Ref: YOUTECH256SKI-ST-1.0

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

DOCUMENT VERSION	**1.0**
DOCUMENT DATE	**27-NOVEMBER-2021**

You Tech Solutions Sdn Bhd

51-1, Lorong Perda Utama 3, Taman Prominence,

14000 Bukit Mertajam, Penang, Malaysia

Tel: +604 297 4507

Website: https://www.youtech.com.my/

Prepared by:

DOCUMENT REVISION HISTORY

Version No.	Published Date	Description of changes	Author
0.1	28-JAN-2021	First release	Wilson Lim
0.2	05-FEB-2021	MYSEF Review Update	Kenny Chan and Wilson Lim
0.3	10-MAY-2021	EOR Amendment	Kenny Chan and Wilson Lim
0.4	24-MAY-2021	EOR Amendment	Kenny Chan and Wilson Lim
0.5	09-AUG-2021	TOE Feature Enhancement	Kenny Chan and Wilson Lim
0.6	16-AUG-2021	Included new SFR	Kenny Chan and Wilson Lim
0.7	10-SEP-2021	EOR Amendment	Kenny Chan and Wilson Lim
1.0	27-NOV-2021	Final Release	Kenny Chan and Wilson Lim

TABLE OF CONTENTS

1 Security Target Introduction

1.1 Security Target Reference

Security Target Title:	YOUTech256SKI Token (v2.5) and YOUTech256SKI Cipher System (v9.78 build 504) with Secret Key Infrastructure Security Target
Security Target Version:	1.0
Security Target Date:	27-November-2021

Table 1 - ST Reference

1.2 TOE Reference

	TOE NAME:	**TOE VERSION:**
TOE Name & Version:	YOUTech 256 SKI Token	V2.5
TOE Initial:	YOUTECH256SKIT	
TOE Name & Version:	YOUTech 256 SKI Cipher System	v9.78 build 504
TOE Initial:	YOUTECH256SKICS	

Table 2 - TOE Reference

1.3 Terminology and Acronyms

Acronyms	Full Name
YOUTECH256SKI	YOUTech 256 Cipher with Secret Key Infrastructure
YOUTECH256SKIT	YOUTech 256 SKI Token
YOUTECH256SKICS	YOUTech 256 SKI Cipher System
SKI	Secret Key Infrastructure
PKC	Public Key Cryptography
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy

PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
USB	Universal Serial Bus
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithms
SKI	Secret Key Infrastructure
FIPS PUBS	Federal Information Processing Standards Publications
CBC	Cipher Block Chaining

1.4 Product Overview

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). YOUTECH256SKI is a data at endpoint security solution positioned as the best "Last Line of Defense" for all types' of data security. This platform is able to adapt into any types of industry and environment. The technology platform is currently using 256-bit AES encryption algorithm (the most trusted AES encryption technology) with Secret Key Infrastructure (SKI). The cutting edge technology of YOUTECH256SKI is the ability to perform encryption (which is currently the only commercially available solution in the market) with Secret Key Infrastructure. The purpose of this functionality is to strengthen the "Last Line of Defense" over the secured data/information within secured or even unsecured working environment.

Please refer to

- Table 3: YOUTECH256 Product Specification

Table 3 – YOUTECH256SKI Product Specification

Type	Version	Specification
YOUTECH256SKI Token (Hardware)	2.5	• USB2.0 Mass Storage controller • 2GB Storage • Built in with SKI (Secret Key Infrastructure) • For second authentication purpose
YOUTECH256SKI Firmware (Software)	1.20.15.7	• To initiate YOUTECH256SKI Cipher System Installer
YOUTECH256SKI Cipher System (Software)	9.78 (Built : 504)	• To encrypt & decrypt the file in secured storage. • To verify first Factor Authentication via database at Third Party Verifier Server • To verify second Factor Authentication with Token (SKI) via database at Third Party Verifier Server • Change user password
YOUTECH256SKI Third Party Verifier Server	2.0i	• 1 Processor (Intel Xeon-Gold 6242 – 2.8 Ghz / 16 Core, 256 GB RAM, 1TB HDD • This server consists the following software: - Operating System: Microsoft Server Standard 2019 - Database: PostgreSQL version 9.6 - ODBC: PostgreSQL Unicode version 9.05.04.00 - YOUTECH256 Management Platform - YOUTECH256 Verifier
YOUTECH256SKI Management Application (Windows Application)	2.0	• Manage SKI Hardware ID and User Account Details

YOUTECH256SKI PostgreSQL Database	9.6	• To store user account details and SKI Hardware ID

1.5 TOE Overview

TOE Overview summarizes the usage and major security features of the TOE. TOE Overview provides context for the evaluated TOE by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.5.1 Usage and Major Security Feature of the TOE

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.

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.

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.

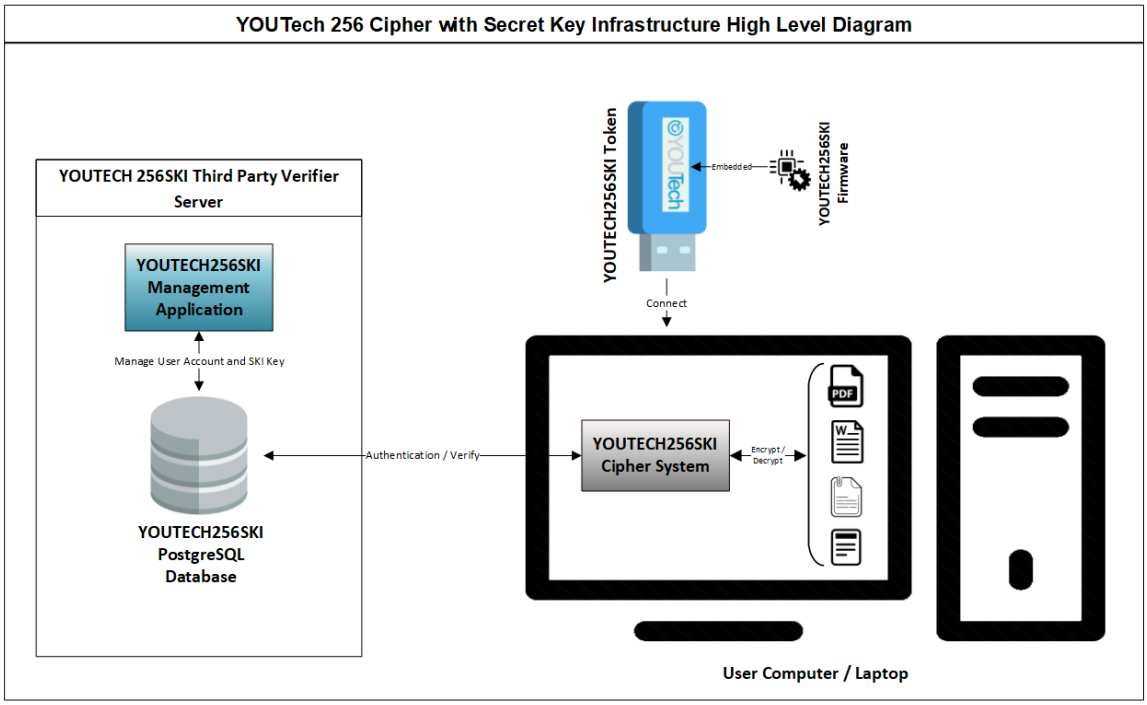

Figure 1 - YOUTech 256 Cipher with Secret Key Infrastructure High Level Diagram

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.

The major security features of the TOE included in the evaluation is:

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

For more details, refer to Logical Scope Section.

1.5.2 TOE Type

YOUTECH256SKI is a solution to provide file encryption with multi-factors authentication capability which can be categorised as a data protection product.

1.5.3 Non-TOE hardware/firmware/software required by the TOE

The following figure shows the typical operational environment of the TOE.

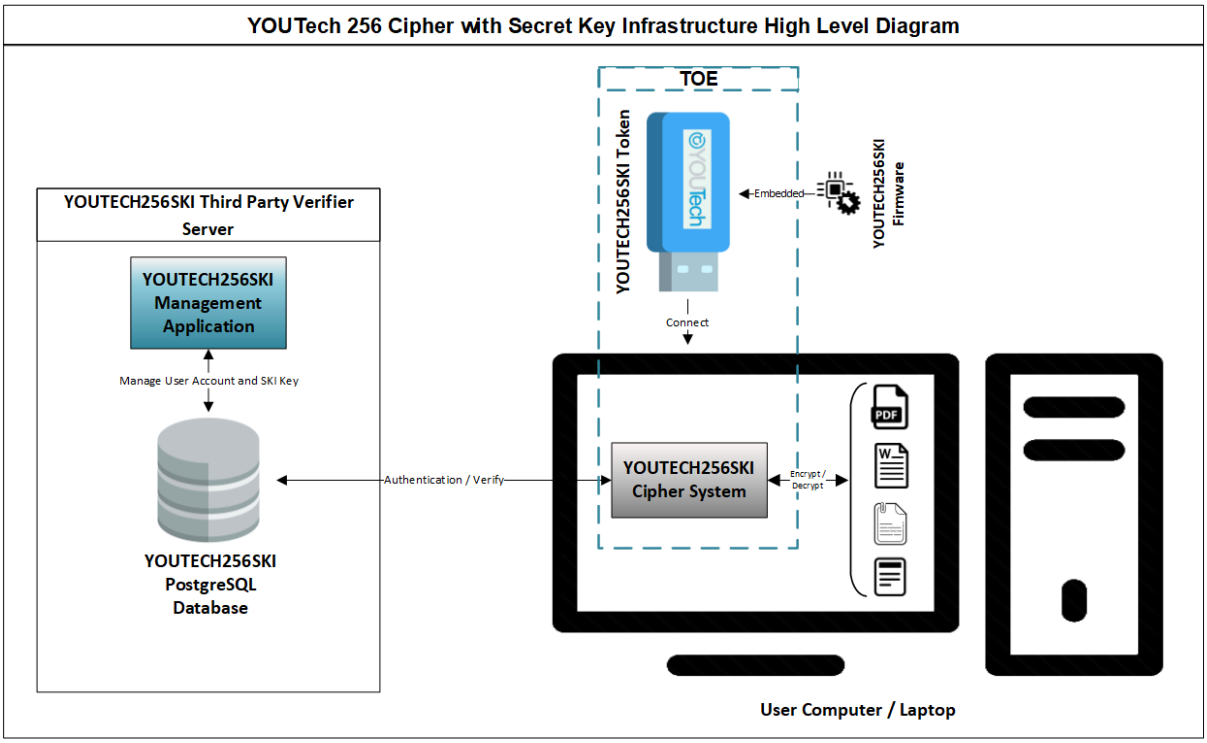

Figure 2 - TOE typical operational environment

The supporting hardware and software for TOE are as following:

a) YOUTECH256SKI Third Party Verifier Server

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

b) 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.

c) YOUTECH256SKI PostgreSQL Database

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

d) 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

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.6.1 Physical Scope of the TOE

As illustrated in Figure 2 - TOE typical operational environment, the TOE consists of two main components:

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

1.6.2 Logical Scope of the TOE

The logical scope of TOE is described based on the following security functional requirement.

1.6.2.1 User Data Protection

TOE offers end users to encrypt their files or data in Computer or Laptop with multi-factors authentication capability. Files will be encrypted automatically by YOUTECH256SKICS once YOUTECH256SKIT had been removed from the Computer or Laptop. File will only decrypted by YOUTECH256SKICS during presence of YOUTECH256SKIT with valid Username and Password is authenticated by YOUTECH256SKICS.

1.6.2.2 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 authentication had been successfully verified.

1.6.2.3 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.

1.6.2.4 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.

2 Conformance Claims

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

CCv3.1 conformant	The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 5.
Part 2 conformant	The ST is Common Criteria Part 2 conformant.
Part 3 conformant	The ST is Common Criteria Part 3 conformant.
Package conformant	EAL 2.
Protection Profile conformance	None.

3 TOE Security Problem Definition

3.1 Assumption

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

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.

Table 4: Assumptions

3.2 Threats

This section describes the threats that are addressed by the TOE:

T. DATA	An unauthorized person may successfully access the user protected data.
T.AUDIT	An unauthorized person or authorized user may intentionally or unintentionally perform malicious actions such as Username or Password brute-force attack.
T.SESSIONHIJACK	An unauthorized person may obtain access to the TOE while in idle mode.

Table 5: Threats

3.3 Organizational Security Policies

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

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

Table 6 : Organizational Security Policies

4 Security Objectives

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

4.1 Security Objectives for the TOE

The security objectives for the TOE as following:

O.DATA	The TOE shall ensure that only authorized person can accesses the User protected data.
O.AUDIT	The TOE shall record the security events generated by TOE and prevent the system logs from being tampered.

Table 7: Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

OE.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 with the operating procedures stipulated in the user guidance.
OE.IDLE	The TOE environment shall be secured during idle.

Table 8: Security Objectives for the Operational Environment

4.2.1 Security Objectives Rationale

Table 9 maps security objectives to threats and assumptions described in Section 4. The table illustrates that each threat is countered by at least one security objective, that each assumption is upheld by at least one security objective, and that each objective counters at least one threat or upholds at least one assumption.

Threats and Assumptions / Security Objectives	T.DATA	T.AUDIT	T.SESSIONHIJACK	A.USER	A.IDLE
O.DATA	✓				
O.AUDIT		✓			
OE.USER				✓	
OE.IDLE			✓		✓

Table 9 - Security Objectives Rationale Mapping

5 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE.

5.1 Extended Security Functional Requirement (SFR)

There are no extended SFR components defined for this evaluation.

5.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

6 TOE Security Requirements

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

6.1 Conventions

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

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

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

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

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

6.2 Security Functional Requirements (SFR)

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

Component	Component Name
Class FDP: USER DATA PROTECTION	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Class FIA: Identification and authentication	
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
Class FCS: Cryptographic support	
FCS_CKM.1	Cryptographic key generation
FCS_COP.1	Cryptographic operation
Class FAU: Security audit	
FAU_GEN.1	Audit data generation
FAU_STG.1	Protected audit trail storage

Table 10: Security Functional Requirements List

6.2.1 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**access control policy**] on [

Subject	Operations	Object
User	Login with YOUTECH256SKIT and user credential (username and password) at YOUTECH256SKICS. 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.	User's perform File Encryption and Decryption with presence of YOUTECH256SKIT and valid Username and Password.
User	Login with YOUTECH256SKIT and user credential (username and password) at YOUTECH256SKICS. Files in the protected folder require YOUTECH256SKIT to decrypt and the files will automatically encrypt by	YOUTECH256SKICS automatically encrypt user files after system is left idle for specific timeframe.

	YOUTECH256SKICS once YOUTECH256SKIT is left idle on the system for specific time based on user preference on YOUTECH256SKICS.	
User	Login with invalid credentials during 2nd Factor Authentication. YOUTECH256SKICS will halt for 1 minute and re-initialize to prevent from brute force attack.	YOUTECH256SKICS will re-initialized to prevent user from perform password brute force attack.

].

FDP_ACF.1 Security attribute based access control

Hierarchical No other components.

Dependencies FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

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

Subject	Object Controlled	Objective
YOUTECH256SKIT	Serve as a private key for file encryption.	YOUTECH256SKIT is required for user identification purpose.
Credentials (Username and Password)	Perform authentication to identify user for YOUTECH256SKIT.	Credentials serve as second factor authentication.

].

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

Subject	Object Controlled	Rules
YOUTECH256SKIT	Serve as a private key for file encryption.	Permission is granted to YOUTECH256SKICS for file decryption process to happen when valid YOUTECH256SKIT, Username and Password is presence
Credentials (Username and Password)	Perform authentication to identify user for YOUTECH256SKIT.	

].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subject to objects based on the following additional rules: [

Subject	Object Controlled	Rules
YOUTECH256SKIT	Serve as a private key for file encryption.	YOUTECH256SKICS shall decrypt the encrypted files when valid YOUTECH256SKIT, Username and Password is presence
Credentials (Username and Password)	Perform authentication to identify user for YOUTECH256SKIT.	

].

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

Subject	Object Controlled	Rules
YOUTECH256SKIT	Serve as a private key for file encryption.	YOUTECH256SKICS shall not decrypt the encrypted files when invalid YOUTECH256SKIT, Username or Password is presence.
Credentials (Username and Password)	Perform authentication to identify user for YOUTECH256SKIT.	

].

6.2.2 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical	FIA_UAU.1 Timing of authentication
Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical	No other components.
Dependencies	No dependencies.
FIA_UAU.5.1	The TSF shall provide [**two-factors authentication mechanism**] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [**YOUTECH256SKIT and a valid set of user credential**].

FIA_UID.2 User identification before any action

Hierarchical	FIA_UID.1 Timing of identification
Dependencies	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical	No other components
Dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Advanced Encryption Standard (AES)]** and specified cryptographic key sizes [**256 Bit**] that meet the following: [**FIPS PUB 197**].

Application Notes	Cipher Block Chaining Mode (CBC) is used as the mode of operation for YOUTECHSKI AES 256 Encryption Algorithm. SHA-2 512 bits hashing algorithm is used for private key exchange.

FCS_COP.1 Cryptographic operation

Hierarchical	No other components
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [**file encryption and decryption**] in accordance with a specified cryptographic algorithm [**Advanced Encryption Standard (AES)**] and cryptographic key sizes [**256 Bit**] that meet the following: [**FIPS PUB 197**].
Application Notes	Cipher Block Chaining Mode (CBC) is used as the mode of operation for YOUTECHSKI AES 256 Encryption Algorithm. SHA-2 512 bits hashing algorithm is used for private key exchange.

6.2.4 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical	No other components
Dependencies	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: ~~a) Start-up and shutdown of the audit functions;~~ b) All auditable events for the [***not specified***] level of audit; and c) [**(i) User login and logout** **(ii) Authentication failure** **(iii) File encryption and decryption**].

FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**None**]

FAU_STG.1 Protected audit trail storage

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [***Prevent***] unauthorised modifications to the stored audit records in the audit trail.

6.3 Security Assurance Requirements

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

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

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

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

Table 11: Security Assurance Requirements for EAL2

7 TOE Summary Specifications

TOE addressed the security functional requirements as following:

7.1 User Data Protection

TOE shall enforce Access Control Policy which pre-built in the YOUTECH256SKICS. Only one user role who is user, required to perform two factors authentication (YOUTECH256SKIT and user credential) then only the YOUTECH256SKICS will decrypt the files. 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.

Relevant SFR: FDP_ACC.1, FDP_ACF.1

7.2 Identification and Authentication

TOE user can access TOE by providing YOUTECH256SKIT, Username and Password which created by YOUTECH256SKI Management Application. After being authenticated, user could decrypt or read the encrypted files in protected folder. User will be authenticated with two factors authentication – YOUTECH256SKIT and user credential. If invalid token or Username and Password been provided, an application error will be triggered.

YOUTECH256SKIT has a unique device key which been hardcoded into token microchip when manufacturing the token. The device key will be retrieved and stored in YOUTECH256SKI PostgreSQL

Database which will be paired with user account that created with YOUTECH256SKI Management Application. However, user account creation and device key pairing security are not part of the scope.

Relevant SFR: FIA_UAU.2, FIA_UAU.5, FIA_UID.2

7.3 Cryptographic Support

TOE will perform file encryption or decryption based on AES 256-bit encryption key with SHA-2 512 bits hashing algorithm for private key exchange. The protected files will be encrypted when the YOUTECH256SKIT been unplugged from user computer / laptop. The encrypted files can only be decrypted once the user connect the correct YOUTECH256SKIT and provide the correct user credential.

Relevant SFR: FCS_CKM.1, FCS_COP.1

7.4 Security Audit

The TOE will generate audit records for selected security events in audit trail. The events that being audited as following:

- User login and logout
- Authentication failure
- File encryption and decryption

Each audited events will be recorded along with date and time of event, type of event, subject identity and outcome (success or failure) of the event. The timestamp is rely based on the underlying of YOUTECH256SKI Third Party Verifier Server operating system. Furthermore, the start-up and shutdown of the audit function are not applicable and only can be turn off (not disable temporary) if the TOE are being turn off/power off. Additional security measure had been made the audit log file from direct access to prevent from log tampering thus audit log can only be viewed from YOUTECH256SKICS.

Relevant SFR: FAU_GEN.1, FAU_STG.1

8 Rationale

8.1 Protection Profile Conformance Claim Rationale

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

8.2 Security Objectives Rationale

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

8.2.1 Rationale of Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.DATA An unauthorized person may successfully accesses the user protected data.	**O.DATA** The TOE shall ensure that only authorized person can accesses the User protected data.	This security objective counters threat because TOE shall prevent unauthorised data access to be happened without correct YOUTECH256SKIT and user credential.
T.AUDIT An unauthorized person or authorized user may intentionally or unintentionally perform malicious actions undetected.	**O.AUDIT** The TOE shall record the security events generated by TOE and prevent the system logs from being tampered.	The security objectives counters threat because it concerns with TOE recording the security events performed by authorized or unauthorized person and the system logs is being protected from being tampered.
T.SESSIONHIJACK An unauthorized person may obtain access to the TOE while in idle mode.	**OE.IDLE** The TOE environment shall be secured during idle.	The security objective counters threat because TOE environment shall prevent unauthorized person using user's idle session to obtain unauthorized access to TOE.

Table 12 - Rationale of Security Objectives Mapped to Threats

8.2.2 Rationale of Security Objectives Mapped to OSP

OSP	Security Objectives	Rationale
P.ROLE Only authorized user assigned by the organization have access to the TOE and TOE environment.	**OE.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 with the operating procedures stipulated in the user guidance.	The security objective counters OSP because the TOE users is assigned by organization and trusted to be non-hostile and will follow guidance documentation in handling the TOE.

Table 13 - Rationale of Security Objectives Mapped to OSP

8.2.3 Rationale of Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
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.	**OE.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 with the operating procedures stipulated in the user guidance.	The security objective counters assumption because authorized TOE user shall be non-hostile, assigned by organization and follows guidance documentation accordingly; However TOE user is not free from human error and mistakes.
A.IDLE The TOE environment must be protected during idle.	**OE.IDLE** The TOE environment shall be secured during idle.	The security objective counters assumption because TOE environment shall be protected during idles with password protection or other secure mechanism.

Table 14 - Rationale of Security Objectives Mapped to Assumptions

8.3 Extended Security Functional Requirement Rationale

Not applicable since there is no Extended Security Functional Requirement (SFR) declared in ST.

8.4 Extended Security Assurance Requirement Rationale

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

8.5 Security Functional Requirements Rationale

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

8.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.DATA The TOE shall ensure that only authorized person can accesses the User protected data.	FDP_ACC.1 FDP_ACF.1 FIA_UAU.2 FIA_UAU.5 FIA_UID.2 FCS_CKM.1 FCS_COP.1	This SFR requires the TOE to perform two factors authentication before the protected file being decrypted. Then only the user able to read the proper content of the files. TOE encrypt file 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.
O.AUDIT The TOE shall record the security events generated by TOE and prevent the system logs from being tampered.	FAU_GEN.1 FAU_STG.1	This SFR requires the TOE to have feature to generate security event audit logs with reliable timestamp and prevent the system logs from being tampered.

Table 15 - Rationale for SFR Mapped to Security Objectives for TOE

8.5.2 SFR Dependency Rationale

The following table provides a demonstration that all SFRs dependencies included in the ST have been satisfied.

SFR	Dependency	Dependency Met?	Justification
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Partial, FMT_MSA.3 is not applicable for TOE requirements.	FMT_MSA.3 is not applicable as there is no security attributes to initialise
FIA_UAU.2	FIA_UID.1	No, FIA_UID.1 is not applicable for TOE requirements.	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FIA_UAU.5	-	Yes	-

FIA_UID.2	-	Yes	-
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Partial, FCS_CKM.4 is not applicable for TOE requirement due to out of scope.	FCS_CKM.4 is not applicable as the key management is out of scope.
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Partial, FCS_CKM.4 is not applicable for TOE requirement due to out of scope.	FCS_CKM.4 is not applicable as the key management is out of scope.
FAU_GEN.1	FPT_STM.1	No	FPT_STM.1 is not applicable as the timestamp is provided by TOE environment.
FAU_STG.1	FAU_GEN.1	Yes	-

Table 16 - SFR Dependencies

----------END OF DOCUMENT----------