23 APR 2021
Document Version 1.0

SECUREPAY SECURITY TARGET

SecurePay

For more information visit us at

www.securepay.my

Document management

Document identification

Document title	SecurePay Security Target
Document version	1.0
Document date	23-APR-2021
Release Authority	SecurePay Sdn bhd

Document history

Version	Date	Description
0.1	19-JUNE-2020	Initial Released
0.2	18-AUG-2020	Added TOE Summary Specification (TSS) in Section 6
0.3	01-MAR-2021	Updated Section 1, Section 4, Section 5 and Section 6
0.4	21-APR-2021	Updated Section 1
1.0	23-APR-2021	Final Released

Table of Contents

1 Security Target introduction

1.1 ST Reference

ST Title	SecurePay Security Target
ST Version	1.0
ST Date	23-APR-2021

1.2 TOE Reference

TOE Title	SecurePay Platform
TOE Version	4.9.1

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Terms	Descriptions
Authentication Data	It is information used to verify the claimed identity of a user.
Admin	Users that are allowed to perform both TOE configuration and monitoring application
Authorised User	Authorised user is a user that has the privilege (assigned by Admin) to perform either TOE monitoring only or both TOE configuration and monitoring
API	Application Programming Interface
DNSSEC	Domain name system security extensions
HTTPS	Hypertext Transfer Protocol Secure
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
SME	Small to Medium Enterprise
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TOE	Target of Evaluation
User data	Data created by and for the user, which does not affect the operation of the TSF.
User	TOE users which are Admin and Authorised User

1.5 TOE Overview

1.5.1 TOE Usage and Major Security Functions

The TOE is SecurePay Platform version 4.9.1. The TOE is a software platform as a service whilst installed, configured and deployed on an enterprise cloud environment. The TOE is used by corporate, SME's or merchants as a secure payment processing platform for their customers. Users also able to perform e-commerce transaction, sending bills, bulk payments, collections and statutory payments. The TOE is connected to various banks which facilitate same day processing, ensure data integrity, reduces processing discrepancies and faster response time. It is simple, robust, user friendly, scalable, secured and available 24x7.

Below are the primary features of the TOE:

- E-Commerce – Users able to use the TOE as an e-commerce portal and conduct business over the internet.
- Collection – Users able to create bill form and payment form for their customers
- Payment Processing – The TOE provides a secure payment processing platform and it is connected to various major banks in Malaysia
- API integration – Third-party developers able to use and access the TOE via API integrations

The following table highlights the range of security functions implemented by the TOE.

Security function	Description
Secure Payment	The TOE able to protect the user data and payment transaction from disclosure and modification by using HTTPS (TLS v1.2). Domain securepay.my is signed with DNSSEC. DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records
Identification and authentication	The TOE requires that each user is successfully identified and authenticated before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
Security Audit	The TOE generates audit records for security events. Admin and Authorised User has the ability to view and export the audit and transaction logs.

1.5.2 TOE Type

The TOE is a secure payment processing platform that enable users to perform e-commerce transaction, sending bills, bulk payments, collections and statutory payments. The TOE provides security functionality such as Secure Payment, Security Audit, Identification and Authentication and Security Management. The TOE can be categorised as *Other Devices and Systems* in accordance with the categories identified in the Common Criteria Portal (www.commoncriteriaportal.org).

1.5.3 Supporting Hardware, Software and/or Firmware

The underlying hardware and software that is used to support the TOE are:

Minimum System Requirements	
Hardware and OS requirements for the server that will be hosting the TOE	
Processor	Intel Core 2 Duo processor
Operating System	• Ubuntu 18.04 • FreeBSD 11
Memory (RAM)	1GB RAM
Storage	100GB of storage
Database	POSTGRESQL v12
Supporting Software	• Java 8 • Ruby 2.6 • Rails 6
Admin and Authorised User	
Web Browser	• Chrome 35 • Safari 10 • Firefox (Latest version) • Microsoft Edge • Microsoft Internet Explorer 11
PC System Requirement	• OS X 10.10 • Windows 7

1.6 TOE Description

1.6.1 Physical Scope of the TOE

A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

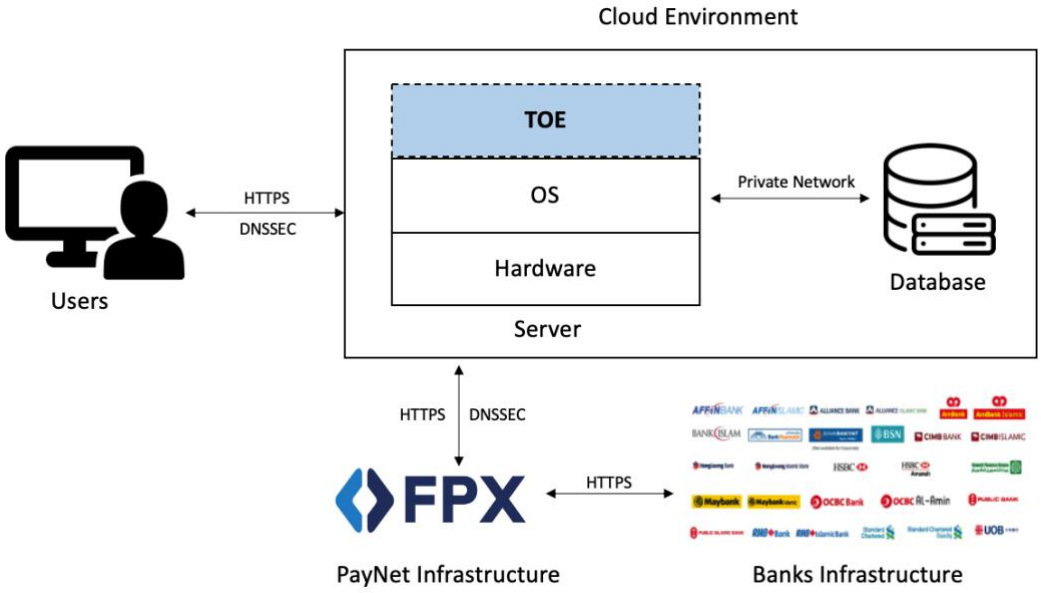

Figure 1 – TOE

The users are accessing the TOE via the internet connection. The primary access to the TOE are via a web application by browsing to https://www.securepay.my or via API (API URL for merchant integration is https://securepay.my/api). Merchant can access the information via API and received the json format response.

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

a) **Secure Payment.** The TOE can protect the user data and payment transaction from disclosure and modification by using HTTPS (TLS v1.2). Domain securepay.my is signed with DNSSEC. DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records

b) **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to key in a valid email and password in order to access the TOE. The acceptable minimum password length is 8-characters. The TOE checks the credentials presented by the user against the authentication information stored in the database.

c) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE restricts access to the management functions based on the role of the user. The TOE defines two security management roles: Admin and Authorised User. Refer below:

- Admin user has the ability to perform Announcements management, Users management, Accounts management, Banks management, Payments management, External Payments management, Plans management, Domains management, Admins management, Feedbacks management, View & Export Audits and Options management

- Authorised user has the ability to perform Collections management, Catalogs management, Stores management, Products management, Shippings management, Discounts management, Customers management, Accounts management and API management

d) **Security Audit.** The TOE generates audit records for security events. The Admin and authorised user have the ability to view and export the audit logs. The types of audit logs are:

- Payment Transaction Status

- Bill Transaction Status

- Settlements Transaction Status

- User Signed In/ Signed Out

- Changes on user account

2 Conformance Claim

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

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

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 5), April 2017
- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5), April 2017. The assurance level for this evaluation is Evaluation Assurance Level 2 (EAL2)

3 Security Problem Definition

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats:

Identifier	Threat statement
T.WEB_ATTACK	An unauthorized person may attempt to compromise the integrity, availability and confidentiality of enterprise information by performing web application attacks.
T.NOMGMT	An unauthorized person modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.UNAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.PSWD_CRACKING	An unauthorized person may take advantage of weak administrative passwords to gain privileged access to the TOE functions.
T.AUDREC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behaviour of TSF data without being detected.

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Identifier	Assumption statement
A.NOEVIL	It is assumed that the person who manages the TOE is not hostile and is competent.
A.NOTRST	The TOE can only be accessed by authorized users.
A.CLOUD	The cloud environment will provide a load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services in order to prevent the attacker from performing any malicious activity against the TOE and to prevent application failure
A.TIMESTAMP	The underlying operating system will have a reliable time source that the TOE can utilize for generating audit log timestamps.

4 Security Objectives

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Identifier	Objective statements
O.ACC_CTRL	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.
O.AUTH	The TOE must provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE.
O.MANAGE	The TOE must allow TOE Admin to effectively manage the TOE and users, while ensuring that appropriate controls are maintained over those functions.
O.PASSWORD	The TOE must ensure that the TOE user password has a minimum length of 8 characters.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes

4.3 Security Objectives for the Environment

Identifier	Objective statements
OE.ADMIN	The owners of the TOE must ensure that the Admin who manages the TOE is not hostile and is competent.
OE.AUTHDATA	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users

OE.CLOUD	The cloud environment shall provide load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services so that the TOE is protected from any malicious activity and application failure
OE.TIMESTAMP	The platform on which the TOE is installed shall have a reliable time source (ideally set via the internet using reliable sources, such as NIST) for the generation of timestamps for audit purposes.

4.4 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

OBJECTIVES / THREATS/ ASSUMPTIONS	T.WEB_ATTACK	T.NOMGMT	T.UNAUTH	T.PSWD_CRACKING	T.AUDREC	A.NOEVIL	A.NOTRST	A.CLOUD	A.TIMESTAMP
O.ACC_CTRL	✔	✔	✔						
O.AUTH		✔	✔						
O.MANAGE		✔							
O. PASSWORD				✔					
O.TOECOM	✔								
O.AUDREC					✔				
OE. ADMIN						✔			
OE.AUTHDATA			✔				✔		
OE.CLOUD								✔	
OE.TIMESTAMP									✔

4.4.1 TOE Security Objectives Rationale

The following table demonstrates that all security objectives for the TOE are trace back to the threats in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.WEB_ATTACK	O. ACC_CTRL	The objective ensures that only authenticated and authorized users can access the TOE functionality and protected application resources.
	O.TOECOM	The objectives ensures that the TOE protect the confidentiality of communications between distributed TOE components.
T.AUDREC	O.AUDREC	The objectives ensures that the TOE provide readable audit trail and a means to search the information contained in the audit trail.
T.NOMGMT	O.ACC_CTRL	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized admin to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.
	O.AUTH	The objective ensures that the TOE restricts access to the TOE objects to the authorized users
T.UNAUTH	O.ACC_CTRL	The objective ensures that the TOE restricts access to the TOE objects to the authorized users.
	O.AUTH	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	OE.AUTHDATA	The TOE must ensure to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE.
T.PSWD_CRACKING	O.PASSWORD	The TOE must ensure that all users adhere with the acceptable password policy (minimum 8 character) to avoid from unauthorised user taking advantage of weak password and gain unauthorised access to the TOE functions.

4.4.2 Environment Security Objectives Rationale

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Assumptions	Objective	Rationale
A.NOEVIL	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.NOTRST	OE.AUTHDATA	This objective ensures that only authorised user able to access the TOE and all access credentials, such as passwords or other authentication information are protected by that users
A.CLOUD	OE.CLOUD	This objective ensures that the cloud environment that the TOE resides provide a load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services in order to protect the TOE from any malicious activity and application failure
A.TIMESTAMP	OE.TIMESTAMP	This security objective has been established to directly address this assumption.

5 Security Requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions 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 a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security Functional Requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Identifier	Title
Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control
Identification and Authentication	
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Verification of Secret
FIA_UAU.1	Timing of Authentication
FIA_UAU.2	User authentication before any action
FIA_UAU.6	Re-Authentication
FIA_UID.2	User identification before any action
Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Trusted Path	
FTP_TRP.1	Trusted Path

5.2.2 FAU_GEN.1 Audit Data Generation

Hierarchical to:	No other components.
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) [**Specifically defined auditable events listed in the Notes section below**].
FAU_GEN1.2	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**].
Dependencies:	FPT.STM.1 Reliable time stamps
Notes:	Auditable events within the TOE: • Payment Transaction Status • Bill Transaction Status • Settlements Transaction Status • User Signed In/ Signed Out • Changes on user account

5.2.3 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**Admin and Authorised User**] with the capability to read [**all audit information**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.4 FDP_ACC.1 Subset Access Control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table 1 below**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	**Table 1 - Subject, Object and Operations for FDP_ACC.1**

Subject	Object	Operation

	Admin	Login	Login
		Dashboard	View
		Announcements	View, Create, Edit, Delete, Export
		Users	View, Edit, Export
		Accounts	View, Edit, Export
		Banks	View, Edit, Export
		Payments	View, Export
		External Payments	View, Export
		Plans	View, Create, Edit, Delete, Export
		Domains	View, Export
		Admins	View, Create, Edit, Export
		Feedbacks	View, Edit, Delete, Export
		Audits	View, Export
		Options	View, Edit
	Authorised User	Login	Login
		Dashboard	View, Export
		Collections	View, Create, Edit, Stop, Delete, Export
		Catalogs	View, Create, Edit, Delete, Export
		Stores > List	View, Create, Edit, Delete, Export
		Stores > Pages	View, Create, Edit, Delete, Export
		Products > List	View, Create, Edit, Delete, Export
		Products > Categories	View, Create, Edit, Delete, Export

		Shippings > Shipments	View, Export
		Shippings > Shipping profiles	View, Create, Edit, Delete, Export
		Discounts	View, Create, Edit, Delete, Export
		Customers	View, Create, Edit, Delete, Export
		Account > Info	View, Edit
		Account > Domains	View, Create, Delete, Export
		Account > Reports	View
		Account > Subscription	View, Upgrade Plan, Export
		Account > Audits	View, Export
		API	View, Create, Edit, Export

5.2.5 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**as listed in the Table 1**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) If the User is successfully authenticated accordingly, then access is granted based on privilege allocated;** **b) If the User is not authenticated successfully, therefore, access permission is denied**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

Notes:	None.

5.2.6 FIA_ATD.1 User Attribute Definition

Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a. Email,** **b. Password** **c. PIN Code**].
Dependencies:	No dependencies
Notes:	None.

5.2.7 FIA_SOS.1 Verification of Secret

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet **[a minimum length of 8-characters]**
Dependencies:	No dependencies
Notes:	None.

5.2.8 FIA_UAU.1 Timing of Authentication

Hierarchical to:	No other components.
FIA_UAU.1.1	The TSF shall allow **[initiation of the activate account]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.9 FIA_UAU.2 User Authentication Before Any Action

Hierarchical to:	FIA_UAU.1 Timing of authentication

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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.10 FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [**no user interaction has been detected over 30 minutes**].
Dependencies:	No dependencies
Notes:	None.

5.2.11 FIA_UID.2 User Identification Before Any Action

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies.
Notes:	None.

5.2.12 FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify, delete]*** the security attributes [**Admin Account, TOE Configuration, Users Account**] to [**Admin and Authorised User**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.13 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to:	No other components
FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP
FMT_MSA.3.2	The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.14 FMT_MTD.1 Management of TSF Data

Hierarchical to:	No other components
FMT_MTD.1.1	The TSF shall restrict the ability to [***change***] the [**User Password/Admin Password**] to [**Authorised User and Admin**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.15 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**all management functions stated in Section 5.2.4 - Table 1**]
Dependencies:	No dependencies.
Notes:	None.

5.2.16 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Authorised User and Admin**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

Notes:	None.

5.2.17 FTP_TRP.1 Trusted Path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].
FTP_TRP.1.2	The TSF shall permit [***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***, [**and all further communication after authentication**]].
Dependencies:	No dependencies
Notes:	None.

5.3 TOE Security Assurance Requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours. 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). EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

Below are the assurance class and assurance components for EAL2:

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description

Assurance class	Assurance components
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	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_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Security Requirements Rationale

5.4.1 Dependency Rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FAU.GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform. This has been addressed in Section 3.4 by A.TIMESTAMP.
FAU.SAR.1	FAU.GEN.1 Audit data generation	FAU.GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static Attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.6	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_TRP.1	No dependencies	N/A

5.4.2 Mapping of SFRs to Security Objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.ACC_CONTROL	FDP_ACC.1	The requirement helps meet the objective by identifying the objects and users subjected to the access control policy.
	FDP_ACF.1	The requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy.
O.AUTH	FIA_UAU.1	The requirement helps meet the objective by allowing the users to change password and activate account before the user is authenticated. It also helps meet the objective by authenticating the users before any TSF mediated actions.
	FIA_ATD.1	The requirement helps meet the objective by maintaining the email, passwords and PIN code
	FIA_UAU.2	The requirement helps meet the objective by authenticating the users before any TSF mediated actions.
	FIA_UAU.6	The requirement helps meet the objective by re-authenticating the users after 30 minutes inactive user interaction.
	FIA_UID.2	The requirement helps meet the objective by identifying the users before any TSF mediated actions.
O.MANAGE	FMT_MSA.1	The requirement helps meet the objective by restricting the ability to modify user permission group to Authorised User and Admin
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP
	FMT_MTD.1	The requirement helps meet the objective by allowing only users/authorised user and admin to change user password/admin password
	FMT_SMF.1	The requirement helps meet the objective by specifying the management functions of the TOE. Refer to Table 1 for list of management function.
	FMT_SMR.1	The requirement helps meet the objective by maintaining Admin and manages multiple user roles.
O.PASSWORD	FIA_SOS.1	The requirement helps meet the objective by providing a minimum length of 8 characters.

Security objective	Mapped SFRs	Rationale
O.TOECOM	FTP.TRP.1	The requirement helps meet the objective by protecting the traffic transmitted from disclosure and modification
O.AUDREC	FAU_GEN.1	The requirement helps meet the objective by outlining what events must be audited
	FAU_SAR.1	The requirement helps meet the objective by ensuring that users are identified to the TOE

6 TOE Summary Specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Security Audit;
- Identification and Authentication;
- Security Management; and
- Secure Payment

6.2 Security Audit

The TOE will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the transaction event) for the following auditable events (**FAU_GEN.1**):

- Payment Transaction Status
- Bill Transaction Status
- Settlements Transaction Status
- User Signed In/ Signed Out
- Changes on user account

The TOE's Admin and Authorised user have the capability to view and export these audit records via the web interface (**FAU_SAR.1**). Timestamps for the server are generated for audit logs by utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

6.3 Identification and Authentication

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (**FDP_ACC.1**). All TOE users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

The TOE maintains two types of users which are Admin and Authorised user (**FMT_SMR.1**). These users may access the TOE via the web interface that the platform provides. During the user registration, user need to register a valid email, password and PIN no in order to access the TOE (**FIA_ATD.1**). The acceptable minimum password length is 8 characters (**FIA_SOS.1).** Admin and Authorised user also need to activate their account after registration (FIA_UAU.1). Admin and Authorised user must be authenticated to the TOE prior performing any TOE functions by entering a valid email and password (**FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FDP_ACF.1**). If there is no user interaction over 30 minutes, all users will be directed to the login page and need to re-authenticate (**FIA_UAU.6)**

6.4 Security Management

The TOE provides a suite of management functions only to Admin and Authorised user. These functions allow for the configuration of TOE to suit the environment in which it is deployed. Additionally, management roles may perform the following tasks (**FMT_SMF.1, FMT_MTD.1, FMT_MSA.1 and FMT_MSA.3**):

User Role	Menu / Function	Operation
Admin	Login	Login
	Dashboard	View
	Announcements	View, Create, Edit, Delete, Export
	Users	View, Edit, Export
	Accounts	View, Edit, Export
	Banks	View, Edit, Export
	Payments	View, Export
	External Payments	View, Export
	Plans	View, Create, Edit, Delete, Export
	Domains	View, Export
	Admins	View, Create, Edit, Export
	Feedbacks	View, Edit, Delete, Export
	Audits	View, Export
	Options	View, Edit
Authorised User	Login	Login

	Dashboard	View, Export
	Collections	View, Create, Edit, Stop, Delete, Export
	Catalogs	View, Create, Edit, Delete, Export
	Stores > List	View, Create, Edit, Delete, Export
	Stores > Pages	View, Create, Edit, Delete, Export
	Products > List	View, Create, Edit, Delete, Export
	Products > Categories	View, Create, Edit, Delete, Export
	Shippings > Shipments	View, Export
	Shippings > Shipping profiles	View, Create, Edit, Delete, Export
	Discounts	View, Create, Edit, Delete, Export
	Customers	View, Create, Edit, Delete, Export
	Account > Info	View, Edit
	Account > Domains	View, Create, Delete, Export
	Account > Reports	View
	Account > Subscription	View, Upgrade Plan, Export
	Account > Audits	View, Export
	API	View, Create, Edit, Export

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (**FDP_ACC.1 and FDP_ACF.1**).

6.5 Secure Payment

When a user accesses the TOE on their browser, by typing in the website address, the TOE will initiate a secure channel establishment with the user's browser (**FTP_TRP.1**). The TOE implements Transport Layer Security (TLS v1.2) secure communication protocol. The TOE also protect the user data and payment transaction from disclosure and modification by using HTTPS (TLS v1.2). The domain securepay.my is registered securely and is signed with DNSSEC. DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records