

Echelon V4.5
Security Target Lite r1.0

UbimInfo Co., Ltd.

The certified ST is written in Korean(including some English).This document is a translation of the original from Korean into English.

Revision history					
Document name		Echelon V4.5-ASE.1-ST			
Version	created by	Date	Content	Reviewed by	remark
1.0	young ko	2024.09.08	Initial version	Jinhyun Baek	

Contents

1. Security Target Introduction	1
1.1. ST REFERENCE	1
1.2. TOE REFERENCE	1
1.3. TOE overview	2
1.3.1. TOE overview	2
1.3.2. TOE type and scope	2
1.3.3. TOE usage and major security features	2
1.3.4. TOE operational environment	3
1.3.5. Non-TOE hardware, software Identification	4
1.4. TOE Description	6
1.4.1. Physical scope of the TOE	6
1.4.2. Logical scope of the TOE	8
1.5. Conventions	12
1.6. Terms and definitions	13
1.7. ST organization	19
2. Conformance claim	20
2.1. CC conformance claim	20
2.2. PP conformance claim	20
2.3. Package conformance claim	20
2.4. Conformance claim rationale	20
3. Security objectives	21
3.1. Security objectives for the operational environment	21
4. Extended components definition	22
4.1. Cryptographic support	22
4.1.1. Random Bit Generation	22
4.2. Identification and authentication	22
4.2.1. TOE Internal mutual authentication	22
4.3. User data protection	22
4.3.1. User data encryption	22
4.4. Security Management	23
4.4.1. ID and password	23
4.5. Protection of the TSF	24
4.5.1. Protection of stored TSF data	24
5. Security requirements	25
5.1. Security audit (FAU)	26
5.2. Cryptographic support (FCS)	30
5.3. User data protection (FDP)	37
5.4. Identification and authentication	38
5.5. Security management	40
5.6. Protection of the TSF	42
5.7. TOE access	44
6. Security assurance requirements	45

6.2. Development	48
6.3. Guidance documents	49
6.4. Life cycle support	50
6.5. Tests	50
6.6. Vulnerability assessment	51
7. Security requirements rationale	52
7.1. Dependency rationale of security functional requirements	52
7.2. Dependency rationale of security assurance requirements	53
8. TOE Summary Specification	54
8.1. Security audit (FAU)	54
8.1.1. Security audit	54
8.1.2. Audit data review	54
8.1.3. Audit Data Loss Prevention	54
8.2. Cryptographic support (FCS)	56
8.2.1. Cipher key Generation	56
8.2.2. Cipher key Distribution	56
8.2.3. Cipher key Destruction	56
8.2.4. Cryptographic operation	56
8.3. User data protection (FDP)	58
8.4. Identification and authentication (FIA)	59
8.5. Security Management (FMT)	60
8.6. Protection of the TSF (FPT)	61
8.6.1. Internal TSF data transfer protection	61
8.6.2. Stored TSF data protection	61
8.6.3. Self Test	62
8.7. TOE access (FTA)	63
8.7.1. Limitation on concurrent sessions	63
[table 1] ST reference	1
[table 2] TOE reference	1
[table 3] TOE major security functions	2
[table 4] verified cryptographic module information	4
[table 5] hardware/software minimum specifications	4
[table 6] essential software description	5
[table 7] external IT entities	5
[table 8] Physical scope of the TOE	6
[Table 9] 3rd party software required for TOE operation	7
[table 10] Potential Security Violation Response Table	26
[table 11] auditable events	26
[table 12] other auditable events	27
[Table 13] methods of selection and ordering	28
[table 14] User Data cipher key Reference Standards	30
[table 15] User data cipher key generation method and type	30
[table 16] TSF Data cipher key Generation Reference Standards	31
[table 17] TSF data cipher key generation method and type	31

[table 18] Cryptographic key distribution algorithm and reference standards-----	32
[table 19] cipher key distribution method and type-----	32
[Table 20] Encryption Key Destruction Method and Reference Standard-----	33
[table 21] Cryptographic Operation (User Data Encryption) Algorithms and Reference Standards--	34
[table 22] List of User Data Cryptographic Operations-----	34
[table 23] Cryptographic operation (TSF data encryption) algorithm and reference standards----	35
[table 24] List of TSF Data Cryptographic Operations-----	35
[table 25] List of cryptographic operations for encrypted communications based on standard protocols-----	35
[table 26] Random number Generation Algorithms and Reference Standards-----	36
[table 27] Password Generation Rules-----	38
[table 28] List of security functions-----	40
[table 29] TSF data list-----	40
[Table 30] TOE inter-component cryptographic communication standard-----	42
[Table 31] Stored TSF Data Protection Policy-----	42
[Table 32] List of self-tests by TOE component-----	42
[Table 33] Rationale for the dependency of the security functional requirements-----	52
[Table 34] cipher key distribution method and type-----	56
[Table 35] Random number Generation Algorithms and Reference Standards-----	57
[Table 36] List of user data encryption/decryption methods-----	58
[figure 1] Plug-in type operational environment (Agent, management server separate type)-----	3
[figure 2] Physical scope of the TOE-----	7
[figure 3] Logical scope of the TOE-----	8

1. Security Target Introduction

1.1. ST REFERENCE

Classification	Description
Title	Echelon V4.5 ST
Identification	Echelon V4.5-ASE.1-ST-r1.0(Lite)
Version	r1.0
publication Date	2024. 9. 8
Author	UbimInfo Co., Ltd.
Common Criteria Version	Common Criteria for information Technology Security Evaluation V3.1 r5
Protection Profile	Korean National Protection Profile for Database Encryption V3.0 KECS-PP-1232-2023
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keyword	Database, Encryption

[table 1] ST reference

1.2. TOE REFERENCE

Classification	Description	
TOE Identification	Echelon V4.5	
TOE type	Datebase Encryption	
TOE version	V4.5	
build version	V4.5.0.0.2	
TOE Components	Management tool	Echelon V4.5-AdministratorV1.02
	Manager	Echelon V4.5-ManagerV1.02
	Agent	Echelon V4.5-AgentV1.02
Release Date	2024. 4. 3	
TOE developer	UbimInfo Co., Ltd.	
publication Date	2024. 9. 8	
Guidance	Echelon V4.5-PRE.1-r1.2 Echelon V4.5-OPE.1-r1.2 Echelon V4.5-OPE.2-r1.2	

[table 2] TOE reference

1.3. TOE overview

This chapter describes the TOE overview, TOE types and scope, TOE usage and major security features, TOE operating environment, and non-TOE hardware/software.

1.3.1. TOE overview

Echelon V4.5(hereinafter referred to as 'TOE') is a database encryption product that encrypts the database (hereinafter referred to as 'DB') to prevent unauthorized exposure of information to be protected.

The encryption target of the TOE is user data managed by the database management system (hereinafter referred to as 'DBMS') in the operating environment of the organization. The User data is encrypted by column, and part or all of user data can be subject to encryption according to the security policy of the organization operating the TOE.

The DBMS that controls the DB in the operational environment of the organization is different from the DBMS that is directly used by the TOE to control the TSF data (security policy, audit data, etc).

1.3.2. TOE type and scope

The TOE provides encryption/decryption functions for each column of user data in the form of software, and the TOE can be classified as a plug-in type and consists of a management tool, manager, and agent.

1.3.3. TOE usage and major security features

The TOE encrypts user data according to the policy set by the authorized administrator. The TOE provides major security functions such as the following table to prevent leakage of confidential information and to operate the TOE safely in the operating environment of the organization.

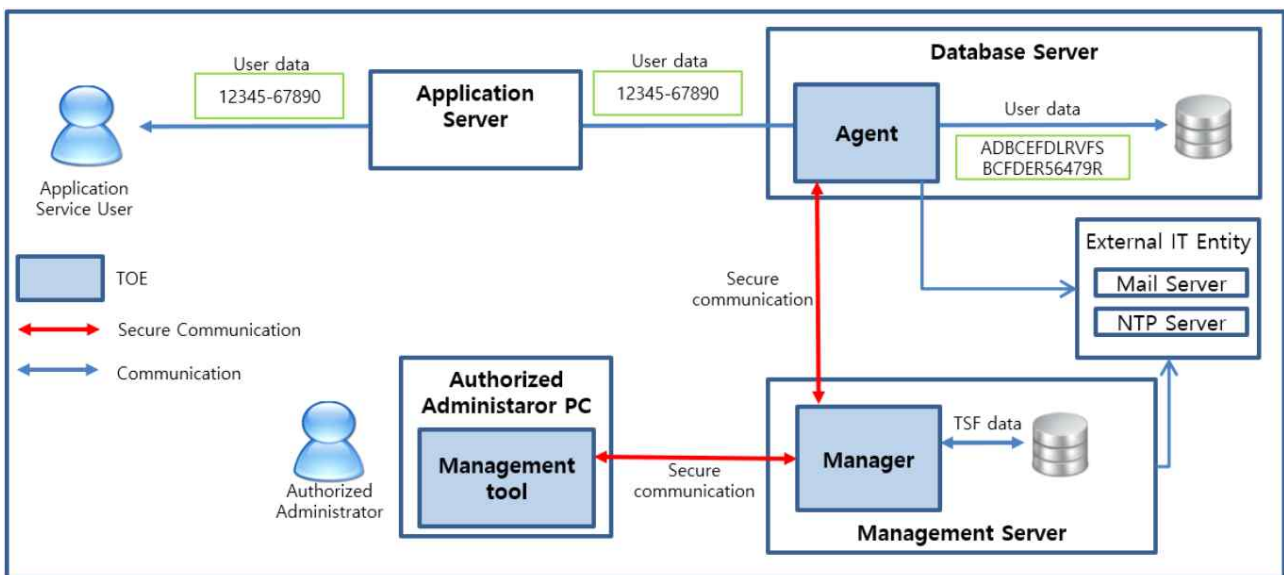
Classification	description
security audit	<ul style="list-style-type: none">· Ability to generate audit data including the date and time of the event, the type of event, the subject identity, the outcome of the event(success/failure)· Audit data review function for security administrators· Audit data loss prevention function
Cryptographic support	<ul style="list-style-type: none">· Function to generate, distribute, and destroy encryption keys through a verified cryptographic module (KCMVP)· Function to protect the encryption key (DEK) for user data using the key encryption key (KEK)· Function to perform cryptographic operation (data encryption/decryption) using encryption key for user data
User data protection	<ul style="list-style-type: none">· Ability to generate different ciphertext for the same plaintext per column for user data· Data protection function by destroying original data (overwriting '0')
Identification	<ul style="list-style-type: none">· ID/password based user authentication mechanism

Classification	description
Authentication	<ul style="list-style-type: none"> · Mutual authentication function between TOE components · Reuse prevention function to protect authentication data
security management	<ul style="list-style-type: none"> · Management of functions of the TSF, management of TSF data(Cipher key, ID/PW, etc).
TSF protection	<ul style="list-style-type: none"> · TSF data protection function transmitted between TOE components · TSF data protection function stored in storage controlled by TSF · TSF self-test, integrity verification function
TOE access	<ul style="list-style-type: none"> · TOE access session management function of security administrator

[table 3] TOE major security functions

1.3.4. TOE operational environment

The TOE provides column-level encryption/decryption functions through a plug-in type to protect user data, and the operating environment for operating the TOE is shown in the [figure 1].



[figure 1] Plug-in type operational environment (Agent, management server separate type)

The TOE consists of management tool, manager, and agent and the functions provided by each component are as follows.

The management tool is an administrator access tool that provides the ability for administrators (security manager) to perform security management and encryption key management (encryption key generation/destruction/inquiry function), and to review audit history.

The manager installed on the management server performs core functions such as security management, encryption key management, audit history management, and notification services.

The agent installed on the database server performs encryption/decryption of user data according to the security policy sent from the manager.

An application server and an external IT entity (NTP server, mail server, etc.) are required for TOE operation. The NTP server is used to reliable time information for the security audit data generated by the manager, and the mail server sends e-mail to the authorized administrator.

TOE components (management tool, manager, agent) perform encrypted communication based on standard protocols. The contents of the verified cryptographic module that passed KCMVP installed in each the component are as shown in the [table 4].

Classification	Contents
cryptographic module name	MPowerCrypto V3.0
Verification number	CM-249-2029.6
verification level	VSL1
developer	UbimInfo Co.,Ltd.
verification date	2024-06-17
expiration date	2029-06-17

[table 4] verified cryptographic module information

1.3.5. Non-TOE hardware, software Identification

The minimum hardware and software requirements for TOE installation and operation are as follows.

TOE	Classification	Specification	
Management tool	H/W	CPU	Intel Core i3 @ 3.40GHz or higher
		RAM	8GB or higher
		HDD	Space required for TOE Installation is 830MB or higher
		NIC	Ethernet 10/100/1000 Mbps * 1 port
	OS	Windows Server 2022 Standard (64bit)	
	S/W	Eclipse RCP 4.19.0, JRE 11.0.24	
Manager	H/W	CPU	Intel Core i3 @ 3.40GHz or higher
		RAM	8GB or higher
		HDD	Space required for TOE Installation is 860MB or higher
		NIC	Ethernet 10/100/1000 Mbps * 1 port
	OS	Ubuntu 22.04.4(64bit)(Kernel: 5.15.0-119)	
	S/W	PostgreSQL 16.4, MPowerPlus 1.3.1, JRE 11.0.24	
Agent	H/W	CPU	Intel Core i3 @ 3.40GHz or higher
		RAM	8GB or higher
		HDD	Space required for TOE Installation is 310MB or higher
		NIC	Ethernet 10/100/1000 Mbps * 1 port
	OS	Oracle Linux 9.2(64bit)(Kernel:5.15.0-101)	
	S/W	Oracle 19.3.0.0.0, MPowerPlus 1.3.1, JRE 11.0.24	

[table 5] hardware/software minimum specifications

The Management tool that requires Eclipse RCP and JRE software to provide a GUI to authenticated administrators is installed on the authorized administrator PC.

The Manager that requires software such as MPowerPlus and JRE is installed on the management server and the manager stores the audit history in DBMS (PostgreSQL).

The Agent that requires software such as MPowerPlus and JRE is installed on the database

server, and the agent encrypts user data and stores it in DBMS (Oracle).

The software description required for TOE operation is as follows.

Classification	software	contents	note
common software	JRE(11.0.24)	· Framework environment required to run TOE components (management tool, manager and agent)	
Management tool	Eclipse RCP (4.19.0)	· Abbreviation for Rich Client Platform, a feature-rich standalone application based on the Eclipse platform.	
Manager	MPowerPlus (1.3.1)	· An integrated platform solution that provides functions such as database linkage, XML environment setting loading, log output, and mail transmission as a Java-based program	
	PostgreSQL (16.4)	· Database for storing TSF data generated by the TOE	
Agent	MPowerPlus (1.3.1)	· An integrated platform solution that provides functions such as database linkage, XML environment setting loading, log output, and mail transmission as a Java-based program	
	Oracle (19.3.0.0.0)	· A database for storing user data created by the application.	

[table 6] essential software description

External IT entities required for TOE operation are as follows.

Classification	contents	note
mail server	· Mail server for sending mail to authorized administrators	
NTP server	· Server for synchronizing the time of systems in the networked TOE operating environment (reliable time information for security audit data)	

[table 7] external IT entities

1.4. TOE Description

The TOE is operated in the plug-in type to perform encryption/decryption of user data. The administrator accesses the manager through management tools to set policies, and the agent performs encryption/decryption of user data based on the set policies. The physical and logical scopes of the TOE are as follows.

1.4.1. Physical scope of the TOE

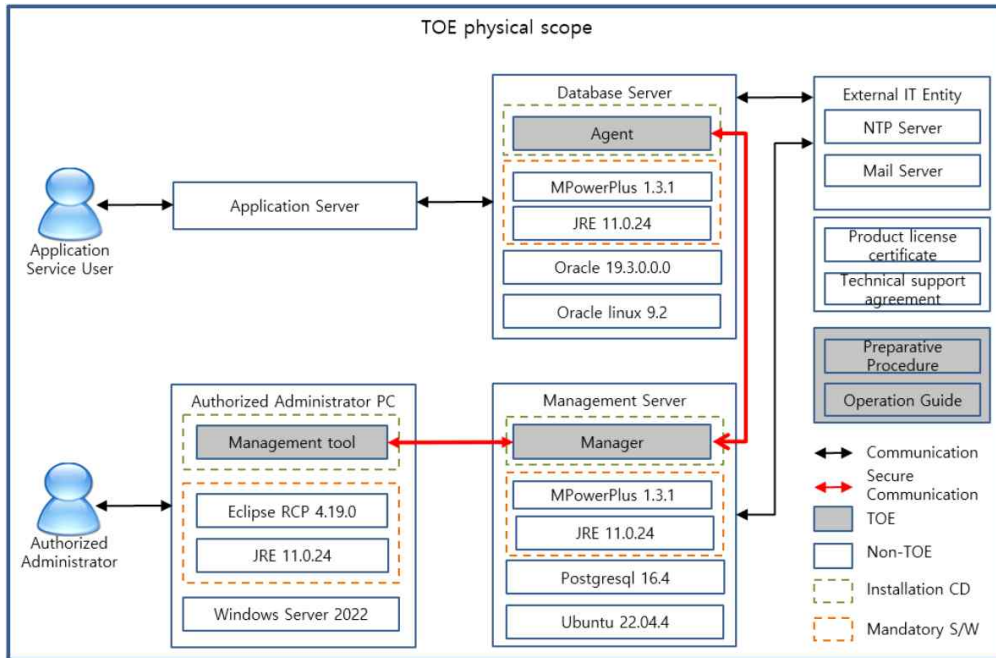
The physical scope of the TOE is as follows.

classification		Components	production type	Deployment type
TOE	Management tool	Echelon V4.5-AdministratorV1.02 (EchelonV4.5@AdministratorV1.02.msi)	SW	CD
	Manager	Echelon V4.5-ManagerV1.02 (EchelonV4.5@ManagerV1.02.jar)		
	Agent	Echelon V4.5-AgentV1.02 (EchelonV4.5@AgentV1.02.jar)		
Guidance Documents	Preparative Procedure	Echelon V4.5-PRE.1-r1.2 (Echelon V4.5-PRE.1-r1.2.pdf)	PDF	
	Operation Guide	Echelon V4.5-OPE.1-r1.2 (Echelon V4.5-OPE.1-r1.2.pdf) Echelon V4.5-OPE.2-r1.2 (Echelon V4.5-OPE.2-r1.2.pdf)		
Mandatory S/W		JRE 11.0.24 (PKG_JRE11_Windows.zip, jre-11.0.24_linux-x64_bin.tar.gz) Eclipse RCP 4.19.0 (Eclipse_RCP_4.19.0.zip) MPowerPlus 1.3.1 (MPowerPlus1.3.1.zip)	SW	
Certificate	Product license certificate		Paper	1 copy
	Technical support agreement		Paper	1 copy

[table 8] Physical scope of the TOE

The TOE package consists of a CD 1EA and documents (product license certificate, technical support agreement) and is provided by direct delivery method. The CD consists of TOE installation files (management tool, manager, agent), manuals, and required software. The TOE installation files are provided in the form of software, and preparative procedures necessary for installation, Operation Guide(administrator manual and user operation manual) necessary for operation are provided as PDF files. In addition, essential software (JRE, Eclipse, MPowerPlus) required for TOE installation is included, which is excluded from the scope of the TOE.

The physical scope of the TOE is Management tool, Manager, Agent, non-TOE operational environment. It is structured as follows.



[figure 2] Physical scope of the TOE

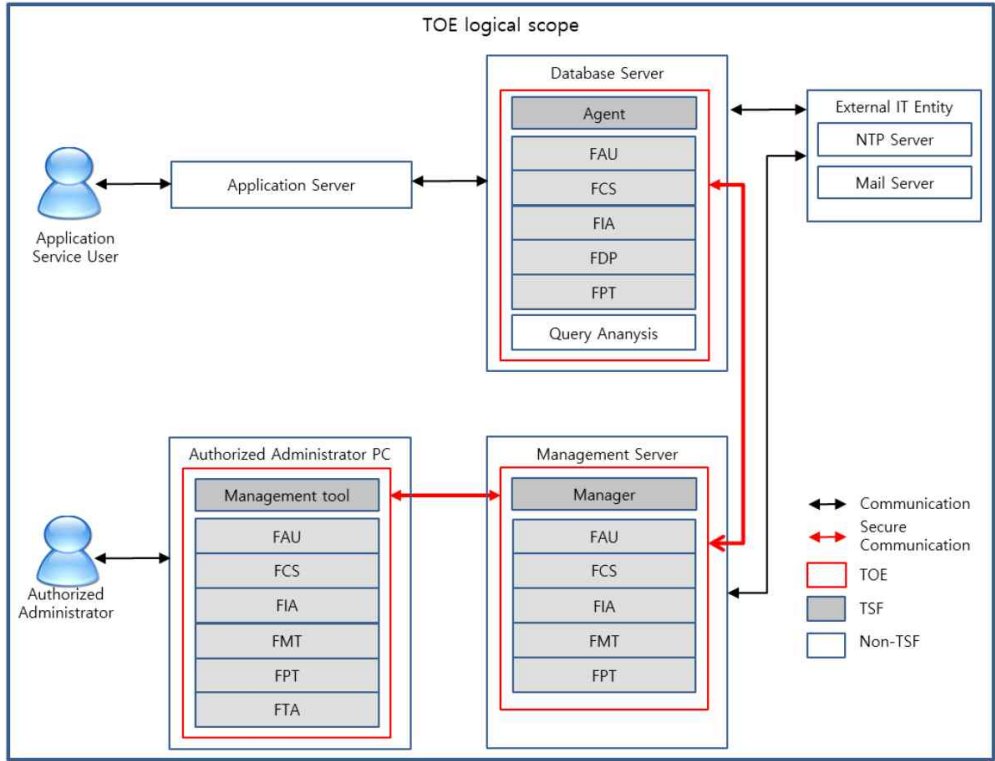
The 3^d party software required for TOE operation is as follows.

classification	version	contents	note
BC-FJA	2.0.0	· Library for encrypted communication based on standard protocol between TOE components	

[Table 9] 3^d party software required for TOE operation

1.4.2. Logical scope of the TOE

The logical scope of the TOE consists of security audit, cryptographic support, user data protection, identification and authentication, security management, protection of TSF, and TOE access. [Figure 3] shows the logical scope of each TOE component.



[figure 3] Logical scope of the TOE

○ Management tool

• Security audit(FAU)

When a security-related event occurs in the management tool, it is transmitted to the manager and the audit data is saved. Audit data includes information about event date and time, event type, subject identity, and outcome of the event(success or failure), and all generated audit data provides the ability to be reviewed by authorized administrators.

• Cryptographic support(FCS)

The management tool performs cryptographic operations using the verified cryptographic module passed the Korea Cryptographic Module Validation Program(KCMVP) and destroys the cryptographic key by overwriting it with "0".

• Identification and authentication(FIA)

The management tool performs mutual authentication when communicating with a physically separated manager. The management tool performs administrator authentication based on an ID and password (9 to 30 characters, including uppercase and lowercase English letters, numbers, and special characters), masks input characters (●) to prevent password exposure, and blocks account access for 10 minutes after 3 failed authentication attempts.

- **Security management(FMT)**

The management tool provides security administrators with security functions (password management, encryption key management, configuration information management, encryption key history inquiry, audit data inquiry, integrity check) and TSF data(configuration information) management functions.

- **Protection of the TSF(FPT)**

The management tool performs self-tests and integrity checks at initial startup, periodically during normal operation, and at the administrator's request. TSF data transmitted between the management tool and the manager is protected from unauthorized exposure or modification by encrypted communication based on standard protocols.

- **TOE access(FTA)**

When the security manager accesses the site, it verifies whether the IP address is one of the permitted IP addresses and only allows access for permitted IP and single sessions. If the inactivity period exceeds a certain period of time, the security manager session is terminated.

○ **Manager**

- **Security audit(FAU)**

The manager saves audit data when a security-related event occurs and sends an alert email to the system administrator if the audit event is a potential security violation. Audit data includes information about event date and time, event type, subject identity, and event outcome (success or failure).

A warning mail is sent to the administrator when the capacity of the DBMS that stores audit data exceeds 80%. If it exceeds 90%, a warning message and the oldest stored audit record are overwritten to prevent loss of audit data.

- **Cryptographic support(FCS)**

The manager generates and distributes all cryptographic keys to protect data transmitted between TOE components (management tool and manager, agent and manager), and performs cryptographic operations using the verified cryptographic module passed the KCMVP and destroy the encryption key by overwriting it with "0".

- **Identification and authentication(FIA)**

The manager performs mutual authentication when communicating with a physically separated management tool (agent) and maintains session information generated through a random number generator when identifying and authenticating the security manager, thereby blocking attempts to reuse authentication data.

- **Security management(FMT)**

The manager performs security functions (password management, encryption key management, configuration information management, encryption key history inquiry, audit data inquiry,

integrity check) and TSF data(configuration information) management functions requested by the security administrator through the management tool.

- **Protection of the TSF(FPT)**

The manager performs self-tests and integrity checks at initial startup, periodically during normal operation, and at the administrator's request. TSF data transmitted between TOE components (management tool and manager, agent and manager) is protected from unauthorized exposure and modification by encrypted communication based on standard protocols, and stored TSF data is protected by using the KCMVP cryptographic module.

- **Agent**

- **Security audit(FAU)**

When a security-related event occurs in the agent, it is sent to the manager to store audit data. The audit data includes information about the event date and time, event type, subject identity, and event outcome (success or failure).

- **Cryptographic support(FCS)**

The agent performs cryptographic operations using the verified cryptographic module passed the KCMVP to protect user data, and destroys the cryptographic key by overwriting it with "0".

- **User data protection(FDP)**

The agent performs encryption and decryption on user data on a column-by-column basis according to the policy set by the security manager, and then performs a destruction operation (overwriting with "0") to protect the original data.

- **Identification and authentication(FIA)**

The agent performs mutual authentication when communicating with a physically separate manager.

- **Protection of the TSF(FPT)**

The agent performs self-tests and integrity checks at initial startup, periodically during normal operation, and at the administrator's request. TSF data transmitted between the agent and the manager is protected from unauthorized exposure or modification by encrypted communication based on standard protocols.

- **Non-security features included in the evaluation scope include:**

- **Agent**

- Query analysis: A function that analyzes the query requested by the user and excludes it from TOE evaluation scope.

- **Manager**

- None

- Management tool

- None

1.5. Conventions

The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation.

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST.

Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is marked 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 ST, which are the same as in the CC, must follow those in the CC.

Agent

TOE component that provides encryption operation function for user data using TOE

Approved cryptographic algorithm

A cryptographic algorithm selected by Korea Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability

Application Server

The application server defined in this PP refers to the server that installs and operates the application, which is developed to provide a certain application service by the organization that operates the TOE. The pertinent application reads the user data from the DB, which is located in the database server, by the request of the application service user, or sends the user data to be stored in the DB to the database server.

Approved mode of operation

The mode of cryptographic module using approved cryptographic algorithm

Assets

Entities that the owner of the TOE presumably places value upon

Assignment

The specification of an identified parameter in a component (of the CC) or requirement

Attack potential

Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation

Augmentation

Addition of one or more requirement(s) to a package

Authorized Administrator

Authorized user to securely operate and manage the TOE

Authentication Data

Information used to verify the claimed identity of a user

Authorized User

The TOE user who may, in accordance with the SFRs, perform an operation

BC-FJA(Bouncy Castle FIPS Java API)

Cryptographic library that meets the level 1 requirements of FIPS 140-2

Certificate

An electronic certificate that acts like an online seal/identification card.

Column

A set of data values of a particular simple type, one for each row of the table in a relational database

Component

Smallest selectable set of elements on which requirements may be based

Critical Security Parameters (CSP)

Information related to security that can erode the security of the encryption module if exposed or changed (e.g., verification data such as secret key/private key, password, or Personal Identification Number).

Class

Set of CC families that share a common focus

Database

A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this ST, refers to the relational database.

Database Server

The database server defined in this ST refer to the server in which the DBMS managing the protected DB is installed in the organization that operates the TOE

DBMS(Database Management System)

A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this PP, refers to the database management system based on the relational database model.

Data Encryption Key(DEK)

Key that encrypts and decrypts the data

Decryption

The act that restoring the ciphertext into the plaintext using the decryption key

Dependency

Relationship between components such that if a requirement based on the depending component is included in the ST, a requirement based on the component that is depended upon must normally also be included in the ST.

Echelon V4.5

A DB encryption product that performs the function of preventing unauthorized exposure of information to be protected by encrypting the database.

Eclipse RCP

Abbreviation for Rich Client Platform, a standalone application with rich features based on the Eclipse platform.

Encryption

The act that converts the plaintext into the ciphertext using the encryption key

Element

Indivisible statement of a security need

External Entity

Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Evaluation Assurance Level (EAL)

Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Family

Set of components that share a similar goal but differ in emphasis or rigour

Identity

Representation uniquely identifying entities (e.g. user, process or disk) within the context of the TOE

Iteration

Use of the same component to express two or more distinct requirements

KCMVP(Korea Cryptographic Module Validation Program)

A system to validate the security and implementation conformance of cryptographic modules used for the protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions.

JRE(Java Runtime Environment)

Framework environment required to run the management tools, managers, and agents that make up TOE.

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Mail Server

A server that forwards e-mail to another e-mail server using SMTP.

Management access

The access to the TOE to manage the TOE by administrator, remotely

Management tool

A TOE component that has the function of setting and controlling encryption policies according to the definition of the TOE's role and managing encryption keys (user data, TSF data) used in the TOE.

Manager

TOE component that provides encryption key generation used in TOE and TOE security audit history storage and notification service functions

Manual recovery

Recovery through an update server, etc. by the user execution or user intervention

MPowerCrypto V3.0

A verification-based cryptographic module that is installed in TOE components (management tool, manager, and agent) and is responsible for cryptographic operations.

MPowerPlus

An integrated platform solution that provides functions such as database connection, XML environment setting loading, log output, and mail transmission through Java-based programs.

NTP Server

Time synchronization server via network protocol

Object

Passive entity in the TOE containing or receiving information and on which subjects perform

Operations

Operation (on a component of the CC) Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation (on a subject))

Specific type of action performed by a subject on an object

Oracle

An abbreviation for Oracle Database, an RDBMS created by a representative American software company founded by Larry Ellison in 1977.

Oracle linux

A Linux distribution distributed by Oracle, partly based on the GNU General Public License, since late 2006.

Organizational Security Policies

Set of security rules, procedures, or guidelines for an organization wherein the set is currently given by actual or virtual organizations, or is going to be given

Private Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed Protection Profile (PP) Implementation-independent statement of security needs for a TOE type

PostgreSQL

An object-relational database management system that emphasizes extensibility and standards compliance.

Protection Profile(PP)

Implementation-independent security requirements specification appropriate to the TOE type

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private keys

Random bit generator

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string 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.

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

Refinement

Addition of details to a component

Role

Predefined set of rules on permissible interactions between a user and the TOE

Security Function Policy (SFP)

A Set of rules that describes the specific security action performed by TSF (TOE security functionality) and describe them as SFR (security function requirement)

Secret Key

A cryptographic key which is used in an symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Security attribute

The characteristics of the subject used to define the SFR, user (including the external IT product), object, information, session and/or resources. These values are used to perform the SFR

Selection

Specification of one or more items from a list in a component

Self-test of cryptographic module

Pre-operational and conditional tests performed by the cryptographic module

Shall/must

The 'shall' or 'must' presented in Application notes indicates mandatory requirements applied to the TOE

SSL(Secure Sockets Layer)

This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network

Standard Protocol

Secure Socket Layer, the predecessor of Transport Layer Security, is a security protocol that supports secure communication through encrypted connections.

Symmetric cryptographic technique

Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique

Subject

Active entity in the TOE that performs operations on objects

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

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 Functionality (TSF)

Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

Unique identification information

Identification information given to each component to indicate the uniqueness of the TOE component.

Ubuntu

A Linux distribution developed by forking Debian Linux and focusing on ease of use compared to Debian.

User

Refer to "External entity"

User Data

Data for the user, that does not affect the operation of the TSF

Windows Server 2022

A computer operating system developed by Microsoft.

1.7. ST organization

Chapter 1 introduces the Security Target, providing ST reference, TOE reference, TOE overview, TOE description..

Chapter 2 declares conformance to the CC, PP, and package as a conformance declaration, and describes the rationale for the conformance declaration and how to comply with the ST.

Chapter 3 defines the security objectives for the operational environment

Chapter 4 defines extended components that require additional definition according to TOE characteristics.

Chapter 5 describes the security function requirements provided by the TOE.

Chapter 6 describes the assurance requirements provided by the TOE.

Chapter 7 describes the rationale of security requirements.

Chapter 8 describes the TOE summary specification to accurately provide the TOE security functionality.

2. Conformance claim

2.1. CC conformance claim

Classification		Description
CC		Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 <ul style="list-style-type: none"> · 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	Part 2 Security functional components	Extended: FCS_RBG.1, FDP_UDE.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1
	Part 3 Security assurance components	Conformant
	Package	Augmented: EAL1 augmented (ATE_FUN.1)

2.2. PP conformance claim

Classification	Description
title	Korean National Protection Profile for Database Encryption
version	3.0
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Issue Date	2023. 4. 27
Evaluation Criteria Version	CC V3.1 r5
Certification Number	KECS-PP-1232-2023
conformance	strict PP conformance

2.3. Package conformance claim

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

2.4. Conformance claim rationale

If strict conformance is required by the PP to which conformance is being claimed no conformance claim rationale is required.

3. Security objectives

The followings are the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

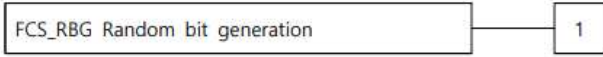
3.1. Security objectives for the operational environment

Organizational Security Policy	Contents
OE.PHYSICAL_CONTROL	<ul style="list-style-type: none"> The place where the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.
OE.TRUSTED_ADMIN	<ul style="list-style-type: none"> 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 guidances.
OE.SECURE_DEVELOPMENT	<ul style="list-style-type: none"> The developer who uses the TOE to interoperate with the 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.LOG_BACKUP	<ul style="list-style-type: none"> The authorized administrator of the TOE shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.
OE.OPERATION_SYSTEM_REINFORCEMENT	<ul style="list-style-type: none"> 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. Timestamp	<ul style="list-style-type: none"> The TOE must accurately record security-related events using a reliable timestamp provided by the TOE operating environment.
OE. Secure DBMS	<ul style="list-style-type: none"> The DBMS that interacts with the TOE stores audit records, so the stored audit records must be protected from unauthorized deletion and modification.
OE. Secure Channel	<ul style="list-style-type: none"> Since the mail server linked with TOE sends a security warning email to the security manager, the channel between TOE and the mail server must be safely protected with encrypted communication.

4. Extended components definition


4.1. Cryptographic support

4.1.1. Random Bit Generation

Family	This family defines requirements for the TSF to provide the capability that generates random bits required for TOE cryptographic operation.	
Behaviour		
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.
FCS_RBG.1	Random bit generation	
	Hierarchical to	No other components.
	Dependencies	No dependencies.
FCS_RBG.1.1	The TSF shall generate random bit using the specified random bit generator that meets the following [assignment: list of standards].	

4.2. Identification and authentication

4.2.1. TOE Internal mutual authentication

Family	This family defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.	
Behaviour		
Component leveling		
	FIA_IMA.1 TOE Internal mutual authentication requires that the TSF provides mutual authentication function between TOE components in the process of user identification and authentication.	
Management	FIA_IMA.1	There are no management activities foreseen.
Audit	FIA_IMA.1	The following actions are recommended to record if FAU_GEN Security audit data generation family is included in the PP/ST: a) Minimal: Success and failure of mutual authentication
FIA_IMA.1	FIA_IMA.1 TOE Internal mutual authentication	
	Hierarchical to	No other components.
	Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication between [assignment: different parts of TOE] using the [assignment: authentication protocol] that meets the following [assignment: list of standards].	

4.3. User data protection

4.3.1. User data encryption

Family	This family provides requirements to ensure confidentiality of user data.
Behaviour	

Component leveling	<div style="border: 1px solid black; display: inline-block; padding: 2px;">FDP_UDE User data encryption</div> — <div style="border: 1px solid black; display: inline-block; padding: 2px;">1</div>
	FDP_UDE.1 User data encryption requires confidentiality of user data
Management	FDP_UDE.1 The following actions could be considered for the management functions in FMT: a) Management of user data encryption/decryption rules
Audit	FDP_UDE.1 The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST: a) Minimal : Success and failure of user data encryption/decryption
FDP_UDE.1	FDP_UDE.1 User data encryption Hierarchical to No other components. Dependencies FCS_COP.1 Cryptographic operation
FDP_UDE.1.1	TSF shall provide TOE users with the ability to encrypt/decrypt user data according to [assignment: the list of encryption/decryption methods] specified.

4.4. Security Management

4.4.1. ID and password

Family Behaviour	This family defines the capability that is required to control ID and password management used in the TOE, and set or modify ID and/or password by authorized users.
Component leveling	<div style="border: 1px solid black; display: inline-block; padding: 2px;">FMT_PWD ID and password</div> — <div style="border: 1px solid black; display: inline-block; padding: 2px;">1</div>
	FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.
Management	FMT_PWD.1 The following actions could be considered for the management functions in FMT: a) Management of ID and password configuration rules.
Audit	FMT_PWD.1 The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST: a) Minimal: All changes of the password.
FMT_PWD.1	Management of ID and password Hierarchical to No other components. Dependencies FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [assignment: list of functions] to [assignment: the authorized identified roles]. 1. [assignment: password combination rules and/or length] 2. [assignment: other management such as management of special characters unusable for password, etc.]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [assignment: list of functions] to [assignment: the authorized identified roles]. 1. [assignment: ID combination rules and/or length] 2. [assignment: other management such as management of special characters

unusable for ID, etc.]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time].

4.5. Protection of the TSF

4.5.1. Protection of stored TSF data

Family This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Behaviour
Component
leveling



FPT_PST.1 Basic protection of stored TSF data, requires the protection of TSF data stored in containers controlled by the TSF.

Management

FPT_PST.1

There are no management activities foreseen.

Audit

FPT_PST.1

There are no auditable events foreseen.

FPT_PST.1

Basic protection of stored TSF data

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PST.1.1

The TSF shall protect [assignment: TSF data] stored in containers controlled by the TSF from the unauthorized [selection: disclosure, modification].

5. Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to the PP.

The security functional requirements included in this ST are derived from CC Part 2 and Chapter 4 Extended Components Definition.

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

Security functional class	Security functional component		note
	identification No.	Security functional component name	
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 (User data encryption)	
	FCS_CKM.1(2)	·Cryptographic key generation (TSF data encryption)	
	FCS_CKM.2	·Cryptographic key distribution	
	FCS_CKM.4	·Cryptographic key destruction	
	FCS_COP.1(1)	·Cryptographic operation (User data encryption)	
	FCS_COP.1(2)	·Cryptographic operation (TSF data encryption)	
	FCS_RBG.1(Extended)	·Random bit generation	
FDP	FDP_UDE.1(Extended)	·User data encryption	
	FDP_RIP.1	·Subset residual information protection	
FIA	FIA_AFL.1	·Authentication failure handling	
	FIA_IMA.1(Extended)	·TOE Internal mutual authentication	
	FIA_SOS.1	·Verification of secrets	
	FIA_UAU.2	·User authentication before any action	
	FIA_UAU.4	·Single-use authentication mechanisms	
	FIA_UAU.7	·Protected authentication feedback	
	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_PWD.1(Extended)	·Management of ID and password	
	FMT_SMF.1	·Specification of management functions	
	FMT_SMR.1	·Security roles	
FPT	FPT_ITT.1	·Basic internal TSF data transfer protection	
	FPT_PST.1(Extended)	·Basic protection of stored TSF data	
	FPT_RCV.1	·Manual recovery	
	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(1)	·TOE session establishment	

5.1. Security audit (FAU)

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 [[table 10] Potential Security Violation Response Table] upon detection of a potential security violation.

Potential Security Violation		Potential Security Violation Response
Admin login failed 3 times		Send mail to authorized administrator, Terminate the process, Block login (10 minutes)
Integrity failure	executable file	Send mail to authorized administrator
	configuration file	Send mail to authorized administrator
Audit data storage saturation	When 80% of the threshold is exceeded	Send mail to authorized administrator
	When 90% of the threshold is exceeded	Send mail to authorized administrator
Failed self-test of cryptographic module		Send mail to authorized administrator, Terminate the process
Abnormal termination of process		Send mail to authorized administrator

[table 10] Potential Security Violation Response Table

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 11] auditable events, [[table 1 2] Other auditable events].

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 [Refer to the contents of “additional audit record” in [table 10] Additional audit record].

Security functional component	Auditable event	Additional audit record
FAU_ARP.1	·Actions taken due to potential security violations	
FAU_SAA.1	·Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.3	·Actions taken due to exceeding of a threshold	
FAU_STG.4	·Actions taken due to the audit storage failure	
FCS_CKM.1(1)	·Success and failure of actions	
FCS_CKM.1(2)	·Success and failure of actions	

Security functional component	Auditable event	Additional audit record
FCS_CKM.2	·Success and failure of actions	
FCS_CKM.4	·Success and failure of actions	
FCS_COP.1(1)	·Success and failure of cryptographic operations, types of cryptographic operations	
FCS_COP.1(2)	·Failure of cryptographic operation, type of cryptographic operation	
FDP_UDE.1	·Success and failure of user data encryption/decryption	
FIA_AFL.1	·The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_IMA.1	·Success and failure of mutual authentication	
FIA_UAU.2	·All uses of the authentication mechanism	
FIA_UAU.4	·Attempt to reuse authentication data	
FIA_UID.2	·All use of the user identification mechanism, including the user identity provided	
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 ·Changes in agent registration status	Modified values of TSF data
FMT_PWD.1	·All changes to ID and password	
FMT_SMF.1	·Use of the management functions	
FMT_SMR.1	·modifications to the group of users that are part of a role	
FPT_TST.1	·Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	·Rejection 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.	
FTA_TSE.1	·Denial of a session establishment due to the session establishment mechanism. All attempts at establishment of a user session.	

[table 11] auditable events

Security functional component	Auditable event	note
-	·Timestamp information for time change confirmation	

[table 12] other auditable events

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 [Among the auditable events of FIA_UAU.2, there is an authentication failure audit event, among the auditable events of FPT_TST.1, there is an integrity violation audit event and a self-test failure event of a verified cryptographic module, an abnormal process termination, possible audit data loss of FAU_STG.3, and the full of audit trail of FAU_STG.4.] 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 capability to apply [[Table 13] methods of selection and ordering] of audit data based on [[Table 13] methods of selection and ordering].

condition	ordering method	note
· OR : IP, Term · AND : count	· Audit history generation date (descending order)	

[Table 13] methods of selection and ordering

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, [None] if the audit trail exceeds [80% of storage space].

FAU_STG.4 Prevention of audit data loss

Hierarchical to FAU_STG.3 Action in case of possible audit data loss

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall “*overwrite the oldest stored audit records*” and [Send security manager warning mail] if the audit trail is full.

5.2. Cryptographic support (FCS)

FCS_CKM.1(1) Cryptographic key generation (User data encryption)

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 **data encryption keys(DEK)** in accordance with a specified cryptographic key generation algorithm [[table 15] User data cipher key generation method and type] and specified cryptographic key sizes [[table 15] User data cipher key generation method and type] that meet the following: [[table 14] User Data cipher key Reference Standards].

classification	Algorithm	Standards
Random number generator	ARIA128_CTR_DRBG ¹⁾	TTAK.KO-12.0189/R2

[table 14] User Data cipher key Reference Standards

classification	Cryptographic key generation algorithm	cryptographic algorithm	cryptographic Key Size	note
user data cipher key	ARIA128_CTR_DRBG	ARIA	K =128, 192, 256	
		SEED	K =128	

[table 15] User data cipher key generation method and type

1) Block cipher-based random number generator with 128-bit key length

FCS_CKM.1(2) Cryptographic key generation (TSF data encryption)

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 [[table 17] TSF data cipher key generation method and type] and specified cryptographic key sizes [[table 17] TSF data cipher key generation method and type] that meet the following: [[table 16] TSF Data cipher key Generation Reference Standards].

classification	Algorithm	description	Standards
key derivation	SHA-256_HMAC_PBKDF2	salt : 16byte iteration : 2048	TTAK.KO-12.0334:2018
Random number generator	ARIA128_CTR_DRBG	-	TTAK.KO-12.0189/R2

[table 16] TSF Data cipher key Generation Reference Standards

classification		Cryptographic key generation algorithm	cryptographic algorithm	cryptographic Key Size	note
KEK	password derivation (for password key)	SHA-256_HMAC_PBKDF2	ARIA	K =256	
	Random number generator based	ARIA128_CTR_DRBG	ARIA	K =128	
TSF data cipher key		ARIA128_CTR_DRBG	ARIA	K =128,192,256	
			SEED	K =128	
For mutual authentication	private authentication Key	ARIA128_CTR_DRBG	RSA-PSS	P =2048 hash=SHA-256	
	Public authentication key				

[table 17] TSF data cipher key generation method and type

FCS_CKM.2 Cryptographic key distribution

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_CKM.2.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [[table 18], [table 19] cipher key distribution method and type] that meets the following: [[table 18] Cryptographic key distribution algorithm and reference standards].

classification	Algorithm	description	Standards
Key agreement algorithm	ECDHE	P-256	NIST SP 800-52 Rev.2

[table 18] Cryptographic key distribution algorithm and reference standards

classification	usage	Distribution process	cryptographic algorithm	distribution method
user data cipher key	For encrypting and decrypting user data	auto	AES-GCM	· Encrypted with symmetric encryption key by manager and sent to agent

[table 19] cipher key distribution method and type

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 destruct cryptographic keys in accordance with a specified cryptographic key destruction method [[table 20] Encryption Key Destruction Method and Reference Standard] that meets the following: [[table 20] Encryption Key Destruction Method and Reference Standard].

classification	contents	Standards
Dest#1	· Overwrite 3 times with value '0'	-
Dest#2	· Perform the zeroization operation of the cipher key by calling the destroy() interface.	-

[Table 20] Encryption Key Destruction Method and Reference Standard

FCS_COP.1(1) Cryptographic operation (User data encryption)

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 [[table 22] List of User Data Cryptographic Operations] in accordance with a specified cryptographic algorithm [[table 22] List of User Data Cryptographic Operations] and cryptographic key sizes [[table 22] List of User Data Cryptographic Operations] that meet the following: [[table 21] Cryptographic Operation (User Data Encryption) Algorithms and Reference Standards].

Classification	cryptographic algorithm	Standards
block cipher algorithm	ARIA	KS X 1213-1:2019
	SEED	TTAS.KO-12.0004/R1:2005
hash algorithm	SHA-256	KS X ISO/IEC 10118-3_2001:2018

[table 21] Cryptographic Operation (User Data Encryption) Algorithms and Reference Standards

Classification	cryptographic algorithm	contents		Operation Mode	note
User Data	ARIA	Key Size	K =128,192,256	approved mode	
		Mode	CBC		
	SEED	Key Size	K =128		
		Mode	CBC		
	SHA	SHA-256			

[table 22] List of User Data Cryptographic Operations

FCS_COP.1(2) Cryptographic operation (TSF data encryption)

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 [[table 24] List of TSF Data Cryptographic Operations, [table 25] List of cryptographic operations for encrypted communications based on standard protocols] in accordance with a specified cryptographic algorithm [[table 24] List of TSF Data Cryptographic Operations, [table 25] List of cryptographic operations for encrypted communications based on standard protocols] and cryptographic key sizes [[table 24] List of TSF Data Cryptographic Operations, [table 25] List of cryptographic operations for encrypted communications based on standard protocols] that meet the following: [[table 23] Cryptographic operation (TSF data encryption) algorithm and reference standards].

Classification	cryptographic algorithm	Standards
block cipher	ARIA	KS X 1213-1:2019
	SEED	TTAS.K0-12.0004/R1:2005
	AES-GCM	ISO/IEC 18033-3:2010 ISO/IEC 19772:2020
hash	SHA	KS X ISO/IEC 10118-3_2001:2018 ISO/IEC 10118-3:2018
digital signature	RSA-PSS	KS X ISO/IEC 14888-2:2011
key agreement	ECDHE	NIST SP 800-52 Rev.2
key derivation	PBKDF2	TTAK.K0-12.0334:2018 NIST SP 800-135 Rev.1
message digest	HMAC	ISO/IEC 9797-2:2021

[table 23] Cryptographic operation (TSF data encryption) algorithm and reference standards

Classification	cryptographic algorithm		contents		note
TSF Data	key derivation	PBKDF2	HMAC-SHA-256		
	block cipher	ARIA	Key Size	K =128,192,256	
			Mode	CBC	
	block cipher	SEED	Key Size	K =128	
			Mode	CBC	
hash	SHA	SHA-256			
digital signature	RSA-PSS	P =2048, hash=SHA-256			

[table 24] List of TSF Data Cryptographic Operations

Classification	cryptographic algorithm		contents		note
TSF Data	key derivation	PBKDF2	HMAC-SHA-256		
	block cipher	AES-GCM	Key Size	K =128	

Classification	cryptographic algorithm		contents		note
			Mode	GCM	
	hash	SHA	SHA-256		
	key agreement	ECDHE	P-256		
	message digest	HMAC	HMAC-256(K =256)		

[table 25] List of cryptographic operations for encrypted communications based on standard protocols

FCS_RBG.1 Random number generation (Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FCS_RBG.1.1 The TSF shall generate random bit using the specified random bit generator that meets the following [[table 26] Random number Generation Algorithms and Reference Standards]

classification	Algorithm		Standards
Random number generator	Block cipher-based	ARIA128_CTR_DRBG	TTAK.KO-12.0189/R2
	Hash-based	SHA-256_HASH_DRBG	NIST SP 800-90A Rev.1

[table 26] Random number Generation Algorithms and Reference Standards

5.3. User data protection (FDP)

FDP_UDE.1 User data encryption (Extended)

Hierarchical to No other components.

Dependencies FCS_COP.1 Cryptographic operation

FDP_UDE.1.1 The TSF shall provide a function that can encrypt/decrypt the user data to the TOE user according to the specified [encryption/decryption method by column, [One-way encryption per column]].

FDP_RIP.1 Subset residual information protection

Hierarchical to No other components.

Dependencies No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to, deallocation of the resource from the following objects: [user data].

5.4. 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 [3] unsuccessful authentication attempts occur related to [administrator' s authentication attempt].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [Send security administrator alert email, close management tool, disable login function (10 minutes)]

FIA_IMA.1 TOE Internal mutual authentication (Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [Management tool and Manager, Agent and Manager] using the [Self-Implemented Authentication Protocol] that meets the following [None].

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 [[table 27] Password Generation Rules]].

Classification	Generation Rules
Compliance	<ul style="list-style-type: none"> · Length: 9 to 30 characters · Allowable characters: English uppercase letters, English lowercase letters, special characters, numbers · Combination rules: Must include at least one English uppercase letter, English lowercase letter, special character, or number
Prohibited Items	<ul style="list-style-type: none"> · Do not set the same password as the user account (ID) · Prohibition of consecutive repeated 3 or more input of the same letter/number · Prohibit sequential input of 3 or more consecutive letters or numbers on the keyboard · Prohibition of reuse of the password used immediately before

[table 27] Password Generation Rules

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 user

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [Administrator authentication mechanism]

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

[

- The input password is masked (●) so that it cannot be seen on the screen.
- In case of identification and authentication failure, feedback on the failure is not provided.

]

to the user while the authentication is in progress.

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 user

5.5. 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 *conduct management actions of* the functions [[table 28] List of security functions] to [the authorized administrator].

security function	Contents	Management action			
		determine the behaviour	disable	enable	modify the behaviour
Password Management	· change password for administrator/ CipherKey	0	-	-	-
Configuration file management	· Managemnet of configuration information	0	-	-	-
login management	· Security manager login/logout	0	-	-	-
cipher key management	· generation/inquiry/destruction cipher key	0	-	-	-
Audit history inquiry	· Audit history information inquiry	0	-	-	-
Help	· TOE components integrity check	0	-	-	-

[table 28] List of security functions

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 *manage* [[table 29] TSF data list] to [Authorized Administrator].

TSF data		contents	management			
			create	query	modify	delete
password	for cipher key	· Authentication information for the cipher key	-	-	0	-
Admin info.	id	· Information for Administrator Authentication	-	-	0	-
	password					
unique information		· Information to indicate the uniqueness of TOE components	-	-	-	0
KEK	password-derived (for cipher key)	· password derived key for cipher key	-	-	-	-
	Random number generator based	· Random number generator based KEK	-	-	-	0
user data cipher key		· user data cipher key	0	0	-	0
TSF data cipher key		· TSF data cipher key	0	0	0	0
For mutual authentication	private authentication Key	· Private key for mutual authentication	-	0	-	0

TSF data		contents	management				
			create	query	modify	delete	
Public authentication key		· Public key for mutual authentication	-	0	-	0	
audit history information		· Audit history information generated by TOE	-	0	-	-	
Preferences information	IP agent	Management tool	· IP address of management tool for access control	-	0	0	-
			· IP address of agent for access control	-	0	0	-
	Admin Email Address	· Administrator email address for sending emails	0	0	0	-	
	Mail server address	· Mail server address for sending mail	0	0	0	-	
	Mail server id	· Mail server id for sending mail	0	0	0	-	
	Mail server password	· Mail server password for sending mail	0	0	0	-	
	TOE component version information	· Manager/Agent/Management Tool Version Information	-	0	-	-	
	TOE Agent Information	· Whether the agent is activated	-	0	-	-	

[table 29] TSF data list

FMT_PWD.1 Management of ID and password(Extended)

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [None] to [Authorized Administrator].

1. [None]

2. [None]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the id of [None] to [Authorized Administrator].

1. [None]

2. [None]

FMT_PWD.1.3 The TSF shall provide the capability for *setting ID and password when installing*.

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: [

List of security functions specified in FMT_MOF.1

TSF data management list specified in FMT_MTD.1

ID and password management list specified in FMT_PWD.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 [Security Manager].

FMT_SMR.1.2 TSF shall be able to associate users and their roles defined in FMT_SMR.1.1.

5.6. Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to No other components.

Dependencies No dependencies.

FPT_ITT.1.1 The TSF shall protect the TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

Classification	version	Cryptographic algorithm	Confidentiality	Integrity	Standards
TLS	v1.3	TLS_AES_128_GCM_SHA256	AES128-GCM	HMAC-256	RFC 8446

[Table 30] TOE inter-component cryptographic communication standard

FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PST.1.1 The TSF shall protect [[table 31] Stored TSF Data Protection Policy] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

Classification	contents	
Authentication information	for certificate	· password
	for cipher key	· password
	for administrator	· ID/Password
cipher key info	· Certificate, symmetric key, asymmetric key (private key)	
Setting information	· TOE Operation Information	
DB account information	· ID/Password	

[Table 31] Stored TSF Data Protection Policy

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 *at the initial start-up, periodically during normal operation, upon the request of authorized user* to demonstrate the correct operation of [*management tool, manager, agent*].

FPT_TST.1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [*configuration file*].

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [*executable file*].

Classification	Whether the process is running	Integrity Test		Point of view	note
		Executable file	Configuration file		
Management tool	0	0	-	On startup, Periodically (1 hour), Upon administrator request	If self-test and integrity check fail, send email to security manager
Manager	0	0			
Agent	0	0			

[Table 32] List of self-tests by TOE component

FPT_RCV.1 Manual recovery

Hierarchical to No other components.

Dependencies AGD_OPE.1 Operational user guidance

FPT_RCV.1.1 After [integrity check failure event] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

5.7. 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

belonging to the same user according to the rules [limiting the maximum number of concurrent sessions to 1 for users who have the same **administrator**, rules on the maximum number of concurrent sessions{None}].

FTA_MCS.2.2 The TSF shall enforce a limit of [1] session per **administrator** by default.

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 [Security Manager Inactivity Period 10 minutes].

FTA_TSE.1 TOE session establishment

Hierarchical to No other components.

Dependencies No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **the administrator's management access session** establishment based on [access IP, [*none*]].

6. Security assurance requirements

Assurance requirements of this ST are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

Security assurance class	Security assurance component	
	identification No.	Security assurance component name
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

6.1. Security Target evaluation

ASE_INT.1 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.

6.2. 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.

6.3. 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 Operational user guidance

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_PRE.1.1C 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_PRE.1.2C 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.

6.4. Life cycle support

ALC_CMC.1 TOE 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.

6.5. 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.

6.6. 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.

7. Security requirements rationale

7.1. Dependency rationale of security functional requirements

The following table shows dependency of security functional requirements.

No.	SFR	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	Rationale(1)
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	Rationale(2)
7	FAU_STG.4	FAU_STG.1	Rationale(2)
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	10, 12
		FCS_CKM.4	11
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	10, 13
		FCS_CKM.4	11
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
		FCS_CKM.4	11
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
12	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	11
13	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9
		FCS_CKM.4	11
14	FCS_RBG.1	-	-
15	FDP_UDE.1	FCS_COP.1	12
16	FDP_RIP.1	-	-
17	FIA_AFL.1	FIA_UAU.1	20 Rationale(3)
18	FIA_IMA.1	-	-
19	FIA_SOS.1	-	-
20	FIA_UAU.2	FIA_UID.1	22 Rationale(4)
21	FIA_UAU.4	-	-
22	FIA_UAU.7	FIA_UAU.1	20 Rationale(3)
23	FIA_UID.2	-	-
24	FMT_MOF.1	FMT_SMF.1	28
		FMT_SMR.1	29
25	FMT_MTD.1	FMT_SMF.1	28
		FMT_SMR.1	29
26	FMT_PWD.1	FMT_SMF.1	28
		FMT_SMR.1	29
27	FMT_SMF.1	-	-
28	FMT_SMR.1	FIA_UID.1	23 Rationale(4)

No.	SFR	Dependency	Reference No.
29	FPT_ITT.1	-	-
30	FPT_PST.1	-	-
31	FPT_TST.1	-	-
32	FPT_RCV.1	AGD_OPE.1	EAL1+
33	FTA_MCS.2	FIA_UID.1	23 Rationale(4)
34	FTA_SSL.3	-	-
35	FTA_TSE.1	-	-

[Table 33] Rationale for the dependency of the security functional requirements

Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1, but it satisfies the dependency because it uses reliable timestamp provided by OE.Timestamp, the security objective for the operating environment of this Security Target.

Rationale (2): FAU_STG.3 and FAU_STG.4 have dependencies on FAU_STG.1, but they satisfy the dependencies because they use the security objective OE. Secure DBMS for the operating environment protected from unauthorized deletion or modification.

Rationale(3): FIA_AFL.1, FIA_UAU.7 depend on FIA_UAU.1, but are satisfied by FIA_UAU.2, which has a hierarchical relationship with FIA_UAU.1.

Rationale(4): FIA_UAU.2, FMT_SMR.1, and FTA_MCS.2 depend on FIA_UID.1, but are satisfied by FIA_UID.2, which has a hierarchical relationship with FIA_UID.1.

7.2. 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 ST since it is not necessarily required to show the correspondence between the tests and the TSFIs.

8. TOE Summary Specification

This chapter explains whether the assurance method for the TOE security function is appropriate for the security function provided by the TOE.

The security functions provided by the TOE include security audit(FAU), cryptographic support (FCS), user data protection(FDP), identification and authentication(FIA), security management (FMT), Protection of the TSF(FPT), TOE access (FTA).

8.1. Security audit(FAU)

This chapter explains whether the assurance method for the TOE security function is appropriate for the security function provided by the TOE.

8.1.1. Security audit

The TOE generates audit data for auditable events that occur during operation. The generated audit data is stored in the database, and a reliable timestamp (time in the OS where the server is installed) provided by the TOE operating environment is used to ensure that the audit data is generated sequentially.

The TOE generates and stores auditable events according to the date and time of the event, the type of event, the identity of the subject who caused the event, details of work, and results (success/failure).

※ SFR Mapping

FAU_GEN.1

8.1.2. Audit data review

The TOE stores audit data in a database and provides the ability for security administrators to review all audit data so that information in the audit record can be interpreted appropriately. In addition, audit data can be reviewed by AND conditions of the review period, IP, and number of inquiries, and the security administrator can search audit data using the interface provided by the management tool.

※ SFR Mapping

FAU_SAR.1, FAU_SAR.3

8.1.3. Audit Data Loss Prevention

The TOE stores audit records generated by the TOE in the database in the TOE operating environment and periodically checks the audit record storage space. If the remaining space of the storage set in the TOE exceeds the threshold (80%), an audit log is created for the event exceeding the storage and a warning mail is sent to the security manager. And if the remaining space exceeds the threshold (90%), the TOE overwrites the oldest audit data and sends a warning mail to the security administrator.

※ SFR Mapping

FAU_STG.3, FAU_STG.4

8.1.4. Security alarm

The TOE applies a combination of rules that indicate potential security violations to the audit data and issues a security alarm that sends a warning email to the defined administrator in case of a violation. Potential security violations include:

- If the security manager fails to log in 3 times
- If the integrity check of the TOE executable file and configuration file fails
- When the storage space of the audit history storage exceeds 80% or exceeds 90%
- In the event that the self-test of the verified cryptographic module fails
- If the TOE (manager, management tool, agent) process terminates abnormally

※ **SFR Mapping**

FAU_ARP.1, FAU_SAA.1

8.2. Cryptographic support(FCS)

8.2.1. Cipher key Generation

The TOE generates cryptographic keys using the password derivation, random number generator, and RSA key pair generation functions provided by the KCMVP cyprtophraphic module installed in the TOE and executed in approved mode of operation.

※ SFR Mapping

FCS_CKM.1(1), FCS_CKM.1(2)

8.2.2. Cipher key Distribution

TOE provides standard protocol-based encrypted communication using key setting encryption algorithm (ECDHE) provided by 3rd party software (BC-FJA) between TOE components. The encryption key types and distribution methods are as follows.

classification	usage	Distribution process	crypto-graphic algorithm	Standards
encrypted channel	key agreement	auto	ECDHE	NIST SP 800-52 Rev.2
user data cipher key	For encrypting and decrypting user data	auto	AES-GCM	ISO/IEC 18033-3:2010 ISO/IEC 19772:2020

[Table 34] cipher key distribution method and type

※ SFR Mapping

FCS_CKM.2

8.2.3. Cipher key Destruction

TOE provides two types of destruction methods to safely destroy encryption keys and core security parameters. Encryption keys used in core security parameters and verified encryption modules are destroyed by overwriting them three times with the value of '0' (Destruction #1), and The cipher key for the encryption algorithm provided by 3rd party software (BC-FJA) is destroyed by performing key zeroing by calling the destroy() interface (destruction #2).

※ SFR Mapping

FCS_CKM.4

8.2.4. Cryptographic operation

TOE performs cryptographic operations using key derivation, block cipher, hash, digital signature, and message authentication algorithms provided by the verification-based cryptographic module and key derivation, block cipher, key agreement, and message authentication provided by 3rd party software (BC-FJA).

※ SFR Mapping

FCS_COP.1(1), FCS_COP.1(2)

8.2.5. random number generation

TOE generates random numbers required for generating encryption keys using a random number generator provided by 3rd party software (BC-FJA) and a random number generator that is the encryption algorithm of the KCMVP cryptographic module. The random number generation method is shown in the table below.

Classification	algorithm		Standards
Random number generator	Block cipher-based	ARIA128_CTR_DRBG	TTAK.KO-12.0189/R2
	Hash-based	SHA-256_HASH_DRBG	NIST SP 800-90A Rev.1

[Table 35] Random number Generation Algorithms and Reference Standards

※ **SFR Mapping**

FCS_RBG.1(Extended)

8.3. User data protection(FDP)

The TOE provides a column-level encryption/decryption function for data stored in the DBMS to be protected through the KCMVP cryptographic module, and provides a function that prevents the same ciphertext from being generated for the same plaintext when encrypting user data. And to protect user data, all plain text original data used for user data encryption/decryption is deleted.

The security manager sets the DB encryption policy in the management tool, the set policy is stored in the database via the manager, and the agent performs two-way encryption and one-way encryption of user data according to the set DB encryption/decryption policy. Two-way encryption uses a block cipher algorithm to encrypt and decrypt user data, and one-way encryption uses a hash algorithm to encrypt user data. The encryption/decryption methods and list of user data are as follows.

classification		Way	Algorithm	contents
Column based Cipher method	Encryption	two-way	ARIA SEED	<ul style="list-style-type: none"> · Enc([plaintext(random number + user data)]) = [cipher text] · Random number acquisition through random number generator · Generate different cipher texts for the same plain text (user data) through encryption algorithms
	Decryption	two-way	ARIA SEED	<ul style="list-style-type: none"> · Dec([ciphertext]) = [random number + plaintext(user data)] · Remove random numbers from plain text
	Encryption	one-way	SHA-256	<ul style="list-style-type: none"> · Generating cipher text using hash algorithm (SHA-256)

[Table 36] List of user data encryption/decryption methods

After encryption/decryption, the agent initializes user data to “0” and releases the memory area to completely delete user data from the memory area.

※ SFR Mapping

FDP_UDE.1(Extended), FDP_RIP.1

8.4. Identification and authentication(FIA)

The TOE provides mutual authentication between TOE components, administrator identification and authentication functions when a security administrator accesses the manager through management tools.

8.4.1. Security manager identification and authentication

The security manager must register an account (ID and password) and an allowed IP so that he/she can create his/her own information when installing the manager, and the management tool performs security manager authentication using the ID and password before the security manager performs security management functions.

When performing the identification and authentication of the security manager, the management tool masks (●) the password entered by the security manager so that it cannot be seen on the screen, and only provides an authentication failure message saying "Login failed." If authentication fails for a defined number of consecutive attempts (3 times), the manager blocks access attempts to the account for 10 minutes (fixed value), saves an audit record for authentication failures, and sends a warning email to the security manager.

TOE provides a verification mechanism that satisfies the administrator password creation rules at the time of administrator authentication and password change as follows.

- The length must be 9 to 30 characters, and the allowed characters are English uppercase letters, English lowercase letters, special characters, and numbers, and the combination rule must include at least one English uppercase letter, English lowercase letter, special character, and number.
- Passwords that are identical to the user account (ID), passwords entered by repeating the same letters/numbers more than three times in a row, passwords entered by sequentially entering three or more consecutive letters or numbers on the keyboard, and passwords used immediately before cannot be used.

In addition, the manager provides a function to prevent reuse of authentication data by using random number information generated by a random number generator to ensure the uniqueness of the session used when the security manager accesses the management tool.

※ SFR Mapping

FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

8.4.2. mutual authentication

When communicating between TOE components, mutual authentication is performed through digital signature verification using the unique value (Unique ID) issued between the management tool and the manager (agent and manager) in real time.

※ SFR Mapping

FIA_IMA.1(Extended)

8.5. Security Management(FMT)

8.5.1. Security role

When the TOE installs the manager, it generates the ID/password of the security manager and identifies/authenticates the security manager through this. The security role provided by the TOE is limited to the security manager only, and only the security manager can change the ID/password through the management tool. Lastly, in the TOE, the ID/password combination rules and length required for identification/authentication of the security administrator are fixed and do not provide a separate management function.

※ SFR Mapping

FMT_PWD.1(Extended), FMT_SMR.1

8.5.2. Security Feature Behavior Management

The TOE provides security management functions only when administrator's identification and authentication are successfully performed. Only the security manager can access the security management interface through the secure channel.

※ SFR Mapping

FMT_MOF.1, FMT_SMF.1

8.5.3. TSF data management

Only security administrators who have successfully authenticated the TOE can manage TSF data.

※ SFR Mapping

FMT_MTD.1, FMT_SMF.1

8.6. Protection of the TSF(FPT)

8.6.1. Internal TSF data transfer protection

TOE performs encrypted communication based on standard protocol (TLS V1.3) for TSF data transmission for the purpose of protecting internal TSF data transmission, and protects transmitted data through the encrypted communication.

※ SFR Mapping

FPT_ITT.1

8.6.2. Stored TSF data protection

The TOE stores important information(cryptographic key, password, etc.) using encryption, when storing it in containers controlled by the TSF.

※ SFR Mapping

FPT_PST.1(Extended)

8.6.3. Self Test

The TSF testing consists of self-test of process and integrity verification. If the self-test/integrity-check fails, a warning mail is sent to the e-mail address set by the security administrator. The TOE periodically (1 minute) checks whether the processes between TOE components are running,

The TOE performs an integrity verification test (verified cryptographic module, execution/configuration file) at startup, periodically (1 hour), and upon request from the security manager

In addition, if the integrity verification result for the integrity check target fails, the TOE must perform manual recovery (refer to the administrator manual for reinstallation, regeneration commands, etc.) as information such as the TOE agent is tampered with.

※ SFR Mapping

FPT_TST.1, FPT_RCV.1

8.7. TOE access(FTA)

8.7.1. Limitation on concurrent sessions

TOE allows access sessions based on the management tool access IP, limits simultaneous access sessions to a maximum of 1, and terminates the session if the management tool inactivity period exceeds 10 minutes.

※ SFR Mapping

FTA_MCS.2, FTA_SSL.3, FTA_TSE.1