OTACToken V1.0

Security Target V1.7

Revision History

Configuration document no.	Detail	Data	Created by
OTACToken V1.0 Security Target V1.0	Initial Registration	2022-05-30	SSenStone
OTACToken V1.0 Security Target V1.1	Modify Physical scope	2023-01-25	SsenStone
OTACToken V1.0 Security Target V1.2	operating environment change	2023-02-06	SsenStone
OTACToken V1.0 Security Target V1.3	Component change	2023-02-13	SsenStone
OTACToken V1.0 Security Target V1.4	etc	2023-03-06	SsenStone
OTACToken V1.0 Security Target V1.5	Add SFR (FTA_TSE.1)	2023-03-21	SsenStone
OTACToken V1.0 Security Target V1.6	TOE summary specification revision	2023-03-24	SSenStone
OTACToken V1.0 Security Target V1.7	Change model name	2023-04-24	SSenStone

Contents

1. ST Instroduction

1.1 ST reference

Item	Specification
Title	OTACToken V1.0 Security Target
Version	V1.7
Publication Date	2023-04-24
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	v3.1 R5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Author	SSenStone Inc.
Keywords	Authentication, One-way Authentication, Simple Authentication, One-time Authentication Code

1.2 TOE reference

Item		Specification
TOE		OTACToken V1.0
Version		V1.0.02.02.02
Components	OTACToken Server	· OTACToken Server V1.0.02
	OTACToken APP(Android)	· OTACToken App(Android) V1.0.02
	OTACToken APP(iOS)	· OTACToken App(iOS) V1.0.02
	Manual	OTACToken V1.0 Administrator's Manual V1.4
		OTACToken V1.0 User Manual V1.4
		OTACToken V1.0 Installation Guide V1.4
Developer		SSenStone Inc.

1.3 TOE overview

In Chapter 1, we describe the purpose and major security characteristics of Target of Evaluation(hereinafter referred to as "TOE"), TOE types, and hardware/software/firmware other than the Target of Evaluation required in TOE.

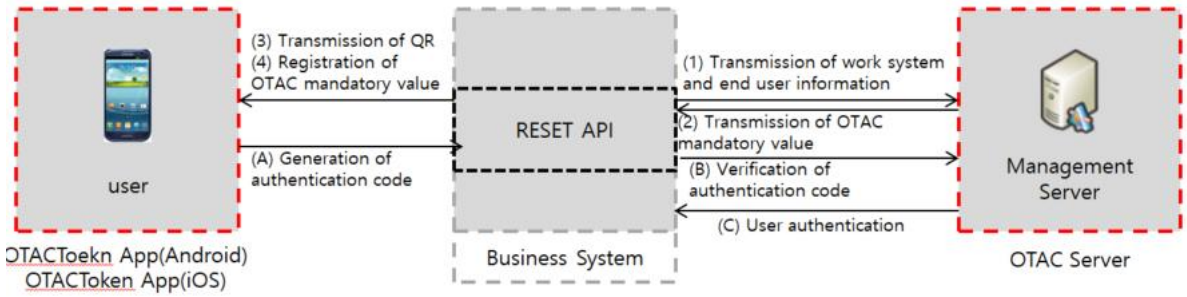
The purpose of the TOE is a product that provides an authentication function using a one-time random unique identification authentication code.
It performs the security functions provided by the TOE through the web browser (Chrome).
To protect the communication data between the TOE and the web browser, it performs socket communication through HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) and

encrypts it through the TSL protocol to ensure data protection.

The TOE provides the administrator screen for security management as a web UI.
After being initialized, the TOE periodically performs integrity checks, performs identification and authentication, and authentication failure response capabilities while limiting duplicate logins for the same administrator.
If the repository protection limit set by the authorized administrator to protect the audit data repository is exceeded, a warning email will be sent to the administrator, and TOE also provides TSF protection functions such as security audit functions for recording and managing audit data, protection function of data saved in the repository controlled by the TSF and TSF self-test, etc. for major events during the operation of security functions and management functions. In addition, the TOE provides access and integrity functions for managing the authorized administrator's access sessions.

The OTACToken Server performs authentication based on the authentication code generated by the OTACToken APP (Android)/OTACToken APP (iOS) after registering the linked work system on OTACToken APP(Android)/OTACToken APP(iOS). When the end user requests login through the work system with the authentication code generated by the OTACToken APP (Android)/OTACToken APP (iOS), the login verification request will be sent through API linked to the work system. Upon receiving the login verification request, the OTACToken Server transmits the verification result to the work system through the authentication code verification.

- Subject to issue authentication code : OTACToken APP(Android) / OTACToken APP(iOS)
- Subject to perform the verification of authentication code : OTACToken Server



[Figure 1] Business system registration and authentication process

Authentication Phase	Operating Procedure
Work System Registration	(1) Transmission of work system and end user information > (2) Transmission of OTAC mandatory value > (3) Transmission of QR > (4) Registration of OTAC mandatory value
Authentication	(A) Generation of authentication code > (B) Verification of authentication

Code Verification	code > (C) User authentication

TOE is a simple authentication solution that allows users to access the work systems through mobile devices using an OTAC authentication code for various work services. It will be provided in software form.

TOE consists of an OTAC Token Server for security management and an OTAC Token App(Android/iOS) that generates one-time authentication codes.

● OTACToken Server

OTAC Server performs tasks such as managing the administrator's password and service, and auditing data retrieval.

● OTACToken App(Android)/OTACToken App(iOS)

OTAC Token App (Android/iOS) generates one-time authentication codes that cannot be reused, and performs login for the linked work system.

The requirements for hardware, software and operating system to install the TOE are as in the following.

• The requirements for hardware, software and operating system to install the TOE

1) OTACToken Server

Item		Specification
Hardware	CPU/ Memory/ Hard Disk	・CPU : Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 4core or higher ・Memory : 8GB or higher ・Disk : Space required for TOE installation is 150 MB or higher
	NIC	・10/100/1000 Ethernet Port x 1EA or higher
Software	OS	・Ubuntu 18.04 (64bit) (kernel 5.4.0-139)
	DBMS	・MariaDB 10.11.2
	etc	・Apache Tomcat 9.0.73
		・jre 1.8.0_362

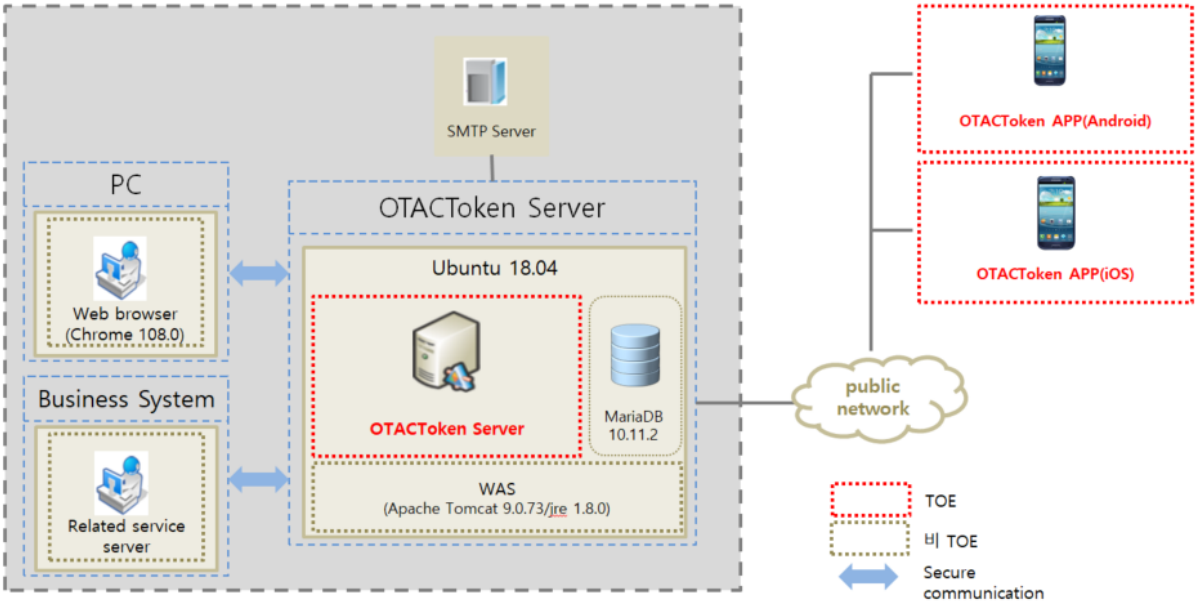
2) Managed PC

Item	Specification
Software	Chrome 108.0

3) OTACToken APP(Android) / OTACToken APP(iOS)

Product	Model	OS		Build version	SDK Version(Android API Version)	APK Version
		Version	Kernel			
SAMSUNG Galaxy S22	SM-S901N	13	5.10.81-android12-9-25490797-abS901NKSU2BVL3	TP1A.220624.014.S901NKSU2BVL3	13	1.0.02
iPhone 13	A2633	15.4.1	-	-	15.4.1	1.0.02

[Figure 2] shows the operational environment where the TOE is operated.



[Figure 2] TOE operational environment

TOE operating environment consists of the OTACToken Server and the OTACToken APP (Android) / OTACToken APP (iOS).

The security management of TOE is performed through a web browser (Chrome) that supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer).

OTACToken APP (Android) / OTACToken APP (iOS) performs the function of generating a one-time authentication code for user authentication of the work system when it is executed.

● **DBMS(MariaDB)**

MariaDB, an open-source relational database management system, is installed in the DBMS that is

linked with the Ubuntu operating system, and stores audit data and service (work system) information generated by TOE.

● **Web Server (Apache Tomcat)**

This is used to provide web-based management functions through the web browser.

● **Tomcat Encryption Function**

The authorized administrator communicates using the OTACToken Server and browser activated in Apache Tomcat that supports HTTPS protocol.

- Confidentiality : AES 128 bit
- Integrity : SHA 256 bit
- Key exchange : RSA 2048 bit

● **SMTP Server**

The mail server sends an e-mail to the authorized administrator who is the recipient designated by the OTACToken Server about the potential security violation.

1.4 TOE description

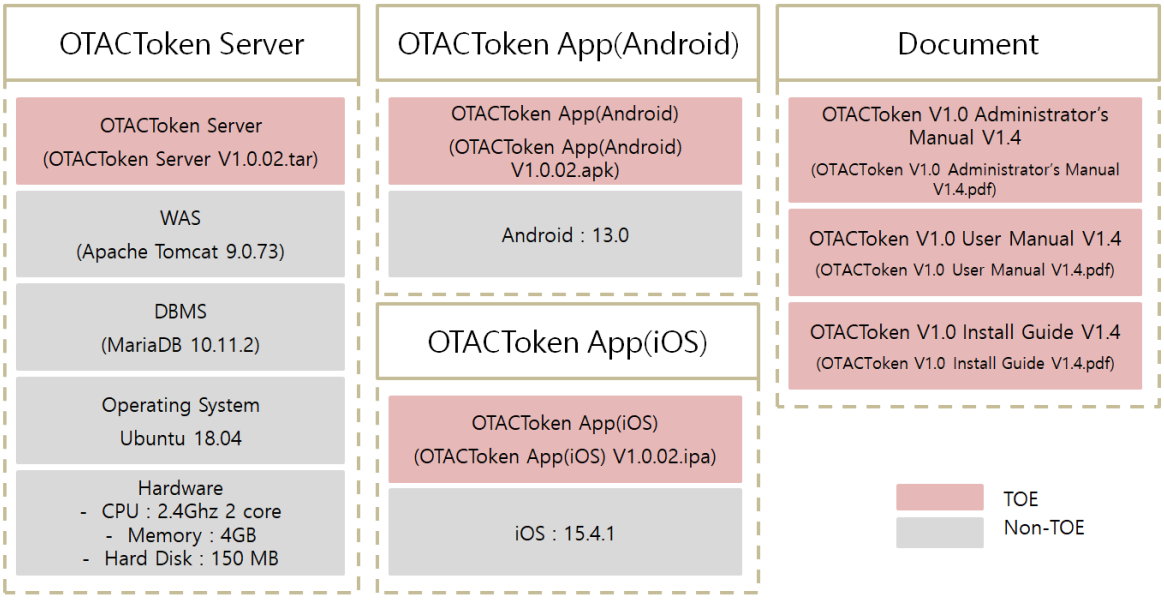
In this part, the physical scope of the TOE such as TOE components, hardware, software, firmware and guidelines are described and security features provided by the TOE are explained in detail in the logical scope of the TOE.

1.4.1 Physical scope

The physical scope that makes up the TOE is the OTACToken Server, OTACToken App(Android), OTACToken APP(iOS) and guidelines (administrator manual, user manual, Installation Guide) as shown in the below [Figure 3].

Hardware, operating system, DBMS, WAS, JDK, Wrapper which are operating environments of the TOE are excluded from the physical scope of the TOE.

Hardware, operating system, DBMS which are operating environments of the TOE are excluded from the physical scope of the TOE.

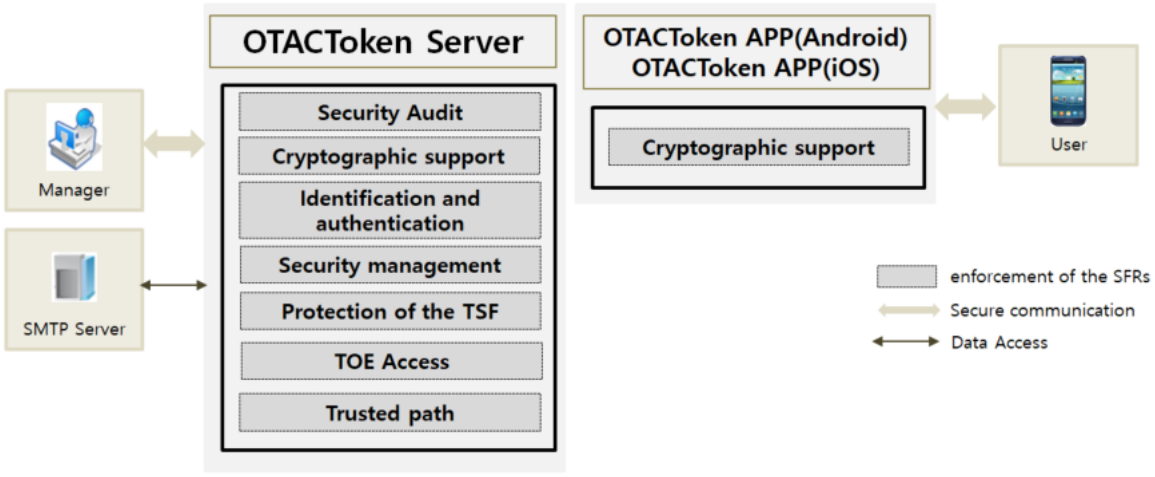


[Figure 3] Physical scope

Distribution Type	quantity	Detail		
		Scope	Type	Identifier
CD-ROM	1	OTACToken Server	S/W	· OTACToken Server V1.0.02 : OTACToken Server V1.0.02.tar
	1	OTACToken App(Android)		· OTACToken App(Android) V1.0.02 : OTACToken App(Android) V1.0.02.apk
	1	OTACToken App(iOS)		· OTACToken App(iOS) V1.0.02 : OTACToken App(iOS) V1.0.02.ipa
	1	Administrator's Manual	PDF	· OTACToken V1.0 Administrator's Manual V1.4 : OTACToken V1.0 Administrator's Manual V1.4.pdf
	1	User Manual		· OTACToken V1.0 User Manual V1.4 : OTACToken V1.0 User Manual V1.4.pdf
	1	Installation Guide		· OTACToken V1.0 Installation Guide V1.4 : OTACToken V1.0 Installation Guide V1.4.pdf

1.4.2 Logical scope

The logical scope of the TOE is as in [Figure 4] below.



[Figure 4] Logical scope

Includes logical scopes in each module.

● **OTACToken Server**

[Security Audit]

TOE generates audit data for TSF data management and security management provided through a web browser.

Audit data will be generated for security management and configuration, information changes, identification and authentication of TSF data, integrity checks, starting and ending of audit functions, and audit data for security violations.

The generated audit data includes the log creation time, the subject's identity, the event result(success or failure), the items related to the event type, and audit data that is additionally created.

The audit data will be stored in a DBMS and be provided to authorized administrators in an appropriate format through a web browser.

[Cryptographic support]

TOE generates symmetric keys through a random bit generator, encrypts the generated OTAC information using the symmetric key, and then transmits the encrypted data to the work system.

- Random Number Generator : SP 800-90A HMAC DRBG(Deterministic Random Bit Generator)
- Symmetric Key Algorithm : AES 128 Bit

[Identification and authentication]

. When attempting identification and authentication, the administrator will be identified by ID and

the administration authentication will be performed before any action. The password for authentication will be displayed as '•' and only information on the cause of authentication failure is provided to prevent password exposure.
The administrator's password must be created according to password rules, and if identification and authentication are successful, the administrator maintains security management authority.
When attempting authentication through a web browser, if the authentication attempt failure count (5 times) is exceeded, the account will be locked for 5 minutes.

[Security management]
TOE sets security policies for each service (work system) and manages administrators and registered users.

[Protection of the TSF]
TOE protects the TSF data transmitted between the TOE and web browsers from exposure or modification and also protects the stored information from unauthorized exposure or modification.
TOE also periodically performs integrity checks and self-tests after startup.

[TOE Access]
The administrator automatically terminates the session if it is not used for a period of inactivity and requires reauthentication for reuse.
In addition, for administrator sessions for security management, the maximum number of session connections is limited to one to prevent duplicate logins.

[Trusted path]
The TOE provides a communication path that protects communication data from being altered or exposed by remote users through a trusted path.

● **OTACToken APP(Android)/OTACToken APP(iOS)**
[Cryptographic support]
TOE reads and decrypts the OTAC information provided by the QR code, and generates a new symmetric key to encrypt the OTAC information and store it in the APP storage space.

- Public Key Algorithm : RSA 2048 Bit
- Symmetric Key Algorithm : AES 128 Bit

TOE also provides the OTAC data by decrypting the stored OTAC information using the symmetric key when a request for OTAC code generation is made for user authentication.

1.5 Operation

This security Target objectives uses English for some abbreviations and clear meaning. The notation, form and preparation rules used follow the common evaluation criteria.

Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is maked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection

This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized.*

Refinement

This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text.**

1.6 Terms and definitions

Terms used in this PP, which are the same as in the CC, must follow those in the CC.

Term	Definitions
Attack potential	Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation.
Management access	The access to the TOE by using the HTTPS, SSH, TLS, etc to manage the TOE by administrator, remotely.
Recommend/be recommended	The 'recommend' or 'be recommended' presented in Application notes is not mandatorily recommended, but required to be applied for secure operations of the TOE.
Random bit generator (RBG)	A device or algorithm that outputs a binary sequence that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the sequence can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a "seed key," and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Symmetric cryptographic technique	Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique.
Iteration	Use of the same component to express two or more distinct requirements.
Security Target(ST)	Implementation-dependent statement of security needs for a specific identified TOE.
Protection Profile(PP)	Implementation-independent statement of security needs for a TOE type.
Decryption	The act that restoring the ciphertext into the plaintext using the decryption key.
Secret Key	The cryptographic key which is used in symmetric cryptographic algorithm and is associated with on or more entity, it is not allowed to release.
User	Refer to "External entity", authorized administrator and authorized end-user in the TOE.
Selection	Specification of one or more items from a list in a component.
Identity	Representation uniquely identifying entities (e.g. user, process or disk) within the context of the TOE.
Encryption	The act that converting the plaintext into the ciphertext using the cryptographic key.
Element	Indivisible statement of a security need.
Role	Predefined set of rules on permissible interactions between a user and the TOE.
operation (on a component of the CC)	modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection..
operation (on an object)	a specific type of action performed by a subject on an object.
external entity	any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Threat Agent	Unauthorized external entities that pose threats such as illegal access, alteration, or deletion of assets.
Authorized Administrator	Authorized users who safely operate and manage the TOE.
Authorized User	Users who can execute functions according to Security Functional Requirements (SFRs)
End User	A user who wants to use a business system other than the authorized administrator of the TOE

Authentication Data	information used to verify the claimed identity of a user.
Authentication token	Authentication data used by authorized general users to access business systems
Assets	entities that the owner of the TOE presumably places value upon.
Refinement	the addition of details to a component.
Dependency	a relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.
Subject	an active entity in the TOE that performs operations on objects.
Sensitive Security Parameters(SSP)	critical security parameters (CSP) and public security parameters (PSP)
Augmentation	the addition of one or more requirement(s) to a package.
Component	the smallest selectable set of elements on which requirements may be based.
Class	the smallest selectable set of elements on which requirements may be based.
Family	a grouping of components that share a similar goal but may differ in emphasis or rigour.
Target of Evaluation(TOE)	a set of software, firmware and/or hardware possibly accompanied by guidance.
Evaluation Assurance Level((EAL)	an assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.
Can/could	within normative text, "can" indicates "statements of possibility and capability, whether material, physical or causal" (ISO/IEC).
Assignment	the specification of an identified parameter in a component (of the CC) or requirement.
Shall/must	within normative text, "shall" indicates "requirements strictly to be followed in order to conform to the document and from which no deviation is permitted." (ISO/IEC).
DBMS (Database Management System)	A software system composed to configure and apply the database.
SSL(Secure Sockets Layer)	This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network
TLS(Transport Layer Security)	This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246
TOE Security	a set consisting of all hardware, software, and firmware of the TOE

Functionality (TSF)	that must be relied upon for the correct enforcement of the SFRs.
TSF Data	data created by and for the TOE, that might affect the operation of the TOE.

2. Conformance claims

2.1 CC conformance claim

This security target specification complies with the fifth edition of the v3.1 common evaluation standard for information protection systems.

CC

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017)
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017)
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)

Conformance claim

- Common Criteria for Information Technology Security Evaluation part 2 expansion : FCS_RBG.1
- Common Criteria for Information Technology Security Evaluation part 3 : Conformant

2.2 PP conformance claim

There are no expropriating profiles accepted by this statement of security target.

2.3 Package conformance claim

This ST claims conformance to assurance package EAL1 augmented with ATE_FUN.1.

2.4 Conformance claim rationale

Since this statement of security target does not declare compliance with other protection profiles, no theoretical basis for the declaration of compliance is required.

3. Security objectives for the operational environment

3.1 Security objectives for the operational environment

OE. PHYSICAL_CONTROL

The place where TOE are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.

OE. TRUST_ADMIN

The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidelines.

OE. OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

OE. SECURE_DEVELOPEMENT

The developer who uses the TOE to interoperate with the end-user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

OE. TIME_STAMP

The TOE accurately records incidents related to security by receiving reliable time stamps provided by the TOE operating environment.

OE.DBMS

DBMS that saves the TSF data and audit data is operated in a physically safe environment.

OE. Safe operation of business system

TOE is linked to a trusted business system, and data transmitted from the business system is transmitted through a secure channel.

4. Extended components definition

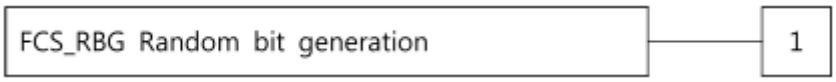
4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

This family defines requirements for the TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Component leveling



FCS_RBG.1 random bit generation, requires TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Management: FCS_RBG.1
There are no management activities foreseen.

Audit: FCS_RBG.1
There are no auditable events foreseen.

4.1.1.1. FCS_RBG.1 Random bit generation

Hierarchical to No other components.
Dependencies No dependencies.
FCS_RBG.1.1The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: list of standards].

5. Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.
The security functional requirements included in this PP are derived from CC Part 2 and Chapter 4 Extended Components Definition.

5.1 Security functional requirements

The following table summarizes the security functional requirements used in the ST.

[Table 1] Security functional component

Security function class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation(1)

	FCS_CKM.1(2)	Cryptographic key generation(2)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation(1)
	FCS_COP.1(2)	Cryptographic operation(2)
	FCS_RBG.1(Extended)	Random bit generation(Extended)
FIA	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF Generation of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
	FIA_UID.2	User identification before any action
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT	FPT_TST.1	TSF testing
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1	TOE session establishment
FTP	FTP_TRP.1	Trusted path

5.1.1 Security audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [the following list of actions] upon detection of a potential security violation.

Potential security violation list	Action list
Integrity verification failed	Send e-mail to authorized administrator
Administrator authorization fail exceeds allowed number	

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit; and
c) [Refer to the "auditable events" in [Table 2] Audit events, [none]].

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 ST, [Refer to the contents of "additional audit record" in [Table 2] Audit events, [none]].

[Table 2] Audit events

Security functional component	Auditable event	Additional audit record
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	-
FIA_AFL.1	Reaching the threshold of failed authentication attempts and the actions taken	-
FIA_UAU.2	authentication success	Administrator access IP address
FIA_UID.2	Failure to use any user identification mechanism, including provided user identity Any use of user identification mechanisms, including provided user identities	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MTD.1	All modifications to the values of TSF data	-
FMT_SMF.1	Use of the management functions	-
FMT_SMR.1	Changes to user groups sharing roles All uses of role privileges	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests	-
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	-
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	-

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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 [

Integrity verification failed

Administrator authorization fail exceeds allowed number

] known to indicate a potential security violation;

b) [none].

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [authorized administrator] with the capability to read [all the audit data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [the following sorting method] of audit data based on [the following criteria with logical relations].

criteria with logical relations		sorting method
Authentication failure audit	AND operation of search conditions by date and user ID	Ascending/descending order by Number, date and time of authentication failure
Authentication audit	AND operation of search conditions by date and user ID	Ascending/descending order by Number, date and time of authentication
User registration audit	AND operation of search conditions by date and user ID	Ascending/descending order by Number, registration date
Admin login audit	AND operation of search conditions by date and	Ascending/descending order by act date

	account (manager ID, manager name)	
Admin Settings audit	AND operation of search conditions by date and account (manager ID, manager name)	Ascending/descending order by act date

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Notification to the authorized administrator] if the audit trail exceeds [the threshold set by the authorized administrator(70%)].

FAU_STG.4 Prevention of audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [Notification to the authorized administrator] if the audit trail is full.

5.1.2 Cryptographic support

FCS_CKM.1(1) Cryptographic key generation(1)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [2048 Bit] that meet the following: [none].

FCS_CKM.1(2) Cryptographic key generation(2)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [128 Bit] that meet the following: [none].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [Overwrite the plaintext encryption key with '0' 3 times] that meets the following: [none].

FCS_COP.1(1) Cryptographic operation(public key)(1)

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [OTAC information value encryption/decryption and secret key encryption] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [2048 Bit] that meet the following: [none].

FCS_COP.1(2) Cryptographic operation(secret key)(2)

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [OTAC information value encryption/decryption and private key encryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 Bit] that meet the following: [none].

FCS_RBG.1 Random bit generation(Extended)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG.1.1The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [none].

list	detail
NIST SP 800-90A	HMAC DRBG(Deterministic Random Bit Generator)

5.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [5] unsuccessful authentication attempts occur related to [authentication of administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*] the TSF shall [lock account for disabled time set by administrator (5 minutes)].

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FIA_ATD.1.1 TSF는 각 사용자에 속한 다음의 보안속성 목록을 유지해야 한다: [아래의 보안속성 목록]

List	List of Security Attributes
Manager	ID, password, security management authority

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following permission criteria].

Acceptable characters (87)	uppercase letters(26)	A – Z
	lowercase letters(26)	a – z
	number(10)	0 – 9
	Special Characters(25)	~!@#$^*()_`-+=|₩,.<>?{}[]
Password Combination Rules	Each English letter, number, and special character must be included.	
	[Administrator password] - 10 ~ 20 characters - ID check - Same characters cannot be used 4 times - Sequential characters cannot be used 4 times	

FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate **OTAC** that meet [the following acceptance criteria defined below].

acceptance criteria defined	Contents

OTAC implementation	A combination of device ID or device identification value anonymized on the server, random value (using Random Number Generator following nist sp 900-80a), Time, TOTP Module (TOTP generation module conforming to RFC6238), etc.
configuration field length	OTAC length set by the administrator

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated **OTAC** for [user authentication].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [contents below] on behalf of the **general user** to be performed before the user is authenticated.

list	Contents
mobile device authentication success	PIN number input success after executing OTACToken APP (Android)/OTACToken APP (iOS)
mobile device authentication failure	PIN number input failure after running OTACToken APP (Android)/OTACToken APP (iOS)

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.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrator**.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [Authentication of Administrator and General Users].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [・, Authentication failure message] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [PIN number input] on behalf of the **general user** to be performed before the **general 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.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **administrator**.

5.1.4 Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions.

FMT_SMR.1 Security roles.

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine, disable, enable, modify the behaviour of*** the functions [list of functions] to [the authorized administrator].

List of functions		determine	enable	modify	disable	The authorized role
OTACToken Server	Service	O	O	O	O	the authorized administrator
	User	O	X	X	X	
	admin password	O	O	O	X	

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions.

FMT_SMR.1 Security roles.

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, modify, delete, [create]* the [the following list of TSF data] to [the authorised administrator].

The authorized role	manage / list of TSF data	Change_default	modify	delete	[create]

the authorised administrator	manager name	X	O	X	O
	Password	X	O	X	O
	Administrator access IP	X	O	X	O
	Whether to receive alarm mail	X	O	X	O
	service ID	X	O	X	O
	service name	X	O	X	O
	ServiceTYPE	X	O	X	O
	OTAC length	X	O	X	O
	OTAC conversion cycle	X	O	X	O
	user state	X	O	X	X

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) TSF function management: items specified in FMT_MOF.1

b) TSF data management: items specified in FMT_MTD.1

c) Security role management: items specified in FMT_SMR.1.

]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator].

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

5.1.5 Protection of the TSF

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of [OTACToken Server].

FPT_TST.1.2 The TSF shall provide **authorised administrator** with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide **authorised administrator** with the capability to verify the integrity of [*OTACToken Server TSF data*].

5.1.6 TOE access

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [restriction to one for the maximum number of concurrent sessions for administrator management access session]

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] sessions per user.

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [Period of inactivity of the authorized administrator (10 minutes)].

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF must be able to reject the **administrator's management connection session** establishment based on [connection IP, whether the same account is locked].

FTA_TSE.1.1 TSF는 [접속 IP, 동일 계정의 잠김 여부]에 기반하여 **관리자의 관리접속 세션** 설정을 거부할 수 있어야 한다.

5.1.7 Trusted path

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication*.

5.2 Security assurance requirement

This section defines the assurance requirements for the TOE. Assurance requirements are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+(ATE_FUN.1). The following table summarizes assurance components.

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction

	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

5.2.1 Security Target evaluation

ASE_INT.1 ST introduction

Dependencies No dependencies.

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements

for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action

elements

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies No dependencies.

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment. Evaluator action elements

ASE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies No dependencies.

Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies	ASE_ECD.1 Extended components definition
Developer action elements	
ASE_REQ.1.1D	The developer shall provide a statement of security requirements.
ASE_REQ.1.2D	The developer shall provide a security requirements rationale.
Content and presentation elements	
ASE_REQ.1.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.1.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.1.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.1.4C	All operations shall be performed correctly.
ASE_REQ.1.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.1.6C	The statement of security requirements shall be internally consistent.
Evaluator action elements	
ASE_REQ.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Developer action elements	
ASE_TSS.1.1D	The developer shall provide a TOE summary specification
Content and presentation elements	
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements	
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies	No dependencies.
Developer action elements	
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements	
ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies	ADV_FSP.1 Basic functional specification
Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.

Content and presentation elements	
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies	No dependencies.
Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
Content and presentation elements	
AGD_PRE1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE1.2C	The preparative procedures shall describe all the steps necessary for secure

installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1 Labelling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E The evaluator shall confirm that the information provided meet requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies No dependencies.

Developer action elements

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements

for content and presentation of evidence.

5.2.5 Tests

ATE_FUN.1 Functional testing

Dependencies	ATE_COV.1 Evidence of coverage
Developer action elements	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
Content and presentation elements	
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
Evaluator action elements	
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1 Independent testing - conformance

Dependencies	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements

for content and presentation of evidence.

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

Dependencies ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements

AVA_VAN.1.1D The developer shall provide the TOE for testing

Content and presentation elements

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Security requirement rationale

5.3.1 Dependency rationale of security functional requirements

The following table shows dependency of security functional requirement.

Number	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.Timestamp
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	OE.DBMS

7	FAU_STG.4	FAU_STG.1	OE.DBMS
8	FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	- 11,12 10
9	FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	- 11,12 10
10	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	- - 8,9
11	FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	- - 8,9 10
12	FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	- - 8,9 10
13	FCS_RBG.1(확장)	-	-
14	FIA_AFL.1	FIA_UAU.1	18
15	FIA_ATD.1	-	-
16	FIA_SOS.1	-	-
17	FIA_SOS.2	-	
18	FIA_UAU.1	FIA_UID.1	22
19	FIA_UAU.2	FIA_UID.1	22
20	FIA_UAU.4	-	-
21	FIA_UAU.7	FIA_UAU.1	18
22	FIA_UID.1	-	
23	FIA_UID.2	-	-
24	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	26 27
25	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	26 27
26	FMT_SMF.1	-	-
27	FMT_SMR.1	FIA_UID.1	22
28	FPT_TST.1	-	-
29	FTA_MCS.2	FIA_UID.1	22
30	FTA_SSL.3	-	-

31	FTA_TSE.1	-	-
32	FTP_TRP.1	-	-

FAU_GEN.1 is dependent on FPT_STM.1 and uses reliable timestamps provided by the TOE operating environment and records tests related to security. Therefore, it satisfies the security target OE.Timestamp for the operating environment.

FAU_STG.3 and FAU_STG.4 have dependent relationships with FAU_STG.1 and this is satisfied by the OE.DBMS operating environment.

5.3.2 Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. but, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

6.1 Security Audit(AUDIT)

6.1.1 Audit data generation(AUDIT.1)

The TOE conducts security managements and generates results for potential security violations of TOE components and results according to identification and authentication, and audit data for events that occur in the system and saves it in DBMS.

Audit data generated in the TOE are as follows.

Audit data	Cases for audits	Remark
User Log	Authentication failure audit	OTAC Server
	Authentication audit	
	User registration audit	
Admin Log	Admin login audit	
	Admin Settings audit	
System Log	Server audit - Server start/stop - audit data capacity exceeded	
	System audit - Self test success/failure - Integrity check success/failure	

For each audit data, audit data is generated by including the log generation time, case type, identify of subject (if available), case results (success or fail) and selective audit review for case type is possible.

Related SFRS : FAU_GEN.1

6.1.2 Audit data review(AUDIT.2)

The TOE provides functions that can review audit data to authorized administrators.
The provided audit data, including administrator identification and authentication history, TSF function change and data value management history, and TOE component start/end history, will be stored in the TOE's operating environment DBMS and provided to authorized administrators in an appropriate format by querying the DBMS.
The accessed audit data can be viewed in order by recording number, authentication failure time, authentication time, registration time, and action date in ascending or descending order.

Related SFRS : FAU_SAR.1, FAU_SAR.3

6.1.3 Audit repository inspection and security violation response (AUDIT.3)

TOE periodically detects potential security threats (such as integrity check failure or exceeding the allowed number of administrator authentication failures) according to a specified cycle (configured at installation), and notifies the administrator of the security threats via email.
If the DBMS warning notification threshold (70%) is exceeded, an email notification will be sent to the authorized administrator to prevent loss of audit data, and if the threshold for data deletion (90%) is exceeded, the oldest audit data is deleted in increments of 50 to prevent loss of audit data.

Related SFRS : FAU_ARP.1, FAU_SAA.1, FAU_STG.3, FAU_STG.4

6.2 Cryptographic support (CKM)

6.2.1 Cryptographic Key Management & Cryptographic operation(CKM.1)

● OTACToken Server

When there is a registration request from a service (work system), the TOE receives and parses information such as User ID and Service ID.
TOE generates a symmetric key using a random bit generator, encrypts the parsed OTAC information using a hash algorithm, and stores it in a database.

- random number generator : SP 800-90A HMAC DRBG(Deterministic Random Bit Generator)
- Symmetric Key Algorithm : AES 128 Bit

- Hash algorithm : SHA 256

TOE encrypts the received symmetric key with a public key and sends it to the service along with the previously encrypted OTAC information.

Afterward, Overwrite the plaintext encryption key with '0' three times to destroy the encryption key.

● OTACToken APP(Android)/OTACToken APP(iOS)

The TOE generates a symmetric key and delivers the public key to the OTACToken Server.

- - Symmetric key algorithm: AES 128 Bit

Then, the encrypted OTAC information value is received from the image provided as QRCODE.

The TOE decrypts the secret key of the OTACToken Server with the private key, and decrypts the encrypted OTAC information value with the decrypted secret key.

- - Public key algorithm: RSA 2048 Bit

The decrypted private key is destroyed using the Keystore/Keychain provided by the OS system.

The TOE generates a new symmetric key with the PIN number input from the user, encrypts the decrypted OTAC information value again, and stores it in the APP storage space.

- - Symmetric key algorithm: AES 128 Bit

When there is an OTAC authentication request from the user, the TOE decrypts the encrypted OTAC information stored in the APP storage space to generate and provide an OTAC value for authentication. (It is created with the service type and OTAC length according to the service policy.)

Related SFRS : FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_RBG.1(확장)

6.3 Identification and authentication (IA)

6.3.1 Authentication failure handling (IA.1)

If TOE reaches the authentication failure limit (5 times, set at installation) during an authentication attempt through the administrator's web browser, the Administrator's account will be locked for the duration of the blocking time (5 minutes) set by the authorized administrator when the authentication failure limit is exceeded.

Related SFRS : FIA_AFL.1

6.3.2 Identification and authentication (IA.2)

The administrator's authentication information consists of an ID and password. The password must include uppercase (A~Z) and lowercase letters (a~z), numbers (0~9), and special characters (!@#$^*()_`-+=|,.<>?{}[]), and must be created according to the combination rule that requires 10 to 20 characters including at least one uppercase letter, one lowercase letter, one number, and one special character.

The password cannot include the ID, and it is prohibited to use four consecutive characters or more than four identical characters or numbers.
To prevent password exposure, only the "·" and authentication failure information will be provided.
The administrator's security management authority will be maintained upon successful identification and authentication.
For OTAC authentication, when a user is identified by receiving a PIN number from a general user, an OTAC is created according to the OTAC implementation method. The generated OTAC is created with the OTAC length set by the administrator according to the OTAC implementation method.

Related SFRS : FIA_ATD.1, FIA_SOS.1, FIA_SOS.2, FIA_UAU.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.1, FIA_UID.2

6.4 Security management(SM)

6.4.1 Security management(SM.1)

TOE performs tasks such as administrator management, service management, and user management.

[Administrator management]
Administrator ID will be created for the top-level administrator in the format of an email address, and the password will be set to consist of 10 to 20 characters of uppercase and lowercase letters, numbers, and special characters, in accordance with the password combination rule. The ID should not be included in password, and the consecutive or identical characters of 4 or more should not be used in creating password.

[Service management]
Administrator registers services and sets security policies by each service (service type, OTAC length, and OTAC conversion period) to create the linked services (business systems).

[User management]
User accounts for OTAC authentication are set to be used or suspended.

[Password management]
Administrator password should be changed.

Related SFRS : FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.5 Protection of the TSF(PT)

6.5.1 Protection of the TSF (PT.1)

TOE provides a function that verifies its own self-tests and the integrity of the TSF at regular intervals (every 6 hours from the start).

TOE performs self-tests and integrity checks and generates audit data for success/failure. If the test fails, a response action will be taken by sending an email to the administrator.

Related SFRS : FPT_TST.1

6.6 TOE access(TA)

6.6.1 Session management(TA.1)

TOE controls the administrator's management access based on the access IP when the administrator attempts to access it, and denies the management access session for access attempts from unauthorized IPs. It also limits the number of concurrent sessions for the administrator to one to prevent duplicate sessions.

TOE terminates inactive sessions of authorized administrators after a set period of inactivity (10 minutes, set at installation), and requires re-authentication afterward.

The TOE rejects the management connection session establishment depending on the access IP and whether the same account is locked.

Related SFRS : FTA_MCS.2, FTA_SSL.3, FTA_TSE.1

6.7 Trusted path(TP)

6.7.1 Trusted path(TP.1)

The TOE provides secure communication (TLS V1.2) to protect communication data from change or exposure during administrator login to protect transmitted data. Therefore, it allows remote users to initialize communication through a secure path.

Related SFRS : FTP_TRP.1