Project Name	CENTAGATE
Document ID.	CTG-ST-3.0
Issue Date	8 May 2017
Document Name	Security Target for CENTAGATE
Dissemination Level	Public
Document Version	3.0
Status	Final
Author(s)	Nickson, Biau

SECURITY TARGET

WWW.SECUREMETRIC.COM

Revision History

No.	Date	Change Description
1	11 March 2016	New Issue
2	2 May 2016	Update based on ADV documentations.
3	8 may 2017	Finalized.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

This introductory section presents security target (ST) identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

1.1 ST and TOE Identification

1.1.1 ST Identification

ST Name/Title	**Security Target for CENTAGATE**
ST Date	8 May 2016
ST Version	3.0
TOE Identification	▪ TOE Web Application Server: CENTAGATE v3.0.10-build13. ▪ TOE Component: Advance Mobile Authentication Applications (Two Platforms) consist of: • CENTAGATE iOS Application v1.0.4-build1. • CENTAGATE Android Application v1.0.10-build1.
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.
PP Conformance	This ST and TOE did not conform to any PP.
Evaluation Assurance Level (EAL)	EAL 4 augmented with ALC_FLR.2.

Table 1: ST Identification

1.1.2 TOE Identification

TOE Name	**CENTAGATE**
TOE Components	▪ TOE Web Application Server: CENTAGATE v3.0.10-build13. ▪ TOE Component: Advance Mobile Authentication Applications (Two Platforms) consist of: • CENTAGATE iOS Application v1.0.4-build1. • CENTAGATE Android Application v1.0.10-build1.

Table 2: TOE Identification

1.2 TOE Overview

LEGEND NOTE: Throughout the document, these basic naming conventions will be used as definition of defining another terminology. The following is the list of naming conventions used in this document:

a) *TOE Administrators: CENTAGATE Administrator & CENTAGATE Company Administrator.*
b) *TOE Users: CENTAGATE Administrator, CENTAGATE Company Administrator & CENTAGATE End User.*

CENTAGATE (also known as the TOE) is an enterprise class authentication solution built on JEE technology, allowing enterprise users to securely perform authentication before login to the application.

CENTAGATE is designed to be a robust, high performance, platform independent, flexible and a component based solution.

Functionalities offered by CENTAGATE can be used through web interfaces (by end users, company admin or CENTAGATE admin) or APIs (by relying on applications that integrate with it). CENTAGATE is a Next-Gen Authentication solution that focuses on advanced technology such as a risk scoring engine (known as Hybrid Risk Scoring Engine) that will calculate user risk based on user previous login behavior and contextual attribute, plus with mobility authentication with end to end security, supported by end to end asymmetric encryption and signature (through the implementation perspective of confidentiality, integrity and authenticity). Overall, this security feature detects possible fraud or digital attacks and provides defend against common authentication attacks with a strong authentication feature supported by the CENTAGATE Advance Mobile Authentication components (running on Android application or iOS application).

CENTAGATE can be configured to provide alerts on various user defined system and security auditable events. These alerts can be delivered through the respective end users, company admin and CENTAGATE admin via email based on the organization security policies. The CENTAGATE Administrator can define the alerts and auditable events based on each application protected by the CENTAGATE security features.

The CENTAGATE provides privileges to CENTAGATE Administrator to provision users by assigning them based on role and authentication scheme. Additionally, the CENTAGATE Administrator shall configured and manage the CENTAGATE based on the related relevant security policies defined by the organization security policies. TOE Administrator shall configure the CENTAGATE via Internet Browser by access the TOE Web Application interfaces.

The TOE also provides various audit reports based on security events such as failed user login and login with flagged risk profiles. The printing of these audit reports support various document formats like MS Excel, CSV and PDF. The following is the descriptions of the TOE components consist of its major security features.

Table 3: List of TOE Components & its Major Security Features

#	Components	Features Descriptions	CENTAGATE Roles
1.	Setting Module (Setting Tab)	**CRL Downloader Configuration:** Function to configure Certification Revocation List (CRL) by download and upload into the CENTAGATE.	CENTAGATE Administrator
		Email Template: Function to setup template for email reply send by TOE Server.	CENTAGATE Administrator Company Administrator
		SMS Template: Function to setup for SMS reply when SMS is being requested.	CENTAGATE Administrator Company Administrator
		SMS Gateway: Function to configure the SMS Gateway.	CENTAGATE Administrator
		SMS OTP Configuration: Function to configure the SMS OTP parameter.	CENTAGATE Administrator
		OTP Configuration: Function to configure the OTP parameter.	CENTAGATE Administrator
		SMTP Configuration: Function to configure the SMTP Server.	CENTAGATE Administrator
		Company Information: Function to fill in the company information.	Company Administrator
		Trust Level: Function to configure the authentication methods to enforce 2FA authentication based on trust levels (Low, Medium & High).	CENTAGATE Administrator Company Administrator
		License Module: Function to upload the License CENTAGATE subscriptions based on expiry, total number of users, total number for token, and total number of company enable the usage of CENTAGATE.	CENTAGATE Administrator
2.	Company Management	**Update License Control:** Function to update the license subscription based on validity (Start Date	CENTAGATE Administrator

#	Components	Features Descriptions	CENTAGATE Roles
	Module (Company Tab)	& End Date) and Quantity (User Created, Apps Can be Created/Protected, SMS Credit).	
3.	Server Status Monitoring (Dashboard Tab)	**Server Status VMs:** Function to provide status on all the status of applications related to CENTAGATE system. Information displayed is Server Time, CPU Usage, Memory Usage, Disk Usage and Status (Online/Offline). Services or applications that were monitored are Reverse Proxy, CENTAGATE Web Service, IDP, Database Server, Queue Management System, Notification Service and Certificate Revocation List (CRL) Download Service.	CENTAGATE Administrator
4.	Application Management Module (App Tab)	**Application Registration & List:** Defined the application to be protected by the CENTAGATE and configure the integration mechanism using SAML, Web SDK, AD Connection or RADIUS.	Company Administrator
5.	Policies Management Module (Policies Tab)	**Create Security Policies & Listing:** Defined the security policies for CENTAGATE to enforce the 2FA mechanism. The Hybrid Risk Scoring Engine is the backend processing data for this function. The information required to enforce the 2FA with Hybrid Risk Scoring Engine: Operating System, Browser Fingerprint, Time, Geo-Location and IP Address.	CENTAGATE Administrator Company Administrator
6.	Group Management Module (Group Tab)	**Group of End Users:** Function to categories each user of the CENTAGATE to specific group and access mechanisms with the enforcement of security policy (2FA access mechanism). The configuration is based on these aspects: Security Policies, Password Setting, Session Setting, Question & Answer Setting and Authentication Options.	CENTAGATE Administrator Company Administrator
7.	User Management Module (User Tab)	**Manage End Users of CENTAGATE:** Function to create end users and manage them by assigning to a group, assigning token and assigning privilege access. Note that, users of the CENTAGATE are managed by the Company	Company Administrator

#	Components	Features Descriptions	CENTAGATE Roles
		Administrator. Company Administrator able to create and manage another Company Administrator.	
8.	Administrator Management Module (Administrator Tab)	**Manage CENTAGATE Administrator & Company Administrator:** Function to create Company Administrators and CENTAGATE Administrator, plus managing these accounts. Note that, CENTAGATE Administrator unable to view and manage the CENTAGATE End Users.	CENTAGATE Administrator
9.	Activities Management (Activities Tab)	**Viewing Activities Record & Configure Record System Notification:** As for CENTAGATE Administrator, configuration on notification of relevant activities related to CENTAGATE. Thus, also allow CENTAGATE Administrator, Company Administrator and CENTAGATE End User to view their current activities that recorded by the CENTAGATE System.	CENTAGATE Administrator Company Administrator CENTAGATE End User
10.	Token Management (Token Device Tab)	**Manage Token devices that are register in the CENTAGATE System:** Able to view the list of all register token linked to the relevant CENTAGATE Company Administrator. Additionally, CENTAGATE Company Administrator able to view the list if token linked to the CENTAGATE End User.	CENTAGATE Administrator Company Administrator
11.	Certificate Management Module (Certificate Tab)	**Register, Manage and Ensure the Validity of Certificate used by the CENTAGATE System:** CENTAGATE Administrator and CENTAGATE Company Administrator allows managing, loading and revoke relevant certificate based on its usage and CRL listing status.	CENTAGATE Administrator Company Administrator
12.	Self Service Module (Self Service Tab)	**Managing linked Token Devices and Authentication Methods:** Each of CENTAGATE Users (CENTAGATE Administrator, CENTAGATE Company Administrator and CENTAGATE End User) is allows managing and configuring their own authentication methods as well as the linked token devices.	CENTAGATE Administrator Company Administrator CENTAGATE End User

1.2.1 Required Firmware/Hardware/Software

The TOE requires a range of hardware and software in order to install the TOE and support the security functionality. This is provided in Table 4 and Table 5 below:

Table 4: CENTAGATE Server Specification

Item	Description	Scope
Hardware	I. Recommended: Intel® Xeon® CPU E5-2620 v3 @ 2.40GHz (15M Cache, 6 cores). Alternative: Intel® Xeon® CPU E5-2609 v3 @ 1.90GHz. II. 16GB RAM to 32GB RAM. III. 900GB to 1TB HDD consist of these aspects: a) OS = 40GB to 100GB b) CENTAGATE = 300GB c) Database = 600GB	Environment
Software	Application server The TOE can be deployed on an JEE 5 compliant application server, which provides a number of resources and services to the TOE, namely: I. Database connectivity services (e.g. object mappings and connection pooling); II. Component creation and management (e.g. session bean pooling and life-cycle management) III. Communication interfaces (e.g. HTTP and JEE).	Environment
	Application Server I. JBoss AS 7.1.1 Final II. Apache 2.4.7	Environment
	OS is running Ubuntu 14.04.3 LTS	Environment
	Database Server is using MariaDB 10.1.	Environment

	Java Virtual Machine TOE is developed in the Java programming language and, as such, runs in a Java Virtual Machine (JVM). Additionally, since the JVM specifications are public, it can be implement by independent vendors.	Environment

The following is the list of TOE mobile application specification as reference to the components of the TOE.

Table 5: CENTAGATE Advance Mobile Authentication Application

Item	Description	Scope
Hardware	Android Device Specification: i. ARMv7, ARMv7s, ARM64. ii. Minimum 500MB RAM. iii. Minimum 5MP Camera. iv. GPS Required. v. 3G Internet Connection (Recommended). vi. Audio Input. vii. Free space more than 10MB.	Environment
	iOS Device Specification: i. ARMv7, ARMv7s, ARM64. ii. Minimum 500MB RAM iii. Minimum 5MP Camera iv. GPS Required. v. 3G Internet Connection (Recommended) vi. Audio Input. vii. Free space more than 10MB.	

Software	Android OS Specification: i. Minimum Version OS 4.2.2 (Jelly Bean). ii. Maximum Version OS 5.1 (Lollipop). iOS OS Specification: i. Minimum version iOS 6.1. ii. Maximum version iOS 9.2.	Environment
	Programming Languages: Java and C programming.	Environment
	Browser: I. Android Browser. II. iOS Safari Browser.	Environment

1.2.2 TOE TYPE

CENTAGATE is an enterprise class authentication solution built on JEE technology, allowing enterprise users to securely perform authentication before logged into the application. Thus, the TOE consists of two types of platforms in which, firstly reside the TOE Server designed as Web Based Application System and the second, as a supporting component reside in the mobile application platforms installed either in iOS or Android.

The solution allows authentication via modern browser such as Internet Explorer (IE), Google Chrome, and Mozilla Firefox or via mobile using CENTAGATE Advance Mobile Authentication application.

1.3 TOE Description

CENTAGATE (TOE) System operates through the ecosystem of the Web Based Application Server and the Advance Mobile Authentication Application by using the Hybrid Risk Scoring Engine (Rules Based and Case Based), thus utilizes the machine learning technology to detect and respond to potential online fraud or intrusion. The Hybrid Risk Scoring Engine will collect user system behaviors and environment attributes in each login activities, based on rules defined by the CENTAGATE Administrators either CENTAGATE Administrator role or CENTAGATE Company Administrator role, whilst with the scoring engine will calculate the risk of each user authentication request and monitor the user behavior through the calculation value that are been processes in the TOE backend system. In the case of high risk detected, the system will prompt for another step of authentication (known as multi-step authentication process) to request for confirmation and validity of the user's credentials before allow to access the protected resources.

Beside the Web Based Authentication provided by the TOE using username and password plus the enforcement of 2 factor authentication (2FA) through the enforcement of token devices such as PKI, FIDO and etc., whilst a step-up authentication utilizes various authentication options that is provided by Advance Mobile Authentication Application. The TOE offers several 2FA and multistep options of authentication methods, which are offering Mobile PKI, CR OTP, OTP and QR Code. To ensure the security of mobile application, the TOE has enforced a strong encryption process whereby it will automatically removed the cryptographic key whenever it detects an untrusted request.

Security Policies components as part of the Hybrid Risk Scoring Engine (Rule Based) can be configured by the TOE Administrators (CENTAGATE Administrator and/or CENTAGATE Company Administrator) to suit the TOE operational environment, based on the security attributes defined in the configuration security policies at such: Browser Type, Operating System type, Time, IP Address and Geo-location. Besides the Security Policies, the TOE Administrators can configure the Case Based Security Policies as part of the Hybrid Risk Scoring Engine, which will provide black list or white list access to the TOE and protected resources (Applications registered in the TOE, App Tab) by comparing the IP Address and/or Country of the users.

The audit and alerts services ensure that all the security events that were recorded by the TOE and summary of audit reports are generated upon request in reporting the overall information. The TOE also supports delivery of alerts on critical security events through emails.

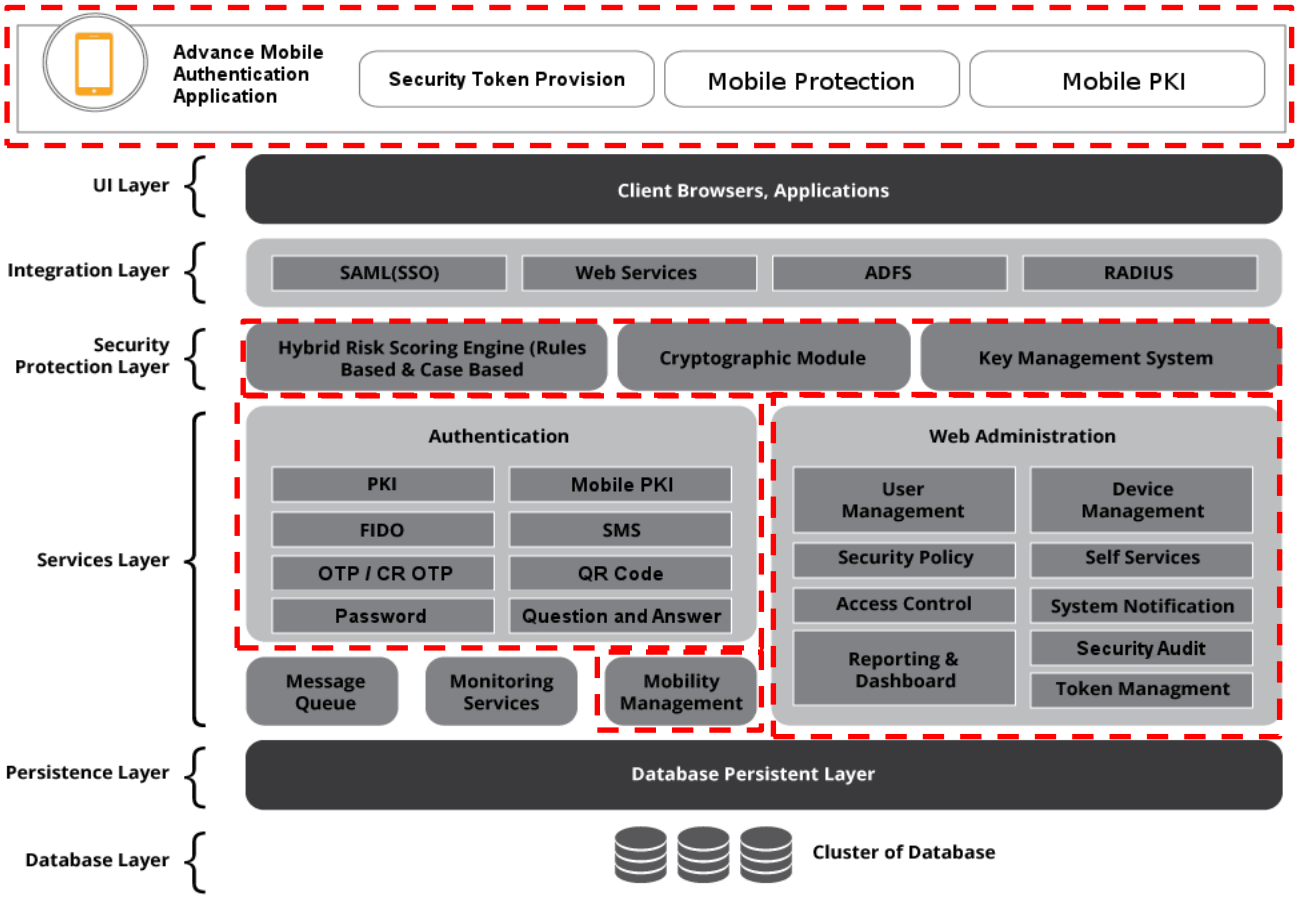

Figure 1: TOE Diagram shows the Logical Scope of the TOE

TOE Boundary

1.3.1 Scope of the TOE

The CENTAGATE (TOE), which comprise of two main components reside in two different platforms of operations. The first TOE is Web Based Application System (TOE Server) that's hold the components as highlighted above in RED Boundary Line, describes as stated below:

a) Hybrid Risk Scoring Engine (Rules Based and Case Based);
b) Cryptographic Module;
c) Key Management System;
d) Authentication Module consists of PKI, Mobile PKI, FIDO, SMS, OTP/CR OTP, QR Code, Password and Q&A (Question and Answer) Model.
e) Web Administration Module consists of User Management, Device Management, Security Policy, Self Services, Access Control, System Notification, Reporting Dashboard, Security Audit and Token Management; and
f) Mobility Management Module.

Note that, in this evaluation, FIDO and OTP Hardware Token is not part of scope of TOE. Secondly, TOE components reside in the other platform which is the smartphone application running on Android and iOS are been used as supporting 2FA authentication processes components known as Advance Mobile Authentication Application. Kindly refer to the Figure 1 for TOE boundary illustration. The Advance Mobile Authentication Application in Android and iOS are part of the scope of the TOE.

Additionally, all underlying hardware and operating system running to support the TOE operational environment is not part of the scope of the TOE.

1.3.1.1 Physical Scope of the TOE

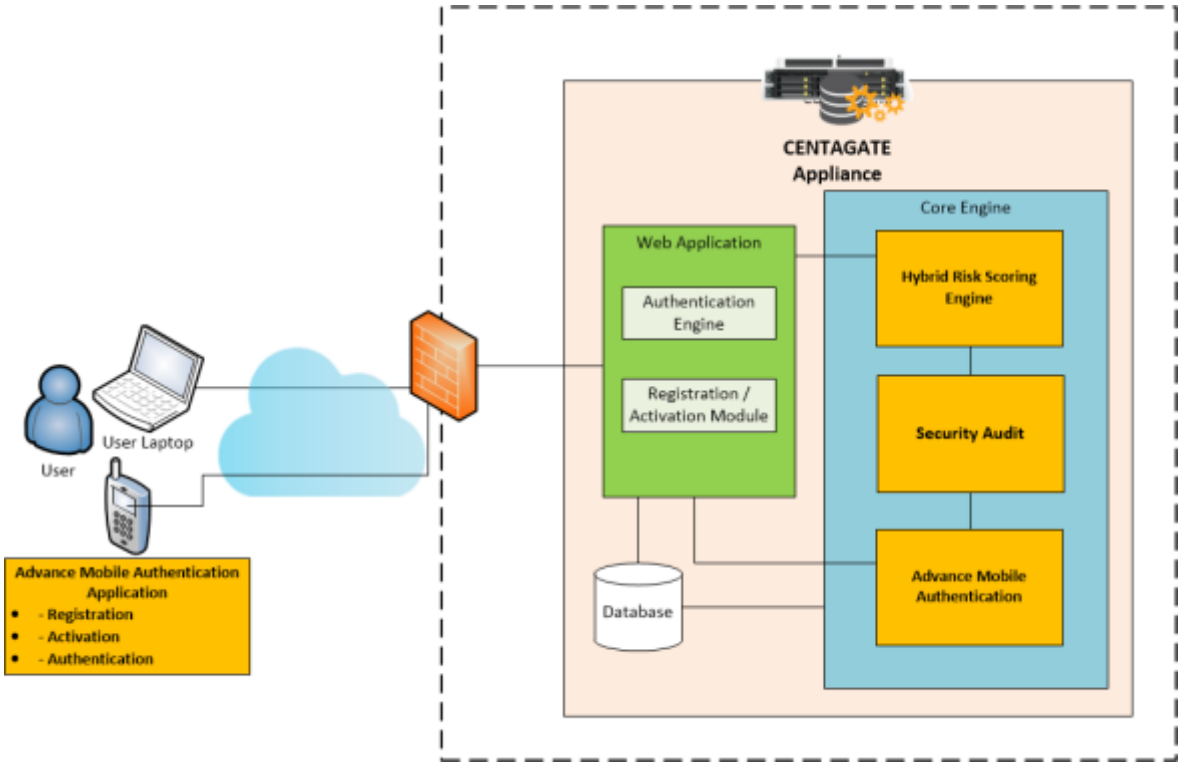

Figure 2: ***TOE Physical Scope of Operational Environment***

CENTAGATE (TOE) System is an authentication platform that enforced secure authentication processes that is capable of calculating risk by its own Hybrid Risk Scoring Engine module capability. The TOE allows authentication process flow to be executed via any relevant Internet Browser and the Hybrid Risk Scoring Engine module will be performed risk calculation. Thus, once the authentication completes the verification process, all the authentication activities will be stored by audit logs function.

Before the TOE is enforce any methods of authentications, the registration process is required to register all the relevant information and components such as the credentials of user linked to the Advance Mobile Authentication Application. There are three ways to register the device via SMS, QR Code, and Offline (Code send for verification in the Challenge and Reponses Process). Offline registration methods only allow binding of OTP Hardware token. This is out of the scope of the evaluation. Also, using SMS to register the device is also out of scope of evaluation.

For QR code registration, CENTAGATE will generate a QR code on the screen that required the CENTAGATE Users to scan the QR code using the Advance Mobile Authentication Application, whilst then a SMS contain the PIN code is sent to CENTAGATE Users using the registered mobile number. Note that, CENTAGATE Users stated here is representing CENTAGATE Administrator, CENTAGATE Company Administrator and CENTAGATE End User.

CENTAGATE Users use the Advance Mobile Authentication Application to perform scans the QR code, which is contains CENTAGATE Users and TOE Server information in an encrypted format. PIN in the SMS send by the TOE Server is to use to derive the key for decrypt the QR code content. When the QR content decrypted successfully, the Advance Mobile Authentication Application in the device that hold its own ECC key and the CENTAGATE Users ECC key is used to generate public keys save in an encrypted format and then sent back to TOE Server.

When TOE Server received those public keys, the next communication onward between the Advance Mobile Authentication Application and the TOE Server will use tokenization processed by enforcing asymmetric encryption together with signature. The next actions include exchange of account information and OTP information between CENTAGATE Server and the CENTAGATE Users Advance Mobile Authentication Application.

During authentication processes, Advance Mobile Authentication Application can be used as one of the authentication factor to access the CENTAGATE Server. The mobility management will handle the tokenization process between CENTAGATE Server and Advance Mobile Authentication Application from end to end perspectives to ensure a secure tokenization process is implemented. With CENTAGATE Advance Mobile Authentication Application, CENTAGATE Users will be able to use Mobile PKI authentication options such as soft certificate and/or Audio Pass, and/or Time-based OTP, CR OTP, and QR Code.

Within the operations of secure authentication via enforce multiple factor of authentication methods, the Hybrid Risk Scoring Engine will be started calculating the risk scores for that methods of authentication processes. It only starts to perform the calculation whenever a CENTAGATE Users has completed a full authentication process.

During the authentication process, CENTAGATE will check CENTAGATE Users risk score that is calculated by Hybrid Risk Scoring Engine and then, determine whether or not is the authentication request is risky and if there is a need to perform step-up authentication (multi-step) for better protection of the authentication processes. The security audit module will log all authentication activities.

Note that all operations of the TOE inclusive of its installation process, management of the TOE and handling of the TOE shall be elaborate further in the Guidance documentations.

1.3.1.2 Logical Scope of the TOE

The following is the list of TOE logical scope that defined in this document, covers by the Security Functional Requirements (SFRs).

A. Security Token Provision

Mobile device with installed Advance Mobile Authentication Application (TOE) can become a security token to authenticate with the TOE Server. Provision of mobile device equipped with Advance Mobile Authentication Application as the Security Token is secured by point-to-point encryption. Asymmetric encryption is used during the initial communication to allow the mobile devices equipped with the Advance Mobile Authentication Application shall submit the generated public keys to TOE Server, thus the communication onward consist of the user information exchange is protected by asymmetric encryption.

B. Mobile Protection

Advance Mobile Authentication Application provides security function where it requires the mobile device user (CENTAGATE Users) to present the application PIN code (symmetric cryptographic process) to access the Advance Mobile Authentication Application installed inside their mobile devices. With the PIN code, process of generating the decryption key to decrypt (symmetric processes) and allow to retrieve the asymmetric keys stored in the secure storage of the Advance Mobile Authentication Application. The cryptographic keys that are used to perform secure authentication processes in the 2FA or/and multi-step, that are need to send back to the TOE Server by perform asymmetric encryption and signature to the response.

C. Mobile PKI (with or without AudioPass)

Advance Mobile Authentication Application capable of performing mobile PKI through a pre-installed software-based certificate (PKCS#12) located in the mobile phone Internet Browser, or using a device called AudioPass that interface with mobile phone via the standard 3.5mm headphone jack. Note that, the AudioPass device token is not part of the scope. The device token on generate the certificate (PKCS#12) for the usage of the Advance Mobile Authentication Application.

D. Hybrid Risk Scoring Engine (Rules Based & Case Based)

Hybrid Risk Scoring Engine will calculate CENTAGATE Users risk scoring based on the authentication process and its behavior. It starts the calculation whenever a user completed a full authentication process. The score will be used by Authentication Module to determine whether step-up authentication is needed or not.

The Hybrid Risk Scoring Engine will collect user system behaviors and environment attributes in each login activities, based on rules defined by the CENTAGATE Administrators either CENTAGATE Administrator role or CENTAGATE Company Administrator role, whilst with the scoring engine will calculate the risk of each user authentication request and monitor the user behavior through the calculation value that are been processes in the TOE backend system. In the case of high risk detected, the system will prompt for another step of authentication (known as multi-step authentication process) to request for confirmation and validity of the user's credentials before allow to access the protected resources.

E. Cryptographic Module

TOE provides various encryptions, including the authentication method use for the CENTAGATE Users and other security function within the TOE system. During mobile device registration (equipped with the Advance Mobile Authentication Application), cryptographic keys distribution module generates a short life AES 256-bit key (there are no key destructions was being performed, whilst key validity through certain defined period of time). The AES key is used to encrypt the CENTAGATE Users and TOE Server information thus return back to screen as a QR code generated by the TOE Server.

A PIN is derived from the AES key and been sends Out-Of-Band to CENTAGATE Users mobile device via SMS. The Advance Mobile Authentication Application in the CENTAGATE Users mobile device, the AES 256-bit key is derived back based on the SMS PIN Code. This AES key is used to encrypt the newly generated public key that is going to send back to the TOE Server. Once public key of Advance Mobile Authentication Application submitted to TOE Server, the following data exchange between the Advance Mobile Authentication Application and the TOE Server will be digitally signed and encrypted using asymmetric keys, include token activation and authentication processes.

The AES key generated by the TOE Server is not applicable for usage if the key generated more than 5 minutes of its limit. Between TOE Server and the Advance Mobile Authentication Application, end-to-end communication is under HTTPS secure channel. Advance Mobile Authentication Application will be removed (made unavailable) for all the keys stored in the devices if it detected that the application run on rooted (Android).

CENTAGATE Users password in the Advance Mobile Authentication Application that is stored in the database is performed a one-way encryption (hashing) to provide the protection.

F. Key Management System

TOE Server uses Key Management System to manage all the cryptographic keys used in the system. This allows the system to handle the key both locally (import from authorized PKI distributors trusted by the organization) and/or using the crypto-hardware such as Hardware Security Module (HSM).

G. Authentication Module

The Authentication Module consist of several components such as: PKI, Mobile PKI, FIDO, SMS, OTP/CR OTP, QR Code, Password and Q&A Model. Note that, the Mobile PKI using AudioPass, Hardware OTP Token and FIDO is not part of TOE Logical Scope.

Informative: CENTAGATE Users stands for roles CENTAGATE Administrator, CENTAGATE Company Administrator and CENTAGATE End User. TOE Administrators is applied for both CENTAGATE Administrator and CENTAGATE Company Administrator.

Table 6: Authentication Module Components

#	Authentication Components	Details
i.	One Time Password (OTP)	OTP is generated by consider the current time of the request, OTP seed, and hashing algorithm to

#	Authentication Components	Details
		ensure the OTP is unique for a specific timespan. OTP is used only once, in an authentication session, and then thrown away and never used again. Note that the Hardware OTP Token is not part of the scope of evaluation. Only OTP generated by the Advance Mobile Authentication Application is part of the scope.
ii.	Challenge & Response (CR) OTP	CR OTP is another variation of OTP authentication whereas the server will generate a challenge, in which will then be used by the CENTAGATE Users to generate the OTP.
iii.	Mobile PKI (Soft Certificate)	Mobile Soft-Cert/PKI is a way to authenticate CENTAGATE Users using PKI certificate stored inside the user's mobile phone within the Advance Mobile Authentication Application. TOE Server will then validate the PKI certificate during authentication process. The validation includes the certificate validity, issuer certificate validity, certificate status, and the certificate owner.
iv.	QR Code & SMS	QR Code authentication is a way to authenticate user by scanning the QR Code showed on the screen. The QR code contains the transaction information, in which will be shown by the Advance Mobile Authentication Application for the CENTAGATE Users to verify. If the transaction details are correct, an OTP, which is basically the signature of the transaction, will be generated and sent back to the TOE Server for verification. TOE Server will generate the signature by rebuilding the challenge based on the transaction information and compare it with the one sent by the CENTAGATE Users. If the signature is the same, then the CENTAGATE Users will be authenticated.
v.	Username & Password	Each of the CENTAGATE Users shall be registered with their own username and password bound to the security configuration policies applied during account creation.

#	Authentication Components	Details
vi.	Question & Answer Model	Part of the 2FA authentication process as one of the option in secure authentication processes or multi-step. CENTAGATE Users required providing legitimate answer for the question asked during the login processes.

H. Web Administration Module

The Web Administration Module consists of several components such as: User Management, Device Management, Security Policy, Self Services, Access Control, System Notification, Security Audit, Token Management, Reporting & Dashboard.

Informative: CENTAGATE Users stands for roles CENTAGATE Administrator, CENTAGATE Company Administrator and CENTAGATE End User. TOE Administrators is applied for both CENTAGATE Administrator and CENTAGATE Company Administrator.

Table 7: Web Administration Module Components

#	Web Administration Components	Details
i.	User Management	User management is a module to manage the CENTAGATE Users in the TOE. This includes user creation, activation, modification, and deletion. Besides basic management, this module enables the TOE Administrators to do password configuration, such as reset password, and manage the authentication methods available for the CENTAGATE Users. User management module also enables TOE Administrators to configure the contextual policy, which is specific for that CENTAGATE Users. The contextual policy can be used as further validation during CENTAGATE Users authentication process.
ii.	Device Management	Device management handles registration and revocation of the mobile devices linked with the TOE Server. During the mobile device registration (provisioning), TOE and mobile device will try to open a secure communication between both parties so that no data leaking or exposure happens during the provisioning which can breach the entire security of the device usage

#	Web Administration Components	Details
		with the TOE. If the device is stolen and keys been compromise, TOE will push a notification to the mobile device and then, the application will delete all the keys stored inside the mobile device, whilst the device provisioning will need to be performed again from the beginning.
iii.	Security Policy	Security policy is a module to configure the security checking for the Hybrid Adaptive Intelligence Authentication platform (part of Hybrid Risk Scoring Engine). Through this module, TOE Administrator can configure the policies to meet their needs, ranging from OS verification, time verification, browser verification, and location verification. For each criteria's, TOE Administrators can choose the condition on how to do the adaptive checking. During authentication, the scoring engine will calculate the CENTAGATE User's login score based on the score given in the security policy and decide whether or not step-up authentication needs to be performed based on the trust level configuration.
iv.	Self Service	Self service module is a module whereby CENTAGATE Users can do operations related with themselves only. This includes changing the password, setting the authentication methods, setting the security questions and answers, and setting the security image to be used during authentication process.
v.	Access Control	Access control module is a module to configure what are the modules accessible for the specific group of people. This is to ensure that CENTAGATE Users cannot access modules, which are not supposed to be accessible by them. Access control can be assigned to multiple users. This is to ease the management of the control, so that TOE Administrators do not have to configure the permission for each CENTAGATE Users. There are three level of access, which is

#	Web Administration Components	Details
		CENTAGATE Administrator, CENTAGATE Company Administrator and CENTAGATE End User. CENTAGATE Administrator is responsible to maintain companies, system configuration, and administration management. CENTAGATE Company Administrator is responsible to maintain own company administrator and CENTGATE End User, manage application integration to CENTAGATE. TOE Administrators manage the security policy of their user authentication. CENTAGATE End user can only manage own authentication methods.
vi.	Security Audit	Security audit provides the review access to the TOE activities reside on authentication or management of the TOE either successful or unsuccessful access. TOE does not provide any function to deletion to the TOE access history information. Every access to the TOE will be logged for auditing, be it successful or failed, along with the time and location of the authentication. All this access data can be used later for report generation to be used by the administrator for auditing and decision-making.
vii.	Token Management	Token management is a module to manage the tokens inside the TOE. The TOE recognizes three types of tokens, namely SMS token, OTP token, and FIDO token. Token management handles all the token related operations such as binding and unbinding token to the CENTGATE Users. By default, TOE enforces the TOE Users to use 2FA to authenticate themselves. This is the minimum recommended way to ensure secure access to the TOE. Upon successful authentication, admin can configure further to support the adaptive authentication. The token register supports the 2FA authentication

#	Web Administration Components	Details
		processes in the TOE system. Adaptive authentication is based on the trust level of the authentication. This is ranging from low trust, medium trust, and high trust. Each of the trust level has its own different value to limit the access to the TOE. Whenever the value does not meet the minimum level set for the trust level, TOE will ask for another authentication (step-up authentication) to verify the identity of the user. All of this can be configured inside the security policy.
viii.	System Notification	System notification is a module, which allows the TOE Administrators to configure on when, and what situation a notification should be sent out. The notification is ranging from events such as license validity to the user management events such as user creation and deletion. The notification can be configured to send via email and/or SMS to the TOE Administrators, users, or both.
ix.	Reporting & Dashboard	Report is a module use to generate data, as requested by the TOE Users, in different formats such as Excel, CSV, and PDF format. The dashboard will give an overview of the data in the TOE. Dashboard for each role is different. CENTAGATE Administrator dashboard will be different than the Company Administrator dashboard. CENTAGATE End User does not have dashboard as this role has limited ability to access the information on the TOE.

I. Mobility Management Module

Mobility management and the Device Management in the Web Administration Module handle registration and revocation of the mobile devices with the TOE. During the mobile device registration (provisioning), TOE and mobile device will try to open a secure communication between both parties so that no data leaking or exposure happens during the provisioning which can breach the entire security of the device usage with the TOE. If the device is stolen and keys been compromise, TOE will push a notification to the mobile device and then, the application will

delete all the keys stored inside the mobile device, whilst the device provisioning will need to be performed again from the beginning.

2 CONFORMANCE CLAIM

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims.

2.1 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 4.
Part 2 conformant	The ST is Common Criteria Part 2 conformant.
Part 3 conformant	The ST is Common Criteria Part 3 conformant with augmentation requirements of ALC_FRL.2.
Package conformant	The ST is package conformant to the package Evaluation Assurance Level EAL4 augmented with ALC_FR.2.
Protection Profile conformance	None.

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

a) Known and presumed threats countered by either the TOE or by the security operational environment;
b) Organizational security policies which is the TOE must comply; and
c) Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspect.

3.1 Threats

The following is the list of threats defined by the TOE.

Table 8: Threats defined by the TOE

Threats Identifiers:	Descriptions:
T.WEB_ATTACK	An attacker may compromise the integrity, availability and confidentially of enterprise information such as customer information, supplier information and relevant information related to the organization by performing web application attacks on the enterprise application authentication module.
T.MOBILE_ATTACK	An attacker may compromise the integrity and confidentially of sensitive data (such as account information and private key data) stored inside the mobile devices by performing mobile application attacks.
T. SUSPICIOUS_REQUEST	An attacker may spoof the user identity after illegally gaining the login credential.
T.DATA_ACCESS	An attacker (either an unauthenticated user or an unauthorized user) may impersonate an authorized user without knowing the authentication credentials to TSF data and /or user data. Plus, an attacker also can be an authorized user that tries to impersonate as another authorized user (with higher authorization or different authorization) without knowing the authentication credentials and gain unauthorized access to TSF data and/or user data.
T.CUMMUNICATION_ATTACK	An attacker can view sensitive data (such as password) and/or manipulate data (account information) between authentication server and mobile application. The password that is being view by attacker can be used for attacker future

Threats Identifiers:	Descriptions:
	login (identity thief). As example, the manipulated data can lead to financial lost such as alter the fund transfer from original account number to attacker account number.
T.USER_ACC_CONTROL	An attacker (either an unauthenticated user or an unauthorized user) may impersonate an authorized user without knowing the authentication credentials and gain unauthorized execution of transaction. An attacker also can be an authorized user that tries to impersonate as another authorized user (with higher authorization or different authorization) without knowing the authentication credentials and gain unauthorized execution of transaction To prevent this attack, user either configuration of risk based scoring engine policy and/or perform approval to the authentication request) in TOE.

3.2 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 9: Threats defined by the TOE

Assumptions Identifier:	Descriptions:
A.NO_EVIL	TOE Administrators and CENTAGATE Users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.
A.TIME_STAMP	The environment will provide reliable time stamps to the TOE.
A.MAIL_SERVER	The environment will provide a mail server to facilitate alerts for TOE. TOE will perform outbound connection to the mail server to send alert in the form of email.
A.PORT_PROTECT	The environment is configured to block all traffic to the Identity access management server (TOE) except for traffic

Assumptions Identifier:	Descriptions:
	required to perform security functionality.
A.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.
A.COMPENT_ADMINSTRATORS	Competent TOE Administrators will be assigned to manage the TOE and the security of the information it contains.
A. MALICIOUS_CODE_NOT_SIGN	It is assumed that all codes used by the TOE for signing are trusted and will be executed by the TOE. Thus, any malicious code destined for the TOE is not signed by a trusted entity, whilst are not allow to be applied to the TOE. Example, a library that performs signature verification, has been replaced by a signed malicious code, and this malicious code will always reply true even though the signature is invalid.
A.OPERATING_SYSTEM	The TOE Administrators shall ensure the OS Backend Server have been hardened to counter the perceived threats.
A. PHYSICAL_PROTECTION	The protection shall ensure TOE hardware will be protected from unauthorized physical modification. Such as access to the hardware based on security camera, room access control to the physical server.

3.3 Organization Security Policies

The Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs is assumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 10: OSPs

OSP Identifiers:	Descriptions:
P.ROLE	Only authorized individuals are assigned by the organization have access to the TOE.
P.CREDENTIAL	Two-Factor Authentication (2FA) refers to option on Mutual SSL Client Authentication, SMS OTP, Time-based OTP, CR OTP, FIDO, Mobile Soft Certificate, Mobile Audio Pass and QR

OSP Identifiers:	Descriptions:
	Code. These available 2FA modules shall be used with the TOE and enforce upon on its usage in ensuring the authentication process are secure and maintain its confidentiality.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from unauthorized deletion or modification.
P.ENFORCE	Enforce user to create the high trust, or medium trust to login the system.

4 SECURITY OBJECTIVES

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 TOE Security Objectives

Table 11: Security Objectives of the TOE (SO)

SO Identifiers:	Descriptions:
O.USER_ACC_CONTROL	The TOE shall ensure the only authenticated and authorized TOE Users can access the TOE functionality and protected application resources.
O.TRAFFIC_PROTECTION	The TOE shall ensure data exchange between server and mobile application is encrypted, assurance of data integrity and mutual authentication.
O.MOBILE_SENSITVE_PROTECTION	The TOE shall ensure data protection against attacks by implementing cryptographic data encryption to mobile application.
O.AUDIT	The TOE shall ensure relevant audit log is tamper resistant.
O.AUTH_MECH	The TOE shall accept multiple authentication mechanism to strengthen users authentication with the supporting platform from the mobile application.
O.ALERT	The TOE shall provide alert mechanism through email to notify TOE Administrators of suspicious request based on risk analysis.

4.2 Security Objective for the Operational Environment

Table 12: Security Objectives of the Operational Environment (SOOE)

SOOE Identifiers:	Descriptions:
OE.NO_EVIL	The TOE Administrators and TOE Users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.
OE.TIME_STAMP	The environment will provide reliable time stamps to the TOE.
OE.MAIL_SERVER	The environment will provide a mail server to facilitate alerts for TOE. TOE will perform outbound connection to the mail server to send alert in the form of email.
OE.PORT_PROTECT	The environment is configured to block all traffic to the TOE server except for traffic required to perform security functionality.
OE.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.
OE.COMPENT_ADMINSTRATORS	The environment will assign the competent Administrators to manage the TOE and the security of the information it contains.
OE.MALICIOUS_CODE_NOT_SIGN	Malicious code destined for the TOE is not signed by a trusted entity. A signed malicious code will be trusted and execute by the TOE. Example, a library that performs signature verification, has been replaced by a signed malicious code, and this malicious code will always reply true even though the signature is invalid.
OE.OPERATING_SYSTEM	The operating system selected had been hardened to counter the perceived threats. The server side hardening includes establish a secure configuration to the OS, configure OS audit logs, configure proper OS authentication and permission, and ensure legacy services are not enabled.
OE.PHYSICAL_PROTECTION	The protection shall ensure TOE hardware will be protected from unauthorized physical modification. Such as access to the hardware based on security camera, room access control to the physical server.

4.3 Security objectives rationale

4.3.1 Security objective for the TOE Rationale

Table 13: Mapping of SO with Threats Rationale

Threats	Objective	Rationale
T.WEB_ATTACK T.USER_ACC_ CONTROL	O.USER_ACC_CONTROL O.AUTH_MECH	**O.USER_ACC_CONTROL** Ensure that only authentication and authorized users can access the TOE functionality and protected application resources. Thus, only legitimate credentials with valid input able to be processed by the TOE.
		O.AUTH_MECH Ensure acceptance of multiple authentication mechanism to strengthen users' authentication via mobile application to mitigate threat due to of user selecting a weak password. Additional factor of authentication by providing more than username and password input of information secure the TOE from attacks related to web application threats.
T.MOBILE ATTACK	O.MOBILE_SENSITVE_ PROTECTION	**MOBILE_SENSITVE_PROTECTION** Helps to mitigate threats from attacker that perform hacking activity on mobile application by having the data encryption applied on the TOE.
T. SUSPICIOUS_ REQUEST	O.ALERT O.TRAFFIC_PROTECTION	**O.ALERT** Ensures that an alert mechanism through email to notify administrators of suspicious request based on risk analysis. Thus, if there any unauthorized activities are detected through notification configured by the TOE Administrator on the TOE.
		O.TRAFFIC_PROTECTION Ensure that request performed are valid

Threats	Objective	Rationale
		between the TOE components (Advance Mobile Authentication Application and the TOE Server) and it is encrypted, whilst assurance of data integrity and mutual authentication.
T.DATA_ACCESS	O.AUTH_MECH O.AUDIT	**O.AUTH_MECH** Ensures that accept multiple authentication mechanism to strengthen user's authentication via mobile application to mitigate threat because of user selecting a weak password.
		O.AUDIT Ensures that all audit logs are tamper resistant. Thus, allows the TOE Administrators to review the activities on the TOE if there any threats performed towards the TOE.
T.CUMMUNICATION_ATTACK	O.TRAFFIC_PROTECTION	**TRAFFIC_PROTECTION** Ensure data exchange between server and mobile application is encrypted, assurance of data integrity and mutual authentication. Thus, if there threats that applied to capture any relevant credentials can be mitigate by additional enforcement on the authentication mechanism.

4.3.2 Security Objectives for the Operational Environment Rationale

Table 14: Mapping of SOOE and Assumptions

Assumptions	Objective	Rationale
A.NO_EVIL	OE.NO_EVIL	This objective for the environment ensures that the assumption is upheld that TOE administrator and users are trusted and will perform their duties correctly, ensuring the TOE operates securely.
A.TIME_STAMP	OE.TIME_STAMP	This objective for the environment ensures that the assumption is upheld that the environment will provide reliable time stamps to support the audit log generation.
A.MAIL_SERVER	OE.MAIL_SERVER	This objective for the environment ensures that the assumption is upheld that the environment will provide a mail server to the TOE as supporting component in the operations, where the mail server will be the platform of sending alert via email.
A.PORT_PROTECT	OE.PORT_PROTECT	This objective for the environment ensures that the assumption is upheld that TOE server is located within the enterprise boundary and is protected from unauthorized logical access (remote access). Additionally, the environment is configured to block all traffic except for the traffic required to perform security functionality.
A.FIREWALL	OE.FIREWALL	This objective for the environment ensures that the assumption is upheld that the gateway filtering is implemented; only allowing HTTP and HTTPS traffic to pass through to TOE.
A.COMPENT_ADMINSTRATORS_AND_OPERATORS	OE.COMPENT_ADMINSTRATORS_AND_OPERATORS	This objectives for the environment ensures that the assumption is upheld that the environment will assigned the competent Administrators to manage the TOE and the security of the information it contains
A.MALICIOUS_CODE	OE.MALICIOUS_CODE_N	This objective for the environment ensures

Assumptions	Objective	Rationale
NOT SIGN	OT_ SIGN	that the assumption is upheld that the TOE will able to filter malicious code destined for the TOE that is not signed by a trusted entity.
A_OPERATING_SYSTEM	OE_OPERATING_SYSTEM	This objective for the environment ensures that the assumption is upheld that the environment in which, the backend server OS of the TOE is hardened inclusive of the mobile OS platforms. Thus, if not, the Advance Mobile Authentication Application as the TOE will removed (made unavailable) key when detected that the OS is rooted or jail broken during start-up of the application.
A_PHYSICAL_ PROTECTION	OE_PHYSICAL_ PROTECTION	This objective for the environment ensures that the assumption is upheld that the TOE Administrators will ensure TOE hardware will be protected from unauthorized physical modification or access.

4.3.1 Organisational Security Policy Rationale

Table 15: Mapping of SOOE and OSPs.

Organisational Security Policy	Objective	Rationale
P.ROLE	O.USER_ACC_CONTROL	**O.USER_ACC_CONTROL** Ensure that only authentication and authorized TOE Users can access the TOE functionality and protected application resources.
P.INTEGRITY	O.MOBILE_SENSITVE_PROTECTION	**MOBILE_SENSITVE_PROTECTION** Helps to mitigate threats from attacker that perform hacking activity on mobile application (Advance Mobile Authentication Application) by having the encryption.
	O.ALERT	**O.ALERT** Ensures that an alert mechanism through email to notify administrators of suspicious

		request based on risk analysis.
	O.TRAFFIC_PROTECTION	**O.TRAFFIC_PROTECTION** Ensure that request will be valid request from the server and it is encrypted, assurance of data integrity and mutual authentication.
	O.AUDIT	**O.AUDIT** Ensures that relevant audit log is tamper resistant in preventing the data been deleted.
P.CREDENTIAL	O.AUTH_MECH	**O.AUTH_MECH** Ensure acceptance of multiple authentication mechanism to strengthen users' authentication via mobile application (Advance Mobile Authentication Application) to mitigate threat due to of user selecting a weak password.
P.ENFORCE	O.USER_ACC_CONTROL	**O.USER_ACC_CONTROL** Ensure that only authentication and authorized users can access the TOE functionality and protected application resources. The policies are enforced for the TOE Administrators, this role create the high trust, medium trust or low trust to login the system.

5 SECURITY REQUIREMENTS

5.1 SFR formatting

The following conventions are a set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.

a) The refinement operation is used to add or remove details to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text** for additional details and ~~strike through underline text~~ for removing detail of a requirement.
b) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by italic text in square brackets, [*selection value*].
c) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment format is indicated by showing the value in square brackets labeled as: [assignment value].
d) The iteration operation is used when a component is repeated with varying operations. Iteration format is denoted by showing the iteration number in parenthesis following the component identifier: (iteration number).

5.2 Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in Table, below.

Table 16: SFRs List.

No	Component	Component Name
Class FAU: Security Audit		
1	FAU_ARP.1	Security alarms
2	FAU_GEN.1	Audit data generation
3	FAU_GEN.2	User identity association
4	FAU_SAR.1	Audit review
5	FAU_SAR.2	Restricted audit review
6	FAU_SAA.1	Potential violation analysis
7	FAU_SAA.2	Profile based anomaly detection

No	Component	Component Name
Class FDP: User data protection		
8	FDP_ACC.1	Subset access control
9.	FDP_ACF.1	Security attribute based access control
Class FIA: Identification and Authentication		
10.	FIA_AFL.1	Authentication failure handling
11	FIA_ATD.1	User attribute definition
12	FIA_UID.1	Timing of identification
13	FIA_UID.2	User identification before any action
14	FIA_UAU.1	Timing of identification
15	FIA_UAU.2	User authentication before any action
16	FIA_UAU.6	Re-authenticating
17.	FIA_UAU.5	Multiple authentication mechanisms
Class FMT: Security management		
18.	FMT_MSA.1	Management of security attributes
19	FMT_MSA.3	Static attribute initialisation
20	FMT_SMF.1	Specification of Management Functions
21	FMT_SMR.1	Security roles
Class FTA: TOE Access		
22	FTA _TAH.1	TOE access history
Class FCS: Cryptographic key management		

No	Component	Component Name
23	FCS_CKM.1	Cryptographic key generation
24	FCS_CKM.2	Cryptographic key distribution
26	FCS_CKM.4	Cryptographic key destruction
27	FCS_COP.1	Cryptographic operation

5.2.1 Security Audit (FAU)

5.2.1.1 *Security Alarms (FAU_ARP.1)*

Hierarchical to: No Other components

FAU_ARP.1.1	The TSF shall take [send an email alert to TOE Administrators that provided the link to access the TOE Server for further investigate the event details] upon detection of a potential security violation.
Dependencies	FAU_SAA.1Potential violation analysis
Application Notes:	*In any of security violation events related to the TOE, such as unauthorized access to the TOE by unknown users by using only username and password without the enforcement of 2FA mechanism; thus, the TOE shall send an email alert to the TOE Administrators upon the event. Plus, the email contains the link to access the TOE to allow TOE Administrators further investigate the event details.*

5.2.1.2 *Potential violation analysis (FAU_SAA.1)*

Hierarchical to: No other components

FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [repetitive of login failure attempts, repetitive of unsuccessful access requests] known to indicate a potential security violation; b) [NONE].
Dependencies	FAU_GEN.1 Audit data generation

5.2.1.3 *Profile based anomaly detection (FAU_SAA.2)*

Hierarchical to: No other components.

FAU_SAA.2.1	The TSF shall be able to maintain profiles of system usage, where an Individual profile represents the historical patterns of usage performed by the member(s) of [Profile Target Group].
FAU_SAA.2.2	The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
FAU_SAA.2.3	The TSF shall be able to indicate a possible violation of the enforcement of the SFRs when a user's suspicion rating exceeds the following threshold conditions [when user login with score less than the defined in the trust level configuration (Security Policy Tab in the TOE), the login attempt is considered as risk to the TOE/protected resources and email will be sent to TOE Administrators as an alert. There are 3 trust levels defined in the Security Policy Tab (TOE Server), which is Low Trust (require 25-49 score), Medium Trust (50-74) and High Trust (75 and above)].
Dependencies:	FIA_UID.1 Timing of identification
Application Notes:	*Definition of* Profile Target Group*: Group of users that is assigned under the defined security policy. Where Security Policy contains list of rules based on user login history and/or condition that define the risk scoring.*

5.2.1.4 *Audit data generation (FAU_GEN.1)*

Hierarchical to: No other components.

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: ~~a) Start-up and shutdown of the audit functions;~~ b) All auditable events for the [*detailed*] level of audit; and c) [Refer to Appendix B and additionally, the following events recorded, as stated below: i. Repeated login failure, repeated unsuccessful access requests; ii. User information (including user email, name, and authentication status); and iii. Case information (remark and date time).]
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Audit Severity].
Dependencies:	FPT_STM.1 Reliable time stamps (Fulfilled by Environment).
Application Notes:	*Refinement on the FAU_GEN.1.1 (Item a), in which there is no function of the TOE that allows the TOE Administrators to enable/disable the audit functions without the needs of shutdown/turn on the TOE as a whole.* *The requirement of FPT_STM.1 is been provided by the underlying operating system hosting the TOE Server. Thus, TOE Administrators shall ensure the underlying operating system provide reliable timestamps and hardened for security measurement.*

5.2.1.5 *User identity Association (FAU_GEN.2)*

Hierarchical to: No other components.

FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event
Dependencies	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

5.2.1.6 *Audit review (FAU_SAR.1)*

Hierarchical to: No other components.

FAU_SAR.1.1	The TSF shall provide [TOE Administrators] with the capability to read [Audit Time, Audit Detail, Subject of the audit event] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information**.**
Dependencies	FAU_GEN.1 Audit data generation

5.2.1.7 *Restricted audit review (FAU_SAR.2)*

Hierarchical to: No other components.

FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
Dependencies	FAU_SAR.1 Audit review

5.2.2 Identification and authentication (FIA)

5.2.2.1 *Authentication failure handling (FIA_AFL.1)*

Hierarchical to: No other components

FIA_AFL.1.1	The TSF shall detect when [*an administrator configurable positive integer within [3 to 10]*] unsuccessful authentication attempts occur related to [access to the TOE/protected resources]**.**
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [block the user account]**.**
Dependencies:	FIA_UAU.1 Timing of authentication

5.2.2.2 *User attribute definition (FIA_ATD.1)*

Hierarchical to: No other components.

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [a. User Name; b. Type of authentication mechanism assigned; c. Credential for the assigned authentication mechanism; d. Role; e. Authentication Failure counter; and f. Status]**.**
Dependencies	No dependencies

5.2.2.3 *User authentication before any action (FIA_UAU.2)*

Hierarchical to: FIA_UAU.1 Timing of authentication

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

5.2.2.4 *Multiple authentication mechanisms (FIA_UAU.5)*

Hierarchical to: No other components.

FIA_UAU.5.1	The TSF shall provide [2-factor authentication (2FA) mechanism, kindly refer to Appendix D column: Authentication, for details] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [refer to Appendix D column: Method of Authentication, for details].
Dependencies:	No dependencies.

5.2.2.5 *Re-authenticating (FIA_UAU.6)*

Hierarchical to: No other components.

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [a. Session timeout; and b. Suspicious transaction or login request detected].
Dependencies:	No dependencies.
Application Notes:	*The TOE will return a parameter "multiStepAuth=true", to reflect the requirement of performing a step-up re-authentication.*

5.2.2.6 *Timing of identification (FIA_UID.1)*

Hierarchical to: No other components.

FIA_UID.1.1	The TSF shall allow [Username, Password, 2-factor authentication (2FA)] 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.
Dependencies:	No dependencies.
Application Notes:	Based on the configuration, user can perform login using the following combination: a) Username + password; b) Username + password + 2FA; c) Username + password + 2FA + step-up (when risk detected); d) Username + password + 2FA + stop login (when risk detected); e) Username + password + step-up (when risk detected); or

f) Username + password + stop login (when risk detected).

5.2.2.7 *User authentication before any action (FIA_UID.2)*

Hierarchical to: FIA_UID.1 Timing of identification

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

5.2.2.8 *FIA_UAU.1 Timing of authentication (FIA_UAU.1)*

Hierarchical to: No other components

FIA_UAU.1.1	The TSF shall allow [company registration, forgot password] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification.

5.2.3 Security management (FMT)

5.2.3.1 *Management of security attributes (FMT_MSA.1)*

Hierarchical to: No other components.

FMT_MSA.1.1	The TSF shall enforce the [access control SFP: P.CREDENTIAL] to restrict the ability to [*change default, query, modify, delete*,] the security attributes [Refer to Appendix C] to [TOE Administrators].
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
Application Notes	*Refer to Appendix C for details on TOE Administrators and its roles.*

5.2.3.2 *Static attribute initialisation (FMT_MSA.3)*

Hierarchical to: No other components

FMT_MSA.3.1	The TSF shall enforce the [access control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [TOE Administrators] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes. FMT_SMR.1 Security roles**.**

5.2.3.3 *Specification of Management Functions (FMT_SMF.1)*

Hierarchical to: No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [Refer Appendix C]
Dependencies:	No dependencies.

5.2.3.4 *Security roles (FMT_SMR.1)*

Hierarchical to: No other components

FMT_SMR.1.1	The TSF shall maintain the roles [CENTAGATE Administrator, Company Administrator, End user].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

5.2.4 TOE access (FTA)

5.2.4.1 *TOE access history (FTA_TAH.1)*

Hierarchical to: No other components.

FTA_TAH 1.1	Upon successful session establishment, the TSF shall display the [*date, time, method, location*] of the last successful session establishment to the user.
FTA_TAH 1.2	Upon successful session establishment, the TSF shall display the [*date, time, method, location*] 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.
Dependencies	No dependencies.

5.2.5 User Data Protection (FDP)

5.2.5.1 *Security attribute based access control (FDP_ACF.1)*

Hierarchical to: No other components.

FDP_ACF.1.1	The TSF shall enforce the [access control SFP] to objects based on the following**:** [Refer to Appendix C with the security attributes: username, password and 2-factor authentication inclusive of components reside in the Advance Mobile Authentication Application].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Refer to Appendix C with the security attributes: username, password and 2-factor authentication inclusive of components reside in the Advance Mobile Authentication Application].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [None].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None].
Dependencies:	FDP_ACC.1 Subset access control.

FMT_MSA.3 Static attribute initialization

5.2.5.2 *Subset access control FDP_ACC.1*

Hierarchical to: No other components.

FDP_ACC.1.1	The TSF shall enforce the [access control SFR: P.ROLE] on [Refer to Appendix C with the security attributes: username, password and 2-factor authentication inclusive of components reside in the Advance Mobile Authentication Application]
Dependencies:	FDP_ACF.1 Security attribute based access control

5.2.6 Cryptographic support (FCS)

5.2.6.1 *Cryptographic key generation (FCS_CKM.1)*

Hierarchical to: No other components.

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with specified cryptographic key generation algorithm [AES, ECC] and specified cryptographic key sizes [AES: 128-bit, AES: 256-bit, ECC: 521-bit] that meet the following**:** [NIST; FIPS-197; NIST.SP.800-57]**.**
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Application Notes:	*Based on the stated key sizes, algorithms and standards used for the cryptographic operations in the TOE, shall emulates the cryptographic operations based on TOE operations either in the mode usage of: symmetric or asymmetric.*

5.2.6.2 *Cryptographic key distribution (FCS_CKM.2)*

Hierarchical to: No other components

FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[**a short life AES 256bits key is generated. Part of the key sends Out-Of-Band to user mobile phone via SMS. AES 256bits key is derived from the SMS containing the PIN code; use for public key exchange between the TOE Server and TOE Users (Advance Mobile Authentication Application). Once TOE Users Public Key submit to TOE Server, the following data exchange will be in digitally signed and encrypted using asymmetric key. This end-to-end communication between

both entities (TOE Server & Advance Mobile Authentication Application) is under HTTPS secure channel] that meets the following: **[**PKCS#11**].**

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Application Notes:	*Based on the stated key sizes, algorithms and standards used for the cryptographic operations in the TOE, shall emulates the cryptographic operations based on TOE operations either in the mode usage of: symmetric or asymmetric. This is for the mobile provisioning security function related to Advance Mobile Authentication Application.*

5.2.6.3 *Cryptographic key destruction (FCS_CKM.4)*

Hierarchical to: No other components**.**

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[**send push notification from TOE Server to mobile devices of the TOE Users (Advance Mobile Authentication Application when untrusted access in the mobile application is detected, such as e.g. device android OS are rooted**]** that meets the following: **[**PKCS#11**].**
Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation**]**
Application Notes:	*Note that, the definition of "destroy" in the SFR statement are means to explained that the key will be made unavailable for any access either the TOE, TOE Users or any external parties.*

5.2.6.4 *Cryptographic operation (FCS_COP.1)*

Hierarchical to: No other components.

FCS_COP.1.1	The TSF shall perform **[**data encryption and/or decryption, digital signature generation and/or verification, Cryptographic key agreement and cryptographic key sizes **[**ECC: 521-bit, RSA: 2048-bit, RSA: 4096-bit**]** that meet the following: **[**NIST; FIPS-197; NIST.SP.800-57**].**
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Application Notes: *Based on the stated key sizes, algorithms and standards used for the cryptographic operations in the TOE, shall emulates the cryptographic operations based on TOE operations either in the mode usage of: asymmetric.*

5.3 Security Requirements Rationale

Table 17: SFRs Rationale

Objectives	SFR	Rationale
O.USER_ACC_CONTROL	FIA_ATD.1	The requirement meets the objective O.USER_ACC_CONTROL by defining the attributes from TOE Users authentication.
	FIA_AFL.1	O.USER_ACC_CONTROL Is fulfilled by detect invalid login attempt to the TOE. And is fulfilled by limit access of unauthorized user to access the TOE. The account will be disabled if invalid credentials have met the maximum attempts allowed.
	FIA_UAU.5.	The requirement meets the objective O.USER_ACC_CONTROL by providing A mechanism to accept credentials to support TOE Users authentication.
	FIA_UID.1	The requirement meets the objective O.USER_ACC_CONTROL by allowing authentication methods on behalf of the user to be performed before the user is identified.
	FIA_UID.2	The requirement meets the objective O.USER_ACC_CONTROL by allowing user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
	FAU_SAA.1	The requirement meets the objective O.USER_ACC_CONTROL applying a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
	FAU_GEN.1	The requirement meets the objective O.USER_ACC_CONTROL by generating an audit record of auditable events.
	FAU_GEN.2	The requirement meets the objective O.USER_ACC_CONTROL by audit events resulting from actions of identified users; the O.USER_ACC_CONTROL shall be able to associate

Objectives	SFR	Rationale
		each auditable event with the identity of the user that caused the event.
	FDP_ACF.1	The requirement meets the objective O.USER_ACC_CONTROL by enforcing the [access control SFP] to objects based on the following: ▪ O.USER_ACC_CONTROL enforces the rules to determine if an operation among controlled subjects and controlled objects is allowed. ▪ O.USER_ACC_CONTROL explicitly deny access of subjects to objects based on the following additional rules.
	FIA_UAU.6	O.USER_ACC_CONTROL Re-authenticates the user in the case of session time out.
	FMT_SMR.1	O.USER_ACC.CONTROL is fulfilled as the roles to access the TOE are defined through legitimate users registered in the TOE with assigned specific privileges to access the TOE security functions.
O.TRAFFIC_PROTECTION	FCS_CKM.1	O.TRAFFIC_PROTECTION is fulfilled by generating a cryptographic to secure the data for the transfer.
	FCS_CKM.2	O.TRAFFIC_PROTECTION is fulfilled by ensures the secure cryptographic distribution between TOE Server and mobile application (Advance Mobile Authentication Application).
	FCS_CKM.4	This requirement supports O.TRAFFIC_PROTECTION by providing a method for removing the cryptographic keys, thereby ensuring that an unauthorized user does not access the keys.
	FCS_COP.1	This requirement supports O.TRAFFIC_PROTECTION by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing through or being stored on the TOE, or data passing between the TOE and an external device.

Objectives	SFR	Rationale
	FAU_SAA.1	O.TRAFFIC_PROTECTION fulfills by applying a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
	FAU_GEN.1	O.TRAFFIC_PROTECTION fulfills by generating an audit record of the following auditable events.
	FIA_UAU.5	The requirement meets the objective O.TRAFFIC_PROTECTION by providing a mechanism to accept credentials to support user authentication.
	FIA_UAU.6	O.TRAFFIC_PROTECTION is fulfilled by re-authenticates the user in the case of session time out/ suspicious transaction.
	FIA_UID.2	The requirement meets the objective O.TRAFFIC_PROTECTION by allowing user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user
	FMT_MSA.1	O.TRAFFIC_PROTECTION is fulfills by enforcing the OSP to restrict the ability to change default, query, modify and delete the security attributes values.
	FMT_MSA.3	O.TRAFFIC_PROTECTION is fulfilled by enforcing the security policies in providing restrictive default values for security attributes that are use in enforcing the SFP.
	FMT_SMF.1	O.TRAFFIC_PROTECTION is capable of performing management as defined in the Appendix C whilst mapped back to the role of the TOE and its subjects.
	FTA_TAH.1	Upon successful session establishment, O.TRAFFIC_PROTECTION will display the [date, time, method, location] of the last successful session establishment to the user Upon successful session establishment, the O.TRAFFIC_PROTECTION will display the [date, time, method, location] of the last unsuccessful

Objectives	SFR	Rationale
		attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. The O.TRAFFIC_PROTECTION will not erase the access history information from the user interface without giving the user an opportunity to review the information.
	FDP_ACF.1	The requirement meets the objective O.TRAFFIC_PROTECTION by enforcing the [access control SFP] to objects based on the following stated in Appendix C. O.TRAFFIC_PROTECTION enforces the rules to determine if an operation among controlled subjects and controlled objects is allowed. O.TRAFFIC_PROTECTION explicitly deny access of subjects to objects based on the following additional rules.
O.MOBILE_SENSITVE _PROTECTION	FCS_CKM.1	O.MOBILE_SENSITVE_PROTECTION Is fulfills by generating a cryptographic to secure the data for the transfer.
	FCS_CKM.4	This requirement supports O.MOBILE_SENSITVE_PROTECTION by providing a method for removing the cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorized and any valid request known by the TOE.
	FCS_COP.1	This requirement supports O.MOBILE_SENSITVE_PROTECTION by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing through or being stored on the TOE, or data passing between the TOE and an external device.
	FDP_ACC.1 FDP_ACF.1	This requirement supports O.MOBILE_SENSITVE_PROTECTION by providing the subject and object for the protection of the user data through the enforcement of 2FA credentials.

Objectives	SFR	Rationale
O.AUDIT	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_ARP.1 FAU_SAA.2	O.AUDIT fulfills based on these requirements: ▪ FAU_GEN 1: generates the required audit data. ▪ FAU_GEN 2: Associate each auditable event with the identity of the user that caused the event. ▪ FAU_SAR 1: allow only TOE Administrators to read audit data and the audit reports are presented in MS Excel, CSV or PDF formats. ▪ FAU_SAR 2: Denies the audit data access to all the users except those who have been granted the read access. ▪ FAU_ARP 1: Generates email-based alerts as configured in the TOE for reporting access control violations. ▪ FAU_SAA.2. Detect potential violation of the enforcement by applying set of rules in the recorded audit events.
	FTA_TAH.1	FTA_TAH.1 is fulfills based on the track record of the last successful session establishment by the user. Upon successful session establishment, the TOE display date, time, method and location of the last successful and unsuccessful session establishment for his review.
	FAU_SAA.1	FAU_SAA.1 TSF will be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs and O.AUDIT generates an audit on this events.
	FIA_AFL.1	O.AUDIT will be able to detect when an administrator configurable positive integer within 3 to 10 unsuccessful authentication attempts occur, and generate an audit on this events. When the defined number of unsuccessful authentication attempts has been met, the TSF shall block the user account and generate an audit on these events.
O.AUTH_MECH	FIA_UAU.5	O.AUTH_MECH is fulfills in the following manner

Objectives	SFR	Rationale
		by providing a mechanism to accept credential in the form of 2FA authentication as listed in the Appendix D.
	FIA_UAU.1 FIA_UAU.2	O.AUTH_MECH is fulfills by providing relevant information before the process of authentication performed by the TOE Users.
O.ALERT	FAU_ARP 1	O.ALERT is fulfilled in the following manner FAU_ARP 1: Generates email based alerts as configured in the TOE for reporting access control violations.

5.4 Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components to Evaluation Assurance Level 4 (EAL4).

This section contains the assurance requirements for the TOE.

Table 18: SARs.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1Implementation representation of the TSF ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined lifecycle model ALC_TAT.1 Well-defined development tools ALC_FLR.2 Flaw reporting 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.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing

Assurance Class	Assurance components
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability	AVA_VAN.3 Focused vulnerability analysis

5.5 Assurance Requirements Rationale

This ST claims compliance to the assurance requirements from the CC EAL4 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The TOE is intended to address the common authentication and authorization attacks on the web-based applications.

Thus, provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behavior.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

5.6 Rationale for not addressing all dependencies

FPT_STM.1 is a dependency of FAU_GEN.1 that has not been included. Which is the operational environment shall provides reliable timestamps for the TOE in supporting of the TOE activities recorded under the Security Audit functions.

6 TOE SUMMARY SPECIFICATION

This section provides the TOE summary specification in which, illustrates the justification of CENTAGATE security features in achieving the requirements stated in the TOE Security Functional Requirements section (SFR).

6.1 TOE Mobile App: CENTAGATE Advance Mobile Authentication Application

A. Security Token Provision

TOE as a authentication platform, provide facility to enable strong multifactor authentication, allow authentication to be supported by mobile devices through CENTAGATE Advance Mobile Authentication Application and the Hybrid Risk Scoring Engine that will calculate assumption risks based on TOE Users authentication procedures and audit log record all the authentication securely by implementing the Case-Based or Rules-Based security policies through the TOE Users authentication process flow behavior.

Between the TOE Server and the TOE Mobile App, the TOE Users shall use the TOE Mobile App as support components of the TOE authentication procedures in enabling the 2-Factor Authentication. Thus, ensuring the TOE Mobile App is not been compromise, the provision features allows the TOE to protect via cryptographic process by enabling symmetric encryption by PIN enable features plus asymmetric encryption for secure exchange cryptographic keys between TOE Server and TOE Mobile App.

SFRs Mapped:	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1.

B. Mobile Protection

In additional to the TOE security features in the TOE Mobile App, the mobile protection provides security enforcement of PIN code symmetric encryption in protecting the TOE Mobile App from any unauthorized access by illegitimate individuals. With the PIN code, process of generating the decryption key to decrypt (symmetric processes) and allow to retrieve the asymmetric keys stored in the secure storage of the Advance Mobile Authentication Application. The cryptographic keys that are used to perform secure authentication processes in the 2FA or/and multi-step process flow in the authentication procedures in the TOE operational environment.

SFRs Mapped:	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1.

C. Mobile PKI (with or without AudioPass)

In the process of secure authentication procedure that enables the 2-Factor Authentication process flow (2FA), the mobile PKI capabilities in the Advance Mobile Authentication Application to store securely the software-based certificate (PKCS#12) located in the mobile phone Internet Browser, or using a device called AudioPass that interface with mobile phone via the standard 3.5mm headphone jack. Note that, the AudioPass device token is not part of the TOE scope.

Options of using Mobile PKI (with or without the AudioPass) are based on the access control options registered in the TOE Server by the TOE Administrators. Enforcement of 2FA or enable mode of multistep authentication procedure are based on the configuration applied and enforced by the TOE through security policies configuration with trust level enable.

SFRs Mapped:	FIA_ATD.1, FIA_UAU.5, FIA_UID.1, FMT_SMR.1, FDP_ACF.1, FDP_ACC.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1.

6.2 TOE Server: CENTAGATE Web Based Application System

A. Hybrid Risk Scoring Engine

The functions of the Hybrid Risk Scoring Engine as the backend components of the TOE that enforce the security criteria in determining the access control risk towards the TOE and the TOE Users through the authentication process flow by calculating based upon several factors such as IP Address, Geo-Location and etc. thus, to ensure the risk that been introduced during the authentication processes are been reduced.

Furthermore, in the events of the risk authentication process are been identify through the Hybrid Risk Scoring Engine calculation, trust level mechanism will activate and enforcing the multistep authentication procedure to ensure the TOE Users are legitimate users with the appropriate authentication support components relies on the Advance Mobile Authentication Application at the TOE Users registered mobile device. Note that, each legitimate TOE Users will have different mode of 2-factor authentication based on the assigned authentication components that mapped towards Group assignment.

Each TOE Users Group have unique configuration of the support components of the TOE such as Q&A (Question & Answer), OTP Token, CR OTP, SMS, PKI, FIDO (not in the TOE scope), QR Code, Mobile Cert and Mobile AudioPass that configured by the TOE Administrators of the TOE. The configuration of the Group is based on the organization security policies, in ensuring the assets (protected resources) are protected and maintain securely by the TOE operational environment. In the events of risky authentication processes, the multistep will initiate the TOE Users validation upon authentication process flow, thus leading towards the activation of Trust level security mechanism in determining the next TOE 2FA requirements to be initiated.

SFRs Mapped:	FAU_ARP.1, FAU_SAA.1, FAU_SAA.2, FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FIA_UID.2, FIA_UAU.1, FMT_SMR.1, FTA_TAH.1, FDP_ACF.1 and FDP_ACC.1.

B. Cryptographic Module

The TOE provides various encryptions, including the authentication method use for the CENTAGATE Users and other security function within the TOE system. During mobile device registration (equipped with the Advance Mobile Authentication Application), cryptographic keys distribution module generates a short life AES 256-bit key. The AES key is used to encrypt the CENTAGATE Users and TOE Server information thus return back to screen as a QR code generated by the TOE Server.

The TOE Server will send out PIN Code via SMS platform (Out-of-Band) to the TOE Users mobile devices that are intended to receive the code for TOE Advance Mobile Authentication Application activation in the process of exchange public keys between the TOE mobile app and the TOE Server. The Advance Mobile Authentication Application in the CENTAGATE Users mobile device, the AES 256-bit key is derived back based on the SMS PIN Code. This AES key is used to encrypt the newly generated public key that is going to send back to the TOE Server. Once public key of Advance Mobile Authentication Application submitted to TOE Server, the following data exchange between the Advance Mobile Authentication Application and the TOE Server will be digitally signed and encrypted using asymmetric keys, include token activation and authentication processes.

The AES key generated by the TOE Server is not applicable for usage if the key generated more than 5 minutes of its limit. Between TOE Server and the Advance Mobile Authentication Application, end-to-end communication is under HTTPS secure channel. Advance Mobile Authentication Application will be removed (mad unavailable) all the keys stored in the devices if it detected that the application run on rooted (Android) or jail broken (iOS) environment.

Hashing is being implemented in the Advance Mobile Authentication Application that is use for password storage with encryption applied, preventing unauthorized access to the TOE mobile app.

SFRs Mapped:	FMT_SMR.1, FDP_ACF.1, FDP_ACC.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1.

C. Key Management System

TOE Server has its own Key Management System to manage all the cryptographic keys used in the system. This allows the system to handle the key both locally and using the crypto-hardware such as Hardware Security Module (HSM). Thus, certificates pre-installed in the TOE will validated all the usage of the certificates within the TOE operational environment in ensuring there is no illegitimate or unknown type of certificate been used that is not recognized by the TOE. Nonetheless, if the HSM is not being deployed or unavailable, trusted parties that endorsed by the organization shall provide relevant cryptographic keys and certificates that is being use by the TOE for its operational environment requirements.

SFRs Mapped:	FMT_SMR.1, FDP_ACF.1, FDP_ACC.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1.

D. Authentication Module

The Authentication Module consists of several components such as: PKI, Mobile PKI, FIDO, SMS, OTP/CR OTP, QR Code, Password and Q&A Model. Note that, the Hardware OTP Token and FIDO is not part of TOE Logical Scope. Informative: CENTAGATE Users stands for roles CENTAGATE Administrator, CENTAGATE Company Administrator and CENTAGATE End User.

In the Table 6 explained the list of authentication components of the TOE supported the TOE Users in the authentication processes, in ensuring secure enforcement of the authentication mechanism by applying 2-factor authentication procedure.

Thus, in the process of TOE Users authentication in access the TOE or the protected resources (assets of the organization), the enforcement of 2FA mechanism with supported of Trust Level validation of the vector validation by the mechanism of Hybrid Risk Scoring Engine calculation, whilst allowing the protected resources compromise value of risk is been reduced.

The configuration of the Trust Level mechanism that initiate additional 2FA authentication procedure is configured by the TOE Administrators and assigned to specific Group with accessibility of the 2FA configuration unique design that enforce the organization security policies. This also applied for Trust Level configuration and Security Policy configuration in the TOE.

SFRs Mapped:	FAU_SAA.1, FAU_SAA.2, FIA_ATD.1, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FIA_UID.2, FMT_SMR.1, FDP_ACF.1 and FDP_ACC.1.

E. Web Administration Module

The Web Administration Module consists of several components such as: User Management, Device Management, Security Policy, Self Services, Access Control, System Notification, Security Audit, Token Management, Reporting & Dashboard, whilst as stated in Table 7.

In general, the Web Administration Module is meant to be access only by the TOE Administrators (CENTAGATE Administrator and CENTAGATE Company Administrator). In which, this module allows the TOE Administrator to perform management of the TOE in the aspects of managing TOE Users, TOE configuration, access control to the TOE, enforcement of rules in the Security Policies, registration of devices related to the enforcement of secure authentication, configuration of the Trust Level that support the Hybrid Risk Scoring Engine component of the TOE, audit tracking review and others.

Additionally, components of the TOE been managed by the TOE Administrators such as: User Management, Device Management, Security Policy, Self Service, Access Control, Security Audit, Token Management, Dashboard and Reporting. Details of these components, kindly refer to Table 7.

Note that, the CENTAGATE Administrator is only allowed to manage the CENTAGATE Company Administrator but not the CENTAGATE End Users. The CENTAGATE Company Administrator is not allowed to manage the CENTAGATE Administrator. Thus, the concepts of management of the TOE Users are from Top to Bottom.

SFRs Mapped:	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAA.2, FAU_SAR.1, FAU_SAR.2, FIA_AFL.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_TAH.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.6, FIA_UID.1 and FIA_UID.2.

F. Mobility Management Module

Mobility management and the Device Management in the Web Administration Module handle registration and revocation of the mobile devices with the TOE. During the mobile device registration (provisioning), TOE and mobile device will try to open a secure communication between both parties so that no data leaking or exposure happens during the provisioning which can breach the entire security of the device usage with the TOE.

In the events of incidents that leads to the supporting mobile devices that contain the TOE mobile app went missing, the TOE will push a notification to the mobile device and then, the application will delete all the keys stored inside the mobile device, whilst the device provisioning will need to be performed again from the beginning.

SFRs Mapped:	FMT_SMR.1, FDP_ACF.1, FDP_ACC.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1.

APPENDIX A

CC	Common Criteria
EAL	Evaluation Assurance Level
I T	Information Technology
PP	Protection Profile
SF	Security Function
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
FIDO	The FIDO (Fast Identity Online)
PKI	Public Key Infrastructure
Mobile PKI	Mobile devices-based Public Key Infrastructure. In this case, achieve via using a PKI based smart card device called "Audio Pass" and/or PKI certificate that is preinstalled into the mobile devices.
Audio Pass	Is a PKI based smart card device, with a standard 3.5mm headphone jack as the interface to communicate with mobile devices to perform digital signature and/or asymmetric encryption and decryption.
OTP	One time password. Also, here are been refer to as time-based OTP.
CR OTP	Challenge response based one-time password
QR Code	Quick Response Code. Is a two-dimensional barcode.

APPENDIX B

This following is the list the details of the ID code and Type of Audit Log Events prompt whilst recorded by the TOE audit log functions under Security Audit component (Web Administration Module).

Table 19: ID Code Audit Log Record & Details.

ID Code Audit Log Record & Details.	
'1001','Company creation successful' '1002','Company creation failed' '1003','Company update successful' '1004','Company update failed' '1005','Company deletion successful' '1006','Company deletion failed' '1053','Permission not allowed' '1101','User creation successful' '1102','User creation failed' '1103','User update successful' '1104','User update failed' '1105','User deletion successful' '1106','User deletion failed' '1107','User self-registration successful' '1108','User self-registration failed' '1109','Company self-registration successful' '1110','Company self-registration failed' '1111','User import successful' '1112','User import failed' '1113','User activation request successful' '1114','User activation request failed' '1115','User forgot password request successful' '1116','User forgot password request failed' '1117','User unlocking successful' '1118','User unlocking failed'	'1121','User logout' '1122','User activation successful' '1123','User activation failed' '1124','Set persistent ID successful' '1201','Password update successful' '1202','Password update failed' '1205','User activation change password successful ' '1206','User activation change password failed' '1207','Password validation successful' '1208','Password validation failed' '1209','Password reset successful' '1210','Password reset failed' '1300','Authentication successful' '1301','Authentication failed' '1302','SMS OTP generation successful' '1304','Authentication random string generation successful' '1305','Authentication random string generation failed' '1307','Authentication token refresh failed' '1308','OTP challenge code generation successful' '1309','OTP challenge code generation failed' '1312','Authentication authenticated with risk'
'1313','Authentication request reject successful'	'1603','Group update failed'

'1315','Failed to get device usage' '1400','Email server addition successful' '1401','Email server addition failed' '1402','Email server update successful' '1403','Email server update failed' '1409','Email sending failed' '1410','Email server reading failed' '1411','Email addition to queue successful' '1412','Email addition to queue failed' '1501','SMS sending successful' '1502','SMS sending failed' '1503','SMS addition to queue successful' '1504','SMS addition to queue failed' '1506','SMS gateway information read failed' '1507','SMS gateway save failed' '1601','Group creation failed' '1602','Group creation successful'	'1604','Group update successful' '1606','Group reading successful' '1608','Group list reading successful' '1609','Group deletion failed' '1610','Group deletion successful' '1701','License update failed' '1702','License update successful' '1703','License reading failed' '1801','Certificate registration successful' '1802','Certificate registration failed' '1803','Certificate unregistration successful' '1804','Certificate unregistration failed' '1805','Set CRL service configuration successful' '1806','Set CRL service configuration failed' '1807','Get CRL service configuration failed' '1808','Add CRL successful' '1809','Add CRL failed'
'1810','Start CRL service successful' '1811','Start CRL service failed' '1812','Execute CRL service successful' '1813','Execute CRL service failed' '1901','Token addition failed' '1902','Token addition successful' '1905','Token import failed' '1906','Token import successful' '1907','Token reading failed' '1909','Token activation code request failed' '1910','Token activation code request successful' '1911','Token activation failed' '1912','Token activation successful' '1913','Token registration failed'	'1914','Token registration successful' '1915','Token unregistration failed' '1916','Token unregistration successful' '1917','Token update failed' '1918','Token update successful' '1919','Token syncing failed' '1920','Token syncing successful' '1921','Token default mobile setting failed' '1922','Token default mobile setting successful' '2000','Data inconsistencies' '2001','System failure' '2002','System startup' '2003','System shutdown' '2100','Template saving failed' '2101','Template saving successful'

'2102','Template reading failed' '3000','App creation successful' '3001','App creation failed' '3002','App update successful' '3003','App update failed' '3004','App deletion successful' '3006','App secret key regeneration successful' '3008','Apps update metadata successful' '3010','App connected' '3100','Plan successfully created' '3102','Plan update successful' '3103','Plan update failed' '3104','Plan deletion successful' '3105','Plan deletion failed' '3106','Plan read failed' '3300','Rules policy creation successful' '3301','Rules policy creation failed' '3302','Rules policy update successful' '3304','Rules policy deletion successful' '3305','Rules policy deletion failed' '3306','New cases creation successful' '3307','New cases creation failed' '3400','Device creation successful'	'3401','Device creation failed' '3402','Device update successful' '3403','Device update failed' '3404','User device registration successful' '3405','User device registration failed' '3406','User device update successful' '3407','User device update failed' '3408','User device unregistration successful' '3409','User device unregistration failed' '3410','User device detected as possible attack' '3411','User device read failed' '3500','Push message successful' '3501','Push message failed' '3600','Contextual policy creation successful' '3601','Contextual policy creation failed' '3602','Contextual policy update successful' '3603','Contextual policy update failed' '3604','Contextual policy deletion successful' '3605','Contextual policy deletion failed' '3800','Validate TAC successful' '3802','Add transaction successful' '3900','Fail to get server status' '5101','Update Notification Setting Failure'
'5111','Insert Message Queue Log Failure' '5200','Delete Notification Setting Success' '5201','Update Notification Setting Success' '5203','Insert Notification Setting Success' '5207','Insert Notification Event Type Success' '5211','Insert Message Queue Log Success' '5212','Delete Message Queue Log Error Success'	'5213','Update Message Queue Log Error Success' '5215','Insert Message Queue Log Error Success' '5216','Resend Message Queue Log Error Success' '1121','User logout' '1300','Authentication successful' '1301','Authentication failed'

'1302','SMS OTP generation successful' '1304','Authentication random string generation successful' '1308','OTP challenge code generation successful' '1309','OTP challenge code generation failed'	'1312','Authentication authenticated with risk' '1313','Authentication request reject successful' '1314','Authentication request reject failed' '1316','QR challenge code generation successful' '1317','QR challenge code generation failed'].

APPENDIX C

The following is the list the functionality of the TOE accessible for the TOE Administrators. The details included the operations of authentication procedure using the mobile application (Advance Mobile Authentication Application).

Table 20: Mapping of the TOE Administration Accessibility

Subject	Object that can access	Operation that related to the module
CENTAGATE Admin	Dashboard ->System Overview	Overview of the system such as total company created, total user created, total tokens in the CENTAGATE.
CENTAGATE Admin	Dashboard -> Server Status Monitoring	Monitor the status of the server instances such as server time, CPU usage, memory usage and disk usage.
CENTAGATE Admin / Company Admin	Self Service -> Change Password	Change login password.
CENTAGATE Admin / Company Admin	Self Service -> My Profile	View and update own information
CENTAGATE Admin / Company Admin	Self Service -> Authentication Methods	Register / unregister authentication methods.
CENTAGATE Admin / Company Admin	Self Service -> Question & Answer	Setup security question and answer
CENTAGATE Admin / Company Admin	Self Service -> Security Image	Setup security image and security phrase
CENTAGATE Admin	Companies -> Company List	Search and list companies. From the list, can further go in to update or delete the company
CENTAGATE Admin	Companies -> Add Company	Add a new company
CENTAGATE Admin	Administrators -> Administrator List	Search and list administrator. From the list, can further go in to update or delete the administrator.
CENTAGATE Admin	Administrators -> Add Administrator	Add new CENTAGATE admin or

Subject	Object that can access	Operation that related to the module
		company admin
CENTAGATE Admin	Administrators -> Authentication Usage	Show graph report on authentication usage
CENTAGATE Admin	Administrators -> Authentication Usage Map	Show authentication location report on world map
CENTAGATE Admin / Company Admin	Groups -> Group List	Search and list group. From the list, can further go in to update or delete the administrator
CENTAGATE Admin / Company Admin	Groups -> Add Group	Add new user group
CENTAGATE Admin / Company Admin	Policies -> Security Policy List	Search and list security policy. From the list can further go in to update or delete the security policy
CENTAGATE Admin / Company Admin	Policies -> Add Security Policy	Add new security policy.
CENTAGATE Admin / Company Admin	Policies -> New Cases List	Search and list the new cases.
CENTAGATE Admin / Company Admin	Activities -> Activity List	Search and list the activity list (security audit)
CENTAGATE Admin / Company Admin	Activities -> Authentication Log	Search and list the authentication log (security audit)
CENTAGATE Admin / Company Admin	Activities -> Report	Generate reports
CENTAGATE Admin / Company Admin	Activities -> Notification List	Search and list the notification. From the list can further go in to update or delete the notification.
CENTAGATE Admin / Company Admin	Activities -> Notification Log	Show the notification log
CENTAGATE Admin / Company Admin	Activities -> Add Notification	Add new notification

Subject	Object that can access	Operation that related to the module
CENTAGATE Admin / Company Admin	Token/Devices -> Token List	Search and list the token. From the list can further go in to update the token
CENTAGATE Admin / Company Admin	Token/Devices -> Import Tokens	Import OTP token
CENTAGATE Admin / Company Admin	Token/Devices -> Device List	Search and list the mobile device. From the list can further go in to update the device status.
CENTAGATE Admin / Company Admin	Token/Devices -> Device Usage	Display graph report on device usage
CENTAGATE Admin	Certificates -> CRL List	Search and list the CRL. From the list can further download the CRL
CENTAGATE Admin / Company Admin	Certificates -> Certificate List	Search and list the certificate. From the list can further unregister or view and download the certificate
CENTAGATE Admin	Certificates -> Trusted Certificate List	Search and list the trusted certificate. From the list can further unregister or view and download the trusted certificate
CENTAGATE Admin	Certificates -> Register Trusted Certificate	Register trusted certificate to the system
CENTAGATE Admin	Settings -> CRL Downloader Config	Configure the CRL downloader service
CENTAGATE Admin / Company Admin	Settings -> Email Template	Configure email template
CENTAGATE Admin / Company Admin	Settings -> SMS Template	Configure SMS template
CENTAGATE Admin	Settings -> SMS Gateway Config	Configure SMS gateway
CENTAGATE Admin	Settings -> SMS OTP Config	Configure SMS OTP parameter

Subject	Object that can access	Operation that related to the module
CENTAGATE Admin	Settings -> OTP Config	Configure OTP parameter
CENTAGATE Admin	Settings -> SMTP Config	Configure SMTP server
CENTAGATE Admin / Company Admin	Settings -> Trust Level	Configure authentication methods that is allowed to use at every trust level
CENTAGATE Admin	Settings -> License	Upload CENTAGATE license
Company Admin	Dashboard	Overview on the company such as how many user, token, group, application and certificate registered under the company. And company license validity
Company Admin	Apps -> App List	Search and list application. From the list can further go in to update and delete the application.
Company Admin	Apps -> Add App	Add application. Application refers to integration application interface. Currently supports Web SDK, SSO, LDAP and RADIUS
Company Admin	Users -> User List	Search and list company admin or end user. From the list can further go in to update and delete company admin or end user.
Company Admin	Users -> Add User	Add new company admin or end user
Company Admin	Users -> Import Users	Bulk import end user
Company Admin	Users -> Authentication Usage	Show graph report on authentication usage
Company Admin	Users -> Auth Usage Map	Show authentication location report on world map
Company Admin	Settings -> Update Company	Update company information

APPENDIX D

The following is the list of details of usage on the authentication methods and mechanisms as components of 2FA for the TOE authentication procedure.

Table 21: Authentication Components

Authentication	Method of authentication
PKI token (out of scope)	The user prompted to select the valid certificate from the list, and then TOE will verify the certificate serial number / fingerprint that stored in the DB.
Hardware CR OTP (out of scope)	User needs to have CR OTP token to use this feature. User will request for a challenge from the TOE, which will then be used by the user to generate the OTP.
Hardware OTP (out of scope)	User needs to have OTP token to use this feature. User will generate an OTP from the OTP token and enters it into the TOE. Once sent, TOE will verify the OTP by comparing with an OTP that is generated by the server based on current server time.
Mobile CR OTP	TOE will generate a challenge, which needs to be entered by the user to generate an OTP. Prior to entering the challenge and generating the OTP, user will need to enter the mobile application PIN.
Mobile OTP	TOE will send a push notification to users mobile, user will enter mobile application PIN, if the PIN is correct, to access the private key stored in secure container and generate digital signature for server validation
Mobile soft cert (PKI)	TOE will validate PKI certificate stored in user's mobile phone by certificate validity, issuer certificate validity, certificate status, and the certificate owner
Mobile audio pass (Out of Scope)	TOE will generate challenge and PKI certificate will be used to sign the challenge. The signature will then be sent back to the TOE by the mobile application and verified for its validity.
FIDO (out of scope)	User need to plugged in the token then click on the button of the token to submit the validation, TOE will verify the token serial number stored in the DB with the physical hardware

Authentication	Method of authentication
QR Code	TOE will send a push notification to users mobile, user will enter mobile application PIN, if the PIN is correct, to access the private key stored in secure container and generate digital signature for server validation