Echelon V3.5
Security Target v1.2

UbimInfo Co., Ltd.

The Security Target related to the certified TOE. This Security Target is written in korean and translated from Korean into English.

Revision history			
Document name	Echelon V3.5-ASE.1-ST		
version	Date	Content	비고
1.0	2022.12. 3	Draft	
1.1	2022. 1. 4	· TOE physical scope modification	
1.2	2023. 2. 1	· Redefining SFR Terminology · FAU_GEN.1.2, FAU_STG.3.1, Reflection of FTA_SSL.5.1 assignment/selection operations	

Contents

1. Security Target Introduction

This chapter describes the ST reference, TOE reference, TOE overview, TOE Description, Conventions, Terms and Composition of Security Target

1.1. ST Reference

Classification	Description
Title	Echelon V3.5 ST
Identification	Echelon V3.5-ASE.1-ST-r1.2
Version	r1.2
publication Date	February 1, 2023
Author	UbimInfo Co., Ltd.
Common Criteria Version	CC V3.1 r5
Protection Profile	Korean National Protection Profile for Database Encryption V1.1
	KECS-PP-0820a-2017
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keyword	Database, Encryption

[table 1] ST reference

1.2. TOE Reference

Classification		Identifier Information
TOE Identification		Echelon V3.5
TOE type		Database Encryption
TOE version		V3.5
build version		3.5.0.0.3
TOE Components	management tool	Echelon V3.5-AdministratorV1.04
	Manager	Echelon V3.5-ManagerV1.04
	Agent	Echelon V3.5-AgentV1.04
Release Date		December 3, 2022
Author		UbimInfo Co., Ltd.
publication Date		February 24, 2023
Guidance		Echelon V3.5-PRE.1-r1.1 Echelon V3.5-OPE.1-r1.1 Echelon V3.5-OPE.2-r1.0

[table 2] TOE reference

1.3. TOE overview

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

1.3.1. TOE overview

Echelon V3.5 (hereinafter referred to as 'TOE') is a DB 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 in column units, 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 manages the DB in the organization's operating environment is distinguished from the DBMS that the TOE directly uses to manage 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 method 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 security manager. The TOE provides major security functions such as [Table 3] to prevent leakage of confidential information and to operate the TOE safely in the operating environment of the organization.

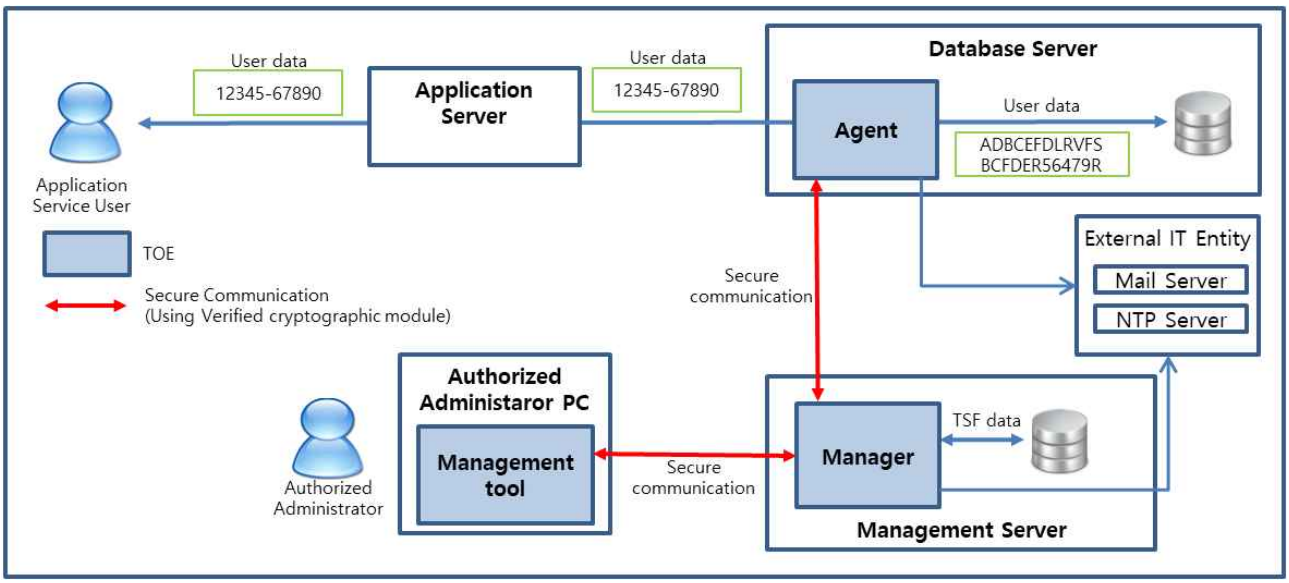
components	description
security audit	· Ability to create audit data including the date and time of the incident, the type of incident, the identity of the person who caused the incident, work details and results (success/failure) · Audit data review function for security administrators · Audit data loss prevention function
Cryptographic support	· Function to generate, renew, and destroy cryptographic keys through verified cryptographic modules · Function to protect the encryption key (DEK) for user data using the key encryption key (KEK) · Function to perform cryptographic calculation (data encryption/decryption) using encryption key for user data
User data protection	· Ability to generate different ciphertext for the same plaintext per column for user data · Data protection function by destroying original data (overwriting ‘0’)
Identification and Authentication	· ID/password based security administrator identification function · Mutual authentication function between TOE components · Reuse prevention function to protect authentication data

components	description
security management	· Encryption key lookup, administrator ID/password and environment setting management function
TSF protection	· TSF data protection function transmitted between TOE components · TSF data protection function stored in storage controlled by TSF · TSF self-test function
TOE access	· Access session management function of security manager

[table 3] TOE major security functions

1.3.4. TOE operational environment

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



[figure 1] Plug-in type operational environment (Agent, management server integrated 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 view audit history.

The manager installed on the Echelon 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 acquire trusted time information for the security audit data generated by the manager, and the mail server sends e-mail to the authorized

administrator.

When data is transmitted between components(management tool, manager, agent), the TOE performs encrypted communication using the public key encryption(RSAES) and block cipher algorithms(ARIA) provided by the verified cryptographic module.

[Table 4] shows the information on the verified cryptographic module that performs cryptographic operations during TOE operation.

Classification	Contents
cryptographic module name	MPowerCrypto V2.5
Verification number	CM-154-2024.9
verification level	VSL1
developer	UbimInfo Co.,Ltd.
verification date	2019-09-03
expiration date	2024-09-03

[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.

Classification	Item		Specification
Management tool	H/W	OS	Windows 10 Pro(64bit)
		CPU	Intel Core i3 @ 3.40GHz or higher
		RAM	8GB or higher
		HDD	Space required for TOE Installation is 1 GB or higher
		NIC	Ethernet 10/100/1000 Mbps * 1 port
	S/W		Eclipse RCP 4.19.0, JRE 11.0.16
Manager	H/W	OS	Ubuntu 18.04.6(64bit)(Kernel:4.15.0-204)
		CPU	Intel Core i3 @ 3.40GHz or higher
		RAM	8GB or higher
		HDD	Space required for TOE Installation is 1 GB or higher
		NIC	Ethernet 10/100/1000 Mbps * 1 port
	S/W		PostgreSQL 14.7, MPowerPlus 1.3.1, JRE 11.0.16
Agent	H/W	OS	Oracle linux 8.7(64bit)(Kernel:4.18.0-425)
		CPU	Intel Core i3 @ 3.40GHz or higher
		RAM	8GB or higher
		HDD	Space required for TOE Installation is 1 GB or higher
		NIC	Ethernet 10/100/1000 Mbps * 1 port
	S/W		Oracle 19.3.0.0.0, MPowerPlus 1.3.1, JRE 11.0.16

[table 5] hardware/software minimum specifications

The Management tool including Eclipse RCP and JRE software to provide GUI to the authorized administrator is installed on the authorized administrator PC.

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

The Agent including 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(11.0.16)	· 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 (14.7)	· 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	

Classification	software	contents	note
		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 (Acquiring trusted time information for security audit data)	

[table 7] external IT entities

1.4. TOE Description

The TOE is operated in the form of a plug-in 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

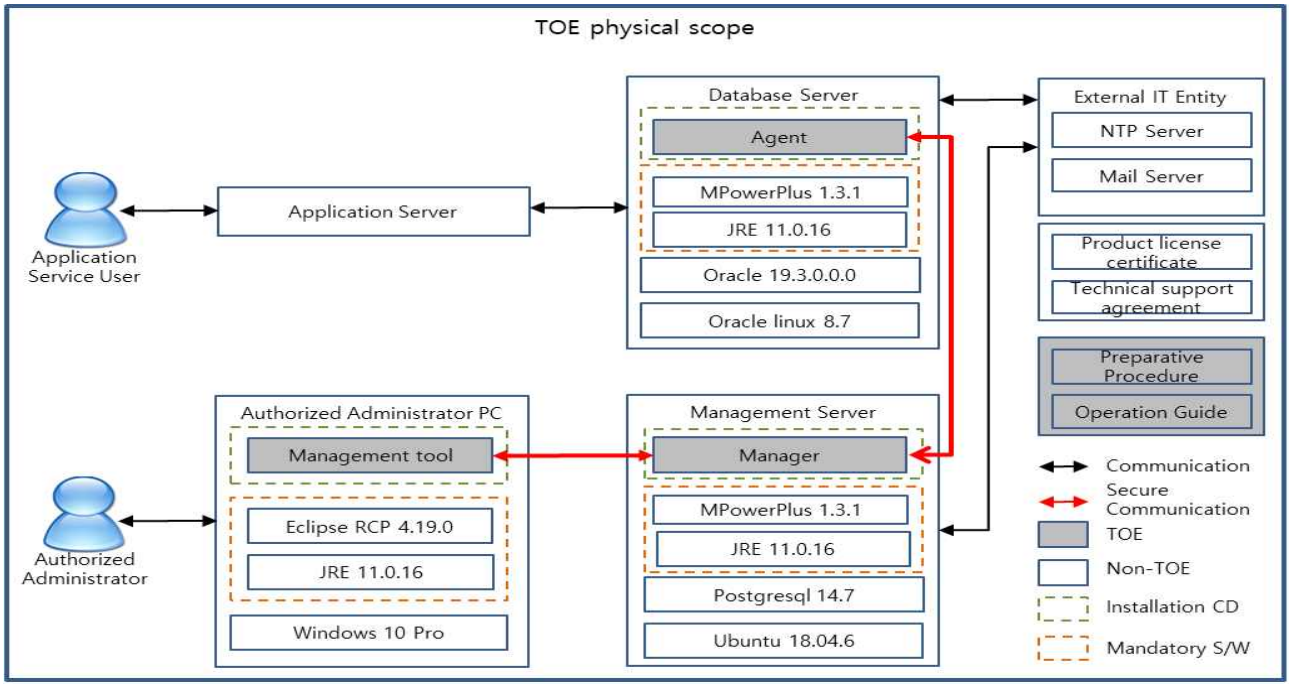
The physical scope of the TOE is as follows.

classification		Components	production type	Deployment type
TOE Components	Management tool	Echelon V3.5-AdministratorV1.04 (EchelonV3.5@AdministratorV1.04.msi)	SW	CD
	Manager	Echelon V3.5-ManagerV1.04 (EchelonV3.5@ManagerV1.04.jar)		
	Agent	Echelon V3.5-AgentV1.04 (EchelonV3.5@AgentV1.04.jar)		
Guidance Documents	Preparative Procedure	Echelon V3.5-PRE.1-r1.1 (Echelon V3.5-PRE.1-r1.1.pdf)	PDF	
	Operation Guide	Echelon V3.5-OPE.1-r1.1 (Echelon V3.5-OPE.1-r1.1.pdf) Echelon V3.5-OPE.2-r1.0 (Echelon V3.5-OPE.2-r1.0.pdf)		
Mandatory S/W		JRE 11.0.16 (PKG_JRE11_Windows.zip, jre-11.0.16_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	-
		Technical support agreement	Paper	-

[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 preparation procedures necessary for installation, administrator manuals necessary for operation, and operation manuals are provided as PDF files. do. In addition, essential software (JRE, Eclipse, MPowerPlus) required for TOE installation is included, which is excluded from the scope of the TOE.

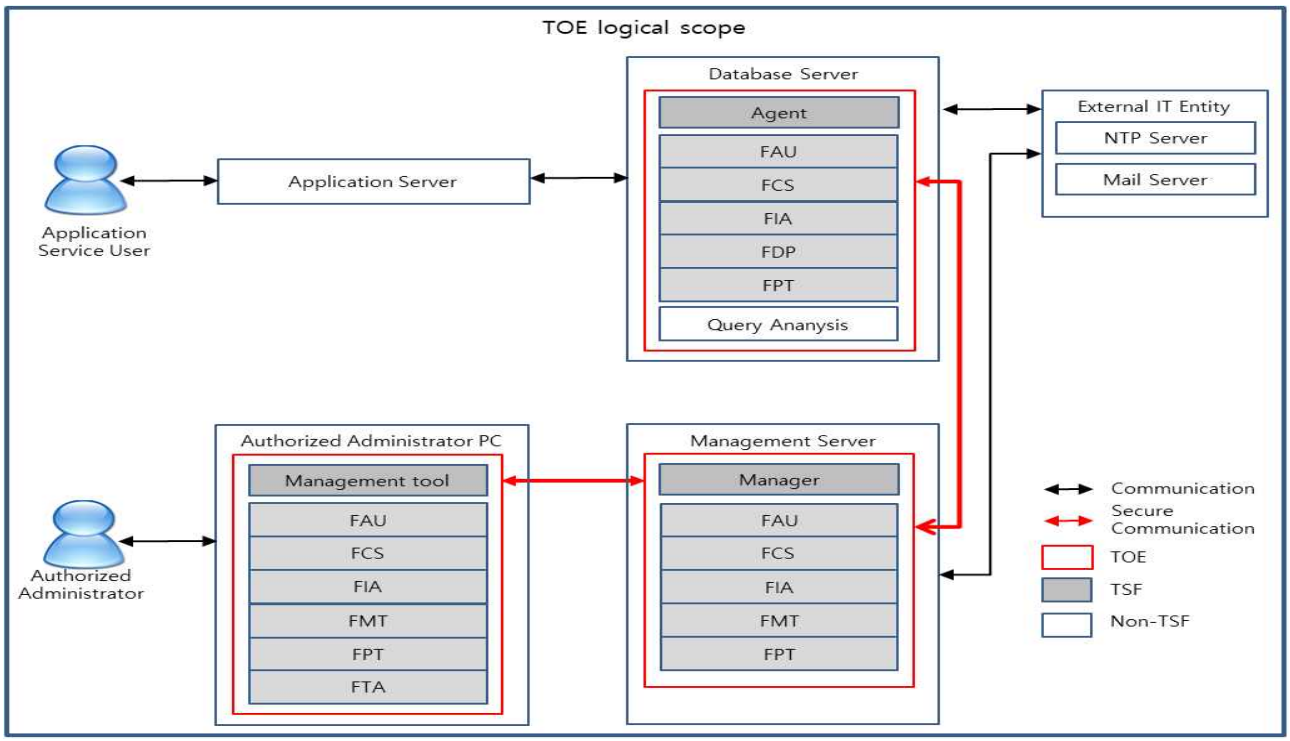
The physical scope of the TOE is Management tool, Manager, Agent, non-TOE operational environment. It is structured as follows.



[figure 2] Physical scope of the TOE

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. Through this, the TOE provides secure security functions. [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 incident 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 event result (success or failure), and all generated audit data provides the ability to be searched and reviewed by authorized administrators.

• Cryptographic support(FCS)

The management tool generates and distributes all cryptographic keys to protect user data and data transmitted between TOE components (management tool, manager), and performs cryptographic operation using cryptographic algorithms of verified cryptographic modules whose safety and suitability for implementation are verified. and destroy the encryption key by overwriting it with "0".

• Identification and authentication(FIA)

When the management tool communicates with the physically separated manager, it performs mutual authentication through its own authentication protocol, and performs ID/password-based identification and authentication before all actions of the administrator who want to use the security management function. The management tool provides a function to protect authentication feedback for authentication data input. The administrator must set the password to be 9 or more and 30 or less 30 digits with a combination of three types of English letters, numbers, and special characters.

• Security management(FMT)

The management tool provides security functions (password management, cipher key management, environment configuration information management, cipher key history inquiry, audit data inquiry, integrity check) and TSF data management function (environment configuration information) to authorized administrators.

• Protection of the TSF(FPT)

The management tool performs self-tests and integrity checks periodically during initial start-up and normal operation to prove the correct operation of the management tool process, TSF data and executable TSF code, and also performs integrity verification tests on the TOE at the request of an authorized administrator. TSF data and TOE configuration (security policy, etc.) transmitted between the management tool and manager are protected from unauthorized disclosure and tampering by using verified cryptographic modules.

• TOE access(FTA)

When an authorized administrator connects, it verifies whether the IP address is allowed, allows access only to the allowed IP and single session, and terminates the authorized administrator session when the inactivity period exceeds a certain time.

○ Manager

• Security audit(FAU)

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

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 saved 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 operation using cryptographic algorithms of verified cryptographic modules whose safety and suitability for implementation are verified. and destroy the encryption key by overwriting it with "0".

• Identification and authentication(FIA)

When communicating with a physically separated management tool (agent), the manager performs mutual authentication through its own authentication protocol. When the authentication and identification of the security manager is successfully completed, attempts to reuse authentication data are blocked by maintaining the authentication session with the encryption key used during encrypted communication.

• Security management(FMT)

The manager performs security functions (password management, cipher key management, environment configuration information management, cipher key history inquiry, audit data inquiry, integrity check) and TSF data management function (environment setting information) requested by the security manager through the management tool.

• Protection of the TSF(FPT)

During initial start-up and during normal operation, the manager periodically conducts self-tests and integrity checks to prove the correct operation of the manager process, TSF data, and executable TSF code, and also performs integrity verification tests for the manager at the request of an authorized administrator. TSF data transmitted between TOE components (management tool and manager, agent and manager) and TOE configuration (security policy, etc.) are protected from unauthorized disclosure and tampering by using verified cryptographic modules.

○ Agent

• Security audit(FAU)

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

• Cryptographic support(FCS)

To protect user data and data transmitted between the agent and the manager, the agent performs cryptographic operations using the cryptographic algorithm of the verified cryptographic module whose safety and suitability for implementation have been verified. The encryption key is destroyed by overwriting it with "0".

• User data protection(FDP)

The agent encrypts/decrypts user data column by column according to the policy set by the authorized administrator. After encrypting/decrypting the original data, it is deleted without saving to prevent reuse.

• Identification and authentication(FIA)

When an agent communicates with a physically separated manager, it performs mutual authentication through its own authentication protocol.

• Protection of the TSF(FPT)

The agent periodically performs self-tests and integrity checks during initial start-up and normal operation to prove the correct operation of the agent process, TSF data, and executable TSF code. Protect TSF data and TOE configuration (security policy, etc.) transmitted between agent and manager from unauthorized disclosure and tampering by using verified cryptographic modules.

○ Non-security functions excluded from the evaluation scope are as follows.

• Management tool

- query analysis: The query analysis is a function that analyzes the query language requested by the user and is excluded from evaluation.

• Manager

- None

• Agent

- None

1.5. Conventions

The notation, formatting and conventions used in this PP 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.

Precautions for application

Application notes are provided to clarify the meaning of a requirement, provide information about options in implementation, and define “pass/fail” criteria for a requirement.

Application notes are provided along with the applicable requirements where necessary.

1.6. Terms and definitions

In this document, among the terms used in the Security Target, the same terms as those used in the CC follow the CC.

Agent
TOE component that provides cryptographic calculation function of user data using TOE

Application Server
The Application Server defined in this Security Target means the server in which the application developed to provide specific application services in the TOE operating organization is installed and operated. The application plays a role of reading user data from the DB existing in the database server upon request of the user of the application service, or transmitting user data to be stored in the DB to the database server.

Approved mode of operation
Operation mode of the cryptographic module using the cryptographic algorithm to be verified

Approved cryptographic algorithm
Block cipher, hash function, message authentication code, random number generator, key setting, public key cryptography, and digital signature cryptographic algorithm selected by cryptographic module verification organizations in consideration of safety, reliability, and interoperability

Assets
An entity that the owner of the TOE attaches value to

Attack potential
Degree of effort required to attack the TOE, identified in terms of the attacker's expertise, resources, motivation, etc.

Augmentation
Adding one or more requirements to a package

Authentication Data
Information used to prove your identity

Authorized Administrator
Authorized users who safely operate and manage the TOE

Authorized User
Users who can execute functions according to Security Functional Requirements(SFRs)

Class
A collection of CC families with the same security objective

column

A set of data values with a specific data type corresponding to one value in each row in a relational database table.

Component

A set of elements, the smallest selected unit that can be used to form the basis of a requirement

CSP(Critical Security Parameters)

Security-related information (e.g. private/private keys, authentication data such as passwords or personal identification numbers) that could compromise the security of cryptographic modules if exposed or altered.

Database Server

Database Server defined in this Security Target means the server where the DBMS that manages the DB to be protected in the TOE operating organization is built.

DB(Database)

A set of data organized according to a certain structure in order to receive, store, and supply data in response to the needs of multiple users so as to support multiple application tasks at the same time. A database related to encryption by column required by this Security Target means a relational database.

DBMS(Database Management System)

As a software system configured to configure and apply the database, the DBMS related to encryption by column required by this Security Target refers to a database management system based on the relational database model.

Decryption

Restoring ciphertext to its original plaintext using a decryption key

DEK(Data Encryption Key)

Key to encrypt/decrypt data

Dependency

As a relationship between components, if requirements based on dependent components are included in a PP, ST, or package, requirements based on dependent components (to that component) are also included in the PP, ST, or package. relationships that should be included in

EAL(Evaluation Assurance Level)

An assurance package consisting of three part assurance requirements with predefined assurance levels in the CC.

Echelon V3.5

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 stand-alone application with rich features based on the Eclipse platform.

Element
The smallest unit of indivisible security requirements (things)

Encryption
Converting plaintext to ciphertext using an encryption key

External Entity
An entity (person or IT) that interacts with (or can interact with) the TOE from outside the TOE.

Family
A collection of components that have a similar purpose but differ in emphasis or rigor.

Identity
A unique representation that identifies an authorized user. It can be the user's real name, abbreviation or pseudonym.

JRE(Java Runtime Environment)
Framework environment required to run management tools, managers and agents that make up the TOE

KEK(Key Encryption Key)
A key that encrypts and decrypts other cryptographic keys

Mail Server
A server that forwards e-mail to other e-mail servers using SMTP

Manager
A TOE component that provides the TSF data encryption key generation used by the TOE, storage of the TOE security audit history, and notification service

Management access
An administrator's attempt to access using HTTPS, SSH, TLS, IPSec, etc. for the purpose of TOE management

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

MPowerCrypto V2.5
Verified cryptographic module installed in TOE components (management tool, manager, and

agent) and responsible for cryptographic operation

MPowerPlus

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.

NTP Server

Time sync server via network protocol

Object

A passive entity within the TOE that is subject to operations and contains or receives information.

Operation(on a component of the CC)

Modifying or iterating a component. Operations allowed for components include assignment, repetition, refinement, and selection.

Operation(on a subject)

A specific action performed by a subject on an object

Oracle

Abbreviation for RDBMS Oracle database made by a leading American software company founded by Larry Ellison in 1977.

Oracle linux

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

Organizational Security Policies

A set of security rules, procedures, practices, and guidelines currently imposed and/or believed to be imposed in the operational environment by a real or imaginary organization.

PostgreSQL

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

PP(Protection Profile)

Implementation-independent security requirements specification suitable for TOE type

Private Authentication Key

A private key used in an authentication mechanism of an authentication protocol or public key algorithm that authenticates the identity of a sender in an authenticated communication session.

Private Key Transport Key

The private key used to decrypt the encryption key encrypted with the public key transmission key. The key transmission key is mainly used to set the encryption key or other key materials.

Private Key
It is used with an asymmetric cryptographic algorithm, and the cryptographic key that is uniquely associated with one entity (the subject using the private key), must not be disclosed.

Public Authentication Key
A public key used in an authentication mechanism of an authentication protocol or public key algorithm that authenticates the identity of a sender in an authenticated communication session.

Public Key(asymmetric) cryptographic algorithm
Cryptographic algorithms using public and private key pairs

Public Key Transport Key
A public key used to encrypt a cryptographic key using a public key algorithm, and a key transmission key are mainly used to establish cryptographic keys or other key materials.

Public Key
An encryption key that is used with an asymmetric encryption algorithm and is uniquely associated with one entity (subject using the public key). Disclosure is possible

RBG(Random number generator)
A device or algorithm that outputs a statistically independent and unbiased binary sequence. Random number generators used for cryptographic applications usually generate bit strings of 0s and 1s, which can be combined into blocks of random numbers.
Random number generators are classified into deterministic and nondeterministic methods. A deterministic random number generator consists of an algorithm that generates a string of bits from an initial value called a seed key, while a non-deterministic random number generator generates an output that depends on an unpredictable physical source.

Refinement
To specify by adding details to a component

Role
A set of predefined rules that establish allowed interactions between users and the TOE.

security Administrator
An administrator who can execute functions according to SFRs (Security Functional Requirements) provided by the TOE

Security attribute
Characteristics of subjects, users (including external IT products), objects, information, sessions and/or resources used to define SFRs, the values of which are used to perform SFRs.

Secret Key
A cryptographic key that is used in conjunction with a secret key cryptographic algorithm and is

uniquely associated with one or more entities; must not be disclosed.

Selection

specifying one or more items from a list described in a component

Self-test

Pre-operational and conditional tests executed by the cryptographic module

SFP(Security Functino Policy)

A set of rules that describe specific security actions performed by the TOE Security Functionality (TSF) and can be expressed as Security Functional Requirements (SFRs)

ST(Security Target)

Implementation-dependent security requirements specification suitable for a specific TOE

Symmetric Authentication Key

A symmetric key used in symmetric key algorithms that provides origin authentication and protects the integrity of communication sessions or information.

Symmetric cryptographic technique

An encryption technique that uses the same secret key in both encryption and decryption modes, also called secret key cryptography

Symmetric Data Encryption Key

A symmetric key used in a symmetric key algorithm that provides confidentiality protection for information.

Subject

An active entity within the TOE that performs operations on objects.

User Data

Data for users that do not affect TSF (TOE Security Functionality)

Threat Agent

Unauthorized external entities that pose threats such as illegal access, alteration, or deletion of assets

TOE(Target of Evaluation)

A set of software, firmware and/or hardware accompanied by possible documentation

TSF(TOE Security Functionality)

A set consisting of all hardware, software, and firmware of the TOE that contribute to the correct execution of SFRs (Security Functional Requirements)

TSF Data

Data generated by and for the TOE that may affect the operation of the TOE

Ubuntu

It is a computer operating system developed and distributed by British company Canonical. It is developed as a fork of Debian Linux, and is a Linux distribution that focuses on ease of use compared to Debian.

Windows 10

A computer operating system developed by Microsoft.

1.7. ST organization

Chapter 1 introduces the Security Target and provides reference to the Security Target and TOE overview information.

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 supported by the operational environment so that the TOE security functionality can be accurately provided.

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

In this Security Target, the following evaluation criteria were complied with.

classification		contents
CC		Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 · 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, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1,FPT_PST.1, FTA_SSL.5
	Part 3 Security assurance components	Conformant
	Package	Augmented: EAL1 augmented (ATE_FUN.1)

[table 9] Security Target Common Criteria Conformance

2.2. PP conformance claim

This security target complies with the protection profile as follows.

classification	contents
title	Korean National Protection Profile for Database Encryption
version	1.1
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Issue Date	2019.12.11
Evaluation Criteria Version	CC V3.1 r5
Certification Number	KECS-PP-0820a-2017
conformance	strict PP conformance

[table 10] Security Target Common Criteria Conformance

This Security Targe complied with the “Korean National Protection Profile for Database Encryption V1.1(2019.12.11.)”

2.3. Package conformance claim

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

2.4. Conformance claim rationale

This security target accepts the TOE type, security problem definition, security objective and security requirements of the protection profile equally and adheres to and adheres to the experienced 'National Database Encryption Profile V1.1'.

Classifi-cation	ST	PP	rationale
TOE Type	Database Encryption	Accept PP	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017)
Security objectives for the operational environment	OE.PHYSICAL_CONTROL	Accept PP	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017)
	OE.TRUSTED_ADMIN		
	OE.SECURE_DEVELOPMENT		
	OE.LOG_BACKUP		
	OE.OPERATION_SYSTEM_REINFORCEMENT		
	OE.TIMESTAMP	OE.TIME_STAMP	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017) - OE added according to precautions for application of FAU_STG.1, which is a PP selection SFR
	OE.SECURE DBMS	OE.SECURE DBMS	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017) - OE added according to the application notes of FPT_STM.1, which is a PP selection SFR
Security requirements	FAU_ARP.1	FAU_ARP.1	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017)
	FAU_GEN.1	FAU_GEN.1	
	FAU_SAA.1	FAU_SAA.1	
	FAU_SAR.1	FAU_SAR.1	
	FAU_SAR.3	FAU_SAR.3	
	FAU_STG.3	FAU_STG.3	
	FAU_STG.4(1)	FAU_STG.4	
	FAU_STG.4(2)	FAU_STG.4	
	FCS_CKM.1(1)	FCS_CKM.1(1)	
	FCS_CKM.1(2)	FCS_CKM.1(2)	
	FCS_CKM.2	FCS_CKM.2	
	FCS_CKM.4	FCS_CKM.4	
	FCS_COP.1(1)	FCS_COP.1(1)	
	FCS_COP.1(2)	FCS_COP.1(2)	
	FCS_RBG.1(Extended)	FCS_RBG.1(Extended)	
	FDP_UDE.1(Extended)	FDP_UDE.1(Extended)	
	FDP_RIP.1	FDP_RIP.1	
	FIA_AFL.1	FIA_AFL.1	
	FIA_IMA.1(Extended)	FIA_IMA.1(Extended)	
	FIA_SOS.1	FIA_SOS.1	

Classifi-cation	ST	PP	rationale
	FIA_UAU.2	FIA_UAU.1	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017) - Use FIA_UAU.2 in a hierarchical relationship according to the precautions for application of PP FIA_UAU.1
	FIA_UAU.4	FIA_UAU.4	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017)
	FIA_UAU.7	FIA_UAU.7	
	FIA_UID.2	FIA_UID.1	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017) - Use FIA_UID.2 in a hierarchical relationship according to the precautions for application of PP FIA_UID.1
	FMT_MOF.1	FMT_MOF.1	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017)
	FMT_MTD.1	FMT_MTD.1	
	FMT_PWD.1(Extended)	FMT_PWD.1(Extended)	
	FMT_SMF.1	FMT_SMF.1	
	FMT_SMR.1	FMT_SMR.1	
	FPT_TST.1	FPT_TST.1	
	FPT_ITT.1	FPT_ITT.1	
	FPT_PST.1(Extended)	FPT_PST.1(Extended)	
	FTA_MCS.2	FTA_MCS.2	
	FTA_SSL.5(Extended)	FTA_SSL.5(Extended)	
	FTA_TSE.1	FTA_TSE.1	
Security assurance requirements	ASE_INT.1	ASE_INT.1	· Equivalent to national database encryption PP V1.1(KECS-PP-0820a-2017)
	ASE_CCL.1	ASE_CCL.1	
	ASE_OBJ.1	ASE_OBJ.1	
	ASE_ECD.1	ASE_ECD.1	
	ASE_REQ.1	ASE_REQ.1	
	ASE_TSS.1	ASE_TSS.1	
	ADV_FSP.1	ADV_FSP.1	
	AGD_OPE.1	AGD_OPE.1	
	AGD_PRE.1	AGD_PRE.1	
	ALC_CMC.1	ALC_CMC.1	
	ALC_CMS.1	ALC_CMS.1	
	ATE_FUN.1	ATE_FUN.1	
	ATE_IND.1	ATE_IND.1	
	AVA_VAN.1	AVA_VAN.1	

[table 11] Conformance claim rationale

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

Security objectives for the operating environment are resolved or counteracted by threats, assumptions, and organizational security policies. The security objectives for the operating environment are described below.

Organizational Security Policy	Contents
OE.PHYSICAL_CONTROL	· 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	· 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	· 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	· 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	· 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	· The TOE shall accurately record security-related events using the reliable timestamp provided by the TOE operating environment.
OE.SECURE DBMS	· Since the DBMS interacting with the TOE stores the audit records, it must be protected from unauthorized deletion and modification of the stored audit records.

[table 12] Identification of security objectives for the operating environment

4. Extended components definition

The extended components added in this ST are as follows.

security function class	security function component	
	identification No.	Security function component name
Cryptographic support	FCS_RBG.1	·Random number Generation
Identification and authentication	FIA_IMA.1	·TOE Internal mutual authentication
User data protection	FDP_UDE.1	·User data encryption
Security Management	FMT_PWD.1	·ID and password
Protection of the TSF	FPT_PST.1	·Protection of stored TSF data
TOE Access	FTA_SSL.5	·Session locking and termination

[table 13] List of TOE Security Functional Requirements Extension Component

4.1. Cryptographic support

4.1.1. Random number Generation

Family Behaviour	This family defines requirements for the TSF to provide the capability that generates Random numbers required for TOE cryptographic operation.
Component leveling	FCS_RBG Random number Generation - 1 FCS_RBG.1 Random number generation, requires TSF to provide the capability that generates Random numbers 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 number generation** Hierarchical to No other components. Dependencies No dependencies.
FCS_RBG.1.1	The TSF shall generate Random numbers required to generate an cryptographic key using the specified Random number generator that meets the following [assignment: list of standards].

4.2. Identification and authentication

4.2.1. TOE Internal mutual authentication

Family Behaviour	This family defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.
Component leveling	FIA_IMA TOE Internal mutual authentication - 1 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 b) Minimal: Modification of authentication protocol

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 Behaviour	This family provides requirements to ensure confidentiality of user data.
Component leveling	FDP_UDE User data encryption - 1 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	**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	FMT_PWD ID and password - 1 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	**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 Behaviour	This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.
Component leveling	FPT_PST Protection of stored TSF data - 1 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].

4.6. TOE Access

4.6.1. Session locking and termination

Family Behaviour	This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.
Component leveling	- 1 - 2 FTA_SSL Session locking and termination - 3 - 4 - 5

In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending one additional component as follows.

※ The relevant description for four components contained in CC Part 2 is omitted.

FTA_SSL.5 The management of TSF-initiated sessions, provides requirements that the TSF locks or terminates the session after a specified time interval of user inactivity.

Management FTA_SSL.5

The following actions could be considered for the management functions in FMT:

a) Specification for the time interval of user inactivity that is occurred the session locking and termination for each user

b) Specification for the time interval of default user inactivity that is occurred the session locking and termination

Audit FTA_SSL.5

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive session

FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to No other components.

Dependencies [FIA_UAU.1 authentication or No dependencies.]

FTA_SSL.5.1 The TSF shall [selection:

• lock the session and re-authenticate the user before unlocking the session,

• terminate] an interactive session after a [assignment: time interval of user inactivity].

5. Security requirements

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

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

In addition, the security functional requirements are classified into mandatory SFRs and optional SFRs, as follows.

Mandatory SFRs(M-SFRs): are required to be mandatorily implemented in the Database Encryption

Optional SFRs: are not required to be mandatorily implemented in database encryption.

However, when the TOE additionally provides related capabilities, the ST author must include the corresponding SFRs.

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

Security functional class	Security functional component		note
	identification No.	Security functional component name	
FAU	FAU_ARP.1	·Security alarms	M-SFRs
	FAU_GEN.1	·Audit data generation	M-SFRs
	FAU_SAA.1	·Potential violation analysis	M-SFRs
	FAU_SAR.1	·Audit review	M-SFRs
	FAU_SAR.3	·Selectable audit review	M-SFRs
	FAU_STG.3	·Action in case of possible audit data loss	M-SFRs
	FAU_STG.4	·Prevention of audit data loss	M-SFRs
FCS	FCS_CKM.1(1)	·Cryptographic key generation (User data encryption)	M-SFRs
	FCS_CKM.1(2)	·Cryptographic key generation (TSF data encryption)	M-SFRs
	FCS_CKM.2	·Cryptographic key distribution	M-SFRs
	FCS_CKM.4	·Cryptographic key destruction	M-SFRs
	FCS_COP.1(1)	·Cryptographic operation(User data encryption)	M-SFRs
	FCS_COP.1(2)	·Cryptographic operation(TSF data encryption)	M-SFRs
	FCS_RBG.1(Extended)	·Random number generation	M-SFRs
FDP	FDP_UDE.1(Extended)	·User data encryption	M-SFRs
	FDP_RIP.1	·Subset residual information protection	M-SFRs
FIA	FIA_AFL.1	·Authentication failure handling	M-SFRs
	FIA_IMA.1(Extended)	·TOE Internal mutual authentication	M-SFRs
	FIA_SOS.1	·Verification of secrets	M-SFRs
	FIA_UAU.2	·User authentication before any action	M-SFRs
	FIA_UAU.4	·Single-use authentication mechanisms	M-SFRs
	FIA_UAU.7	·Protected authentication feedback	M-SFRs
	FIA_UID.2	·User identification before any action	M-SFRs

Security functional class	Security functional component		note
	identification No.	Security functional component name	
FMT	FMT_MOF.1	·Management of security functions behaviour	M-SFRs
	FMT_MTD.1	·Management of TSF data	M-SFRs
	FMT_PWD.1(Extended)	·Management of ID and password	M-SFRs
	FMT_SMF.1	·Specification of management functions	M-SFRs
	FMT_SMR.1	·Security roles	M-SFRs
FPT	FPT_ITT.1	·Basic internal TSF data transfer protection	M-SFRs
	FPT_PST.1(Extended)	·Basic protection of stored TSF data	M-SFRs
	FPT_TST.1	·TSF testing	M-SFRs
FTA	FTA_MCS.2	·Per user attribute limitation on multiple concurrent sessions	M-SFRs
	FTA_SSL.5(Extended)	·Management of TSF-initiated sessions	M-SFRs
	FTA_TSE.1	·TOE session establishment	M-SFRs

[table 14] List of TOE Security Functional Requirements

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 15] 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 history 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 15] 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 16]** auditable events, [*[table 17] 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 15]** auditable events, [*no other components*]].

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 the activity	

Security functional component	Auditable event	Additional audit record
FCS_CKM.2	·Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	
FCS_CKM.4	·Success and failure of the activity (only applying to destruction of key related to user data encryption/decryption)	
FCS_COP.1(1)	·Success and failure of the activity	
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 Modify of authentication protocol	
FIA_UAU.2	·All use of the authentication mechanism	
FIA_UAU.4	·Attempts 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	Modified values of TSF data
FMT_PWD.1	·All changes of the password	
FMT_SMF.1	·Use of the management functions	
FMT_SMR.1	·Modifications to the user group of rules divided	
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	·Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5	·Locking or termination of interactive session	
FTA_TSE.1	·Denial of a session establishment due to the session establishment mechanism ·All attempts at establishment of a user session	

[table 16] auditable events

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

[table 17] 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 [authentication failure audit event among auditable events of [**FIA_UAU.2** certification failure audit event, integrity violation audit event among audit target events of FPT_TST.1 and self-test failure case of verified cryptographic modules, audit history storage overflow of FAU_STG.3, audit of FAU_STG.4 History store saturation, process abnormal termination] known to indicate a potential security violation
b) [assignment: *any other rules*]

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 18] Audit data retrieval criteria and ordering methods] of audit data based on [[table 18] Audit data retrieval criteria and ordering methods]

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

[table 18] Audit data retrieval criteria and ordering methods

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 cryptographic keys in accordance with a specified cryptographic key generation algorithm [[table 20] User data cipher key generation method and type] and specified cryptographic key sizes [[table 20] User data cipher key generation method and type] that meet the following: [[table 19] User Data cipher key Reference Standards].

classification	Algorithm	description	Standards
Random number generator	ARIA_CTR_DRBG[1)]	|K|=128	TTAK.KO-12.0189/R1:2015 ISO/IEC 18031:2011

[table 19] User Data cipher key Reference Standards

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

[table 20] User data cipher key generation method and type

1) Block cipher based Random number generator

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 22] TSF data cipher key generation method and type] and specified cryptographic key sizes [[table 22] TSF data cipher key generation method and type] that meet the following: [[table 21] 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-Part2
Random number generator	ARIA_CTR_DRBG	|K|=128	TTAK.KO-12.0189/R1:2015 ISO/IEC 18031:2011

[table 21] TSF Data cipher key Generation Reference Standards

classification		Cryptographic key generation algorithm	cryptographic algorithm	cryptographic Key Size	note
key for encryption	password derivation	SHA-256_HMAC_PBKDF2	ARIA	|K|=256	
	Random number generator	ARIA_CTR_DRBG	ARIA	|K|=128	
TSF data cipher key		ARIA_CTR_DRBG	ARIA	|K|=128,192,256	
			SEED	|K|=128	
private key transfer key		ARIA_CTR_DRBG	RSAES	|P|=2048 hash=SHA-256	
public key transfer key					
private authentication key		ARIA_CTR_DRBG	RSA-PSS	|P|=2048, hash=SHA-256	
public authentication key					
symmetric cipher key		ARIA_CTR_DRBG	ARIA	|K|=128	
Symmetric authentication key		ARIA_CTR_DRBG	HMAC	HMAC-256	

[table 22] 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 23] cipher key distribution method and type] that meets the following: [[table 23] Cryptographic key distribution algorithm and reference standards].

classification	Algorithm	description	Standards
public key encryption algorithm	RSAES	|P|=2048	KS X ISO/IEC 18033-2:2077
block cipher algorithm	ARIA	|K|=128	KS X 1213-2:2014

[table 23] Cryptographic key distribution algorithm and reference standards

classification	usage	cryptographic algorithm	distribution method
symmetric cipher key	For encrypted communication between components	RSAES	· In the management tool (agent), the Symmetric Cipher Key and the symmetric authentication key are encrypted using the public key encryption algorithm and transmitted to the manager
Symmetric authentication key	For verifying integrity between components		
user data cipher key	For user data encryption/decryption	ARIA	· After encrypting the user data encryption key using the Symmetric Cipher Key and block encryption algorithm transmitted to the manager, the agent is transmitted.

[table 24] 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 [None] that meets the following: [[table 24] Cryptographic key destruction algorithm and reference standard].

classification		Cryptographic key storage[2)]	Destruction method	Detailed method of destruction	Destruction point
key for encryption	password derivation	memory	memory zeroing	Overwrite all key memory areas with 0x00	After decryption of the key for encryption of the key for the random number generator
	Random number generator	file	delete	Delete file after overwriting file contents with 0x00	When calling the encryption key destruction interface
User data cipher key		DB	delete	Execute the SQL statement to overwrite the information stored in the DB with 0x00 and then delete it.	When calling the encryption key destruction interface
TSF data cipher key		DB	delete		
private key transfer key		DB	delete		
public key transfer key		DB	delete		
		file	delete	Delete file after overwriting file contents with 0x00	
private authentication key		DB	delete	Execute the SQL statement to overwrite the information stored in the DB with 0x00 and then delete it.	When calling the encryption key destruction interface
		file	delete	Delete file after overwriting file contents with 0x00	
public authentication key		DB	delete	Execute the SQL statement to overwrite the information stored in the DB with 0x00 and then delete it.	
		file	delete	Delete file after overwriting file contents with 0x00	
symmetric cipher key		memory	memory zeroing	Overwrite all key memory areas with 0x00	At the end of communication
Symmetric authentication key		memory	memory zeroing	Overwrite all key memory areas with 0x00	At the end of communication

[table 25] cipher key destruction method and type

2) Encryption keys (key encryption key for random number generator, etc.) stored in files and DBs are loaded into memory when used, and memory zeroing is performed by overwriting all key memory areas with 0x00 after use.

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 [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [[table 27] List of User Data Cryptographic Operations] and cryptographic key sizes [[table 27] List of User Data Cryptographic Operations] that meet the following: [[table 26] Cryptographic Operation (User Data Encryption) Algorithms and Reference Standards].

Classification	cryptographic algorithm	Standards
block cipher algorithm	ARIA	KS X 1213-2:2014
	SEED	TTAS.KO-12.0004/R1:2005
hash algorithm	SHA-256	KS X ISO/IEC 10118-3:2066

[table 26] 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 27] 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 [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [[table 29] List of TSF Data Cryptographic Operations] and cryptographic key sizes [[table 29] List of TSF Data Cryptographic Operations] that meet the following: [[table 28] Cryptographic operation (TSF data encryption) algorithm and reference standards].

Classification	cryptographic algorithm	Standards
block cipher algorithm	ARIA	KS X 1213-2:2014
	SEED	TTAS.KO-12.0004/R1:2005
hash algorithm	SHA	KS X ISO/IEC 10118-3:2066
public key cryptography	RSAES	KS X ISO/IEC 18033-2:2077
digital signature	RSA-PSS	ISO/IEC 14888-2:2008
message digest	HMAC	KS X ISO/IEC 9797-2:2008

[table 28] Cryptographic operation (TSF data encryption) algorithm and reference standards

Classification	cryptographic algorithm		contents		Operation Mode	note
TSF Data	block cipher	ARIA,	Key Size	|K|=128,192,256	approved mode	
			Mode	CBC		
		SEED	Key Size	|K|=128		
			Mode	CBC		
	hash	SHA	SHA-256			
	public key cryptography	RSAES	|P|=2048, hash=SHA-256			
	digital signature	RSA-PSS	|P|=2048, hash=SHA-256			
	message digest	HMAC	HMAC-256			

[table 29] List of TSF Data Cryptographic Operations

FCS_RBG.1 Random number generation (Extended)

Hierarchical to No other components.

Dependencies No dependencie

FCS_RBG.1.1 The TSF shall generate Random numbers required to generate an cryptographic key using the specified Random number generator that meets the following [[table 30] Random number Generation Algorithms and Reference Standards].

classification	Algorithm		description	Standards
Random number generator	block cipher	ARIA_CTR_DRBG	|K|=128	TTAK.KO-12.0189/R1:2015

[table 30] 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, [none]].

FDP_RIP.1 Subset residual information protection

Hierarchical to No other components.

Dependencies No dependencie

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].

구분	작업	내용
1	change memory value	Replace the information stored in the memory with a meaningless value (0x00) (Example: Arrays.fill([variable name], 0x00))
2	memory return	Release memory reference address (e.g. [variable name] = null) Perform memory return operation when performing GC in Java later

[table 31] How to recover partial residual information

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 [[table 31] password Generation Rules].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [Send mail to authorized administrator, generate audit history, Terminate the process, Block login (10 minutes)].

FIA_IMA.1 TOE Internal mutual authentication (Extended)

Hierarchical to No other components.

Dependencies No dependencie

FIA_IMA.1.1 The TSF shall perform mutual authentication using [None] in accordance with [Self-Implemented Authentication Protocol] between [Management tool and Manager, Agent and Manager].

FIA_SOS.1 Verification of secrets

Hierarchical to No other components.

Dependencies No dependencie

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [[table 32] secrets Information Generation Rules]].

Classification	Generation Rules
Password Generation Rules	· Length: 9 to 30 characters · Allowed characters: English, special characters, numbers · Combination rules: At least one English letter, special character, and number must be included

[table 32] 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 authorized administrator to be successfully authenticated before allowing any other TSF mediated actions on behalf of that **authorized administrator**

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components.

Dependencies No dependencie

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [Symmetric cryptographic key generated by a random number generator]

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 dependencie

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

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 33] List of security functions] to [Security Manager].

security function	Contents	Management action			
		determine the behavior	disable	enable	modify the behaviour
Password Management	· Create/change password for administrator/ CipherKey	0	-	-	-
Configuration file management	· Creating necessary configuration files when running the Manager/Agent · Create integrity file for configuration file	0	-	-	-
login management	· Security manager login/logout	0	-	-	-
cipher key management	· Create/inquire/discard cipher key	0	-	-	-
Audit history inquiry	· Audit history information inquiry	0	-	-	-
Help	· TOE components integrity check	0	-	-	-

[table 33] 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 34] TSF data list] to [[table 34] Authorized Roles].

TSF data			contents	management			
				create	inquiry	modify	delete
authentication information	ID for administrator		· authentication information for Authorized Administrator	-	-	0	-
	Password for administrator						
password for cipher key			· Password-derived cipher key generation information	-	-	0	-
Random number generator based		cipher key	· Random number generator based cipher Key	-	-	-	0
user data			· user data cipherkey	0	0	0	0
TSF data			· TSF data cipherkey	0	0	0	0
private key transfer key			· private key for key distribution	0	0	0	0
public key transfer key			· public key for key distribution	0	0	0	0
private authentication			· private key for mutual authentication	0	0	0	0

TSF data			contents	management			
				create	inquiry	modify	delete
key							
public authentication key			· public key for mutual authentication	0	0	0	0
Audit history information			· Audit history information generated by the TOE	-	0	-	-
Configuration information	DB account ID/password		· Connection information to DBMS where audit history information is stored	-	-	-	-
	IP	Management tool	· Management tool IP for access control	-	0	0	-
		Agent	· Admin IP for access control	-	0	0	-
	admin email address		· Admin email address for sending mail	0	0	0	-
	mail server address		· mail server address for sending mail	0	0	0	-
	mail server account		· mail server account for sending mail	0	0	0	-
	mail server password		· mail server password for sending mail	0	0	0	-
	Whether to use authentication		· Whether to use mail server authentication for sending mail	0	0	0	-
	Whether to use encryption		· Whether to use mail server encryption for sending mail	0	0	0	-

[table 34] 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 [None].

1. [None]
2. [None]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [None] to [None].

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 dependencie

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 dependencie

FPT_ITT.1.1 The TSF shall protect the TSF data from *disclosure, modification* by **verifying encryption and message integrity** when the TSF data is transmitted among TOE's separated parts.

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

Hierarchical to No other components.

Dependencies No dependencie

FPT_PST.1.1 The TSF shall protect [[table 35] Stored TSF Data Protection Policy] stored in containers controlled by the TSF from the unauthorized *disclosure, modification.*

classification	contents	type	location
Credentials for Administrators	· ID/Password	cipher text	DB
Cipher key information	· Symmetric key, asymmetric key (private key)	cipher text	DB/File
Configuration Info	· TOE operation information	cipher text	DB
DB account information	· ID/Password	cipher text	File

[table 35] Stored TSF Data Protection Policy

FPT_TST.1 TSF testing

Hierarchical to No other components.

Dependencies No dependencie

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

FPT_TST.1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [*Audit history, environment setting information*].

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

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 **administrator** according to the rules for the list of management functions defined in FMT_SMF1.1]

a) limit the maximum number of concurrent sessions to 1 for management access by the same administrator who has the right to perform FMT_MOF.1.1 "Management actions" and FMT_MTD.1.1 "Management."

b) limit the maximum number of concurrent sessions to {None} for management access by the same administrator who doesn't have the right to perform FMT_MOF.1.1 "Management actions" but has the right to perform a query in FMT_MTD.1.1 "Management" only

c) [None]

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

FTA_SSL.5 Management of TSF-initiated sessions(Extended)

Hierarchical to No other components.

Dependencies FIA_UAU.1 authentication or No dependencies.

FTA_SSL.5.1 The TSF shall [

• *terminate*] the administrator's interactive session after a [*10 time interval of the administrator inactivity*]

FTA_TSE.1 TOE session establishment

Hierarchical to No other components.

Dependencies No dependencie

FTA_SSL.3.1 The TSF shall be able to refuse the **management access session of the administrator**, 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

[table 36] TOE Assurance Requirements List

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 proble m 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_CCL.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 com ponents.

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.2.1E 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.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E 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 th e 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), t heir 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 Lavelling 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.	Security functional requirements	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	23 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	27
		FMT_SMR.1	28
25	FMT_MTD.1	FMT_SMF.1	27
		FMT_SMR.1	28
26	FMT_PWD.1	FMT_SMF.1	27
		FMT_SMR.1	28
27	FMT_SMF.1	-	-
28	FMT_SMR.1	FIA_UID.1	23

No.	Security functional requirements	Dependency	Reference No.
			Rationale(4)
29	FPT_ITT.1	-	-
30	FPT_PST.1	-	-
31	FPT_TST.1	-	-
32	FTA_MCS.2	FIA_UID.1	23 Rationale(4)
33	FTA_SSL.5	FIA_UAU.1	20 Rationale(3)
34	FTA_TSE.1	-	-

[table 37] TOE Security Functional Requirements List

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, and FTA_SSL.5 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 PP 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). The security functional requirements are summarized in the following table.

Security functional class	Security functional component		note
	SFR	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 number 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_TST.1	·TSF testing	
FTA	FTA_MCS.2	·Per user attribute limitation on multiple concurrent sessions	
	FTA_SSL.5(Extended)	·Management of TSF-initiated sessions	
	FTA_TSE.1	·TOE session establishment	

[table 38] Security functional requirements

8.1. Security audit(FAU)

The security function components included in the security audit applied to the TOE are as follows.

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). The functional components are summarized as follows.

classification	audit event	security function components
Security Alert Information	· Admin login failed 3 times · Integrity failure · Audit history storage saturation · Failed self-test of cryptographic module · Abnormal termination of process	FAU_ARP.1 FIA_AFL.1 FAU_SAA.1 FAU_STG.3 FAU_STG.4
Login information	· Authorized administrator login/logout information	FIA_UID.1
authentication information	· Any use of the authentication mechanism · About attempts to reuse authentication data	FIA_UAU.1 FIA-UAU.4
Mutual authentication information	· Mutual authentication success/failure information · Change of authentication protocol	FIA_IMA.1
Session information	· About Session Termination on Timeout · Concurrent Sessions Exceeded Information · About Changing User Session Settings	FTA_SSL.5 FTA_MCS.2 FTA_TSE.1
cipher key information	· cipher key generation success/failure information · cipher key distribution success/failure information · cipher key destruction success/failure information	FCS_CKM.1(1) FCS_CKM.2 FCS_CKM.4
Cryptographic information	· Cryptographic operation success/failure information	FCS_COP.1(1)
User data information	· User data encryption/decryption success/failure information	FDP_UDE.1
TSF Self Test Information	· Integrity check pass/fail information (changed TSF value) · Validated cryptographic module self-test success/failure information · Abnormal termination of process	FPT_TST.1
Storage Check Information	· When the storage threshold 80%/90% is exceeded	FAU_STG.3 FAU_STG.4
Security Management Information	· TSF function change information · TSF data value change information (changed TSF value) · Password change information · Management function usage information · Changes to user groups that share roles	FMT_MOF.1 FMT_MTD.1 FMT_PWD.1 FMT_SMF.1 FMT_SMR.1
Audit function	· Audit function start/stop information	

classification	audit event	security function components
information		
Timestamp information	· Timestamp information for time change confirmation	

[table 39] audited event

※ 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 breaches 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)

When the TOE is running, it uses the cryptographic algorithm to be verified in the verified cryptographic module that is executed in verification mode, generates and distributes cryptographic keys, performs cryptographic operations, and performs the destruction of cryptographic keys by initializing them to "0". The verified cryptographic module information installed and operated in the TOE is as follows.

Classification	Contents
cryptographic module name	MPowerCrypto V2.5
Verification number	CM-154-2024.9
verification level	VSL1
developer	UbimInfo Co.,Ltd.
verification date	2019-09-03
expiration date	2024-09-03

[table 40] verified cryptographic module information

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 verified cryptographic module installed in the TOE and executed in verification mode. The table below shows the generation method.

classification		generation algorithm	algorithm	cipher key size	standards
User data cipher key		ARIA_CTR_DRBG	ARIA	|K|=128, 192, 256	TTAK.KO-12.0189/R1:2015 ISO/IEC 18031:2011
			SEED	|K|=128	
KEK	password derivation	SHA-256_HMAC_PBKDF2	ARIA	|K|=256 salt : 16byte iteration : 2048	TTAK.KO-12.0334-Part2
	Random number generator	ARIA_CTR_DRBG	ARIA	|K|=128	TTAK.KO-12.0189/R1:2015 ISO/IEC 18031:2011
TSF data cipher key		ARIA_CTR_DRBG	ARIA	|K|=128,192,256	
			SEED	|K|=128	
private key transfer key		ARIA_CTR_DRBG	RSAES	|P|=2048 hash=SHA-256	TTAK.KO-12.0189/R1:2015 ISO/IEC 18031:2011
public key transfer key					
private authentication key		ARIA_CTR_DRBG	RSA-PSS	|P|=2048 hash=SHA-256	
public authentication key					
symmetric cipher key		ARIA_CTR_DRBG	ARIA	|K|=128	TTAK.KO-12.0189/R1:2015 ISO/IEC 18031:2011
symmetric authentication key		ARIA_CTR_DRBG	HMAC	|K|=128	

[table 41] TSF data encryption key generation method and type

※ SFR Mapping

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

8.2.2. Cipher key Distribution

The TOE distributes cryptographic keys using public key cryptographic algorithms and block cryptographic algorithms, which are cryptographic algorithms subject to verification of verified cryptographic modules loaded in the TOE and executed in verification mode, for cryptographic communication between TOE components, and cryptographic key types and distribution. The method is tabulated as follows.

classification	usage	algorithm	distribution method	standards
symmetric cipher key	For cipher communication between components	RSAES	· In the management tool (agent), the Symmetric Cipher Key and the symmetric authentication key are encrypted using the public key encryption algorithm and transmitted to the manager	KS X ISO/IEC 18033-2:2017
symmetric authentication key	For verifying integrity between components			
User data cipher key	For user data encryption/decryption	ARIA	· After encrypting the user data encryption key using the Symmetric Cipher Key and block encryption algorithm transmitted to the manager, the agent is transmitted.	KS X 1213-2:2014

[table 42] Cryptographic key types and distribution methods

※ SFR Mapping

FCS_CKM.2

8.2.3. Cipher key Destruction

The TOE performs destruction by initializing the cryptographic key that has been used in the TOE to “0”. The table below shows the cryptographic key types and destruction methods.

classification		Cryptographic key storage	Destruction method	Detailed method of destruction	point of destruction
KEK	password derivation	Memory	memory zeroing	· Overwrite all memory areas with 0x00	After decryption of key for encryption of key for random number generator
	Random number generator	File	deleting	· Delete file after overwriting file contents with 0x00	When calling the encryption key destruction interface
User data cipher key		DB	deleting	· Execute the SQL statement to overwrite the information stored in the DB with 0x00 and then delete it.	When calling the encryption key destruction interface
TSF data cipher key		DB	deleting		
private key transfer key		DB	deleting		
public key transfer key		File	deleting	· Delete file after overwriting file contents with 0x00	
private authentication		DB	deleting	· Execute the SQL statement to	

classification	Cryptographic key storage	Destruction method	Detailed method of destruction	point of destruction
key			overwrite the information stored in the DB with 0x00 and then delete it.	
	File	deleting	· Delete file after overwriting file contents with 0x00	
public authentication key	DB	deleting	· Execute the SQL statement to overwrite the information stored in the DB with 0x00 and then delete it.	
	File	deleting	· Delete file after overwriting file contents with 0x00	
symmetric cipher key	Memory	memory zeroing	· Overwrite all memory areas with 0x00	At the end of communication
symmetric authentication key	Memory	memory zeroing	· Overwrite all memory areas with 0x00	At the end of communication

[table 43] Cryptographic Key Types and Destruction Methods

※ SFR Mapping

FCS_CKM.4

8.2.4. Cryptographic operation

The TOE performs cryptographic calculations using block ciphers, hashes, public key cryptography, digital signatures, and message authentication algorithms, which are the cryptographic algorithms subject to verification of the verified cryptographic modules loaded in the TOE and executed in verification mode. Here is a tabular list of operations:

classification	Algorithm		description		Standards
User Data	Cipher Block	ARIA	KeySize	|K|=128,192,256	KS X 1213-2:2014
			Mode	CBC	
		SEED	KeySize	|K|=128	TTAS.KO-12.0004/R1:2005
			Mode	CBC	
	Hash	SHA	SHA-256		KS X ISO/IEC 10118-3_2001:2018
TSF Data	Cipher Block	ARIA	KeySize	|K|=128,192,256	KS X 1213-2:2014
			Mode	CBC	
		SEED	KeySize	|K|=128	TTAS.KO-12.0004/R1:2005
			Mode	CBC	
	Hash	SHA	SHA-256		KS X ISO/IEC 10118-3_2001:2018
	public key cryptography	RSAES	|P|=2048, hash=SHA-256		KS X ISO/IEC 18033-2:2017
	digital signature	RSA-PSS	|P|=2048, hash=SHA-256		ISO/IEC 14888-2:2008
	message authentication	HMAC	HMAC-256		KS X ISO/IEC 9797-2:2008

[table 44] list of cryptographic operations

※ SFR Mapping

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

8.2.5. random number generation

The TOE generates random numbers necessary for cryptographic key generation using a random number generator, which is the cryptographic algorithm subject to verification of the verified cryptographic module installed in the TOE and executed in verification mode. The table below shows the random number generation method.

classification	Algorithm		description	Standards
Random number generator	block cipher based	ARIA_CTR_DRBG	|K|=128	TTAK.KO-12.0189/R1:2015

[table 45] Random number generator Algorithms and Reference Standards

※ SFR Mapping

FCS_RBG.1(Extended)

8.3. Cryptographic support(FCS)

The TOE provides a column-level encryption/decryption function for data stored in the DBMS to be protected through a verified 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	· Enc([plaintext (random number generated by the random number generator provided by the random number verified cryptographic module + 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	· Dec([ciphertext]) = [plaintext(random number + user data)] · Remove random numbers from plain text
	Encryption	one-way	SHA-256	· Generating cipher text using hash algorithm (SHA-256)

[table 46] 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 administrator must register the account (ID and password) and allowed IP so that he can create his/her own information when installing the manager.

The management tool masks (*) the password entered by the security manager so that it cannot be recognized on the screen when performing identification and authentication of the security manager. If authentication fails, only the authentication failure message "Login failed" is provided. If the authentication attempt fails continuously for the defined number of times (3 times), the manager blocks access attempts to the account for 10 minutes (fixed value), saves audit records for authentication failures, and sends a warning mail to the security administrator.

The TOE provides a verification mechanism that satisfies the administrator password generation rule as follows.

- The length is between 9 characters and 30 characters, allowed characters are English, special characters, and numbers, and the combination rule must contain at least one English character, special characters, and numbers.

In addition, the manager provides a function to prevent reuse of authentication data by using a Symmetric Cipher Key generated through a random number generator to ensure the uniqueness of the session used when the security manager accesses through 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 electronic signature verification using the unique value (Unique ID) issued between the management tool and the manager (agent and manager) in real time. The mutual authentication process is as follows.

No.	Sender	Receiver	contents
1	Manager	-	1) Generation of encryption key for each component - KA (pri, pub): Encryption key for manager key distribution (private key, public key) - KB (pri, pub): Digital signature encryption key for manager (private key, public key) - KC (pri, pub): Digital signature encryption key for management tool (private key, public key) - KD (pri, pub): Electronic signature encryption key for agent (private key, public key) 2) Generate Unique ID for each component (using a random number generator)

No.	Sender	Receiver	contents
			- X : Unique ID for manager (32 bytes) - Y: Unique ID for management tool (32 bytes) - Z : Unique ID for agent (32 bytes) 3) Generation of hash value between components (using hash (SHA-256) algorithm) - HashVal1: Hash generation Hash generation (X, Y): Hash value is generated using the hash (SHA-256) algorithm by combining the X string and the Y string (X, Y) - HashVal2: Hash generation (X, Z) 4) Generation of information for each component - B (X, HashVal1, HashVal2): manager information - C(Y, HashVal1): management tool information - D(Z, HashVal2): agent information
2	Security Manager	-	1) Distribution of encryption keys and information by component - Manager: KA(pri), KB(pri), KC(pub), KD(pub), B(X, HashVal1, HashVal2) - Management tools: KA (pub), KB (pub), KC (pri), C (Y, HashVal1) - Agent : KA(pub), KB(pub), KD(pri), D(Z, HashVal2)
3	Management tool	-	1) Create a signature value for UniqueID in the management tool - Signature Value 1: Signature Generation Signature Generation (X, Y): Generate signature value for Y with digital signature private key X using RSA-PSS encryption algorithm (KC(pri), C.Y) 2) Combining data - data : C.Y + signature value 1
4	Management tool	Manager	1) Encrypted Transmission - Generation of 『Symmetric Cipher Key』 through random number generator - Encrypt data with 『Symmetric Cipher Key』 (data : C.Y + signature value 1) - Encrypt 『Symmetric Cryptographic Key』 with KA(pub) using RSAES cryptographic algorithm - Encrypted 『Symmetric Cipher Key』 and data transmission
5	Manager	-	1) Decrypt transmission data - Decrypt 『Symmetric Cryptographic Key』 with KA(pri) using RSAES cryptographic algorithm - Data decryption with 『Symmetric Cipher Key』 (data : C.Y + signature value 1) 2) Management tool UniqueID signature scare - Signature verification Signature verification (X, Y, Z): Perform verification of Y and Z (signature value of Y) with digital signature public key X using RSA-PSS encryption algorithm (KC(pub), C.Y, signature value 1): Mutual authentication fails in case of failure 3) Create hash value - Hash value C: hash generation (B.X, C.Y) 4) Hash Verification - Hash verification (HashVal1, hash value C): Mutual

No.	Sender	Receiver	contents
			authentication fails in case of failure 5) Create signature value for manager Unique ID - Signature value 2: Signature creation (KB(pri), B.X) 6) Combining data - data : B.X + signature value 2 7) Encrypt data with 『Symmetric Cipher Key』 (data : B.X + signature value 2)
6	Manager	Management tool	1) Encrypted data transmission (data : B.X + signature value 2)
7	Management tool	-	1) Decrypt transmission data - Data decryption with 『Symmetric Cipher Key』 (data : B.X + signature value 2) 2) Manager UniqueID signature scare - Signature verification (KB (pub), B.X, signature value 2): mutual authentication fails in case of failure 3) Create hash value - Hash value C: hash generation (B.X, C.Y) 4) Hash Verification - Hash verification (HashVal1, hash value C): Mutual authentication fails in case of failure
8	Management tool	Manager	1) After successful mutual authentication, encryption communication is performed using 『Symmetric Cipher Key』

[table 47] Mutual authentication procedure between TOE components

※ 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 identification and authentication are successfully performed. Only the security manager can access the security management interface through the secure channel. The security functions provided to the security manager are as follows and the ID/password creation rules are as follows.

security function	Contents	Management action			
		determine the behavior	disable	enable	modify the behaviour
Password Management	· Create/change password for administrator/ CipherKey	0	-	-	-
Configuration file management	· Creating necessary configuration files when running the Manager/Agent · Create integrity file for configuration file	0	-	-	-
login management	· Security manager login/logout	0	-	-	-
cipher key management	· Create/inquire/discard cipher key	0	-	-	-
Audit history inquiry	· Audit history information inquiry	0	-	-	-
Help	· TOE components integrity check	0	-	-	-

[table 48] List of security functions

Classification	Generation Rules
ID Generation Rules	· 6 digits or more and 12 digits or less, uppercase letters A to Z
Password Generation Rules	· Length: 9 to 30 characters · Allowed characters: English, special characters, numbers · Combination rules: At least one English letter, special character, and number must be included

[table 49] secrets Information Generation Rules

※ 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. The TSF data that can be managed by the security administrator are as follows.

TSF data			contents	management			
				create	inquiry	modify	delete
authentication information	ID for administrator		· authentication information for Authorized Administrator	-	-	0	-
	Password for administrator						
password for cipher key			· Password-derived cipher key generation information	-	-	0	-
Random number generator based		cipher key	· Random number generator based cipher Key	-	-	-	0
user data			· user data cipherkey	0	0	0	0
TSF data			· TSF data cipherkey	0	0	0	0
private key transfer key			· private key for key distribution	0	0	0	0
public key transfer key			· public key for key distribution	0	0	0	0
private authentication key			· private key for mutual authentication	0	0	0	0
public authentication key			· public key for mutual authentication	0	0	0	0
Audit history information			· Audit history information generated by the TOE	-	0	-	-
Integrity file			· Integrity file information for manager/agent information	-	-	-	-
Configuration information	DB account ID/password		· Connection information to DBMS where audit history information is stored	-	-	-	-
	IP	Management tool	· Management tool IP for access control	-	0	0	-
		Agent	· Admin IP for access control	-	0	0	-
	admin email address		· Admin email address for sending mail	0	0	0	-
	mail server address		· mail server address for sending mail	0	0	0	-
	mail server account		· mail server account for sending mail	0	0	0	-
	mail server password		· mail server password for sending mail	0	0	0	-
	Whether to use authentication		· Whether to use mail server authentication for sending mail	0	0	0	-
	Whether to use encryption		· Whether to use mail server encryption for sending mail	0	0	0	-

[table 50] TSF data list

※ SFR Mapping

FMT_MTD.1, FMT_SMF.1

8.6. Protection of the TSF(FPT)

8.6.1. Internal TSF data transfer protection

The TOE performs encrypted communication for TSF data transmission for the purpose of protecting internal TSF data transmission, and protects communication by using the verified cryptographic module as follows.

No.	Sender	Receiver	contents
1	management tool /agent	-	1) Generate 『Symmetric Cipher Key』 and 『Symmetric Authentication Key』 using a random number generator 2) Generate passphrase and data authentication value - Generates a 『Symmetric Cipher Key』 and a 『Symmetric Authentication Key』 encrypted using 『public transmission key』 and RSAES encryption algorithm - Generates encrypted 『TSF data』 using 『Symmetric Cipher Key』 and ARIA encryption algorithm - Generating message authentication value for TSF data using symmetric authentication key" and HMAC encryption algorithm
2	management tool /agent	Manager	1) Transmission of passphrase and data authentication value - Cipher text (『Symmetric Cipher Key』, 『Symmetric authentication key』, TSF data) - data authentication value
3	Manager	-	1) Transmission data verification - Decryption of 『Symmetric Cipher Key』 and 『Symmetric Authentication Key』 encrypted using RSAES encryption algorithm - Decrypt TSF data encrypted using 『Symmetric Cipher Key』 and ARIA encryption algorithm - Verification of TSF data and message authentication value using 『Symmetric Authentication Key』 and HMAC encryption algorithm - If message verification fails, the communication channel is terminated 2) TSF data result information generation - Generate TSF data result information after performing tasks through TSF data 3) Generate passphrase and data authentication value - Generate encrypted TSF data result information using 『Symmetric Cipher Key』 and ARIA encryption algorithm - Generate message authentication value for TSF data result information using 『Symmetric Authentication Key』 and HMAC encryption algorithm
4	Manager	management tool /agent	1) Transmission of passphrase and data authentication value - Cipher text (TSF data result information) and data authentication value
5	management tool /agent	-	1) Transmission data verification - Decrypt TSF data result information encrypted using 『Symmetric Cipher Key』 and ARIA encryption algorithm - Verification of TSF data result information and message

No.	Sender	Receiver	contents
			authentication value using 『Symmetric Authentication Key』 and HMAC encryption algorithm - If message verification fails, the communication channel is terminated 2) TSF data result information processing
6	management tool /agent /Manager	-	1) Destroy encryption key - Destruction is performed by initializing the memory variables of the 『Symmetric Cipher Key』 and 『Symmetric Authentication Key』 used at the end of communication to 0x00

[table 51] Encrypted communication execution procedure between TOE components

※ SFR Mapping

FPT_ITT.1

8.6.2. Stored TSF data protection

The encryption key protection procedure provided by the TOE is as follows.

○ When generating an encryption key

When the TOE generates an encryption key, it receives the password for the encryption key from the security manager and generates a 『password-derived encryption key』

『Random Number Generator-based Encryption Key』 is generated and stored after being encrypted with 『Password Derived Encryption Key』

『[Other cryptographic keys]』[3]is stored after being encrypted with 『random number generator-based encryption key』 after creation

『Public key transmission key』, 『Public authentication key』 are stored in plain text

○ When operating encryption key

When the TOE starts (login), it receives the password for the encryption key from the security manager and protects the password with its own encoding method.

The TOE loads the 『random number generator-based encryption key』 into the memory in an encrypted state

When the TOE requests encryption/decryption work through [Other Encryption Keys]

- Generate 『Password Derived Encryption Key』 using key derivation algorithm
- Decryption of encrypted 『random number generator cryptographic key』 using 『password derivation cryptographic key』
- Decryption of the encrypted 『[Other Encryption Key]』 using the decrypted 『Random Number Generator Encryption Key』

- Perform encryption operation using the decrypted 『[Other Encryption Key]』
- Destroy the decrypted 『[Other Encryption Key]』 after performing cryptographic operation
- Destruction of the decrypted 『Random Number Generator Encryption Key』
- Destruction of 『Password Derived Encryption Key』

※ In the TOE, the 『Symmetric Encryption Key (Symmetric Authentication Key)』, which exists only in memory, is encrypted with the 『Password Derived Encryption Key』 when generated, loaded into the memory, decrypted only when used, and performs cryptographic calculation. Key

3) Other cryptographic keys represent user data, TSF data, private key transmission key, and personal authentication key.

(Symmetric Authentication Key)" is deleted from the memory after performing the destruction operation.

The encryption key and TSF data protection method described above are listed as follows.

classification			contents	type	location
Credentials for Administrators	ID		· Encrypt with hash algorithm	Cipher Text SHA-256	DB
	PASSWORD				
password derivation		Cipher Key	· Generate password for encryption key using key derivation algorithm (SHA-256_HMAC_PBKDF2)	Plain Text	Memory
random number generator base			· Encrypted storage with key encryption key (password derivation)	Cipher Text ARIA(|K|=256)	File
for user data			· Encrypted storage with key encryption key (random number generator)	Cipher Text ARIA(|K|=128)	DB
for TSF data			· Encrypted storage with key encryption key (random number generator)		DB
private key transfer key			· Encrypted storage with key encryption key (random number generator)		DB/File
public key transfer key			· save plain text	Plain Text	DB/File
private authentication key			· Encrypted storage with key encryption key (random number generator)	Cipher Text ARIA(|K|=128)	DB/File
public authentication key			· save plain text	Plain Text	DB/File
symmetric cipher key			· Encrypted storage with key encryption key (password derivation)	Cipher Text ARIA(|K|=256)	Memory
symmetric authentication key			· Encrypted storage with key encryption key (password derivation)		Memory
Audit history information			· Integrity information for audit history information is stored using an encryption algorithm (SHA-256)	Plain Text	DB
integrity file			· Integrity file storage for manager/agent information using encryption algorithm (SHA-256)	Cipher Text SHA-256	File
Environment configuration information			· Encrypted storage with key encryption key (random number generator)		
			encryption target - DB ID/password	Cipher Text ARIA(|K|=128)	File
			· Encryption with encryption key for TSF data		
			encryption target - management tool ip	Cipher Text ARIA(|K|=128,192,256) SEED(|K|=128)	DB
			encryption target - agent ip		
			encryption target - Security manager email address		
			encryption target - mail server address		

classification	contents		type	location
		- mail server account		
		- Mail server password		
		- Whether authentication is used		
		- whether to use encryption		

[table 52] Stored TSF Data Protection Policy

※ SFR Mapping

FPT_PST.1(Extended)

8.6.3. Self Test

The TOE self-test consists of process operation and integrity verification tests. If the self-test 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, and the check procedure is as follows.

classfication	contents	note
management tool	1) The management tool registers the process start time upon login 2) The management tool updates the process operation time by 1 minute 3) Management tool deletes process operation time upon logout	
Manager	1) The manager registers the process start time when running 2) The manager updates the process operation time every minute and checks whether the process is running for the management tool (agent). - Recognize the termination of the process if the management tool update time exceeds 2 minutes - Acknowledge process termination when agent renewal time exceeds 2 minutes 3) The manager deletes the process operating time upon termination	
agent	1) Agent registers process start time when running 2) The agent updates the process operating time every minute and checks whether the process is running for the management tool (manager). - Recognize the termination of the process if the management tool update time exceeds 2 minutes - Recognize process termination when manager update time exceeds 2 minutes 3) The agent deletes the process operating time upon termination	

[table 53] Process operation check procedure

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, and the test items are as follows.

classification	integrity verification			Execution point	note
	elements	Verification method	algorithm		
management tool	execution file	hash algorithm	SHA-256	When starting, periodic (1 hour), Upon admin request	Verified cryptographic module
	cryptographic module	digital signature	RSA-PSS		
Manager	execution file	hash algorithm	SHA-256		
	cryptographic module	digital signature	RSA-PSS		
	configuration file	hash algorithm	SHA-256		
agent	execution file	hash algorithm	SHA-256		
	cryptographic module	digital signature	RSA-PSS		
	configuration file	hash algorithm	SHA-256		

[table 54] Integrity verification test subject and verification method

※ SFR Mapping

FPT_TST.1

8.7. TOE access(FTA)

8.7.1. Limitation on concurrent sessions

In order to block concurrent access sessions of the same manager, the maximum number of simultaneous accesses to the manager by the security manager is limited to one, and the new session is terminated when a new connection is made with the same account.

※ SFR Mapping

FTA_MCS.2

8.7.2. session management

The TOE limits the number of IPs that the management tool can access to one, and only registered IPs can access the manager. If the security administrator logs in to the management tool and is inactive for 10 minutes, the session is automatically terminated.

When the security manager sets the IP address, the method of specifying and adding an IP address range (eg 192.168.10.2 ~ 253) is not allowed, and it is implemented to add one IP address individually, and when specifying an IP address, it means the entire network range. 0.0.0.0, 192.168.10.*, any, etc. are not allowed.

※ SFR Mapping

FTA_SSL.5(Extended), FTA_TSE.1