Agiletech Systems (M) UNIBOX 2.0 v1.0

Security Target

Evaluation Assurance Level (EAL): EAL1

Doc Ref: AT-001
Doc Ver: 1.14
Date: 14th May 2024

Developed by:

Agiletech Systems (M) Sdn. Bhd.

Prepared by:

MyInfoman
脈資訊管理有限公司

Version History

Version	Date	Description
0.1	8th June 2023	Initial draft.
0.2	15th June 2023	Updated based on feedbacks from Developer.
0.3	7th July 2023	Updated based on feedbacks from Consultant.
0.4	20th July 2023	Updated based on feedbacks from Laboratory.
1.0	28th July 2023	Submission to the Laboratory for evaluation.
1.1	1st August 2023	Updated based on feedbacks from Laboratory.
1.2	10th August 2023	Updated based on feedbacks from Developer.
1.3	30th August 2023	Updated based on feedbacks from Developer.
1.4	8th September 2023	Updated based on Observation Report (OR-001-d1).
1.5	3rd October 2023	Updated based on Observation Report (OR-002-d1). • Added Section 1.4. • Modified Figure 1.
1.6	16th October 2023	Updated based on Observation Report (OR-003-d1) • Modified evaluation platform from Chrome 19 to Chrome 118 in section 1.6. • Modified “phone number” to “mobile number” • Modified Section 5.2.2.1, 5.2.2.2, 5.2.2.4, 5.2.2.5, and 6.2 to incorporate the additional steps in setting up the Authorised User’s merchant, contracts and rate cards.
1.7	22nd November 2023	Updated based on Observation Report (OR-004-d1). • Revised Figure 1 to clarify the access limitations for Authorised User and Super Administrator.
1.8	11th December 2023	Updated based on Observation Report (OR-004-d2).
1.9	18th December 2023	Updated based on Observation Report (OR-005-d1).
1.10	3rd January 2024	Updated based on Observation Report (OR-006-d1).
1.11	5th February 2024	Updated based on Observation Report (OR-007-d1).
1.12	4th March 2024	Updated based on Observation Report (OR-008-d1).
1.13	18th April 2024	Updated based on Observation Report (OR-010-d1).
1.14	14th May 2024	Updated the Operational Guidance document version from v1.9 to v1.10.

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

This security target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 SECURITY TARGET REFERENCE

ST Title:	Agiletech Systems (M) UNIBOX 2.0 v1.0 Security Target
ST Version:	1.14
ST Date:	14th May 2024
Sponsor:	Agiletech Systems (M) Sdn Bhd

1.2 TOE REFERENCE

TOE Name:	UNIBOX 2.0
TOE Version:	1.0
Developer Name:	Agiletech Systems (M) Sdn Bhd

1.3 GLOSSARY

Table 1: Terms and description.

Terms	Description
CRUD	The actions that can be performed by the users of the TOE onto the TSF data, they stand for “Create”, “Read”, “Update” and “Delete”.
Assign	The action of binding a specific attribute or restriction onto a user role or specific user.
Remove	The action of removing a specific attribute or restriction onto a user role or specific user.

1.4 ABBREVIATIONS AND DEFINITION

Abbreviation	Definition
ST	Security Target
TOE	Target of Evaluation
IT	Information Technology
CC	Common Criteria
SFR	Security Functional Requirement
TSF	TOE Security Functionality
TSFI	TSF Interface
EAL	Evaluation Assurance Level
OS	Operating System
PP	Protection Profile
API	Application Programming Interface
TLS	Transport Layer Security
SHA	Secure Hash Algorithm
VPC	Virtual Private Cloud
NTP	Network Time Protocol
PGW	Payment Gateway

1.5 TOE TYPE

The TOE is a secure payment platform which utilizes application programming interface (API) that enables Authorised Users (i.e., merchants) to perform e-commerce transaction with payment channels of choice, inquire and be notified of changes to transaction statuses.

The user role available for the TOE include “Super Administrator” and “Authorised User”. The terms “Super Administrator(s)”, “super administrator(s)”, “Super Admin(s)”, and “super admin(s)” are referring to Super Administrator, which is the user role with the highest privilege and provide the ability to access to all the TOE’s function and modify the security behaviour of the Authorised Users. The term “Authorised User(s)”, “authorised user(s)” are referring to Authorised User, which is the TOE consumer that utilises the TOE’s security functions available to them, which are authorised by the Super Administrator. From this point onwards, when referring to “users”, it will include all the user roles; however when specific user roles are mentioned such as “Super Administrator(s)” or “Authorised User(s)”, only the specified user role will be applied.

The TOE also includes component for API Management, the Authorised Users may access it to oversee all previous and current transactions through an applet named Merchant Access; while the Super Administrator may access it to perform access control and modify behaviour of the API.

The TOE hereafter shall be referred to as UNIBOX 2.0 v1.0. The security function of the TOE includes Identification and Authentication, Security Audit, Security Management, Trusted Path, and Cryptographic Support.

1.6 TOE OVERVIEW

The TOE is a secure payment platform which was developed to provide a authorised and secure payment channels for merchants to connect with payment providers. The services provided by the TOE include transaction initiation, initiate refunds, payment status inquiries, etc..

The TOE also includes an API Management platform which provides front end applications (also known as applet) to perform security management and modify the behaviour of the API.

The TOE is owned and operated by the Agiletech Systems (M) Sdn Bhd since January 2022. The TOE provide a seamless experience for online merchants to connect to their payment provider of choice. Without utilising the TOE, the online merchants are required to establish an entity in the country that they provide their service, and integrate to their payment provider manually. The TOE can be accessed after establishing a business contract by engaging Agiletech Systems (M) Sdn Bhd.

The brand name of the TOE is “UniPin”, while the TOE name is “UNIBOX 2.0”. The name “UniPin” is understood by the market as the solution provider, hence it’s portrayed on the TOE.

The key features of the TOE are listed as below:

- Provide the list of payment channels that support the Authorised Users’ currency of choice;
- Secure transaction between Authorised Users and payment channels through cryptography;

- Automatic update response from payment provider to the TOE, and from the TOE to Authorised User. This automatic response is called “callbacks”, it’s one of the transactions.
- Status inquiries for pending transactions or refunds;
- Audit logging of transaction initiations and statuses, and access to the merchant dashboard (i.e., Merchant Access) and API manager (i.e., Merchant Admin);
- Timely notifications if there are updates to the transactions or refunds; and
- Central management applets which allow Super Administrator to manage and modify security behaviour of the TOE, read audit events such as CRUD actions performed by Super Administrator on the TOE and transactions initiated by the Authorised User to the TOE using the API.
- Please refer to the list below for the specific security behaviours of the TOE and Authorised User’s security behaviours that can be modified by the Super Administrator:
  - Security behaviour of the TOE modifiable by the Super Administrator:
    i. Password quality metrics;
    ii. Payment channel maintenance; and
    iii. Security of the connection required by the Trusted Path.
  - Security behaviour of the Authorised User modifiable by the Super Administrator:
    i. Role and permission;
    ii. Merchant listing;
    iii. Contracts;
    iv. Transaction credentials;
    v. Rate cards; and
    vi. Read access to audit logs.

The security functions implemented in the TOE is stated in table 2.

Table 2: TOE security features

Security Features	Description
Identification and Authentication	The Authorised Users and Super Administrator are required to insert email or mobile number and password to be authorised and gain access to the central management platform. The Authorised Users’ access are control through role-based access control (RBAC).
Security Audit	Audit entries are generated for security related events on all TOE components (i.e., transactions on API, modifications made to applets on the TOE, etc.). The audit logs are only accessible by the Super Administrator. The audit logs are stored on an external audit server where the communication is secured through TLS v1.2 and above.
Security Management	The user roles exist for this TOE are Super Administrator and Authorised User. All users are required to insert email address or mobile number and password before the users are able to use any TOE security functions. Both the Super Administrator and Authorised User can modify their own login contact number and password. The TOE restricts the access of Authorised Users only to the management functions which are determined by the Super Administrator.
Trusted path/ channels	The TOE is able to protect the TOE data from unauthorised modifications and disclosures by securing the communication channel with cryptography. The channels are secured between the Authorised User to the TOE.

Cryptographic Support	The TOE is able to perform SHA-256 hashing cryptographic operations to ensure the authenticity of the transactions, through utilisation of the merchant_code and merchant_key within the pre-determined formulae.

The TOE type is a secure payment platform that provide secure payment channels for all registered merchants to securely transact with their payment provider of choice securely by utilising the relevant security functions such as identification and authentication, security management, security audit, trusted path, and cryptographic support.

1.7 TOE DESCRIPTION

Figure 1 shows the evaluated configuration of the TOE, including the TSFIs, which reflects a typical implementation configuration.

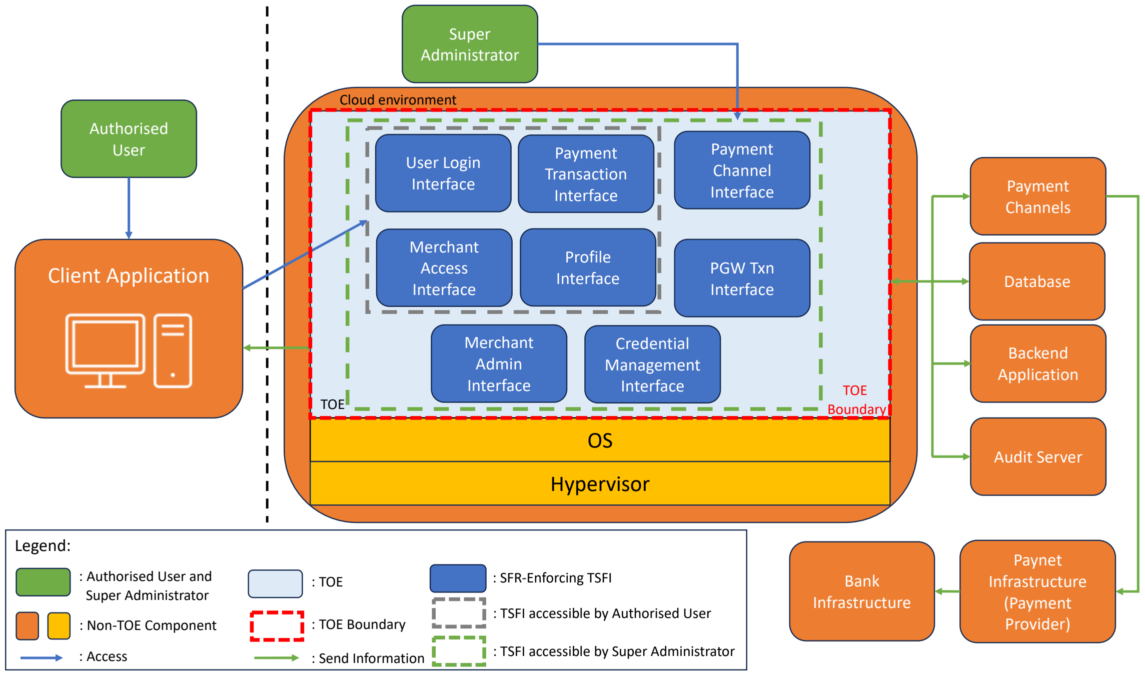

Figure 1: TOE boundary

Authorised User:
The Authorised Users are the end-user customers (i.e., merchants) that utilise the TOE.

The Authorised User can insert their email or mobile number and password at the User Login Interface to gain access into the TOE. Within the TOE, the Authorised User can only have access to the interfaces provided by the Super Administrator. To perform API configuration managements, the Authorised Users are able to access the interfaces through their client applications to oversee all the transactions performed to the API. The Authorised User can also modify their mobile number and password in the Profile Interface.

To perform initiate secure payments, the Authorised Users are required to use their client applications to call out to the API through web browser or command line interface. To ensure that the payload is authentic and not forged, the API will verify the SHA-256 hash value provided by the Authorised Users. The hash value is produced through the inclusion of Merchant_code and Merchant_key unique to each Authorised User and other information into specific formulas provided by the Super Administrator. Once the Authorised Users' payload is authenticated, the API will then establish the necessary connection to database, backend applications, payment channels, or audit server to complete the transaction. The connections aforementioned are all secure through Transport Layer Security (i.e., TLS v1.2 and above).

Super Administrator:
The Super Administrator have the highest privilege on the TOE and are able to authorise Authorised Users for specific accesses. To ensure that the Super Administrator is able to perform the security functions of the TOE, the role has to be manually created by the developers, which consists of steps:

1. Manually setup the Super Administrator's account in the Database directly;
2. Send the email and password for identification and authentication to the Super Administrator through email.

Once the Super Administrator receive the email and password for the identification and authentication through email, the Super Administrator can insert their email or mobile number and password at the User Login Interface to gain access into the TOE. Within the TOE, Super Administrator have full access of the platform. To perform API configuration managements, the Super Administrator is able to access the TOE to manage the security functions, security attribute, access control, security behaviour, and security audit on the TOE.

1.7.1 PHYSICAL SCOPE OF TOE

The TOE comprise of the following:

- The TOE software, i.e. UNIBOX 2.0 v1.0.

The non-TOE comprise of the following:

- **Transport Layer Security.** Cryptography of the communication channel between all users to the TOE; and from TOE to other trusted IT products such as database, backend application, payment channels and audit servers with TLS v1.2 and above is provided by CloudFlare.
- **Secure Connection to Other Trusted IT Product.** The connections between the TOE and other trusted IT product such as databases, backend applications, payment channels, and audit servers are secured through Virtual Private Cloud (VPC) provided by AWS Cloud.
- **Database Server.** The TOE will complete the request by parsing it to external PostgreSQL database servers located in cloud.
- **Backend Applications.** Auxiliary applications to support the implementation of the API.
- **Payment Channels.** The TOE will complete the request by parsing it to external payment channels' web servers. This is not to be confused with the Payment Channel applet.
- **Time Server.** The TOE utilizes Network Time Protocol (NTP) server to synchronize its system clock with a central time source.
- **Client Applications.** The TOE accepts request through HTTP protocol, hence the TOE can be called through browser address bar or Command Line Interface that support cURL command such as PowerShell.
- **Platform for the TOE.** This TOE component operates on Tomcat Apache, with the following operating systems (OS) in cloud:
    a) Alpine Linux version 3 and later (For API)
    b) CloudFlare pages (For Applets)
- **Access for the TOE**. This TOE component can be accessed through the following web browsers:
    a) Internet Explorer 8, 9, 10, 11; and
    b) Chrome 55 or higher.

NOTE: The evaluation of the TOE components are performed on Chrome 118.

- **Audit Server.** Used for external storage of audit data.

1.7.2 TOE GUIDANCE

The TOE guidance documents comprise of the following:

- UNIBOX 2.0 v1.0 User Guide v1.0.0
- AT-003 Agiletech Systems (M) UNIBOX 2.0 v1.0 Preparative Guidance v1.6
- AT-004 Agiletech Systems (M) UNIBOX 2.0 v1.0 Operational Guidance v1.10

1.7.3 LOGICAL SCOPE OF TOE

The logical scope of TOE is described based on several security functional requirements.

1.7.3.1 IDENTIFICATION AND AUTHENTICATION

The Authorised Users and Super Administrator are required to insert email or mobile number and password to be authorised and gain access to the central management platform. The quality of password is also controlled, and they're required to be a minimum 8 and maximum 64 characters which includes at least 1 uppercase and 1 lowercase alphabet, 1 numerical character and 1 special character.

Without properly authenticating and identifying the user's identity, they will not be given access to the TOE.

1.7.3.2 SECURITY MANAGEMENT

The roles exist for this TOE are Authorised User and Super Administrator. All users are required to insert email address or mobile number and password before they are able to use any TOE security functions.

The Authorised User is defined as the TOE consumer. The TOE restricts the access of Authorised Users only to the management functions which are determined by the Super Administrator. The Authorised Users are able to modify their own mobile number and password.

Super Administrator are the TOE's developers that have the highest privilege of the TOE and are able to modify the security behaviour of the TOE and Authorised Users, such as:

- Security behaviour of the TOE modifiable by the Super Administrator:
  - i. Modify login contact number and password;
  - ii. Password quality metrics;
  - iii. Payment channel maintenance; and
  - iv. Security of the connection required by the Trusted Path.
- Security behaviour of the Authorised User modifiable by the Super Administrator:
  - i. Role and permission;
  - ii. Merchant listing;
  - iii. Contracts;
  - iv. Transaction credentials;
  - v. Rate cards; and
  - vi. Read access to audit logs.

1.7.3.3 SECURITY AUDIT

Audit entries are generated for security related events on some of the TOE components (i.e., Authorised User's transactions through API, Super Administrator's modifications made to applets on the TOE, etc.). The audit logs are only accessible (i.e., read access) by the Super Administrator. The audit logs are stored on an external audit server where the communication is secured through TLS v1.2 and above.

The audit logs are not allowed to be modified and deleted.

1.7.3.4 TRUSTED PATH/ CHANNELS

The TOE is able to protect the user data from unauthorised modifications and disclosures by securing the communication channel with cryptography. The channels are secured between the user and the TOE such as:

1) Initial user authentication,
2) Transaction initiations from Authorised User to the TOE through API,
3) Transaction callbacks from the TOE to the Authorised User, and
4) Access to the TOE by Super Administrator and Authorised User.

1.7.3.5 CRYPTOGRAPHIC SUPPORT

The TOE is able to perform SHA-256 hashing cryptographic operations to ensure the authenticity of the transactions, through utilisation of the Merchant_code and Merchant_key within the pre-determined formulae.

These Merchant_code and Merchant_key are generated by the Super Administrator, and they will inform the specific Authorised User of their Merchant_code and Merchant_key through email.

The Merchant_code and Merchant_key are the main variables in differentiating between an authentic transaction and a forged transaction. The pre-determined formulae will ensure that only the original Authorised User can achieve the same hash as the Super Administrator.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

The ST and the TOE described are claimed as followed:

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 **conformant**.
- CC part 2 **conformant**.
- CC part 3 **conformant**.

2.2 ASSURANCE PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 1.

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

3 SECURITY OBJECTIVES

The purpose of the security objectives refers to high-level statements or goals that describe the desired security outcome for the TOE. Security objectives are defined to address the protection needs of the TOE and its operational environment. The security objective on the operational environment is to address the security concerns of the conditions and characteristics in which a TOE is intended to operate.

3.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Table 3: Operational Environment's Security Objectives

Security Objective	Description
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.USER	The Authorised User is not wilfully negligent or hostile and uses the software within compliance of the applied security policy and guidance.
OE.SUPADMIN	The Super Administrator is not careless, wilfully negligent or hostile, and administers the software within compliance of the applied security policy and guidance.
OE.TIMESTAMP	The platform where the TOE is installed shall have a reliable time source.

4 EXTENDED COMPONENTS DEFINITION

4.1 SECURITY OBJECTIVES REQUIREMENTS

This ST does not include extended Security Functional Requirements.

4.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

5 SECURITY REQUIREMENTS

This section provides 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, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

5.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (authorised admins)' and 'FDP_ACC.1(2) Subset access control (devices)'.

5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 4, summarized in Table 4 - Summary of Security Functional Requirements.

Table 4: Summary of Security Functional Requirements

Class	Identifier	Name
Identification and Authentication (FIA)	FIA_UID.2	User identification before any action
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_SOS.1	Verification of secrets
Security Management (FMT)	FMT_SMF.1(1)	Specification of Management Functions (Super Administrator)
	FMT_SMF.1(2)	Specification of Management Functions (Authorised User)
	FMT_SMR.1	Security roles
	FMT_MTD.1(1)	Management of TSF data (Super Administrator)
	FMT_MTD.1(2)	Management of TSF data (Authorised User)
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
Trusted Path/ Channels (FTP)	FTP_TRP.1	Trusted path
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic operation

5.2.1 IDENTIFICATION AND AUTHENTICATION (FIA)

5.2.1.1 FIA_UID.2: User identification before any action

Hierarchical to: 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~~ **Authorised User and Super Administrator.**

5.2.1.2 FIA_ATD.1: User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*email or mobile number, password*].

5.2.1.3 FIA_UAU.2: User authentication before any action

Hierarchical to: 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~~ **Authorised User and Super Administrator.**

5.2.1.4 FIA_SOS.1: Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that ~~secrets~~ **password** meets: [

i. *At least 1 special character;*
ii. *At least 1 uppercase alphabet;*
iii. *At least 1 lowercase alphabet;*
iv. *At least 1 numerical character; and*
v. *Minimum 8 and maximum 64 characters*].

5.2.2 SECURITY MANAGEMENT (FMT)

5.2.2.1 FMT_SMF.1(1): Specification of Management Functions (Super Administrator)

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions **for Super Administrator**: [*Refer to table 5 for the management functions for Super Administrator*].

Table 5: Management functions for Super Administrator.

Function	Description
Authorised User role management	To assign and remove role access for Authorised User.
Authorised User permission management	To assign and remove permission to (CRUD) for Authorised User to only have the capability to read their transaction statuses based on section 5.2.2.2, FMT_SMF.1(2).
Management of Authorised User's merchant listing, contracts, and transaction credentials	To assign and remove the Authorised User's merchant listing and contracts, which include the merchant_code and merchant_key unique to each Authorised User. The contract is required for the Authorised User to perform transaction initiations.
Management of Authorised User's rate cards	To assign and activate the rate cards for the contracts of the Authorised User. The rate card is required for the Authorised User to perform transaction initiation.
Assignation of Authorised User credentials	To assign an initial email or mobile number and password for Authorised User.
Payment channel maintenance	To assign and activate the contracts, rates, and connections to payment channels.
Read access to audit logs	To restrict the read access to audit logs only to Super Administrator.
Management of Super Administrator credentials	To allow the Super Administrator to modify their login contact number and password.

5.2.2.2 FMT_SMF.1(2): Specification of Management Functions (Authorised User)

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions **for Authorised User**: [*Modification of Authorised User's mobile number and password, using Merchant Access to accept the offered contracts, and to check the status of the following operations, which are current transactions, successful transactions, pending transactions, failed transactions, refunds, cancelled transactions*].

5.2.2.3 FMT_SMR.1: Security Roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Super Administrator, Authorised User*].

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

5.2.2.4 FMT_MTD.1(1): Management of TSF data (Super Administrator)

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [modify, delete, [*assign, activate, remove*]] the [*Authorised User role, Authorised User permission, Authorised User credentials, Authorised User's merchant listing, contracts and transaction credentials, Authorised User's rate cards, payment channel, read access to audit logs*] to [*Super Administrator*].

5.2.2.5 FMT_MTD.1(2): Management of TSF data (Authorised User)

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [modify] the [*Authorised User's mobile number, and password*]; **and the ability to** [*accept*] **the** [*offered contracts*]; **and the ability to** [query] **the** [*current transactions, successful transactions, pending transactions, failed transactions, refunds, cancelled transactions*] to [*Authorised User*].

5.2.3 SECURITY AUDIT (FAU)

5.2.3.1 FAU_GEN.1: Audit Data Generation

Hierarchical to: 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) [*Other operations such as:*

i. *CRUD actions performed by Super Administrator on the TOE, such as:*

a. *Create merchant;*
b. *Edit merchant;*
c. *Delete merchant;*
d. *Create contract;*
e. *Edit contract;*
f. *Remove contract;*
g. *Create rate card;*
h. *Remove rate card;*
i. *Create charge rate;*
j. *Edit charge rate;*
k. *Remove charge rate;*
l. *Adding rate;*
m. *Editing rate;*
n. *Deleting percentage rate; and*
o. *Deleting fixed rate.*

ii. *Transactions initiated by the Authorised User to the TOE through API, such as:*

a. *Transaction initiation; and*
b. *Initiate refund.*

iii. *Transactions initiated by the TOE to the Authorised User through API, such as:*

a. *Transaction callback;and*
b. *Refund callback*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) **For operation FAU_GEN.1.1 (c) (i):** Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event**; while for operation FAU_GEN.1.1 (c) (ii) and (iii): Transaction date time, merchant name, and the payment status**; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no additional information*].

APPLICATION NOTE: FPT_STM.1 Reliable time stamps is not provided by the TOE; it's provided by the underlying cloud platform's NTP server. Outlined in Section 3.1, OE.TIMESTAMP.

5.2.3.2 FAU_GEN.2: User Identity Association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.3.3 FAU_SAR.1: Audit Review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*Super Administrator*] with the capability to read: [

i. *CRUD actions performed by Super Administrator on the TOE, such as:*
   a. *Create merchant;*
   b. *Edit merchant;*
   c. *Delete merchant;*
   d. *Create contract;*
   e. *Edit contract;*
   f. *Remove contract;*
   g. *Create rate card;*
   h. *Remove rate card;*
   i. *Create charge rate;*
   j. *Edit charge rate;*
   k. *Remove charge rate;*
   l. *Adding rate;*
   m. *Editing rate;*
   n. *Deleting percentage rate; and*
   o. *Deleting fixed rate.*

ii. *Transactions initiated by the Authorised User to the TOE through API, such as:*
   a. *Transaction initiation; and*
   b. *Initiate refund.*

iii. *Transactions initiated by the TOE to the Authorised User through API, such as:*
   a. *Transaction callback;and*
   b. *Refund callback*]

from the audit records.

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

5.2.4 TRUSTED PATH/ CHANNELS (FTP)

5.2.4.1 FTP_TRP.1: Trusted Path

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] user that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [the TSF, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication*, [transaction initiations from Authorised User to the TOE through API, transaction callbacks from the TOE to the Authorised User, access to the TOE by Super Administrator and Authorised User]*].

5.2.5 CRYPTOGRAPHY SUPPORT (FCS)

5.2.5.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [*SHA-256*] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ **and message digest size [*256 bit*]** that meet the following: [*FIPS 180-4*].

APPLICATION NOTE: As the cryptographic hashing operations do not require cryptographic keys, hence the dependency do not apply.

5.3 DEPENDENCY RATIONALE

Table 6 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

Table 6: Security Functional requirement dependencies

SFR	Dependency	Dependency Satisfied	Rationale
FIA_UID.2	None	-	
FIA_ATD.1	None	-	
FIA_UAU.2	FIA_UID.1	✓	Dependency satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FIA_SOS.1	None	-	
FMT_SMF.1(1)	None	-	
FMT_SMF.1(2)	None	-	
FMT_SMR.1	FIA_UID.1	✓	Dependency satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FMT_MTD.1(1)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1(2)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FAU_GEN.1	FPT_STM.1	✓	This security function is not provided by the TOE; it's provided by the underlying cloud platform's NTP server. Outlined in section 3.1, OE.TIMESTAMP.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Dependency satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FAU_SAR.1	FAU_GEN.1	✓	
FTP_TRP.1	None	-	
FCS_COP.1	FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1	X	As the cryptographic hashing operations do not require cryptographic keys, hence the dependency do not apply
	FCS_CKM.4	X	

5.4 TOE SECURITY ASSURANCE REQUIREMENT

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 1 level of assurance, as defined in the CC Part 3. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

The assurance requirements are summarized in Table 7 for Security Assurance Requirements.

Table 7: Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 IDENTIFICATION AND AUTHENTICATION

The Super Administrator and Authorised Users must be identified and authenticated before granted access to any functionality of the TOE. This is to protect the TOE from illegitimate access and outside threats. They are required to insert email or mobile number and password to access the configuration management function of the TOE. The quality of password is also controlled by ensuring that it contains minimum 8 and maximum 64 characters which includes:

i. 1 special character;
ii. 1 uppercase alphabet;
iii. 1 lowercase alphabet; and
iv. 1 numerical character.

The initial email or mobile number and password are provided by Super Administrator to the Authorised User, and the Authorised User can change their own mobile number and password after that.

FIA_ATD.1 provides the security attributes mandatory for Authorised Users and Super Administrator to gain access to the TOE. FIA_UID.2 requires the Authorised Users and Super Administrator to be successfully identified before gaining access to the TOE functionality; while FIA_UAU.2 further enforces this security function through authentication. FIA_SOS.1 ensures that only quality passwords are allowed to be assigned.

TOE Security Functional Requirements addressed: FIA_UID.2, FIA_ATD.1, FIA_UAU.2, FIA_SOS.1

6.2 SECURITY MANAGEMENT

The TOE security management functionalities is provided by the TOE which allow Super Administrator the capability to assign an initial credential for the Authorised User. Also, they are allowed to manage Authorised User's access role, permission, merchant listing, contracts and transaction credentials and, rate cards through Merchant Admin; then manage the read access to audit logs through PGW Txn applet.

In addition, the Super Administrator is also able to assign, and activate payment channels through Payment Channel applet. Lastly, they are able to manage and modify their own login credentials which are their login mobile number and password.

The TOE security management, FMT_SMR.1 restricts authenticated user roles supported for the security management interface to the 'Super Administrator' and 'Authorised User' roles.

Moreover, FMT_SMF.1 provide the 'Super Administrator' with the highest privilege to manage TOE information related to 'Authorised User'.

For 'Authorised User', they are allowed to modify their own login contact number, and password through the "Profile Interface". However, they are required to be authorised by 'Super Administrator' to accept offered contracts and be allowed to check the status of the following operations, which are current transactions, successful transactions, pending transactions, failed transactions, refunds, cancelled transactions through Merchant Access interface.

Lastly, FMT_MTD.1 enforces that each security roles are only allowed the capabilities based on their roles and permission.

TOE Security Functional Requirements addressed: FMT_SMF.1(1,2), FMT_SMR.1, FMT_MTD.1(1,2)

6.3 SECURITY AUDIT

The TOE generate logs for security related events such as CRUD actions performed by Super Administrator on the TOE, which includes:

i. Create merchant;
ii. Edit merchant;
iii. Delete merchant;
iv. Create contract;
v. Edit contract;
vi. Remove contract;
vii. Create rate card;
viii. Remove rate card;
ix. Create charge rate;
x. Edit charge rate;
xi. Remove charge rate;
xii. Adding rate;
xiii. Editing rate;
xiv. Deleting percentage rate; and
xv. Deleting fixed rate.

And transactions initiated by the Authorised User to the TOE and transactions initiated by the TOE to the Authorised User through API, which includes:

xvi. Transaction initiation;
xvii. Transaction callback;
xviii. Initiate refund; and
xix. Refund callback.

To allow for log generation, the security function is provided by FAU_GEN.1.

To ensure that the generated logs are non-repudiated, the TOE is able to associate the generated logs with identity of the identified users. This is enforced by FAU_GEN.2. The content of the audit log includes, for CRUD actions performed by Super Administrator on the TOE:

i. Date and time of the event;
ii. Type of event;
iii. Subject identity; and
iv. The outcome (success or failure) of the event.

And the content of the audit log includes, for the transactions initiated by the Authorised User to the TOE and transactions initiated by the TOE to the Authorised User through API:

i. Transaction date time;
ii. Merchant name; and
iii. Payment status.

The generated logs are made easily interpreted, and to protect the security of generated logs, all accesses to the logs are prohibited and only allowed to 'Super Administrator', which is provided by FAU_SAR.1.

To ensure the integrity of the audit trail, there can only be read access to the audit logs, no user of the TOE can edit or delete the audit log. For 'Authorised Users', they do not have read access to the audit logs, only 'Super Administrator' are allowed to access the audit logs.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1

6.4 TRUSTED PATH/ CHANNELS

The TOE ensures that the communications between Super Administrator and Authorised Users to TOE are secure. This is employed with the utilisation of cryptography of the communication channel with TLS v1.2 and above.

The communication channel between the Super Administrator and Authorised Users, and the TOE is protected from inadvertent modification and disclosure whenever there are initial user authentication or transaction initiations, transaction initiations from the Authorised User to the TOE through API, transaction callbacks from the TOE to the Authorised User, and access to the TOE by Super Administrator and Authorised User. This security function is provided by FTP_TRP.1.

TOE Security Functional Requirements addressed: FTP_TRP.1

6.5 CRYPTOGRAPHIC SUPPORT

The TOE employs cryptographic hashing operations to prevent the transaction to the TOE from unauthorised modifications, this is to ensure that the Authorised User and the payment provider are able to have secure payment transactions seamlessly.

This is performed by accessing the API through web browser or command line interface, and with the Merchant_code and Merchant_key unique to each Authorised User with SHA-256 and appended together with the transaction initiation requests, which includes:

i. Get Payment Channel List;
ii. Transaction Initiation;
iii. Transaction Callback;
iv. Transaction Inquiry;
v. Initiate Refund;
vi. Refund Callback;
vii. Get Transaction Merchant Report; and
viii. Get Merchant Balance.

In addition, only if the hash submitted by the Authorised User matches the hash function generated by the TOE, will the transaction be completed. If the hashes do not match, the transaction will not be completed and the Authorised User will be presented with an error.

The operation of the SHA-256 hashing function is following the FIPS 180-4 standard.

The cryptographic hashing operations is provided by FCS_COP.1.

TOE Security Functional Requirements addressed: FCS_COP.1