Fortix Security Suite v1.17.1

Security Target

Document Version: 0.5

Document Date: 04 Apr 2019

Blue Fortress Sdn. Bhd
Sw-05-12, Jalan Teknologi, Kota Damansara, 47810 Petaling Jaya, Selangor
+03-6150 4522

Document Revision History

Version	Date	Description	Author
0.1	06 Aug 2018	Initial draft.	Wan Roshaimi
0.2	09 Aug 2018	Amendment on Introduction and numbering.	Wan Roshaimi
0.3	11 Oct 2018	Amendment on the issue that raise by CB during meeting.	Wan Roshaimi
0.4	06 Dec 2018	Amendment on AUDITREC issue that raise by CB during meeting	Wan Roshaimi
0.5	04 Apr 2018	Update on FIA_UAU.6, FMT_MTD.1, FDP_ACC.1, FDP_ACF.1, Section 10.2, Section 10.3, removing the ability of system operator to have any operations related to user management.	Wan Roshaimi

Table of Contents

1 Document Overview

This document is the Security Target (ST) for the Fortix Security Suite. The ST is designed to meet the requirements of the CC, and provides a baseline for the subsequent phases of Target of Evaluation (TOE) evaluation works.

2 Security Target Introduction

2.1 Security Target Reference

Document Title	:	Fortix Security Suite Security Target
Document Version	:	0.5
Document Date	:	04-Apr-19

2.2 TOE Reference

TOE Name	:	Fortix Security Suite
TOE Version	:	1.17.1
TOE Initial	:	Fortix

2.3 Terminology and Acronym

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
PIN	Personal Identification Number

E2EE	End-to-End Encryption
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
KCV	Key Confirmation Value
ACP	Access Control Policy
SEP	Secure ePin Policy
CAPTCHA	Completely Automated Public Turing test to tell Computers and Human Apart

2.4 Reference

CCPart1 Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

CCPart2 Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

CCPart3 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

CEM Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

3 TOE Overview

3.1 TOE Operational Usage

Fortix Security Suite or the TOE consists the Secure ePin module and WebSeal module which is hosted in SafeNet Java Hardware Security Module (HSM).

The Secure ePin module provides PIN delivery using split-channel delivery regardless of customers' locations at any time. This service is typically used for delivering credit cards PIN or sensitive authentication PIN. Customers will receive their PINs that are embedded inside an encrypted PDF document via their emails along with a SMS notification which contains a password to the PDF document.

The WebSeal module (Secure End-to-End encryption) helps application to achieve a true end-to-end encryption, from the web browser/mobile application to the web server or application server, and database server, offering a level of security unavailable from software alternatives to support critical business processes. WebSeal ensures that no sensitive data is accessible in clear while travelling over the network throughout an application's operation cycles. Seeding of E2EE JavaScript is performed here.

One common use case is that after the customer received the authentication PIN from Secure ePin, WebSeal will be leveraged to encrypt the PIN and sent back to the business application as in Figure 1.

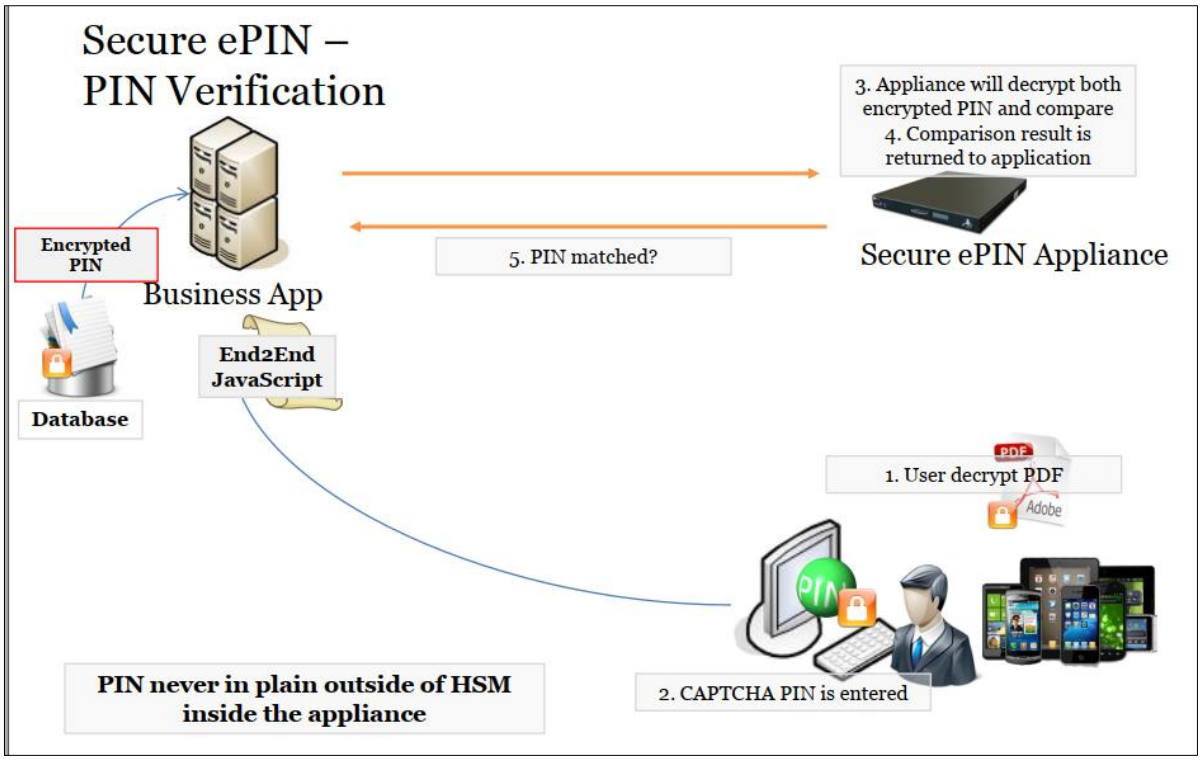

Figure 1- Fortix Security Suite Common Use Case

3.2 Usage and major security features of the TOE

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

a) Identification and Authentication
b) User Data Protection
c) Security Management
d) TOE Access
e) Security Audit

For more details, refer to Section Logical scope.

3.3 TOE Type

The TOE is a web application and web services to support secure delivery of PIN to customers and secure data communication between endpoints.

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

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

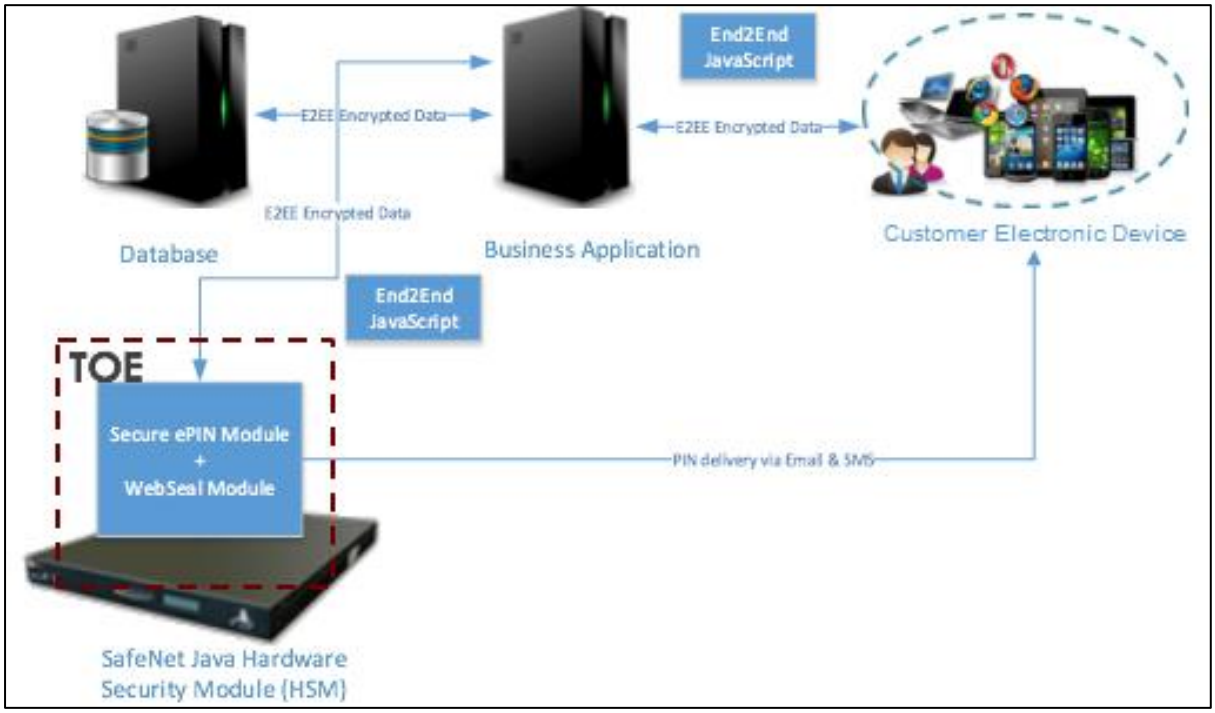

Figure 2 - TOE typical operational environment

The supporting hardware and software for TOE are as following:

a) **SafeNet Java Hardware Security Module (HSM)**
Gemalto's SafeNet Java Luna HSM is a standard FIPS 140 2 Level 3 validated Hardware Security Module that comes with its individual hardened Operating System and allows TOE application to be hosted in its server. SafeNet Java HSM increases application security by providing a trusted execution environment that protects an application's sensitive software components and cryptographic keys from physical, logical and operational threats.

b) **Business Application**
Web server or application server leverages WebSeal Module from Fortix Security Suite to construct web pages with End2End JavaScript to be downloaded by the customer. It receives encrypted PIN from customer and pull encrypted PIN from database. Encrypted PIN from database and encrypted PIN from customer is sent to HSM for verification.

c) **Customer Electronic Device**
Receives the PIN from Secure ePIN Module. When customer access web application via SSL with username, authentication page with End2End JavaScript will be downloaded from the business application. Data

entered by the customer will be encrypted by End2End JavaScript and the encrypted web form is submitted to server.

d) Database
Database stores encrypted PIN of the customer. Encrypted PIN will be sent to the business application as needed.

e) End2End JavaScript
Pieces of JavaScript embedded in web pages that enable end-to-end encryption and decryption of data communicated over the Internet.

4 TOE Description

4.1 Physical Scope of TOE

The guidance document is delivered together with the TOE on separate media support, in order to support the administrator and user in administrating and operating the TOE:

- Fortix Security Suite Administrator Guide
- Fortix Security Suite Developer Guide

4.2 Logical Scope of TOE

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

a) Identification and Authentication

TOE shall allow System Initialization before Root Admin being identified and authenticated. Root Admin, System Admin and System Operator can be authenticated using login ID and password at the TOE Management Console. Web Services user (node) can be authenticated using login ID and password when calling web services.

- TOE shall reauthenticate the Root Administrator, System Administrator and System Operator if idle for 10 minutes on the Web Management Console; TOE shall reauthenticate the Web Services User if idle for 30 minutes after authentication through calling web services API.
- TOE shall maintain several security attributes belonging to individual users.

b) Security Management

There are several roles maintained in TOE: Root Admin, System Admin, System Operator and Web Services user.

The TOE is able to perform several management functions as following:

a. System Initialization
b. HSM Storage Cleanup
c. Backup Database
d. Restore Database
e. SMTP Configuration
f. SMS Configuration
g. SMS Provider Configuration
h. Email Template Management
i. PIN Mailer Template Management
j. Key Import
k. Generate Keypairs
l. Decimalization Table
m. User Management
n. View System Log
o. Node Management
p. Change Own Password

Web Services user does not have management role. Download App Log is not part of the scope.

The authorized roles are able to modify, delete and add TSF data for each management functions mentioned above.

When a new node is added, it will have the "Restricted" state. Root Admin, System Admin, System Operator are able to change default value for Node Management from "Restricted" to "Granted".

c. User Data Protection

TOE shall enforce Access Control Policy to control user access on TOE Management Console functions according to their roles. Different roles will obtain different access functions in the Management Console. Additionally, a business application endpoint is able to use WebSeal End2End JavaScript to encrypt/decrypt data provided by user to be sent over the Internet to itself.

TOE shall also enforce Secure ePIN Policy in generating/converting PIN in CAPTCHA format to be embedded in encrypted PDF file. The encrypted

PDF file will be sent to customer in email and password of the PDF file will be sent using SMS.
However, true random number generation and encryption are executed by HSM which are not part of the scope.

Security attributes shall be used in order to enforce Access Control Policy and Secure ePIN Policy.

Secure ePIN Policy shall be enforced when exporting PIN to the intended user.

d. TOE Access

User will also be denied establishing a session with the TOE if the client did not present a valid certificate for client-side authentication. Additionally, only nodes that have their source IP Address whitelisted can call the web services.

e. Security Audit

TOE shall be able to generate audit record for several auditable events. Each event will be recorded with date and time, type of event, subject identity and outcome of the event. However, the timestamp for the audit record is provided by the HSM operating system, which is not part of the scope.

Audit records can be reviewed by Root Admin, System Admin and System Operator in a suitable manner.

TOE shall protect the audit records from unauthorized deletion or modification.

f. Trusted Channels

TOE shall provide a secure communication channel between WebSeal Module to business application and HSM. Any data transferred between this channels will be in encrypted format to protect from modification and disclosure.

5 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	The ST is package conformant to the package Evaluation Assurance Level EAL2.
Protection Profile conformance	None

6 TOE Security Problem Definition

6.1 Assumption

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

Table 1 - Assumptions

A.ENV	The TOE environment is physically and logically secure.
A.STORAGE	The PIN will be stored securely in TOE environment.
A.ENCRYPT	The TOE environment will encrypt PDF file securely.
A.KEYGEN	The TOE environment will generate and manage the true random number and encryption key securely.
A.SMS	The TOE environment for SMS delivery is secure.
A.ADMIN	The Administrator for the environment will be non-hostile and follows guidance documentation accordingly; however, the Administrator is not free from human error and mistakes.

6.2 Threats

Assets that are protected by the TOE are sensitive data stored in the TOE and TOE configuration data (configuration files and others), TOE data and TOE security functions.

Threat agents are entities that can adversely act on the assets. The threat agents identified are an unauthorized administrator.

Threats may be addressed either by the TOE or by its intended environment.

Table 2 - Threats

T.PIN	An unauthorized administrator may access and view the protected PIN without authorization
T.STORAGE	An unauthorized administrator or unauthorized external IT entity may steal the true random number and encryption key
T.CONFIGDATA	An unauthorized administrator may modify TOE configurations and data.
T.TRANS	An unauthorized administrator may read and modify data in transaction and at rest.
T.IDLE	An unauthorized administrator may obtain access to the TOE while in idle mode.
T.ADMIN	An unauthorized administrator may successfully access the TOE data or security functions without being detected.
T.AUDITREC	An unauthorized administrator (On the OS Level) may delete audit records to destroy evidence of adverse events executed.

6.3 Organizational Security Policies

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

Table 3 - Organizational Security Policies

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

P.PASSWORD	Authorized administrator assigned by the organization shall use complex password to login to the TOE

7 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.

7.1 Security Objectives for the TOE

The security objectives for the TOE as following:

Table 4 - Security Objectives for the TOE

O.PIN	TOE shall prevent an unauthorized administrator from access and view the protected PIN without authorization
O.CONFIGDATA	TOE shall prevent an unauthorized administrator to modify TOE configurations and data.
O.TRANS	TOE shall prevent unauthorized administrator to read and modify data in transaction and at rest.
O.IDLE	TOE shall prevent unauthorized administrator to obtain access to the TOE while in idle mode.
O.ADMIN	TOE shall prevent unauthorized administrator successfully access the TOE data or security functions without being detected.
O.AUDITREC	TOE shall prevent unauthorized administrator (On the OS Level) to delete audit records in order to destroy evidence of adverse events executed.

7.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

Table 5 - Security Objectives for the Operational Environment

OE.ENV	The TOE environment shall be physically and logically secured.

OE.STORAGE	The PIN, true random number and encryption key shall be stored securely in TOE environment.
OE.ENCRYPT	The TOE environment shall encrypt PDF file securely.
OE.KEYGEN	The TOE environment shall generate and manage the true random number and encryption key securely.
OE.SMS	The TOE environment for SMS delivery shall be secured.
OE.ADMIN	The Administrator for the environment shall be non-hostile and follows guidance documentation accordingly; however, the Administrator is not free from human error and mistakes.

8 Extended Components

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

8.1 Extended Security Functional Requirement (SFR)

There are no extended SFR components defined for this evaluation.

8.2 Extended security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

9 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.

9.1 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).

9.2 Security Functional Requirements

This section contains the security functional requirements (SFRs) for the TOE.

9.2.1 Class FIA: Identification and Authentication

9.2.1.1 FIA_UID.1 Timing of Identification

Hierarchical	No other components
Dependencies	No dependencies.
FIA_UID.1.1	The TSF shall allow [**System Initialization**] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application notes	The first user that access the TOE after TOE first time startup have the ability to initialize the system by setting up the root account.

9.2.1.2 FIA_UAU.1 Timing of Authentication

Hierarchical	No other components
Dependencies	FIA_UID.1 Timing of identification

FIA_UAU.1.1	The TSF shall allow [**System Initialization**] 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.
Application notes	The first user that access the TOE after TOE first time startup have the ability to initialize the system by setting up the root account.

9.2.1.3 FIA_UAU.6 Re-authenticating

Hierarchical	No other components
Dependencies	No dependencies
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [**user did not perform any actions for 5 minutes after session establishment with TOE on the management console; user did not perform any actions for 30 minutes after session establishment with TOE on the web services usage**].
Application notes	None

9.2.1.4 FIA_ATD.1 User attribute 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) Login ID** **b) Password** **c) Role** **d) Session ID**].
Application notes	None

9.2.2 Class FMT: Security Management

9.2.2.1 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: [

a. **System Initialization**
b. **HSM Storage Cleanup**
c. **Backup Database**
d. **Restore Database**
e. **SMTP Configuration**
f. **SMS Configuration**
g. **SMS Provider Configuration**
h. **Email Template Management**
i. **PIN Mailer Template Management**
j. **Key Import**
k. **Generate Keypairs**
l. **Decimalization Table**
m. **User Management**
n. **View System Log**
o. **Node Management**
p. **Change Own Password**

].

Application notes Download App Log is not part of the scope.

9.2.2.2 FMT_MTD.1 Management of TSF data

Hierarchical 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 [***[Table 2 - Ability***] the [**Table 2 – TSF Data**] to [**Table 2 – Authorized Roles**].

Table 6: TOE Roles and TSF Data

Authorized Roles	Ability	TSF Data
Root Admin	*Change Default, Query, modify, delete, [add]*	- Nodes
	Query, modify, delete, [add]	- Users
	Query	- Operation state - System log - Own account details
	Modify	- Own password
	Clear	- Unnecessary TOE files
	[execute]	- TOE configuration backup - TOE configuration restore - Keypair generation
System Admin	*Change Default, Query, modify, delete, [add]*	- Users - Nodes

	Query	- **Operation state** - **System log** - **App log** - **Own account details**
	Modify	- **Own password**
	Change Default, Query, modify, delete, [add]	- **Nodes**
	Query, modify, delete, [add]	- **Users**
	[execute]	- **Keypair generation**
System Operator	***Query, modify, delete, [add]***	- **SMTP configuration** - **SMS configuration** - **SMS provider** - **Email template** - **PIN mailer template** - **Decimalization table** - **Users**
	Query, delete, [add]	- **Imported keys**
	Modify	- **Own password**
	Query	- **Operation state** - **Own account details**

	Change Default, Query, modify, delete, [add]	- **Nodes**
	[execute]	- **Keypair generation**

Application notes Web services user cannot perform any management of TSF data.

9.2.2.3 FMT_SMR.1 Security roles

Hierarchical No other components

Dependencies FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**Root Admin, System Admin, System Operator and Web Services user].**

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

Application notes Root Admin account is created by the first user that access the TOE after TOE first time startup. Root Admin account can be used to create other accounts afterward.

9.2.2.4 FMT_MSA.1 Management of security attributes

Hierarchical No other components

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

FMT_MSA.1.1 The TSF shall enforce the [**access control policy**] to restrict the ability to [***Table 2 - Ability***] the security attributes [**Table 2 – TSF Data**] to [**Table 2 - Authorized Roles**].

Application notes	None

9.2.2.5 FMT_MSA.3 Static attribute initialisation

Hierarchical	No other components
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [**Access Control Policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**Root Admin, System Admin and System Operator**] to specify alternative initial values to override the default values when an object or information is created.
Application notes	Root Admin, System Admin and System Operator able to change the default value for Node creation default state from "Forbidden" to "Granted" state.

9.2.3 Class FDP: User Data Protection

9.2.3.1 FDP_ACC.1 (ACP) Subset access control

Hierarchical	No other components
Dependencies	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [**Access Control Policy**] on [

Subject	Objects	Operations
Root Admin	**Login page of Management Console**	**Login with login ID and password, download certificate**
	Overview Page	**View operation state**
	User Management page, Node	**Add, modify, delete information**

	Management Page	
	Change Password Page	View own account details, Modify password
	System Log page	View system log
	Clean Up function	Execute to clean up unnecessary files
	Backup Database function	Execute to backup database
	Restore Database	Execute to restore database
System Admin	Login page of Management Console	Login with login ID and password, download certificate
	Overview Page	View operation state
	User Management page, Node Management Page	Add, modify, delete information
	Change Password Page	View own account details, Modify password
	System Log page	View system log
	Generate Keypairs Page	Generate keypairs
System Operator	Login page of Management Console	Login with login ID and password, download certificate
	Overview Page	View operation state
	SMTP Configuration Page, SMS Configuration Page, SMS Provider Page,	Add, modify, delete information

	Email Template Page, PIN Mailer Template page, Decimalization Table page, User Management Page, Node Management Page	
	Change Password Page	**View own account details, Modify password**
	Node Management Page	**Add, modify, delete information**
Web Services user	**Web services endpoints**	**Make web services API calls to Secure ePIN to generate email with encrypted PDF and SMS with password to be sent to customer**

]

Application notes None

9.2.3.2 FDP_ACC.1 (SEP) 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 [**Secure ePIN policy**] on [

Subject	Objects	Operations
ePIN web services	**PIN, CAPTCHA output**	**Convert PIN into CAPTCHA output**
	PDF File	**Embed PIN (CAPTCHA output) in encrypted PDF file**
	SMS	**Embed password to decrypt PDF file**

]

Application notes None

9.2.3.3 FDP_ACF.1 (ACP) 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	Objects	Security Attributes
Root Admin	**Login page of Management Console**	**Login ID, password**
	User Management page	**Login ID, password, role**
	Node Management page	**Node Name, IP Address, State, Date Added**

	System Log Page	Type, Login ID, User Location, Operation, Detail, Operation Status, DateTime
	Backup Database Page	Recipient IP Address
	Restore Database Page	Originating Database IP Address
	Change Password page	Login ID, password
System Admin	Login page of Management Console	Login ID, password
	User Management page	Login ID, password, role
	Node Management page	Node Name, IP Address, State, Date Added
	System Log Page	Type, Login ID, User Location, Operation, Detail, Operation Status, DateTime
	Change Password page	Login ID, password
	Generate keypairs page	Number of keypairs generated
System Operator	Login page of Management Console	Login ID, password
	Node Management page	Node Name, IP Address, State, Date Added
	System Log Page	Type, Login ID, User Location, Operation, Detail, Operation Status, DateTime
	Operational Admin Management page	a. SMTP Configuration Name, sender email, Secure ePIN subject, SMTP host, SMTP port,

		authentication type, SMTP login, SMTP password **b. SMS Configuration** **Name, Service End Point, Message Template** **c. SMS Provider** **Name, Number Pattern, User, Pass, Code, Notes** **d. Email Template** **Name, HTML path, text path, default template** **e. PIN Mailer Template** **Name, Template file, default template** **f. Import Key** **Name, Key type, Key value, KCV** **g. Decimalization Table** **Name, Value, Default Value**
	Change Password page	**Login ID, password**
Web Services user	**Web services endpoints**	**Login ID, password**

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	Objects	Rules

Root Admin	Login page of Management Console	Successful authentication with correct login ID and password
	Overview page	Able to view operation state
	User Management page	-Able to configure Login ID, Name, Email, Role, Password -Able to edit Name, Email, Role -Able to delete user
	Node Management page	-Able to configure Node name, IP address, state -Able to edit name, IP address -Able to change node default state from "Forbidden" to "Granted" state to allow node to be accessed by the API -Able to revoke access to node -Able to delete node
	System Log page	-Able to view system log
	Clean Up function	-Able to cleanup unnecessary files
	Backup Database page	-Able to add recipient IP
	Restore Database page	-Able to specify originating database IP
	Change Password	Able to change password

System Admin	Login page of Management Console	Successful authentication with correct login ID and password
	Overview page	Able to view operation state
	User Management page	-Able to configure Login ID, Name, Email, Role, Password -Able to edit Name, Email, Role -Able to delete user
	Node Management page	-Able to configure Node name, IP address, state -Able to edit name, IP address -Able to change node default state from "Forbidden" to "Granted" state to allow node to be accessed by the API -Able to revoke access to node -Able to delete node
	System Log page	-Able to view system log
	Generate Keypairs Page	-Able to specify number of keypairs to generate
	Change Password	Able to change password
System Operator	Login page of Management Console	Successful authentication with correct login ID and password
	Overview page	Able to view operation state
	Node Management page	-Able to configure Node name, IP address, state

		-Able to edit name, IP address -Able to change node default state from "Forbidden" to "Granted" state to allow node to be accessed by the API -Able to revoke access to node -Able to delete node
	System Log page	-Able to view system log
	Operational Admin Management page	Able to configure: a. SMTP Configuration Name, sender email, Secure ePIN subject, SMTP host, SMTP port, authentication type, SMTP login, SMTP password b. SMS Configuration Name, Service End Point, Message Template c. SMS Provider Name, Number Pattern, User, Pass, Code, Notes d. Email Template Name, HTML path, text path, default template e. PIN Mailer Template Name, Template file, default template f. Import Key

		Name, Key type, Key value, KCV **g. Decimalization Table** **Name, Value, Default Value** **Able to edit and delete:** **a. SMTP Configuration** **b. SMS Configuration** **c. SMS Provider** **d. Email Template** **e. PIN Mailer Template** **f. Decimalization Table** **Able to delete:** **a. SMTP Configuration** **b. SMS Configuration** **c. SMS Provider** **d. Email Template** **e. PIN Mailer Template** **f. Decimalization Table** **Able to delete:** **a. Imported keys**
	Change Password	**Able to change password**
Web Services user	**Web services endpoints**	**Able to make web services API calls to Secure ePIN to generate email with encrypted PDF and SMS with password to be sent to customer**

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**The first**

user that access the TOE after TOE first time startup have the ability to initialize the system by setting up the root account].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no subjects may delete the account of root admin**].

Application notes None

9.2.3.4 FDP_ACF.1 (SEP) 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 [**Secure ePIN Policy**] to objects based on the following: [

Subject	Objects	Security Attributes
ePIN web services	**PIN, CAPTCHA output**	**Login ID, password, session ID, email ID, phone number**
	PDF file	
	SMS	

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	Objects	Rules
ePIN web services	**PIN, CAPTCHA output**	**Convert PIN into CAPTCHA PIN**
	PDF file template	**Embed CAPTCHA PIN in encrypted PDF file**
	SMS	**Embed password to decrypt PDF file**

].

FDP_ACF.1.3	The TSF shall explicitly authorize 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**].
Application notes	None

9.2.3.5 FDP_ETC.2 Export of user data with security attributes

Hierarchical	No other components
Dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1	The TSF shall enforce the [**Secure ePIN policy**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [**1) Generate PDF based on given PIN offset** a. **PIN offset from business application of existing PIN generation mechanism will be converted into actual PIN by the HSM** b. **PIN transformed into CAPTCHA format** c. **PIN in CAPTCHA format will be embedded inside a PDF file encrypted with random number generated by HSM** d. **The encrypted PDF file will be sent to customer's email** e. **SMS notification containing the password to the encrypted PDF file will be sent to customer**

2) Generate PIN using internal HSM

a. **PIN using true random number generator by HSM**
b. **PIN transformed into CAPTCHA format**
c. **PIN in CAPTCHA format will be embedded inside a PDF file encrypted with random number generated by HSM**
d. **The encrypted PDF file will be sent to customer's email**
e. **SMS notification containing the password to the encrypted PDF file will be sent to customer**

]

Application notes	True random number generation and encryption of PDF file are executed by HSM which are not part of the scope.

9.2.4 Class FTA: TOE access

9.2.4.1 FTA_TSE.1 TOE session establishment

Hierarchical	No other components
Dependencies	No dependencies
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [**user personal authentication certificate and Nodes IP address**]
Application notes	User personal authentication certificate is being used to establish a secure communication with TOE Management Console, Nodes IP is being used to restrict unauthorized IP address from calling the web services API.

9.2.5 Class FAU: Security Audit

9.2.5.1 FAU_GEN.1 Audit data generation

Hierarchical	No other components

Dependencies	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events:[a) ~~Start-up and shutdown of the audit functions~~; b) All auditable events for the [***not specified***] level of audit; and c) [**a) Web Service API Failures** **b) Web Service Authentication Failures** **c) Web Portal Restricted Access** **d) Database Backup & Restore** **e) System Initialization** **f) Nodes Access Grant** **g) User Creation/Delete**].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information:[a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definition of the functional components included in the PP/ST, [**None**].
Application notes	The audit function is pre-configured to be enabled all time and could not be disabled by any user. Timestamp is provided by the environment (HSM operating system).

9.2.5.2 FAU_SAR.1 Audit review

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [**Root Admin, System Admin, System Operator**] with the capability to read [**all audit logs trail data**] 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.
Application notes	None

9.2.5.3 FAU_STG.1 Protected audit trail storage

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.
Application notes	None

9.2.6 Class FTP: Trusted path/channels

9.2.6.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical	No other components
Dependencies	No dependencies
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [***the TSF, another trusted IT product***] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [**1. WebSeal Module, which is the TSF is hosted in HSM. It has End2End (E2EE) Server Library.**

2. Business application (e.g. Web Server), which is another trusted IT product, integrates with WebSeal Module, so that every page it constructed has the End2End JavaScript (e.g. Login page with E2EE JavaScript)

3. Business application send the Login page with E2EE JavaScript to customer.

4. Customer receives the Login page with E2EE JavaScript. Any information or user input will be encrypted by E2EE JavaScript when sending back to Business application.

5. The business application receives the user input in E2EE encrypted format which will be decrypted by WebSeal Module in HSM. HSM is also a trusted IT product which interact with the TSF.

6. WebSeal Module in HSM decrypt the information and send the status back to Business Application.].

Application notes	None

9.3 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 environment.

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

Table 7 - Security Assurance Requirements for EAL2

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: Life-cycle 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

10 TOE Summary Specifications

TOE addressed the security functional requirements as following:

10.1 Identification and Authentication

TOE shall allow System Initialization before Root Admin being identified and authenticated. The first user that access the TOE after TOE first time startup

have the ability to initialize the system by setting up the root account. Root Admin, System Admin and System Operator can be authenticated using login ID and password at the TOE Management Console. Web Services user (node) can be authenticated using login ID and password when calling web services.

TOE shall reauthenticate user if user is idle for 10 minutes.

TOE shall maintain the following list of security attributes belonging to individual users:

a) Login ID

b) Password

c) Role

d) Session ID

Relevant SFR: FIA_UID.1, FIA_UAU.1, FIA_UAU.6, FIA_ATD.1

10.2 Security Management

There are several roles maintained in TOE: Root Admin, System Admin, System Operator and Web Services user. Root Admin account is created by the first user that access the TOE after TOE first time startup. Root Admin account can be used to create other accounts afterward.

The TOE is able to perform several management functions as following:

a. System Initialization
b. HSM Storage Cleanup
c. Backup Database
d. Restore Database
e. SMTP Configuration
f. SMS Configuration
g. SMS Provider Configuration
h. Email Template Management
i. PIN Mailer Template Management
j. Key Import
k. Generate Keypairs
l. Decimalization Table
m. User Management
n. View System Log
o. Node Management
p. Change Own Password

Download App Log is not part of the scope.

The TSF shall restrict the ability to authorized users as following:

Authorized Roles	Ability	TSF Data
Root Admin	*Change Default, Query, modify, delete, add*	- Nodes
	Query, modify, delete, add	- Users
	Query	- Operation state - System log

		- Own account details
	Modify	- Own password
	Clear	- Unnecessary TOE files
	Execute	- TOE configuration backup - TOE configuration restore - Keypair generation
System Admin	*Change Default, Query, modify, delete, add*	- Users - Nodes
	Query	- Operation state - System log - App log - Own account details
	Modify	- Own password
	Change Default, Query, modify, delete, add	- Nodes
	Query, modify, delete, add	- Users
	Execute	- Keypair generation
System Operator	*Query, modify, delete, add*	- SMTP configuration - SMS configuration - SMS provider - Email template - PIN mailer template - Decimalization table - Users
	Query, delete, add	- Imported keys
	Modify	- Own password
	Query	- Operation state - Own account details

	Change Default, Query, modify, delete, add	- Nodes
	Execute	- Keypair generation

Web Services user does not have management role.

When a new node is added, it will have the "Restricted" state. Root Admin, System Admin, System Operator are able to change default value for Node Management from "Restricted" to "Granted".

Relevant SFR: FMT_SMF.1, FMT_MTD.1, FMT_SMR.1, FMT_MSA.1, FMT_SMA.3

10.3 User Data Protection

TOE shall enforce Access Control Policy to control user access on TOE Management Console functions according to their roles. Different roles will obtain different access functions in the Management Console. Additionally, a business application endpoint is able to use WebSeal End2End JavaScript to encrypt/decrypt data provided by user to be sent over the Internet to itself.

The TSF shall enforce Access Control Policy as following:

Subject	Objects	Operations
Root Admin	Login page of Management Console	Login with login ID and password, download certificate
	Overview Page	View operation state
	User Management page, Node Management Page	Add, modify, delete information
	Change Password Page	View own account details, Modify password
	System Log page	View system log
	Clean Up function	Execute to clean up unnecessary files
	Backup Database function	Execute to backup database
	Restore Database	Execute to restore database
System Admin	Login page of Management Console	Login with login ID and password, download certificate
	Overview Page	View operation state
	User Management page, Node Management Page	Add, modify, delete information
	Change Password Page	View own account details, Modify password
	System Log page	View system log
	Generate Keypairs Page	Generate keypairs
System Operator	Login page of Management Console	Login with login ID and password, download certificate
	Overview Page	View operation state

	SMTP Configuration Page, SMS Configuration Page, SMS Provider Page, Email Template Page, PIN Mailer Template page, Decimalization Table page, User Management Page, Node Management Page	Add, modify, delete information
	Change Password Page	View own account details, Modify password
	Node Management Page	Add, modify, delete information
Web Services user	Web services endpoints	Make web services API calls to Secure ePIN to generate email with encrypted PDF and SMS with password to be sent to customer

TOE shall also enforce Secure ePIN Policy in generating/converting PIN in CAPTCHA format to be embedded in encrypted PDF file. The encrypted PDF file will be sent to customer in email and password of the PDF file will be sent using SMS. However, true random number generation and encryption are executed by HSM which are not part of the scope.

The TSF shall enforce the Secure ePIN policy as following:

Subject	Objects	Operations
ePIN web services	PIN, CAPTCHA output	Convert PIN into CAPTCHA output
	PDF File	Embed PIN (CAPTCHA output) in encrypted PDF file
	SMS	Embed password to decrypt PDF file

Security attributes shall be used in order to enforce Access Control Policy and Secure ePIN Policy.

Following are security attributes for Access Control Policy:

Subject	Objects	Security Attributes
Root Admin	Login page of Management Console	Login ID, password
	User Management page	Login ID, password, role
	Node Management page	Node Name, IP Address, State, Date Added

	System Log Page	Type, Login ID, User Location, Operation, Detail, Operation Status, DateTime
	Backup Database Page	Recipient IP Address
	Restore Database Page	Originating Database IP Address
	Change Password page	Login ID, password
System Admin	Login page of Management Console	Login ID, password
	User Management page	Login ID, password, role
	Node Management page	Node Name, IP Address, State, Date Added
	System Log Page	Type, Login ID, User Location, Operation, Detail, Operation Status, DateTime
	Change Password page	Login ID, password
	Generate keypairs page	Number of keypairs generated
System Operator	Login page of Management Console	Login ID, password
	Node Management page	Node Name, IP Address, State, Date Added
	System Log Page	Type, Login ID, User Location, Operation, Detail, Operation Status, DateTime
	Operational Admin Management page	a. SMTP Configuration Name, sender email, Secure ePIN subject, SMTP host, SMTP port, authentication type, SMTP login, SMTP password b. SMS Configuration Name, Service End Point, Message Template c. SMS Provider Name, Number Pattern, User, Pass, Code, Notes d. Email Template

		Name, HTML path, text path, default template e. PIN Mailer Template Name, Template file, default template f. Import Key Name, Key type, Key value, KCV g. Decimalization Table Name, Value, Default Value
	Change Password page	Login ID, password
Web Services user	Web services endpoints	Login ID, password

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed in Access Control Policy:

Subject	Objects	Rules
Root Admin	Login page of Management Console	Successful authentication with correct login ID and password
	Overview page	Able to view operation state
	User Management page	-Able to configure Login ID, Name, Email, Role, Password -Able to edit Name, Email, Role -Able to delete user
	Node Management page	-Able to configure Node name, IP address, state -Able to edit name, IP address -Able to change node default state from "Forbidden" to "Granted" state to allow node to be accessed by the API -Able to revoke access to node -Able to delete node
	System Log page	-Able to view system log

	Clean Up function	-Able to cleanup unnecessary files
	Backup Database page	-Able to add recipient IP
	Restore Database page	-Able to specify originating database IP
	Change Password	Able to change password
System Admin	Login page of Management Console	Successful authentication with correct login ID and password
	Overview page	Able to view operation state
	User Management page	-Able to configure Login ID, Name, Email, Role, Password -Able to edit Name, Email, Role -Able to delete user
	Node Management page	-Able to configure Node name, IP address, state -Able to edit name, IP address -Able to change node default state from "Forbidden" to "Granted" state to allow node to be accessed by the API -Able to revoke access to node -Able to delete node
	System Log page	-Able to view system log
	Generate Keypairs Page	-Able to specify number of keypairs to generate
	Change Password	Able to change password
System Operator	Login page of Management Console	Successful authentication with correct login ID and password
	Overview page	Able to view operation state
	Node Management page	-Able to configure Node name, IP address, state -Able to edit name, IP address -Able to change node default state from "Forbidden" to "Granted" state

		to allow node to be accessed by the API -Able to revoke access to node -Able to delete node
	System Log page	-Able to view system log
	Operational Management page Admin	Able to configure: a. SMTP Configuration Name, sender email, Secure ePIN subject, SMTP host, SMTP port, authentication type, SMTP login, SMTP password b. SMS Configuration Name, Service End Point, Message Template c. SMS Provider Name, Number Pattern, User, Pass, Code, Notes d. Email Template Name, HTML path, text path, default template e. PIN Mailer Template Name, Template file, default template f. Import Key Name, Key type, Key value, KCV g. Decimalization Table Name, Value, Default Value Able to edit and delete: a. SMTP Configuration b. SMS Configuration c. SMS Provider d. Email Template

		e. PIN Mailer Template f. Decimalization Table Able to delete: a. SMTP Configuration b. SMS Configuration c. SMS Provider d. Email Template e. PIN Mailer Template f. Decimalization Table Able to delete: a. Imported keys
	Change Password	Able to change password
Web Services user	Web services endpoints	Able to make web services API calls to Secure ePIN to generate email with encrypted PDF and SMS with password to be sent to customer

In Access Control Policy, the first user that access the TOE after TOE first time startup have the ability to initialize the system by setting up the root account. No user is allowed to delete the root admin account.

The TSF shall enforce the Secure ePIN Policy as following:

Subject	Objects	Security Attributes
ePIN web services	PIN, CAPTCHA output	Login ID, password, session ID, email ID, phone number
	PDF file	
	SMS	

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed, in Secure ePIN Policy as following:

Subject	Objects	Rules
ePIN web services	PIN, CAPTCHA output	Convert PIN into CAPTCHA PIN
	PDF file template	Embed CAPTCHA PIN in encrypted PDF file
	SMS	Embed password to decrypt PDF file

Secure ePIN Policy shall be enforced when exporting PIN to the intended user. The TSF shall export the user data with the user data's associated security attributes. The TSF shall export the user data with the user data's associated security attributes. The TSF shall enforce the following rules when user data is exported from the TOE: [

1) Generate PDF based on given PIN offset
a. PIN offset from business application of existing PIN generation mechanism will be converted into actual PIN by the HSM
b. PIN transformed into CAPTCHA format
c. PIN in CAPTCHA format will be embedded inside a PDF file encrypted with random number generated by HSM
d. The encrypted PDF file will be sent to customer's email
e. SMS notification containing the password to the encrypted PDF file will be sent to customer

2) Generate PIN using internal HSM
a. PIN using true random number generator by HSM
b. PIN transformed into CAPTCHA format
c. PIN in CAPTCHA format will be embedded inside a PDF file encrypted with random number generated by HSM
d. The encrypted PDF file will be sent to customer's email
e. SMS notification containing the password to the encrypted PDF file will be sent to customer]

True random number generation and encryption of PDF file are executed by HSM which are not part of the scope.

Relevant SFR: FDP_ACC.1 (ACP), FDP_ACC.1 (SEP), FDP_ACF.1 (ACP), FDP_ACF.1 (SEP), FDP_ETC.2

10.4 TOE Access

User will be denied establishing a session with the TOE if the client did not present a valid certificate for client-side authentication. Additionally, only nodes that have their source IP Address whitelisted can call the web services.

Relevant SFR: FTA_TSE.1

10.5 Security Audit

TOE shall be able to generate audit record for auditable events as following:

a) Web Service API Failures
b) Web Service Authentication Failures
c) Web Portal Restricted Access
d) Database Backup & Restore
e) System Initialization
f) Nodes Access Grant
g) User Creation/Delete

Each event will be recorded with date and time, type of event, subject identity and outcome of the event. However, the timestamp for the audit record is provided by the HSM operating system, which is not part of the scope.

Audit records can be reviewed by Root Admin, System Admin and System Operator in a suitable manner.

TOE shall protect and prevent the audit records from unauthorized deletion or modification.

Relevant SFR: FAU_GEN.1, FAU_SAR.1, FAU_STG.1

10.6 Trusted channels

TOE shall provide a secure communication channel between WebSeal Module to business application and HSM. Any data transferred between this channels will be in encrypted format to protect from modification and disclosure.

The TSF shall initiate communication via the trusted channel as following:

1. WebSeal Module, which is the TSF is hosted in HSM. It has End2End (E2EE) Server Library.

2. Business application (e.g. Web Server), which is another trusted IT product, integrates with WebSeal Module, so that every page it constructed has the End2End JavaScript (e.g. Login page with E2EE JavaScript).

3. Business application send the Login page with E2EE JavaScript to customer.

4. Customer receives the Login page with E2EE JavaScript. Any information or user input will be encrypted by E2EE JavaScript when sending back to Business application.

5. The business application receives the user input in E2EE encrypted format which will be decrypted by WebSeal Module in HSM. HSM is also a trusted IT product which interact with the TSF.

6. WebSeal Module in HSM decrypt the information and send the status back to Business Application.].

Relevant SFR: FTP_ITC.1

11 Rationale

11.1 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.

11.2 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.

11.2.1 Rationale of Security Objectives Mapped to Threats

Table 8 - Rationale of Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.PIN An unauthorized administrator may access and view the protected PIN without authorization	**O.PIN** TOE shall prevent an unauthorized administrator from access and view the protected PIN without authorization	This security objective counters threat because TOE shall prevent an unauthorized administrator from accessing and view the protected PIN without authorization.
T.STORAGE An unauthorized administrator or unauthorized external IT entity may steal the true random number and encryption key	**OE.STORAGE** The PIN, true random number and encryption key shall be stored securely in TOE environment.	This security objective counters threat because the database and HSM shall prevent an unauthorized administrator or entity to steal the PIN, true random number and encryption key.
T.CONFIGDATA An unauthorized administrator may modify TOE configurations and data.	**O.CONFIGDATA** TOE shall prevent an unauthorized administrator to modify TOE configurations and data.	This security objective counters threat because Access Control Policy in TOE shall only allow authorized administrator to modify TOE configurations and data.
T.TRANS An unauthorized administrator may read and modify data in transaction and at rest.	**O.TRANS** TOE shall prevent unauthorized administrator to read and modify data in transaction and at rest.	This security objective counters threat because the TOE shall encrypt the communication from end to end to prevent unauthorized administrator to read and modify data in transaction.
	OE.ENV The TOE environment shall be physically and logically secured.	This security objective counters threat because the TOE environment shall have physically and logically security mechanism. The location to store database server, HSM and other relevant servers shall have access control mechanism. The user device shall also have authentication mechanism

		to prevent unauthorized usage by unauthorized administrator.
	OE.ENCRYPT The TOE environment shall encrypt PDF file securely.	This security objective counters threat because the HSM shall encrypt the PDF file securely.
	OE.KEYGEN The TOE environment shall generate and manage the true random number and encryption key securely.	This security objective counters threat because the HSM shall generate and manage the true random number and encryption key securely.
	OE.SMS The TOE environment for SMS delivery shall be secured.	This security objective counters threat because the TOE environment shall ensure the SMS is delivered securely to the intended user.
T.IDLE An unauthorized administrator may obtain access to the TOE while in idle mode.	**O.IDLE** TOE shall prevent unauthorized administrator to obtain access to the TOE while in idle mode.	This security objective counters threat because the TOE prevents unauthorized administrator to obtain access to the TOE while in idle mode by requesting user to re-authenticate after 10 minutes idle time.
T.ADMIN An unauthorized administrator may successfully access the TOE data or security functions without being detected.	**O.ADMIN** TOE shall prevent unauthorized administrator successfully access the TOE data or security functions without being detected.	This security objective counters threat because the TOE shall record logs of event of TOE data and security functions.
T.AUDITREC An unauthorized administrator (On the OS Level) may delete audit records to destroy evidence of	**O.AUDITREC** TOE shall prevent unauthorized administrator (On the OS Level) to delete audit records in order to destroy evidence	This security objective counters threat because the TOE shall prevent unauthorized administrator to delete audit records in order to destroy evidence

adverse events executed.	of adverse events executed.	of adverse events executed.

11.2.2 Rationale of Security Objectives Mapped to OSP

Table 9 - Rationale of Security Objectives Mapped to OSP

OSP	Security Objectives	Rationale
P.ROLE Only authorized administrators assigned by the organization have access to the TOE and TOE environment.	**O.CONFIGDATA** TOE shall prevent an unauthorized administrator to modify TOE configurations and data.	This security objective enforces OSP because Access Control Policy in TOE shall only allow authorized administrator to modify TOE configurations and data. Organization shall only assigned authorized administrator to access TOE environment such as HSM, database and others.
P.PASSWORD Authorized administrators assigned by the organization shall use complex password to login to the TOE.	**O.CONFIGDATA** TOE shall prevent an unauthorized administrator to modify TOE configurations and data.	This security objective enforces OSP because Authorized administrators assigned by the organization shall use complex password to login to the TOE.

11.2.3 Rationale of Security Objectives Mapped to Assumptions

Table 10 - Rationale of Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.ENV The TOE environment is physically and logically secure.	**OE. ENV** The TOE environment shall be physically and logically secured.	This security objective upholds assumption because the TOE environment shall have physically and logically security mechanism. The location to store database server, HSM and other relevant servers shall have access control mechanism. The user device shall also have authentication mechanism to prevent unauthorized usage by unauthorized administrator.
A.STORAGE The PIN will be stored securely in TOE environment.	**OE. STORAGE** The PIN, true random number and encryption key shall be stored securely in TOE environment.	This security objective upholds assumption because the TOE environment shall provide an encrypted storage to store the PIN.
A.ENCRYPT The TOE environment will encrypt PDF file securely.	**OE. ENCRYPT** The TOE environment shall encrypt PDF file securely.	This security objective upholds assumption because the HSM shall encrypt the PDF file securely using a secure algorithm and key size.
A.KEYGEN The TOE environment will generate and manage the true random number and encryption key securely.	**OE.KEYGEN** The TOE environment shall generate and manage the true random number and encryption key securely.	This security objective upholds assumption because the HSM shall generate and manage the true random number and encryption key using a secure algorithm and key size. Also, to manage the generation, delivery

		and deletion of the key securely.
A.SMS The TOE environment for SMS delivery is secure.	**OE.SMS** The TOE environment for SMS delivery shall be secured.	This security objective upholds assumption because the SMS getaway shall be configured securely to deliver the SMS to in preventing SMS being tampered or viewed by unauthorized administrator.
A.ADMIN The Administrator for the environment will be non-hostile and follows guidance documentation accordingly; however, the Administrator is not free from human error and mistakes.	**OE.ADMIN** The Administrator for the environment shall be non-hostile and follows guidance documentation accordingly; however, the Administrator is not free from human error and mistakes.	This security objective upholds assumption because the Administrator for the environment shall be non-hostile and follows guidance documentation accordingly; however, the Administrator is not free from human error and mistakes.

11.3 Extended Security Functional Requirement Rationale

Refer to Section 8.1 Extended Security Functional Requirement (SFR) for rationale.

11.4 Extended Security Assurance Requirement Rationale

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

11.5 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.

11.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Table 11 - Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.PIN TOE shall prevent an unauthorized administrator from access and view the protected PIN without authorization	FDP_ACC.1 (SEP)	This SFR require ePIN web services to convert PIN into CAPTCHA output, embed PIN in encrypted PDF and embed password to decrypt the PDF file in an SMS. It traces back to this objective.
	FDP_ACF.1 (SEP)	This SFR require ePIN web services to tie unauthorized administrator login ID, password and session ID to every PIN. It traces back to this objective.
	FDP_ETC.2	This SFR require ePIN web services to generate PIN using internal HSM or generate PDF based on given PIN offset. It traces back to this objective.
O.CONFIGDATA TOE shall prevent an unauthorized administrator to modify TOE configurations and data.	FIA_UAU.1	This SFR shall allow System Initialization on behalf of user before user is authenticated. It also requires each administrator to be successfully authenticated before being allowed to perform any actions on TOE functions and

		configuration data. It traces back to this objective.
	FIA_UID.1	This SFR shall allow System Initialization on behalf of user before user is identified. It also requires each administrator to be successfully identified before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.
	FIA_ATD.1	This SFR provide users with attributes to distinguish one user from another using the login ID, password, role and session ID. It traces back to this objective.
	FMT_SMR.1	This SFR identify the user role that exist in TOE. It traces back to this objective.
O.TRANS TOE shall prevent unauthorized administrator to read and modify data in transaction and at rest.	FMT_SMF.1	This SFR identify management functions that are available in TOE, that are managed by administrator roles in TOE. It traces back to this objective.
	FMT_MTD.1	This SFR restrict the ability to enable, disable and modify TOE functions to administrator. It traces back to this objective.
	FMT_MSA.1	This SFR restrict the ability to enable, disable and modify security attributes to roles in TOE. It traces back to this objective.
	FMT_MSA.3	This SFR enforce Root Admin, System Admin and System Operator to change the default values of Node states based on Access Control Policy. It traces back to this objective.
	FDP_ACC.1 (ACP)	This SFR specify that each user will have privilege to access and use TOE functions based roles. It traces back to this objective.

	FDP_ACF.1 (ACP)	This SFR specify that each user will have privilege to access and use TOE functions based roles. It traces back to this objective.
	FTA_TSE.1	This SFR will deny session establishment if user personal authentication certificate and Nodes IP address are invalid. It traces back to this objective.
	FTP_ITC.1	This SFR shall provide secure communication channel between WebSeal module, Business application and HSM. It traces back to this objective.
O.IDLE TOE shall prevent unauthorized administrator to obtain access to the TOE while in idle mode.	FIA_UAU.6	This SFR re-authenticated the user if user did not perform any actions for 10 minutes after session establishment with TOE. It traces back to this objective.
O.ADMIN TOE shall prevent unauthorized administrator successfully access the TOE data or security functions without being detected.	FAU_GEN.1	This SFR generates audit records from events in TOE to detect any malicious activity. It traces back to this objective.
	FAU_SAR.1	This SFR allow authorized user with administrator's role to read and interpret the audit information in order to detect any malicious activity. It traces back to this objective.
O.AUDITREC TOE shall prevent unauthorized administrator (On the OS Level) to delete audit records in order to destroy evidence of adverse events executed.	FAU_STG.1	This SFR prevent audit records to be modified and deleted. It traces back to this objective.

11.5.2 SFR Dependency Rationale

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

Table 12 - SFR Dependencies

SFR	Dependency	Dependency Met?	Justification
FIA_UID.1	-	-	-
FIA_UAU.1	FIA_UID.1	Yes	-
FIA_UAU.6	-	-	-
FIA_ATD.1	-	-	-
FMT_SMF.1	-	-	-
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_SMR.1	FIA_UID.1	Yes	-
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MSA.3	FMT_MSA.1 FMT_SMF.1	Yes	-
FDP_ACC.1 (ACP)	FDP_ACF.1	Yes	-
FDP_ACC.1 (SEP)	FDP_ACF.1	Yes	-
FDP_ACF.1 (ACP)	FDP_ACC.1 FMT_MSA.3	Yes	-
FDP_ACF.1 (SEP)	FDP_ACC.1 FMT_MSA.3	Yes	-
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Yes	-
FTA_TSE.1	-	-	-
FAU_GEN.1	FPT_STM.1	No	The timestamp is provided by the environment
FAU_SAR.1	FAU_GEN.1	Yes	-
FAU_STG.1	FAU_GEN.1	Yes	-
FTP_ITC.1	-	-	-