Ref: Guardian-CCS (BSA)-ST-1.1

Guardian-CCS Blockchain Secure Authentication (BSA) Security Target

DOCUMENT VERSION	**1.1**
DOCUMENT DATE	**05 AUGUST 2022**

FNS (M) Sdn Bhd

Office Suite 5.01, Level 5, Menara LGB,

No.1, Jalan Wan Kadir, Taman Tun Dr Ismail,

60000 Kuala Lumpur, Malaysia

Tel: +603-7732 6027

Website: https://fnsmalaysia.com/

Prepared by:

DOCUMENT REVISION HISTORY

Version No.	Published Date	Description of changes	Author
0.1	15 November 2021	First Release	Reyes Foong and Celine Deong
0.2	7 April 2022	EOR Amendments	Reyes Foong and Celine Deong
0.3	29 April 2022	EOR Amendments	Reyes Foong and Celine Deong
0.4	12 July 2022	EOR Amendments	Reyes Foong and Celine Deong
1.0	22 July 2022	Document Finalize	Reyes Foong and Celine Deong
1.1	05 August 2022	Amendments on Section 1.6.2 to include “TOE Access”	Reyes Foong and Celine Deong

TABLE OF CONTENTS

1 Security Target Introduction

1.1 Security Target Reference

Security Target Title:	Guardian-CCS Blockchain Secure Authentication (BSA) Security Target
Security Target Version:	1.1
Security Target Date:	05 August 2022

Table 1 - ST Reference

1.2 TOE Reference

	TOE NAME:	**TOE VERSION:**
TOE Name & Version:	Guardian-CCS Blockchain Secure Authentication (BSA)	v1.0.24
TOE Initial:	Guardian-CCS (BSA)	

Table 2 - TOE Reference

1.3 Terminology and Acronyms

Acronyms	Full Name
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
BSA	Blockchain Secure Authentication
MFA	Multi-Factor Authentication
QR	Quick Response
TOTP	Time-based One-Time Password
OTP	One-Time Password
API	Application Programming Interface
CCS	Cross Certification Solution

Table 3 – Terminology and Acronyms

1.4 Product Overview

Guardian-CCS Blockchain Secure Authentication (BSA) is an identity authentication platform that relies on patented hybrid blockchain technology to provide an unbreakable, fast and easy-to-use solution to meet all security needs. Users is allowed to perform one-click authentication on their mobile device to login into respective application with presence of valid User ID and TOE. Besides that, multi-factor authentication is required to initiate for identification process. TOE for this evaluation will only focus on the API engine that used by Guardian-CSS BSA to identify and authenticate user.

The BSA Server consist of the following components:

a) Web Server

b) Guardian-CSS BSA (API)

c) Database

The component that is part of the scope of TOE is Guardian-CSS BSA API. Guardian-CSS BSA API is utilized to perform the following process:

a) Create or Delete Authentication Key

b) Node Verification

c) Device Verification

d) Encrypt and Hash Data

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

Guardian-CSS BSA is the product designed by FNS (Malaysia) Sdn Bhd. This product offer end users to use their own mobile device to perform a one-click passwordless authentication to verify their credentials, only username or user ID is required during authentication and identification process. BSA Server consists of three (3) components which is the web server, Guardian-CSS BSA (API) and database.

In traditional implementations, clients or customers will need to have a set of credentials (e.g. usernames and password) to login into the systems and and this may lead to a burden for customers or clients to remember their password. Losing the password would require customers to go through the hassle of resetting or retrieval of password. This also can lead to unnecessary exposure to security leakages if credentials are used repeatedly. Unauthorized users may obtain access to the

system with the stolen credentials from legitimate users. This TOE can prevent account takeovers and credential stuffing attacks by implementing passwordless authentication.

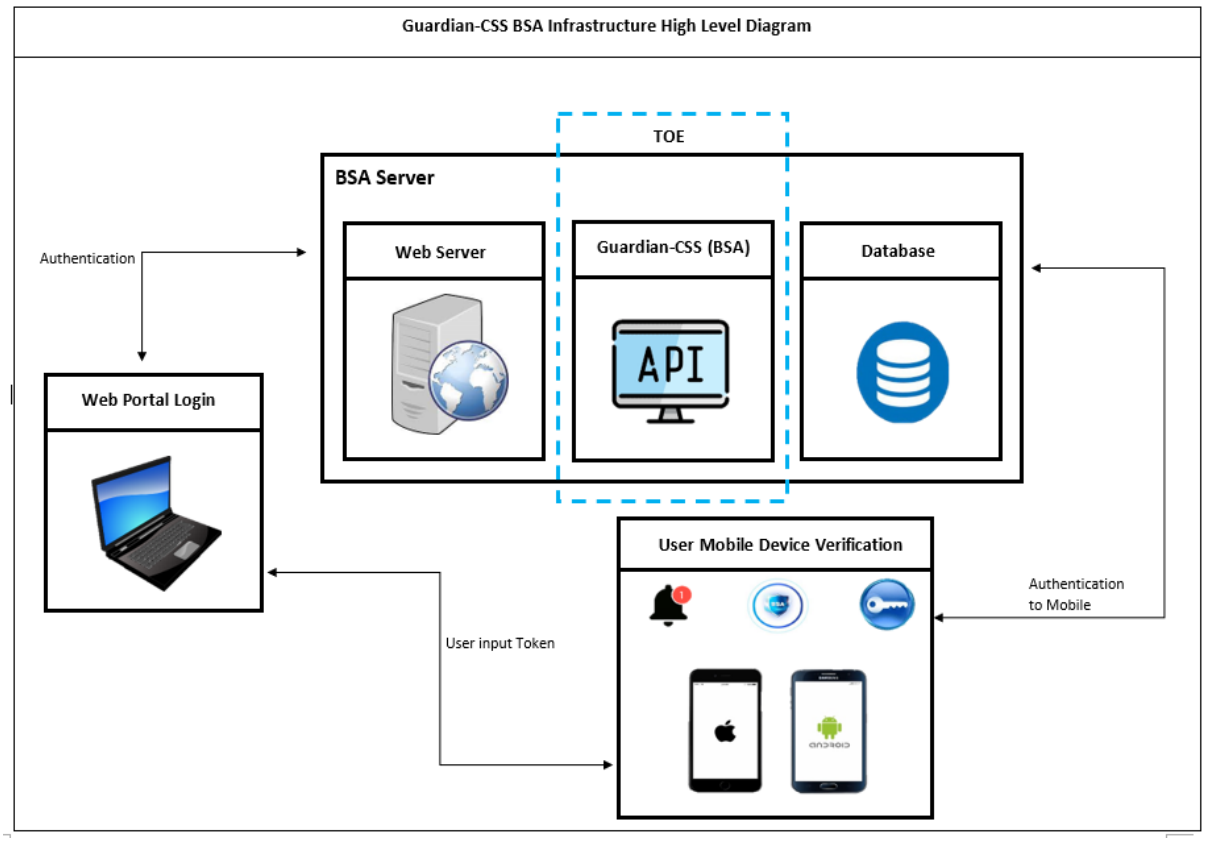

Figure 1 – Guardian-CSS BSA High Level Diagram

Guardian-CSS BSA offers Multi-factor Authentication (MFA) to the users while authenticating through the mobile application. Guardian-CSS BSA secure user credentials without required to be login using password.

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

- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

1.5.2 TOE Type

Guardian-CSS BSA is a privileged Access Management (PAM) system that offer user to perform authentication without password. TOE for this evaluation will only focus on the API engine that used by Guardian-CSS BSA to identify and authenticate user.

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

The following figure shows the high-level architecture diagram of the operational environment of the TOE.

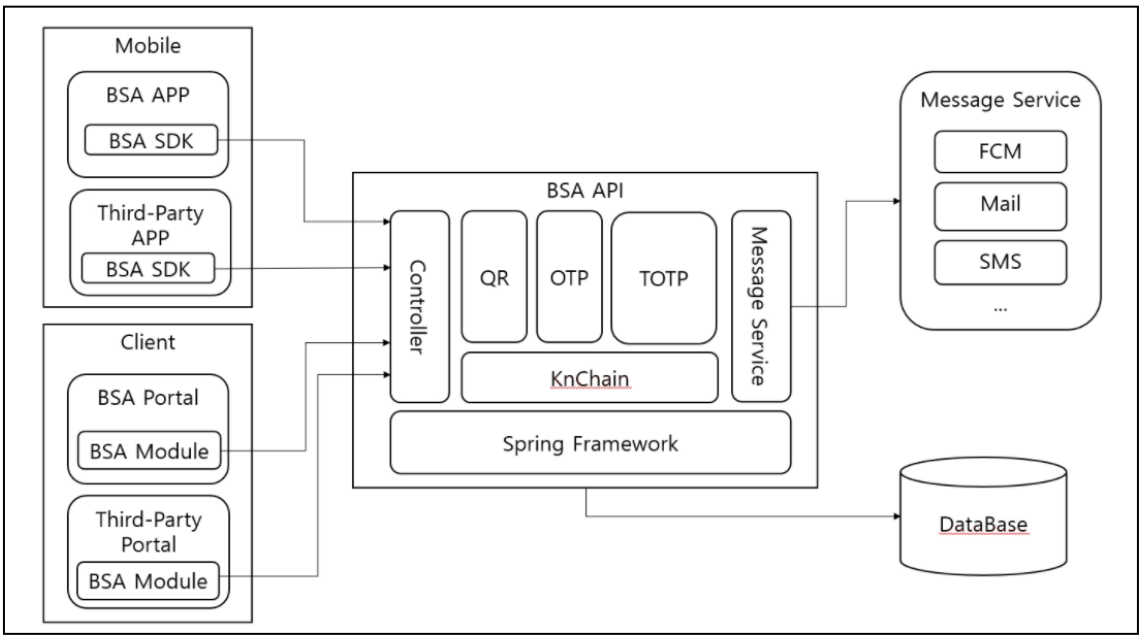

Figure 2 - TOE Typical operational environment

The supporting components for the TOE are as follow:

a) Mobile (Mobile Application)

Mobile require a BSA application to request and retrieves the token via BSA API during the authentication process. Minimum mobile operating system support for Android 6 or above and iOS 13 or above.

b) Client (Web Portal)

Client allows users to access to the web portal (BSA dashboard). User ID is inserted via the web portal, and this will invoke the BSA API to initiate the identification process. The web portal also provides user management capabilities for admin.

c) Message Service

Message Service allow the API endpoint to trigger E-mail or SMS with OTP to the user which the OTP is require during onboarding and identification process.

d) Database

Database is a storage to store all the user account and device attributes.

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 the following components:

a) Controller – Connector to communicate with Web and Mobile Application.

b) QR – User Identification with QR Code.

c) OTP – User Identification with One Time Password.

d) TOTP – User Identification with Time-based One-Time Password.

e) Message Service – Used to deliver OTP to the user during during onboarding and identification process.

f) KnChain – Core API engine for BSA product.

g) Spring Framework – An application framework and inversion of control container for the Java platform application.

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

User data and credentials are protected by ensuring that specific users within the system are assigned with specific roles and privilege access to the TOE. The accessibility to the web portal is protected based on the access control policy.

The TOE can identify and authenticate the credentials of users before allowing the users to access the web portal. TOE will identify the user based on the User ID and will request the user to proceed with the authentication process via QR Scanning, OTP or TOTP from the users' mobile device. Users who are unable to be authenticated are not allowed to access the web portal.

1.6.2.2 Identification and Authentication

TOE requires users to input a valid User ID for the TOE to initiate the identification process. Users required multi-factor authentication to access the BSA mobile application and proceed to authentication process via QR scanning, OTP or TOTP. The TOE shall then authenticate the users by

their respective User ID along with the random selection of user attributes in the database which will generate a token for authentication. Each user will have a unique User ID which cannot be modified after onboarding process.

1.6.2.3 Security Management

FNS Manager (Super Admin) has access to all TOE features, that application to be managed through web portal hosted by FNS. FNS Manager (Super Admin) has the full access rights, role and privileges to the TOE. FNS Manager (Super Admin) could Create, View, Edit, or Delete user data via the web portal. Nonetheless, there are another 3 roles that are allows to access the TOE features, which is: Vendor Manager could View, Edit, or Delete user data via the web portal, Client Manager could View user data via the web portal and User could view their own information. These roles are defined with limited access to the TOE features compared to the TOE FNS Manager (super admin).

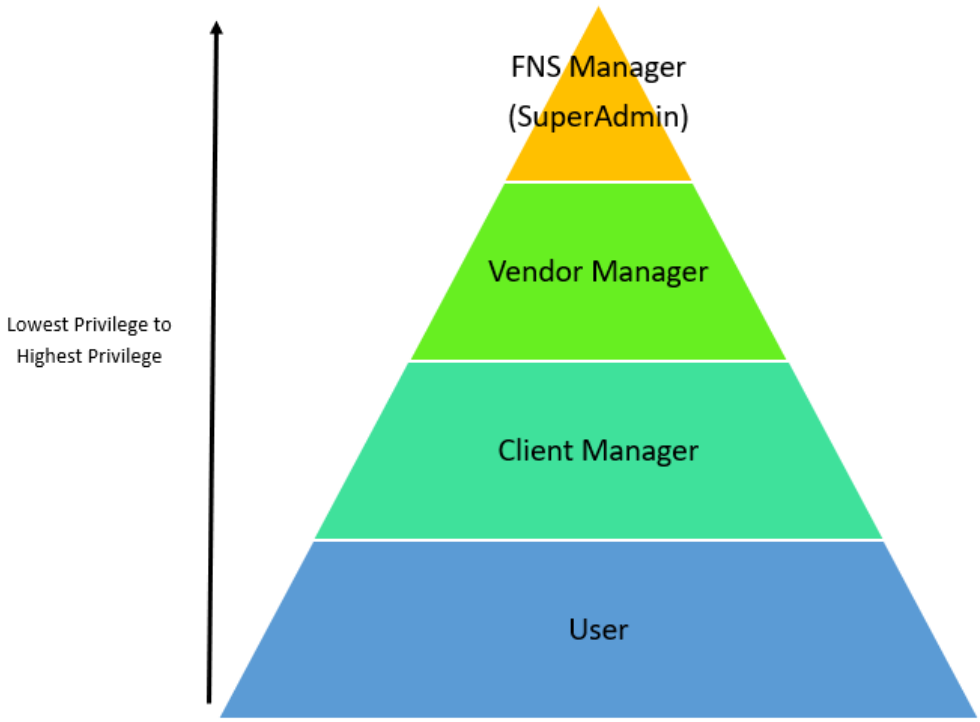

Figure 3 – Hierarchy of TOE Management

1.6.2.4 TOE Access

Users are allowed to check on previous successful or unsuccessful authentication attempt through the TOE. Access history is being stored in the server thus user's is not allowed to tamper or remove the access logs. Such action allows the users to review past authentication history to identify if users identify is being misused.

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.ADMIN	Authorized super administrators are non-hostile and follow guidance; however, they are not free from error.
A.IDLE	The TOE environment must be protected. Session timeout is imposed in client web application and mobile application for 90 seconds. It require 2 Factor Authentication before able to generate OTP.
A.HISTORY	The TOE shall allow the users to review authentication history to identify for misuse of their user account for identification and authentication.

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.SESSIONHIJACK	An unauthorized person may obtain access to the TOE while in idle mode.
T.CONFIG	An unauthorized person may read and modify security TOE functions and configuration data.
T.ACCESS	An unauthorized person may abuse victim identity to authenticate into linked application.

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.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data.
O.ACCESS	TOE shall ensure users are allowed to review authentication history.

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.ADMIN	Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.
OE.IDLE	The TOE environment shall be secured during idle. Default idle is configured as 90 seconds.

Table 8: Security Objectives for the Operational Environment

4.2.1 Security Objectives Rationale

Table 9 maps security objectives to threats and assumptions. 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.SESSIONHIJACK	T.CONFIG	T.ACCESS	A.USER	A.ADMIN	A.IDLE	A.HISTORY
O.DATA	✔							
O.CONFIG			✔					
O.ACCESS				✔				✔
OE.USER					✔			
OE.ADMIN						✔		
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_ATD.1	User attributes definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_SMF.1	Specification of management functions
Class FTA: TOE Access	
FTA_TAH 1	TOE access history

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 [**Table 11**].

Subjects	Objects	Operations
FNS Manager	FNS Manager perform actions such as viewing, modifying, and deleting the data of its user in the presence of TOE.	FNS Manager (Super Admin) can add, change, and delete any of the data of its vendor, client and user.
Vendor Manager	Vendor Manager perform actions such as viewing, modifying, and deleting the data of its client manager data in the presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Vendor manager can block, delete and withdraw their client user's access. Vendor manager privilege can be assigned only by FNS Manager.
Client Manager	Client Manager perform actions such as viewing, modifying, and deleting the data of its own user data in the presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Client manager can block, delete and withdraw its own user. Client manager privilege can be assigned by FNS Manager and its Vendor Manager.

User	Users perform login with valid user ID and presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Not able to view or manage client information. Not able to view or manage other user information. All the above roles can manage user.

Table 11: Subjects, Objects, Operations for FDP_ACC.1

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
Guardian – CCS (BSA)	Serve as an authentication mechanism.	Guardian – CCS (BSA) is required for user authentication purpose.
Credentials (User ID)	Serve as an identification attribute.	User ID is required for user identification purpose.

]

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
Guardian – CCS (BSA)	Serve as an authentication mechanism.	Permission is granted to Guardian – CCS (BSA) for authentication process to

Credentials (User ID)	Serve as an identification attribute.	be initiated when valid User ID is present.

]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subject to objects based on the following additional rules: [**none**]

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

Subject	Object Controlled	Rules
Guardian – CCS (BSA)	Serve as an authentication mechanism.	Guardian – CCS (BSA) shall not send notifications to the user mobile device when invalid user ID is present.
Credentials (User ID)	Serve as an identification attribute.	

].

6.2.2 Class FIA: Identification and Authentication

FIA_ATD.1 User attributes definition

Hierarchical No other components

Dependencies No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) Name;

b) Phone Number;

c) Email;

d) User ID;

e) Device Unique ID;

f) OS Version;

]

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_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 FMT: Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical No other components

Dependencies No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

Subjects	Objects	Operations
FNS Manager	FNS Manager perform actions such as viewing, modifying, and deleting the data of its user in the presence of TOE.	FNS Manager (Super Admin) can add, change, and delete any of the data of its vendor, client and user.
Vendor Manager	Vendor Manager perform actions such as viewing, modifying, and deleting the data of	User can on-board, view its own Auth History, Event and unlink site. Vendor manager can block,

	its client manager data in the presence of TOE.	delete and withdraw their client user's access. Vendor manager privilege can be assigned only by FNS Manager.
Client Manager	Client Manager perform actions such as viewing, modifying, and deleting the data of its own user data in the presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Client manager can block, delete and withdraw its own user. Client manager privilege can be assigned by FNS Manager and its Vendor Manager.
User	Users perform login with valid user ID and presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Not able to view or manage client information. Not able to view or manage other user information. All the above roles can manage user.

6.2.4 Class FTA: TOE Access

FTA_TAH.1 TOE Access History

Hierarchical	No other components
Dependencies	No dependencies
FTA_TAH 1.1	Upon successful session establishment, the TSF shall display the [**Date, Time, Linked Application]** of the last successful session establishment to the user.
FTA_TAH 1.2	Upon successful session establishment, the TSF shall display the [**Date, Time, Linked Application**] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.
FTA_TAH 1.3	The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

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 12: Security Assurance Requirements for EAL2

7 TOE Summary Specifications

TOE addressed the security functional requirements as following:

7.1 User Data Protection

User data and credentials are protected by ensuring that specific users within the system are assigned with specific roles and privilege access to the web portal. The accessibility to the web portal is protected based on the access control policy.

The TOE can identify and authenticate the credentials of users before allowing the users to access the web portal. The TOE will identify the user based on the User ID and will request the user to proceed with the authentication process via QR Scanning, OTP or TOTP from the users' mobile device. Users who are unable to be authenticated are not allowed to access the web portal.

The details of access control policy are as following:

Subjects	Objects	Operations
FNS Manager	FNS Manager perform actions such as viewing, modifying, and deleting the data of its user in the presence of TOE.	FNS Manager (Super Admin) can add, change, and delete any of the data of its vendor, client and user.
Vendor Manager	Vendor Manager perform actions such as viewing, modifying, and deleting the data of its client manager data in the presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Vendor manager can block, delete and withdraw their client user's access. Vendor manager privilege can be assigned only by FNS Manager.
Client Manager	Client Manager perform actions such as viewing, modifying, and deleting the data of its own user data in the presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Client manager can block, delete and withdraw its own user. Client manager privilege can be assigned by FNS Manager and its Vendor Manager.
User	Users perform login with valid user ID and presence of TOE.	User can on-board, view its own Auth History, Event and unlink site. Not able to view or manage client information. Not able to view or manage other user information. All the above roles can manage user.

Relevant SFR: FDP_ACC.1, FDP_ACF.1

7.2 Identification and Authentication

TOE requires users to input a valid User ID for the TOE to initiate the identification process. Users required multi-factor authentication to access the BSA mobile application and proceed to authentication process via QR scanning, OTP or TOTP. The TOE shall then authenticate the users by their respective User ID along with the random selection of user attributes in the database which will generate a token for authentication. Each user will have a unique User ID which cannot be modified after onboarding process. Each user will have the following security attributes:

a) **Name;**

b) **Phone Number;**

c) **Email;**

d) **User ID;**

e) **Device Unique ID;**

f) **OS Version;**

In aspects of access control, each authentication sessions are configurable through system backend. Default idle session shall remain for 90 seconds. Users will have to retrieve the authentication notification for the QR code, TOTP or OTP again. Session timeout can be configured from API backend configuration file.

Relevant SFR: FIA_ATD.1, FIA_UAU.2, FIA_UID.2

7.3 Security Management

TOE FNS Manager (super admin) has access to all TOE features, that application to be managed through web portal hosted by TOE. Super admin has the full access rights, role and privileges to the TOE. FNS Manager (Super Admin) can add, change, and delete any of the data of its vendor, client and user. Nonetheless, there are another 3 roles that are allows to access the TOE features, which is: Vendor Manager, Client Manager and User. These roles are defined with limited access to the TOE features compared to the TOE FNS Manager (super admin).

Relevant SFR: FMT_SMF.1

7.4 TOE Access

Users are allowed to check on previous successful or unsuccessful authentication attempt through the TOE. Access history is being stored in the server thus user's is not allowed to tamper and also remove the access logs.

Relevant SFR: FTA_TAH.1, FTA_TAH.2, FTA_TAH.3

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 authorized person may successfully access 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 unauthorized data access to happened without valid user ID.
T.CONFIG An unauthorized person may read and modify security TOE functions and configuration data.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data.	This security objective counters threat because TOE will prevent unauthorized person to access web portal functions and configuration data. Only TOE authorized administrator shall have access to the web portal.
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.	This security objective counters threat because TOE environment shall prevent unauthorized person using user's idle session to obtain unauthorized access to web portal.
T.ACCESS An unauthorized person may abuse victim identity to authenticate into linked application.	**O.ACCESS** TOE shall ensure users are allowed to review authentication history.	This security objective counters threat because TOE allows user to review past authentication history to identify if users identify is being misuse before.

Table 13 - 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.	This 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 14 - 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 with 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.	This 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.ADMIN Authorized super administrators shall be non-hostile and follow guidance; however, they are not free from error.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective counters assumption because authorized TOE administrator shall be non-hostile, assigned by organization and follows guidance documentation accordingly. However, TOE administrator is not free from human error and mistakes.
A.IDLE The TOE environment must be protected. Session timeout is imposed in client web application and mobile application require 2 Factor Authentication before able to generate OTP.	**OE.IDLE** The TOE environment shall be secured during idle.	This security objective counters assumption because TOE environment shall be protected during idles with QR code, TOTP, or OTP.
A.HISTORY The TOE shall allow the users to review authentication history to identify for misuse of their user account for identification and authentication.	**O.ACCESS** TOE shall ensure users are allowed to review access history.	This security objective counters assumption because users is allowed to review past authentication history to identify for account misuse.

Table 15 - 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	This SFR specify that each user will have privilege to access and use web portal functions-based roles.
	FDP_ACF.1	This SFR requires the TOE to perform identification with unique user ID and multi-factor authentication through the BSA mobile application before legitimate users are given access to the web portal.
	FIA_ATD.1	This SFR requires user security attributes to be used during identification and authentication process. This security attributes will be randomly selected to generate a token for authentication.
	FIA_UAU.2	This SFR require each user to be successfully authenticated through TOE before being allowed to perform any actions on web portal functions and configuration data.
	FIA_UID.2	This SFR require each user to be successfully identified through TOE before being allowed to perform any actions on web portal functions and configuration data.
O.CONFIG TOE shall prevent unauthorized person to access the TOE functions and configuration data.	FMT_SMF.1	This SFR identify management functions that are available in web portal, that are managed by administrator and other roles in TOE.
O.ACCESS TOE shall ensure users are allowed to review access history.	FTA_TAH.1	This SFR allow user's to review past successful and unsuccessful attempt of authentication on linked application.

Table 16 - 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	Partially	FMT_MSA.3 is not applicable as no modifications of user security attribute are allowed.
FIA_ATD.1	-	-	-
FIA_UAU.2	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FIA_UID.2	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FMT_SMF.1	-	-	-
FTA_TAH.1	-	-	-

Table 17 - SFR Dependencies

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