECH256SKI Third Party Verifier Server is a machine to host YOUTECH256SKI Management Application and YOUTECH256SKI PostgreSQL Database

- YOUTECH256SKI Management Application

YOUTECH256SKI Management Application is a Windows-based software to manage all the user accounts and YOUTECH256SKI Token SKI Key of YOUTECH256SKI solution

- YOUTECH256SKI PostgreSQL Database

YOUTECH256SKI PostgreSQL Database is a database storage to store all the user account details and YOUTECH256SKI Token SKI Key mapping data.

- User Computer / Laptop

User Computer/Laptop will be installed with YOUTECH256SKICS and network is required to perform multi factor authentication and allow YOUTECH256SKICS to communicate with YOUTECH256SKI Third Party Verifier Server. Minimum System Requirement as below:

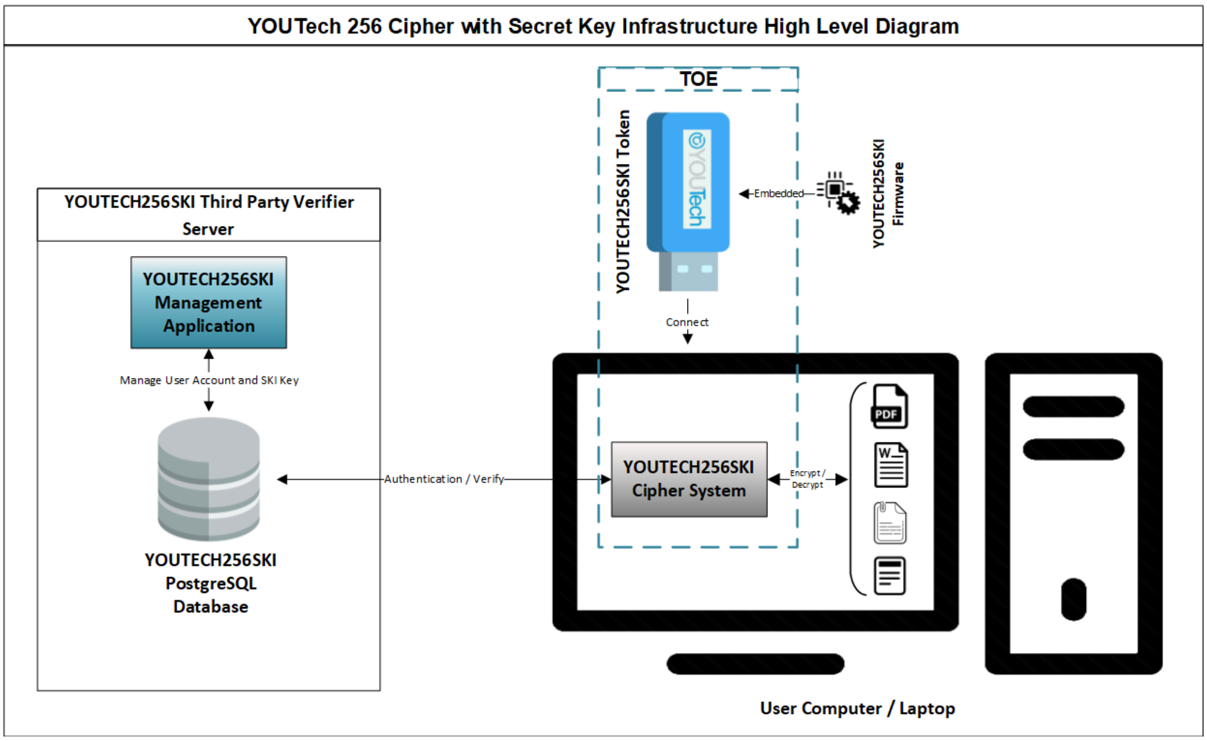
Operating System: Microsoft Windows 10 (32 or 64 bit) and above

RAM: 2 GB

Disk Space: 10 MB

11 The following diagram is a representation of the typical operational environment of the TOE.

Figure 1: TOE typical operation environment


YOUTech 256 Cipher with Secret Key Infrastructure High Level Diagram
TOE
YOUTECH256SKI Token
YOUTech
Embedded
YOUTECH256SKI Firmware
Connect
YOUTECH256SKI Third Party Verifier Server
YOUTECH256SKI Management Application
Manage User Account and SKI Key
YOUTECH256SKI PostgreSQL Database
Authentication / Verify
YOUTECH256SKI Cipher System
Encrypt / Decrypt
PDF
W
User Computer / Laptop

1.5 Clarification of Scope

12 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

13 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

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

1.6 Assumptions

15 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT

environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Operational Environment Assumptions

16 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 4: Assumptions for the TOE environment

Assumption	Statements
A.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE. The users are well-trained; the user shall comply to the operating procedures stipulated in the user guidance.
A.IDLE	The TOE environment must be protected during idle.

1.7 Evaluated Configuration

17 The TOE consists of the following components:

- YOUTECHSKIT – YOUTECH256SKI Token (Hardware); and
- YOUTECHSKICS – YOUTECH256SKI Cipher System (Software)

18 The TOE is delivered as an appliance by the developer and to be configured according to the Preparative Guidance.

1.8 Delivery Procedures

19 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

20 The customer will purchase the product and complete the payment. Once payment is confirmed and legal documentations have been completed, You Tech Solutions personnel can proceed with preparing and delivering the product.

21 You Tech Solutions personnel will make the necessary preparation:

- Prepare the User Guide document for YOUTECH256SKI and deliver through E-mail to the customers.
- Label YOUTECH256SKIT with identification and serial number.
- Register YOUTECH256SKIT at You Tech Solution Database.
- Place YOUTECH256SKIT and Lanyard in a plastic case and package it with a box.
- Apply warranty sticker on the box for warranty period identification purpose.
- Seal the packaging box with security tape to avoid the product being tampered during delivery to the customer.
- The product will be hand-delivered to the customer.

1.8.1 Product Documentation

22 List of documentation and description provided by the developer that the user can use as guidance for installation:

- YOUTECH256SKI Token (v2.5) and YOUTECH256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure Guidance Document v1.0
- [YOUTECH256SKI] INSTALLATION GUIDE WITH REVISION v0.6.

2 Evaluation

23 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_Req) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

25 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference and the TOE references used are consistent.

26 The evaluators examined that the method of identifying configuration items and determined that it describes how configuration items are uniquely identified

27 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure Life Cycle Documentation version 1.0.

2.1.2 Development

Architecture

28 The evaluators examined the security architecture description (contained in [18]) and 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.

29 The security architecture description describes the security domains maintained by the TSF.

30 The initialisation process described in the security architecture description preserves security.

31 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Functional Specification

32 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

33 The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

34 The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

TOE Design Specification

35 The evaluators examined the TOE design (contained in [18]) and determined that the structure of the entire TOE is described in terms of subsystems.

36 The evaluators also determined that all subsystems of the TSF are identified.

37 The evaluators determined that interactions between the subsystems of the TSF were described.

38 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

39 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

40 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

41 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

42 The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

43 The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

44 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

45 The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

46 The evaluators determined that the operational user guidance describes for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

47 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

48 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by CyberSecurity Malaysia MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

49 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

50 At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

51 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 functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 5: Independent Functional Test

TEST ID	DESCRIPTIONS	RESULTS
Test Case A.1 TSFI: Two Factor Authentication	To test that file will only be decrypted when valid Token 1 is inserted into Workstation 1 USB port with valid Username and Password is entered.	Passed. Result as expected.
Test Case A.2 TSFI: Two Factor Authentication	To test that wrong username cannot be identified and the decryption process cannot be executed.	Passed. Result as expected.
Test Case A.3 TSFI: Two Factor Authentication	To test that User cannot proceed with decryption process when username field is left blank.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
Test Case A.4 TSFI: Two Factor Authentication	To test that User with wrong password cannot be authenticated and the decryption process cannot be executed.	Passed. Result as expected.
Test Case B.1 TSFI: User Authentication File Encryption	To test that file decryption process will be initiated with presence of Token 1.	Passed. Result as expected.
Test Case B.2 TSFI: User Authentication File Encryption	To test that the encrypted file is unreadable when changing the file extension to decrypted format with the presence of Token 1 without entering username and password.	Passed. Result as expected.
Test Case B.3 TSFI: User Authentication File Encryption	To test that decrypted file cannot be encrypted by changing the file extension to encrypted format with the presence of Token 1 with entering username and password.	Passed. Result as expected.
Test Case B.4 TSFI: User Authentication File Encryption	To test that encrypted files cannot be decrypted using unregistered YOUTECH256SKIT (Token 2).	Passed. Result as expected.
Test Case B.5 TSFI: User Authentication File Encryption	To test that encrypted files cannot be decrypted using unregistered YOUTECH256SKIT (Token 2) with registered username and password.	Passed. Result as expected.
Test Case C.1 TSFI: User Authentication File Encryption	To test that the files are encrypted and no longer able to read once Token 1 is removed from user computer.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
Test Case C.2 TSFI: User Authentication File Encryption	To test that file format such as image, text file, video, and .EXE file stored in Secure Folder can be encrypted successfully.	Passed. Result as expected.
Test Case C.3 TSFI: User Authentication File Encryption	To test that the file content is unreadable even after change the file extension from encrypted to decrypted format with the absence of YOUTECH256SKIT.	Passed. Result as expected.
Test Case C.4 TSFI: User Authentication File Encryption	To test that file will be encrypted automatically when the YOUTECH256SKIT (Token 1) is removed.	Passed. Result as expected.
Test Case D.1 TSFI: Audit Record	To test that process is being logged by YOUTECH256SKICS and logs file is not able to be viewed by the user directly.	Passed. Result as expected.
Test Case D.2 TSFI: Audit Record	To test that the audit log will generate an audit record for the event of user Login & Logout, Authentication Failure, File encryption & decryption with date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.	Passed. Result as expected.
Test Case D.3 TSFI: Audit Record	To test that log record in YOUTECH256SKICS cannot be modified.	Passed. Result as expected.
Test Case D.4 TSFI: Log Tampering Protection	To verify that TOE timestamp only relies on YOUTECH256SKI Third party Verifier Server operating system.	Passed. Result as expected.
Test Case E.1 TSFI: File Encryption	To verify AES 256-bit is used for encryption & decryption operation.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
Test Case E.2 TSFI: File Encryption	To verify that SHA-2 512 bit is used for private key exchange.	Passed. Result as expected.
Test Case F.1 TSFI: Invalid Authentication	To ensure there is cool down time on YOUTECH256SKICS after consecutive of invalid credential is attempted to entered by the user.	Passed. Result as expected.
Test Case G.1 TSFI: System Idle	To ensure YOUTECH256SKICS will automatically encrypt the files in Secure Folder after idle time had met.	Passed. Result as expected.
Test Case G.2 TSFI: System Idle	To ensure YOUTECH256SKICS will automatically encrypt the files in Secure Folder after idle time had met Folder after idle time of 15 minutes had met.	Passed. Result as expected.

52 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration testing

53 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.

54 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during 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 for exploitation

55 The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) https://cwe.mitre.org

b) https://capec.mitre.org

c) https://nvd.nist.gov

d) https://uwnthesis.wordpress.com

e) https://owasp.org

f) https://www.cvedetails.com

g) https://cvedetails.com

56 The penetration tests focused on:

a) Reverse Engineering;

b) SQL Injection;

c) Sniffing; and

d) Bypassing

57 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 1 of the Security Target (Ref [6]).

2.1.4.4 Cryptographic Validation

58 The validation conducted for the TOE by Malaysian CyberSecurity Malaysia Cryptographic Evaluation Laboratory produced the expected results in Cryptographic Validation Report (Ref [6]).

2.1.4.5 Testing Results

59 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

60 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 YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure performed by CyberSecurity Malaysia MySEF.

61 CyberSecurity Malaysia MySEF found that YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

62 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 remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

63 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

64 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.

3.2 Recommendation

65 The Malaysian Certification Body (MyCB) is strongly recommending that:

a) Developer is recommended to increase the duration for system halted after multiple failed attempts. By baselining the Payment Card Industry Data Security Standard (PCI DSS) Requirement 8, setting the lockout rules for at least 30 minutes helps to prevent several kinds of brute force attacks.

Annex A References

A.1 References

[1] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security on July 2, 2014.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MyCC_REQ), v1, ISCB CyberSecurity Malaysia, 2 Dec 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, 4 Aug 2020.

[6] YOUTECH256SKI Security Target, Version 1.0, 27 November 2021.

[7] YOUTECH256SKI, Evaluation Technical Report, Version 1.0, 27 December 2021.

[8] YOUTECH256SKI TOE Design Documentation, Version 1.0, 27 November 2021.

[9] Cryptographic Algorithm Validation Report for CV10 YOUTech256SKI Cipher System version 9.78, Version 1.0, 10 December 2021.

A.2 Terminology

A.2.1 Acronyms

Table 6: 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

Acronym	Expanded Term
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 7: 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.

Term	**Definition and Source**
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 ---