HEDES v1.0

Security Target

Document Version: v1.4

HumaneSystem Co., Ltd.

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

Document History and Change Management

Doc. Version	Change Date	Author	Content
v1.0	Jul. 1, 2020	HumaneSystem Co., Ltd. Corporate Research Institute	Initial preparation
v1.1	Nov. 13, 2020	HumaneSystem Co., Ltd. Corporate Research Institute	Changes incorporated
v1.2	Nov .27, 2020	HumaneSystem Co., Ltd. Corporate Research Institute	Changes incorporated
v1.3	Dec. 24, 2020	HumaneSystem Co., Ltd. Corporate Research Institute	Typographical errors corrected
v1.4	Jan. 29, 2021	HumaneSystem Co., Ltd. Corporate Research Institute	Reflecting change of identifier for each TOE element

Table of Contents

List of Figures

List of Tables

1. ST Introduction

This document is the Security Target (hereinafter referred to as the "ST") of HEDES v1.0, a DB encryption/decryption product by HumaneSystem Co., Ltd. that intends to achieve EAL1+ level under the Common Criteria.

This ST describing the Target of Evaluation (hereinafter the "TOE") and is structured as follows:

- Chapter 1 ST Introduction describes the ST reference, TOE reference, TOE overview, TOE description, conventions and terms and definitions.

- Chapter 2 Conformance Claims describes the conformance with the Common Criteria, the Protection Profile (PP) and the package, and presents conformance rationale and protection profile conformance statement.

- Chapter 3 Security Problem Definition explains security problems in the TOE and the TOE operational environment from the perspective of threats, organizational security policies and assumptions.

- Chapter 4 Extended Components Definition specifies the extended components additionally defined in the ST.

- Chapter 5 Security Requirements describes security functional requirements and security assurance requirements to satisfy the security objectives, and presents rationale for each of them.

- Chapter 6 TOE Summary Specification explains how the TOE satisfies the security functional requirements specified in Chapter 5.

1.1 ST reference

Classification	Description
Title	HEDES v1.0 Security Target
ST Version	v1.4
Developer	HumaneSystem Co., Ltd. / Corporate Research Institute
Publication Date	January 29, 2021
Common Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria Version	CC v3.1 r5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Configuration Item Identification	hds_st_005
Keywords	Database, Encryption

[Table 1-1] ST reference

1.2 TOE reference

Classification		Description	
TOE Identification		HEDES v1.0	
TOE Build Version		20210129-001	
TOE Component	Policy Server	HEDES Policy Server v1.0-20210129-001 (hedes_policy_server_1.0_002.tar)	S/W (distributed in CD format)
	Agent Server	HEDES Agent Server v1.0-20210129-001 (hedes_agent_server_1.0_002.tar)	
Guidance	Preparative Procedure	HEDES v1.0 Preparative Procedure v1.3 (hds_pre_004.pdf)	PDF (distributed in CD format)
	Operational User Guidance	HEDES v1.0 Operational User Guidance v1.3 (hds_ope_004.pdf)	
Developer		HumaneSystem Co., Ltd. / Corporate Research Institute	

[Table 1-2] TOE reference

1.3 TOE Overview

The TOE encrypts and decrypts user data inside the database (hereinafter the "DB") managed in the Database Management System (hereinafter the "DBMS") of an organization. User data means all data before/after encrypted and stored in the DB, including an organization's confidential data such as personal and sensitive information managed by the organization, which needs to be protected from threats.

The TOE is a database encryption product that performs the function of preventing the unauthorized disclosure of confidential information by encrypting the DB.

The encryption target of the TOE is the DB managed by the DBMS in the operational environment of the organization, and this ST defines user data as all data before/after encrypted and stored in the DB. Part or all of the user data can be the encryption target, depending on the organizational security policies of the organization that runs the TOE.

1.3.1 TOE usage and major security features

The TOE is provided as software and provides the function of column-level encryption/decryption of user data. The TOE is a plug-in type and consists of the Policy Server and the Agent Server.

The TOE provides various security features so that the authorized administrator can operate the TOE securely in the operational environment of the organization. Such security features include the security audit function that records and manages major auditable events; cryptographic support function such as cryptographic key management to encrypt the user and the TSF data and cryptographic operation; user data protection function that encrypts user data and protects the residual information; identification and authentication function such as verification of the identity of the authorized administrator, authentication failure handling, and mutual authentication among the TOE components; security management function for security functions, role definition, and configuration; TSF protection function including protecting the TSF data transmitted among the TOE components, protecting the TSF data stored in the storage that is controlled by the TSF, and TSF self tests; and TOE access function to manage access sessions of the authorized administrator. The Data Encryption Key (DEK) used to encrypt/decrypt user data is protected by encryption with the Key Encryption Key (KEK).

TOE components provide major functions as follows:

- Policy Server
  - Perform life-cycle management such as generation, distribution and destruction of the data encryption key of HEDES
  - Provide the function of managing DB encryption/decryption policies of HEDES
  - Establish the user data encryption/decryption policy by setting different encryption keys and encryption algorithms for each column in order to provide the DB encryption service
  - Provide the administrator interface for the security management of the TOE
  - Provide the function to prevent duplicated login by the administrator and concurrent session login and to ensure automatic logout in case of a prolonged away mode
  - Provide the function to view audit data stored in the local DB
  - Provide the function of security audit including audit record generation, security alarm and audit review
  - Store audit tracing data and take actions if the audit trail is full
  - Provide the encryption of mutual authentication and transmission with the Agent Server, a TOE component

- Agent server
  - Receive the DB encryption/decryption policy from the Policy Server and process the encryption/decryption of user data
  - Apply the cryptographic key and encryption algorithms to user data encryption/decryption according to the policy
  - Send the audit records on the DB encryption/decryption service to the Policy Server
  - Provide the DB plugin module that can perform user data encryption/decryption
  - Provide the encryption of mutual authentication and transmission with the Policy Server, a TOE component

1.3.2 TOE type

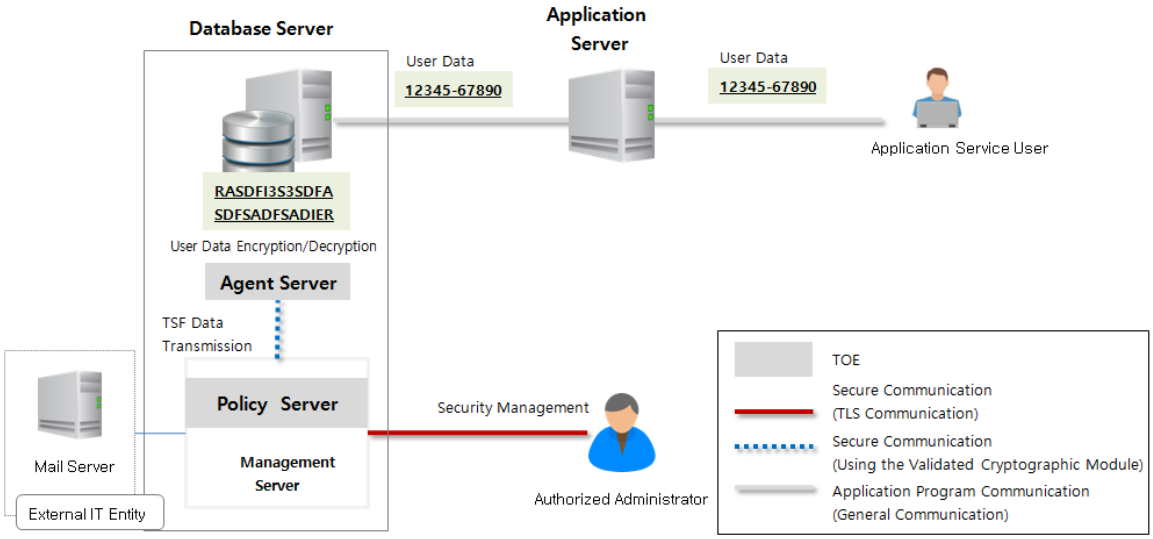
The TOE consists of the Policy Server and the Agent Server, and is installed on the database server where the DB to be protected is located. It encrypts user data on the application server before they are stored in the DB according to the policy established by

the authorized administrator, and decrypts the encrypted user data transmitted from the database server to the application server.

The authorized administrator can perform the encryption/decryption of user data according to scope of the encryption target through the Policy Server, with which he/she can perform the security management.

The Policy Server, which is installed on the database server along with the Agent Server, is an integration-type operational environment that integrates the agent and the management server.

The operational environment where the TOE is operated is shown in [Figure 1-1] below:



[Figure 1-1] Plug-in type operational environment
(Agent, Management Server integrated type)

The authorized administrator establishes the security policy of the TOE by using a web browser on the administrator PC. Then, the Agent Server receives the encryption policy from the Policy Server, encrypts user data received from the application server and stores them in the DB. Logs generated on the Agent Server are sent to the Policy Server and stored in the local DB.

Communication between the administrator PC and the Policy Server is secured with TLS v1.2 protocol set on WAS. TLS v1.2 TLS_DHE_RSA_WITH_AES_256_CBC _SHA256 Cipher Suite is used on WAS.

The validated cryptographic module included in the TOE is specified in [Table 1-3] below:

Validated Cryptographic Module	Cryptographic Module Name	MagicCrypto V2.2.0
	Developer (institutions)	Dream Security
	Validation Date	March 3, 2020
	Validation Level	VSL1
	Validation No.	CM-162-2025.3

[Table 1-3] Validated cryptographic module

1.3.3 Identification of non-TOE hardware and software

Non-TOE hardware and software not subject to the evaluation are necessary for the operation of the TOE. The TOE needs third party software Jetty 9.4.36, MySQL 5.7 and JAVA JRE 1.8.0_281, which are designated as the requirements for the operation of the TOE.

Third party software necessary for the operation of the TOE is listed below:

Third Party S/W	Role
JAVA JRE 1.8.0_281	JAVA runtime environment for the operation of the TOE components
MySQL 5.7	DBMS to be protected. It is a local DBMS to store cryptographic keys and other TSF data on the Policy Server.
Jetty 9.4.36	- Web-based dynamic application server to provide the administrator interface in the Policy Server - The administrator PC and the Policy Server communicate with each other through SSL secure channel.

[Table 1-4] Third party software for the operational environment

A separate external IT entity is necessary for the operation of the TOE. Such external IT entity required by the TOE for the evaluation is as follows:

Classification	Minimum Specification
Mail server	Server to send an email to the authorized administrator if a potential violation is detected

[Table-1-5] External IT entity

The following table describes the minimum requirements of hardware and software for the installation and operation of the TOE:

Classification		Minimum Requirements
H/W	CPU	Intel Xeon CPU E3-1220 @ 3.10 Ghz (4 Core) or higher
	Memory	16 GB or higher
	HDD	Space required for installation of TOE : 300 GB or higher
	NIC	10/100/1000 Mbps * 1 EA or more
S/W	OS	CentOS 7.9 (kernel v3.10, 64 bit)
	JAVA	JAVA JRE 1.8.0_281
	DBMS	MySQL 5.7
	WAS	Jetty 9.4.36

[Table 1-6] Minimum requirements for the hardware and software for the installation and operation of the TOE

The following table describes the specifications of the administrator system of the TOE:

Classification		Minimum Requirements	Remarks
S/W	Web browser	Chrome 88	

[Table 1-7] Specifications of the administrator system of the TOE

1.4 TOE description

This section describes the physical scope and the logical scope of the TOE.

1.4.1 Physical scope of the TOE

The physical scope and boundary of the TOE include the TOE components (Policy Server and Agent Server) and guidance documents. The TOE consists of the software and guidance documents as shown in [Table 1-8] below:

Classification		Contents	File Format	Distribution Format
TOE Component	Policy Server	HEDES Policy Server v1.0-20210129-001 (hedes_policy_server_1.0_002.tar)	S/W	CD
	Agent Server	HEDES Agent Server v1.0-20210129-001 (hedes_agent_server_1.0_002.tar)	S/W	CD
Guidance	Preparative procedure	HEDES v1.0 preparative procedure v1.3 (hds_pre_004.pdf)	PDF	CD
	Operational User Guidance	HEDES v1.0 operational user guidance v1.3 (hds_ope_004.pdf)		

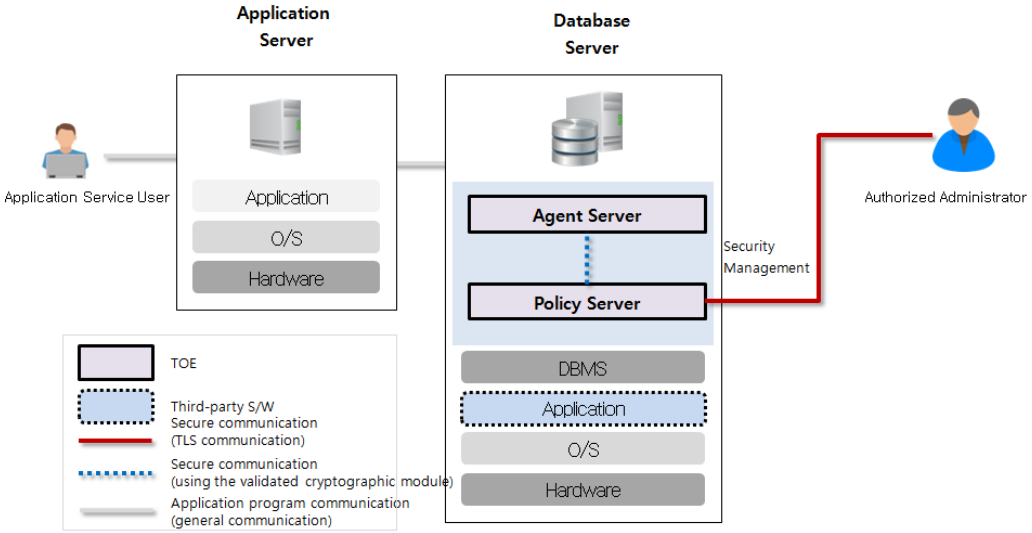
[Table 1-8] Physical scope of the TOE

The cryptographic module included in the TOE is as follows:

Cryptographic Module Name	Validated Cryptographic Module Information		TOE used
MagicCrypto V2.2.0	Validation date	2020.03.03	Policy Server Agent server
	Validation number	CM-162-2025.3	
	Validation level	VSL1	

[Table 1-9] Validated cryptographic module

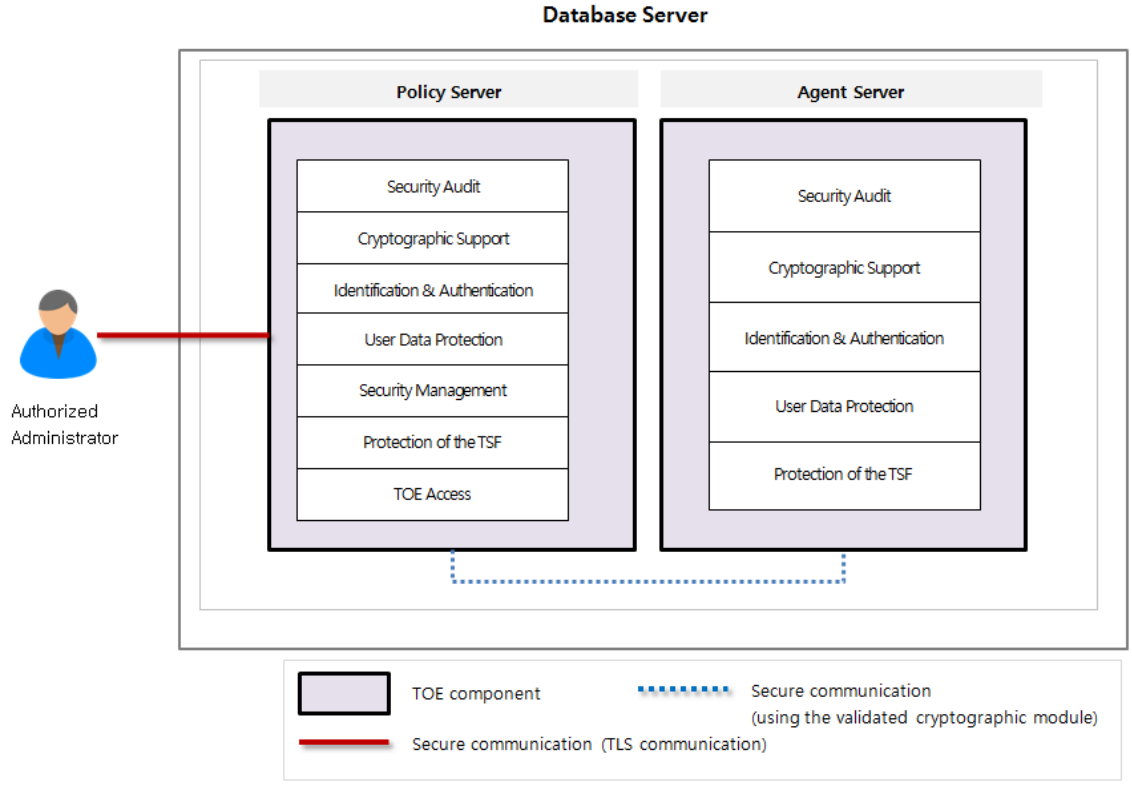
The physical scope of the TOE is shown in [Figure 1-2] below:



[Figure 1-2] Physical scope of the TOE

1.4.2 Logical scope of the TOE

The logical scope of the TOE is shown in [Figure 1-3] below:



[Figure 1-3] Logical scope of the TOE

1.4.2.1 Security audit (FAU)

The TOE provides the authorized administrator with the function to search and view audit information, and also provides audit information such as date, time, IP, event type, event subject, details, etc. It generates audit records in case of auditable events, and sends an alarm email to the authorized administrator upon the detection of a potential security violation. It also stores all the generated audit data in an audit trail storage (DBMS) and securely manage them. The TOE prevents the unauthorized deletion of audit data, and provides the function to protect the audit trail storage by overwriting the oldest stored audit data if the audit trail storage is full.

The TOE sends an alarm email to the email address registered by the authorized administrator in case of an auditable event or a potential violation as listed below:

(1) In case the audit data storage reaches or exceeds the threshold
(2) In case the number of unsuccessful attempts of the administrator authentication or the number of unsuccessful authentication reaches the threshold
(3) In case a new session is denied based on the limitation of the concurrent sessions
(4) In case of an attempt to access from a disallowed IP
(5) In case the integrity and self tests fail
(6) In case self tests of the validate cryptographic module fail

1.4.2.2 Cryptographic support (FCS)

The TOE generates and destructs all cryptographic keys used for the operation of the product through MagicCrypto V2.2.0, the validated cryptographic module whose security and implementation conformance have been validated by the cryptographic module validation scheme. It performs cryptographic operations according to the cryptographic policy that defines cryptographic algorithms.

Original data are deleted when the encryption is performed, and encrypted data are deleted when the decryption is performed. In addition, the cryptographic key is generated and exchanged through MagicCrypto V2.2.0, which is the validated cryptographic module, for the encrypted communication between TOE components.

- Cryptographic key generation: A cryptographic key is generated based on the cryptographic algorithms and cryptographic key sizes in [Table 1-10] and [Table 1-11].

Standard List	Cryptographic Algorithm	Key Size	Use
ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- Generate user data cryptographic key

[Table 1-10] Cryptographic key generation algorithm for user data encryption

Standard List	Cryptographic Algorithm	Key Size	Use
ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- Generate KEK - Generate TSF data cryptographic key

[Table 1-11] Cryptographic key generation algorithm for TSF data encryption

- Cryptographic key distribution: A cryptographic key is distributed online as specified in [Table 1-12].

Standard List	TOE (Sender)	TOE (Receiver)	Cryptographic Key	Distribution Method
ISO/IEC 10118-3, TTAS.KO-12.0004/R1	Agent server	Policy Server	Key encryption key (KEK)	KEK is encrypted with a session key, and distributed from the Agent Server to the Policy Server.
ISO/IEC 10118-3, TTAS.KO-12.0004/R1	Policy Server	Agent server	User data encryption key	User data encryption key is encrypted with a session key, and distributed from the Policy Server to the Agent Server.

[Table 1-12] Cryptographic key distribution method

- Cryptographic key destruction: The TOE overwrites the cryptographic key and critical security parameters with "0" as shown in [Table 1-13].

Cryptographic Key	TOE	Location	Destruction Method	Timing of Destruction
User data encryption/decryption key	Agent server	Memory	Zeroization	Immediately after the encryption/decryption operation on user data
Session key	Policy Server	Memory	Zeroization	Immediately after mutual authentication is removed

	Agent server	Memory	Zeroization	Immediately after mutual authentication is removed
Key encryption key (KEK)	Policy Server	Memory	Zeroization	Immediately before the program is terminated
	Agent server	Memory	Zeroization	Immediately before the program is terminated

[Table 1-13] Cryptographic key destruction method

- Cryptographic operation: Cryptographic operation of user data is performed as shown in [Table 1-14], and cryptographic operation for the encryption of TSF data is performed as shown in [Table 1-15].

Standard List	Cryptographic Algorithm	Key Size	Operation Mode	Padding	Use
KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	- User data encryption/decryption
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	- User data encryption/decryption
ISO/IEC 10118-3	SHA512	None	None	None	- User data encryption

[Table 1-14] Cryptographic operation of user data

Standard List	Cryptographic Algorithm	Key Size	Operation Mode	Padding	Use
KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	- Inter-TSF cryptographic communication - Encryption/decryption of environment configuration file - Encryption/decryption of TSF data
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	- Encryption/decryption of KEK
ISO/IEC 10118-3	SHA512	None	None	None	- Integrity monitoring of the TOE

					- Generation of SALT value of KEK - Generation of SALT value of session key - Mutual verification of session key - Inter-TSF cryptographic communication - Encryption of administrator password
ISO/IEC 18033-2	RSAES (SHA-256)	2048 bits	None	None	- Inter-TSF mutual authentication
ISO/IEC 14888-2	RSA-PSS (SHA-256)	2048 bits	None	None	- Inter-TSF mutual authentication
ISO/IEC 11770-3	ECDH (SHA-256)	256 bits	None	None	- Inter-TSF mutual authentication
TTAS.KO-12.0334	PBKDF2 (SHA-256)	256 bits	None	None	- KEK generation

[Table 1-15] Cryptographic operation of TSF data

1.4.2.3 User data protection (FDP)

The TOE performs the encryption/decryption of user data at the column level by using the validated cryptographic module MagicCrypto V2.2.0 through the encryption policy set by the authorized administrator. The same ciphertext is not generated for the same plaintext when encrypting the user data. After the encryption/decryption is completed, the memory area is initialized with "0" value and the used memory area is deallocated so that the user data are unrecoverable in the memory.

Encryption algorithms listed in [Table 1-16] Cryptographic operation of user data are used for the encryption/decryption of user data. SHA-512 is provided for the one-way encryption algorithm.

Standard List	Cryptographic Algorithm	Key Size	Operation Mode	Padding	Use

KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	- Encryption/decryption of user data
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	- Encryption/decryption of user data
ISO/IEC 10118-3	SHA512	None	None	None	- Encryption of user data

[Table 1-16] Cryptographic operation of user data

1.4.2.4 Identification and authentication (FIA)

The TOE provides the identification and authentication function for the administrator in charge of the security management, and does not provide a reason for failure in the event of an authentication failure. It also provides the function to lock the authentication (10 minutes) if authentication attempts fail consecutively (5 times). The TOE offers the function to prevent the reuse of authentication data of the administrator.

A password used in the process of the identification and authentication of the administrator shall comply with the rule that the password shall have a combination of alphabetic characters, numeric characters and special characters, and is masked with "*" when entered.

The TOE performs the mutual authentication through the protocol developed by HumaneSystem Co., Ltd. for the purpose of the secure communication among the TOE components.

1.4.2.5 Security management (FMT)

The TOE provides the authorized administrator with the security management function such as policy management, administrator management and environment configuration. The authorized administrator performs the security management through the security management interface. In addition, the administrator ID and password are designated during the installation. When the authorized administrator accesses the security management interface, the TOE enforces the authorized administrator to change the password if the password expiration date arrives (expiration period: 100 days). There is only one type of privilege of the authorized administrator, which is the top administrator.

1.4.2.6 Protection of the TSF (FPT)

The TOE protects the TSF data stored in containers controlled by the TSF, and the TSF data transmitted between TOE components. It also checks major security function processes, etc. by conducting TSF self tests. The TOE runs a suite of self tests during initial start-up and periodically during normal operation (1 hour interval), and verifies the integrity of TOE configuration files and major processes during initial start-up and periodically during normal operation. Then, if the integrity was compromised, it sends an alarm email to the administrator.

The Policy Server protects the stored TSF data including the administrator password, encryption keys, TOE configuration values and the DB encryption/decryption policy by using SHA-512 hash and ARIA256-CBC encryption provided by the validated cryptographic module.

For the encrypted transmission of the TSF data between TOE components, the transmitted data (TSF data + SHA512 hash value of the TSF data) are encrypted/decrypted with ARIA-256-CBC cryptographic algorithm, thereby protecting the TSF data from unauthorized disclosure and modification. If the integrity violation is detected in relation to the hash value of the received TSF data, the TSF ignores the received data, and generates the audit data on this event.

1.4.2.6 TOE access (FTA)

The TOE restricts the number of the administrator's management access sessions whose access is allowed to perform the security management function to one. If the same account makes new access, it terminates the existing session and generates audit data. Also, if the administrator remains inactive for 10 minutes, it terminates the existing session and requires the administrator to be reauthenticated.

In the case of the administrator, access sessions are restricted according to the rule for allowing access IP. The TOE allows the management sessions made only from a device (2 or less) whose IP was designated and allowed to access, and generates audit data on the result of the limitation of sessions by the security management interface.

1.5 Terms and definitions

Technical terms in this ST are defined as follows. Terms used in this ST, which are the same as in the CC, are not separately defined herein, but must follow those in the CC.

Private key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Object

Passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

Approved mode of operation

An operation mode of a cryptographic module that uses an approved cryptographic algorithm

Approved cryptographic algorithm

A cryptographic algorithm selected by an institution that validates cryptographic modules taking into account the security, credibility, interoperability and so forth with regard to block cipher, hash function, message authentication code, random bit generator, key settings, public key encryption, and electronic signature cryptographic algorithms

Attack potential

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

Public key

A cryptographic key which is used in as asymmetric cryptographic algorithm and is associated with a unique entity (the subject using the public key). It can be disclosed.

Public Key(asymmetric) cryptographic algorithm

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

Management access

The access to the TOE by using the HTTPS, SSH, TLS, IPSec, etc. to manage the TOE by administrator

Recommend/be recommended

The 'recommend' or 'be recommended' presented in Application notes is not mandatorily recommended, but required to be applied for secure operation of the TOE.

Random bit generator (RBG)

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0- and 1-bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a "seed key," and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Symmetric cryptographic technique

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

Database (DB)

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

Data Encryption Key (DEK)

Key that encrypts and decrypts the data

Iteration

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

Security Function Policy (SFP)

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

Security Target (ST)
Implementation-dependent statement of security needs for a specific identified TOE

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

Security token
Hardware device that implements key generation and electronic signature generation inside the device to save/store confidential information safely

Protection Profile (PP)
Implementation-independent statement of security needs for a TOE type

Decryption
The act that restores the ciphertext into the plaintext using the decryption key

Secret key
A cryptographic key which is used in a symmetric cryptographic algorithm and is uniquely associated with one or several entities, not to be disclosed.

User
Refer to "External entity"

User data
Data for the user, that does not affect the operation of the TSF (TOE security functionality)

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

Identity
Representation uniquely identifying an authorized user. The representation can be the full or abbreviated name or a pseudonym.

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

HEDES Agent Server
A software module that processes the encryption or decryption of the data of a user according to the encryption/decryption policy of the Policy Server

Element
Indivisible statement of a security need

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

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

Operation (on an object)
Specific type of action performed by a subject on an object

External entity
Entity (human or IT entity) interacting (or possibly interacting) with the TOE from outside of the TOE boundary

Threat agent
Unauthorized external entity that can pose illegitimate threats such as adverse access, modification or deletion to an asset

Authorized administrator
Authorized user who securely operates and manages the TOE

Authorized user
User who may, in accordance with the Safety Functional Requirements (SFR), perform an operation

Authentication data
Information used to verify the claimed identity of a user

Self-test
Pre-operational or conditional test executed by the cryptographic module

Assets
Entities that the owner of the TOE presumably places value upon

Refinement
Addition of details to a component

HEDES policy server
A software module for the authorized administrator to manage the establishment of the encryption/decryption policy

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

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

Subject
Active entity in the TOE that performs operations on objects

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

Column

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

Component
Smallest selectable set of elements on which requirements may be based

Class
Set of CC families that share a common focus

Key Encryption Key (KEK)
Key that encrypts and decrypts another cryptographic key

Target of Evaluation (TOE)
Set of software, firmware and/or hardware possibly accompanied by guidance

Evaluation Assurance Level (EAL)
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that forms an assurance package

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

MySQL Plug-In
A form of libraries that can extend additional functions in addition to basic functions of MySQL DBMS

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

Can/could
The 'can' or 'could' presented in Application notes indicates optional requirements applied to the TOE by ST author's choice

Shall/must

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

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

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

Database Server
The server in which DBMS managing the protected DB is installed in the organization that operates the TOE

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

HEDES v1.0
DB security product to perform the column-level encryption/decryption of major information stored in the database to be protected, by using the validated cryptographic module of the National Intelligence Service.

JAVA JDK
Abbreviation of JAVA Development Kit. It is an environment for JAVA development with which JAVA program can be developed and executed.

JRE

Abbreviation of JAVA Runtime Environment. Unlike JAVA JDK, it is an environment to execute a program and not a development environment. It can execute a program developed with a JAVA language only.

Secure Sockets Layer (SSL)

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

Transport Layer Security (TLS)

This is a cryptographic authentication communication protocol between a SSL-based server and a client and is described in RFC 2246.

TOE Security Functionality (TSF)

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

TSF data

Data generated by the TOE and for the TOE, which can affect the operation of the TOE

1.6 Conventions

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

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

Iteration

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

Assignment

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

Selection

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

Refinement

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

2. Conformance Claim

CC, PP and Package that are compliant with ST and TOE are as follows.

2.1 CC Conformance claim

ST complies with the following CC.

Classification	Conformance
Common Criteria	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)
CC Conformance Claim	Part 2 Security Functional Requirements Extended
	Part 3 Security Assurance Requirements Conformant
	Package Augmented: EAL1 augmented (ATE.FUN.1)

[Table 2-1]CC Conformance Claim

2.2 PP conformance claim

This ST strictly complied with the 'National PP of Database Encryption 'V1.1'(KECS-PP-0820a2017_PP_KR).'

Classification	PP	ST	Rationale
Type of TOE	DB Encryption	DB Encryption	Same as PP
Security Function Requirement (SFR)	FAU_ARP.1	FAU_ARP.1	Same as PP
	FAU_GEN.1	FAU_GEN.1	Same as PP
	FAU_SAA.1	FAU_SAA.1	Same as PP
	FAU_SAR.1	FAU_SAR.1	Same as PP
	FAU_SAR.3	FAU_SAR.3	Same as PP
	FAU_STG.3	FAU_STG.3	Same as PP
	FAU_STG.4	FAU_STG.4	Same as PP
	FCS_CKM.1(1)	FCS_CKM.1(1)	Same as PP
	FCS_CKM.1(2)	FCS_CKM.1(2)	Same as PP
	FCS_CKM.2	FCS_CKM.2	Same as PP
	FCS_CKM.4	FCS_CKM.4	Same as PP
	FCS_COP.1(1)	FCS_COP.1(1)	Same as PP
	FCS_COP.1(2)	FCS_COP.1(2)	Same as PP
	FCS_RBG.1(Extended)	FCS_RBG.1(Extended)	Same as PP
	FDP_UDE.1(Extended)	FDP_UDE.1(Extended)	Same as PP
	FDP_RIP.1	FDP_RIP.1	Same as PP
	FIA_AFL.1	FIA_AFL.1	Same as PP
	FIA_IMA.1(Extended)	FIA_IMA.1(Extended)	Same as PP
	FIA_SOS.1	FIA_SOS.1	Same as PP
	FIA_UAU.2	FIA_UAU.2	Same as PP
	FIA_UAU.4	FIA_UAU.4	Same as PP
	FIA_UAU.7	FIA_UAU.7	Same as PP

	FIA_UID.2	FIA_UID.2	Same as PP
	FMT_MOF.1	FMT_MOF.1	Same as PP
	FMT_MTD.1	FMT_MTD.1	Same as PP
	FMT_PWD.1(Extended)	FMT_PWD.1(Extended)	Same as PP
	FMT_SMF.1	FMT_SMF.1	Same as PP
	FMT_SMR.1	FMT_SMR.1	Same as PP
	FPT_ITT.1	FPT_ITT.1	Same as PP
	FPT_PST.1(Extended)	FPT_PST.1(Extended)	Same as PP
	FPT_TST.1	FPT_TST.1	Same as PP
	FTA_MCS.2	FTA_MCS.2	Same as PP
	FTA_SSL.5(Extended)	FTA_SSL.5(Extended)	Same as PP
	FTA_TSE.1	FTA_TSE.1	Same as PP

[Table 2-2] Rationale for PP Conformance Claim

2.3 Package conformance claim

This ST conforms to PP assurance requirement package EAL 1, augmented with the following.

◆ **Assurance Package: EAL1 augmented(ATE_FUN.1)**

2.4 Conformance claim rationale

This ST adopts the TOE type, security objectives and security requirements in the same way as the Protection Profile, and it is demonstrated that this ST conforms to “the National PP for Database Encryption V1.0” “more restrictively and strictly”

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

The following are the security objectives handled through technical and procedural means supported by the operational environment to provide TOE security functionality accurately.

OE. Physical Security	The place of TOE installation and operation shall be equipped with access control and protection facilities so that only authorized administrator can access.
OE. Trusted Administrator	The authorized administrator of the TOE shall be non-malicious, 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 check a spare space of the 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. Time Stamp	The TOE shall accurately record security-relevant events by using reliable time stamps provided by the TOE operational environment.
OE. DBMS	The DBMS interacting with the TOE stores audit trail records, and hence should be protected from unauthorized deletion or modification.

4. Extended Components Definition

This ST defines and uses the following components in addition to the components of CC Part 2. Extended components of this ST are as follows.

The following [Table 4-1] shows the extended security functional requirements components.

Class	Components	
Cryptographic support (FCS)	FCS_RBG.1(Extended)	Random bit generation
Identification & authentication (FIA)	FIA_IMA.1(Extended)	TOE Internal mutual authentication
User data protection (FDP)	FDP_UDE.1(Extended)	User data encryption
Security Management (FMT)	FMT_PWD.1(Extended)	Management of ID and password
Protection of the TSF (FPT)	FPT_PST.1(Extended)	Basic protection of stored TSF data
TOE Access (FTA)	FTA_SSL.5(Extended)	Management of TSF-initiated sessions

[Table 4-1] Extended components

4.1 Cryptographic support (FCS)

4.1.1 Random Bit Generation

FCS_RBG.1	Random bit generation (Extended)
Hierarchical to	No other components.
Dependencies	No dependencies.
FCS_RBG.1.1	The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

4.2 Identification & authentication(FIA)

4.2.1 TOE Internal mutual authentication

FIA_IMA.1	TOE Internal mutual authentication (Extended)
Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] using the [assignment: authentication protocol] that meets the following: [assignment: *list of standards*].

4.3 User data protection (FDP)

4.3.1 User data encryption

FDP_UDE.1	User data encryption (Extended)
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(FMT)

4.4. ID and Password

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 [assignment: *list of functions*] to [assignment: *the authorized 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(FPT)

4.5.1 Protection of stored TSF data

FPT_PST.1	Basic protection of stored TSF data (Extended)
Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_PST.1.1	The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from

the unauthorized [selection: *disclosure, modification*].

4.6 TOE Access(FTA))

4.6.1 Session Locking and Termination

FTA_SSL.5	Management of TSF-initiated sessions (Extended)
Hierarchical to	No other components.
Dependencies	FIA_UAU.1 Authentication or No dependencies.
FTA_MCS.2.1	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 describe security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to this ST.

5.1 Security Functional Requirements

The security function requirements defined in this ST are expressed by selecting the relevant security function components from CC Part 2 to satisfy the security objectives identified in Chapter 4. The following [Table-5-1] provides a summary of the security function components used in this ST.

Security Functional Class	Security Functional Component	
Security Audit (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
Cryptographic Support (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	Random bit generation

	(Extended)	
User Data Protection (FDP)	FDP_UDE.1 (Extended)	User data encryption
	FDP_RIP.1	Protect the residual information Protection
Identification and Authentication (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 (Administrator)
	FIA_UAU.4	Single-use authentication mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action (Administrator)
Security Management (FMT)	FMT_MOF.1	Management of security functions behavior
	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
Protection of the TSF (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
TOE Access (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 5-1] Security functional requirements (SFR)

5.1.1 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 [an email notification to an authorized administrator] upon detection
of a potential security violation.

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 "auditable event" in [Table 5-2] Auditable Event. [None]
FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable) and the outcome (success of failure) of the event: and
b) For each audit event type, based on the auditable event definitions of the functional
components include in the ST, [refer to "Additional Audit Record" in [Table 5-2]
Auditable Event, (*None*)]

Security Functional Component	Auditable Event	Type	Additional Audit Record
FAU_ARP.1	Actions taken due to potential security violations	Target	Identity of the recipient of the response action

FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	Target	
FAU_STG.3	Actions taken due to exceeding of a threshold	Target	
FAU_STG.4	Actions taken due to the audit storage failure	Target	
FCS_CKM.1(1)	Success and failure of the activity	Target	
FCS_CKM.2	Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	Target	Identity of the recipient of the response action
FCS_CKM.4	Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	Target	
FCS_COP.1(1)	Success and failure of cryptographic operation	Target	
FDP_UDE.1	Success and failure of user data encryption/decryption	Target	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the action taken, and the subsequent, if appropriate, restoration to the normal state	Target	
FIA_IMA.1	Success and failure of mutual authentication Modify of authentication protocol	Target	
FIA_UAU.2	All uses of authentication mechanisms	Target	
FIA_UAU.4	Attempts to reuse authentication data	Target	
FIA_UID.2	All use of the User Identification mechanism, including the user identity provided	Target	

FMT_MOF.1	All modifications in the behavior of the functions in the TSF	Target	
FMT_MTD.1	All modifications to the values of TSF data	Target	Modified values of TSF data
FMT_PWD.1	All changes of the password	Target	
FMT_SMF.1	Use of the management functions	Target	
FMT_SMR.1	Modifications to the user group of rules divided	Target	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Target	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	Target	
FTA_SSL.5	Locking or termination of interactive session	Target	

[Table 5-2] Audit event

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 event in FIA_UAU.1
- Integrity violation event among auditable events in FPT_TST.1 · Failure of self test of the KCMVP, [None] known to indicate a potential security violation.

b) [None]

FAU_SAR.1 Audit review
Hierarchical to No other components.
Dependencies FAU_GEN.1 Audit data generation
FAU_SAR.1.1 The TSF shall provide [authorized administrator] with the capability to read [all the audit data] from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

FAU_SAR.3 Selectable audit review
Hierarchical to No other components.
Dependencies FAU_SAR.1 Audit review
FAU_SAR.3.1 The TSF shall provide the capability to apply [the following methods of selection and/or ordering] of audit data based on [the following criteria with logical relations].

Selection Criteria	Allowable Ability
Security name	Selective search using keywords
Occurred module	
Date and time of occurrence	
Type of action	

[Table 5-3] Type of Audit Data and Selection Criteria

FAU_STG.3 Action in case of possible audit data loss
Hierarchical to No other components.
Dependencies No dependencies.
FAU_STG.3.1 The TSF shall [notification to the authorized administrator, [None]] if the audit trail exceeds [Usage rate (60%~~90%) for the threshold of the number of audit data set by the authorized administrator and the maximum capacity of the DB table space].

FAU_STG.4 Prevention of audit data loss

Hierarchical to	FAU_STG.3 Action in case of possible audit data loss
Dependencies	No dependencies.
FAU_STG.4.1	The TSF shall overwrite oldest audit records and [send email alert to the administrator] if the audit trail is full.

5.1.2 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 [Key generation algorithm of [Table 5-4]] and specified cryptographic key sizes [Cryptographic key size of [Table 5-4]] that meet the following: [Standard List of [Table 5-4]].

Standard List	Cryptographic Algorithm	Key Size	Usage
ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- Generate for user data Encryption and decryption key

[Table 5-4] Cryptographic key generation algorithm for user data encryption

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 [Key generation algorithm of [Table 5-5]] and specified cryptographic key sizes [Key size of [Table 5-5]] that meet the following: [Standard List of [Table 5-5]].

Standard List	Cryptographic Algorithm	Key Size	Usage
ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- KEK generation - Generate for TSF data Encryption and decryption key

[Table 5-5] Cryptographic key generation algorithm for TSF data encryption

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 distribution method [Cryptographic key distribution Method of [Table 5-6]] that meet the following: [Standard List of [Table 5-6]]

Standard List	TOE(Sender)	TOE(Receiver)	Cryptographic Key	Distribution Method
ISO/IEC 10118-3, TTAS.KO-12.0004/R1	Agent Server	Policy Server	KEK	KEK is encrypted using a session key and distributed from the Agent Server to the Policy Server.
ISO/IEC 10118-3, TTAS.KO-12.0004/R1	Policy Server	Agent Server	User data encryption and decryption key	The user data encryption key is encrypted using the session key and distributed from the Policy Server to the Agent Server.

[Table 5-6] Cryptographic key distribution method

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]

Cryptographic Key	TOE	Location	Destruction Method	Timing of Destruction
User data encryption/ decryption key	Agent server	Memory	Zeroization	Immediately after the encryption/decryption operation on user data
Session key	Policy Server	Memory	Zeroization	Immediately after mutual authentication is removed
	Agent server	Memory	Zeroization	Immediately after mutual authentication is removed
Key encryption key (KEK)	Policy Server	Memory	Zeroization	Immediately before the program is terminated
	Agent server	Memory	Zeroization	Immediately before the program is terminated

[Table 5-7] Cryptographic key destruction method

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 [Operations list of [Table 5-8]] in accordance with a specified cryptographic algorithm [Cryptographic algorithms of [Table 5-8]]
and cryptographic key sizes [Key size of [Table 5-8]] that meet the following: [Standard List of [Table 5-8]].

Standard List	Cryptographic algorithms	Key size	Operation mode	Padding	Operation list
KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	Encryption· Decryption

TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	Encryption· Decryption
ISO/IEC 10118-3	SHA512	None	None	None	Encryption

[Table 5-8] Cryptographic operation of user data

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 [Operations list of [Table 5-9]] in accordance with a specified cryptographic algorithm [Cryptographic algorithms of [Table 5-9]] and cryptographic key sizes [Key size of [Table 5-9]] that meet the following: [Standard List of [Table 5-9]].

Standard List	Cryptographic Algorithm	Key Size	Operation Mode	Padding	Use
KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	- Inter-TSF cryptographic communication - Encryption/decryption of environment configuration file - Encryption/decryption of TSF data
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	- Encryption/decryption of KEK
ISO/IEC 10118-3	SHA512	None	None	None	- Integrity monitoring of the TOE - Generation of SALT value of KEK - Generation of SALT value of session key

					- Mutual verification of session key - Inter-TSF cryptographic communication - Encryption of administrator password
ISO/IEC 18033-2	RSAES (SHA-256)	2048 bits	None	None	- Inter-TSF mutual authentication
ISO/IEC 14888-2	RSA-PSS (SHA-256)	2048 bits	None	None	- Inter-TSF mutual authentication
ISO/IEC 11770-3	ECDH (SHA-256)	256 bits	None	None	- Inter-TSF mutual authentication
TTAS.KO-12.0334	PBKDF2 (SHA-256)	256 bits	None	None	- KEK generation

[Table 5-9] Cryptographic operation of TSF data

FCS_RBG.1	Random bit generation (extended)
Hierarchical to	No other components.
Dependencies	No dependencies.
FCS_RBG.1.1	The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [ISO/IEC 18031].

5.1.3 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 dependencies.

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

5.1.4 Identification and Authentication (FIA)

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 "*an administrator configurable positive integer within [5]*" unsuccessful authentication attempts occur related to [administrator authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [deactivate the identification and authentication function (default: 10 minutes)].

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 using [Authentication protocol of [Table 5-10]] in accordance with [Standard List of [Table 5-10]] between [TOE components of [Table 5-10]].

Standard List	TOE components	Authentication protocol
None	Policy Server, Agent Server	Mutual signature verification through Pre-Auth Key distribution

[Table 5-10] Mutual authentication method between TOE Components

FIA_SOS.1 Verification of secrets

Hierarchical to No other components.

Dependencies No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined quality metric].

a) Password length: 9 or more and 20 or less

b) Combination rules: English letter (52 letters: a~z, A~Z), Number (10 letters : 0~9), Special character (32 letters: :`~! @ # $ % ^ & * () -_ +

= [] {} ₩ |; : '",. <> /?)

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 dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [ID/Password Authentication Method].

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 ['*', a message that cannot infer the reason for failure in the event of authentication failure] to the user while the authentication is in progress

FIA_UID.2	User identification before any action
Hierarchical to	FIA_UID.1
Dependencies	No dependencies.
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.**

5.1.5 Security Management (FMT)

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 [Security functions behavior of [Table 5-11]] to [Administrator of [Table 5-11]].

Security functions (Policy Server)	Management Type				
	Basic	Query	Insert	Modify	Delete
Set the administrator's email address for the detection of a potential violation	○	○		○	
Apply a set of rules to audit events	○				
View audit records	○	○			
Maintain the threshold on audit data	○	○		○	
Manage actions to be taken in case of imminent audit storage failure	○				
Manage the policy to overwrite the oldest records in case of audit storage failure	○				
Manage the rule for user data encryption/decryption		○	○	○	○
Manage the threshold for unsuccessful authentication attempts	○	○		○	
Manage the authentication protocol for mutual authentication	○				
Manage the quality metrics used to verify passwords	○				
Manage the group of roles that can interact with	○				

the functions in the TSF					
Manage the group of roles that can interact with TSF data	○				
Manage the rules for ID and password setting	○				
Manage the group of users that are part of a role	○				
Manage the types of modification against which the TSF should protect	○				
Manage the mechanism used to provide the protection of the data in transit between different parts of the TSF	○				
Self-tests and integrity verification on TSF	○				
Terminate a session in case of the administrator inactivity	○				
Number of concurrent sessions of administrator access	○				

[Table 5-11] Security function behavior of administrator

FMT_MTD.1	TSF 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*** [TSF data and management ability of [Table 5-11]] to [Administrator].

FMT_PWD.1	Management of ID and password (Extended)
Hierarchical to	No other components.
Dependencies	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].

FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [None] to [None].
FMT_PWD.1.3	The TSF shall provide the capability for *changing the ID and password when the authorized chief administrator accesses for the first time.*

FMT_SMF.1	Specification of management functions
Hierarchical to	No other components.
Dependencies	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [a) Management functions specified in FMT_MOF.1 b) Management functions specified in FMT_MTD.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 [Administrator].
FMT_SMR.1.2	TSF shall be able to associate users and their roles **defined in FMT_SMR.1.1**.

5.1.6 Protection of the TSF (FPT)

FPT_ITT.1	Basic internal TSF data transfer protection
Hierarchical to	No other components.
Dependencies	No dependencies
FPT_ITT.1.1	he 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 dependencies
FPT_PST.1.1	The TSF shall protect [TSF data] stored in the containers controlled by the TSF from unauthorized *disclosure, modification.*

FPT_TST.1	TSF testing
Hierarchical to	No other components.
Dependencies	No dependencies
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of *TSF*.
FPT_TST.1.2	The TSF shall provide the **authorized administrator** with the capability to verify the integrity of *TSF data.*
FPT_TST.1.3	The TSF shall provide the **authorized administrator** with the capability to verify the integrity of *TSF*

5.1.7 TOE Access (FTA)

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 has a list of management functions defined in [FMT_SMF.1.1: a) Limit the maximum number of concurrent sessions to 1 for administrative access by the same administrator who have the authority to p.

b) 'Management behavior' in FMT_MOF.1.1 cannot be performed and 'manage' in FMT_MTD.1.1 maximum number of sessions for the same administrator with the right to perform query only { 1 }.

c) Limit the maximum number of concurrent sessions belonging to the same **Administrator** according to the [None] rule.

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_MCS.2.1	The TSF shall *terminate* the administrator's interactive session after a [10 minutes].

FTA_TSE.1	TOE session establishment
Hierarchical to	No other components.
Dependencies	No dependencies
FTA_TSE.1.1	The TSF shall be able to refuse the **management access session of the administrator**, based on [Access IP, *None*].

5.2 Security Assurance Requirements

Assurance requirements of this Security Target are comprised of assurance components in CC Part3, and the evaluation assurance level is EAL+1. The following table summarizes assurance components.

Security Assurance Class	Security Assurance Component	
Security Target Evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended Component 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 5-12] Security assurance requirements

5.2.1 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 summaries 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.
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.
ASE_CCL.1	**Conformance claims**
	Dependencies : ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements
	Developer action elements
ASE_CCL.1.1D	The developer shall provide a conformance claim
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.

	Content and presentation elements
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
	Evaluator action elements
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies : No dependencies

Developer action elements

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

Content and presentation elements

ASE_OBJ.1.1C The statement of security objective shall describe the security objectives for the operational environment.

Evaluator action elements

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

ASE_ECD.1 Extended component 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 component definition.

Content and presentation elements

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

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

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

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

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

Evaluator action elements

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

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies : ASE_ECD.1 Extended components definition

Developer action elements

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

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements

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

ASE_TSS.1 TOE summary specification

Dependencies : ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

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

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies : No dependencies

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interface as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the

functional specification.

Evaluator action elements

ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies : ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D	The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill 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 provide meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies : No dependencies

Developer action elements

AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST

Evaluator action elements

AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1 TOE Labeling 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 meets 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 followings: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
	Evaluator action elements
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Tests

ATE_FUN.1	**Functional testing**
	Dependencies : ATE_COV.1 Evidence of coverage
	Developer action elements
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the test to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements

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

ATE_IND.1 Independent testing: conformance

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

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

5.3 Security Requirements Rationale

The table below shows dependencies of SFR.

No.	SFR	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.Time Stamp
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	-	OE.DBMS
7	FAU_STG.4	-	OE.DBMS
8	FCS_CKM.1(1)	[FCS_CKM.2 OR FCS_COP1]	10,12
		FCS_CKM.4	11
9	FCS_CKM.1(2)	[FCS_CKM.2 OR FCS_COP1]	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	12,13
16	FDP_RIP.1	-	-
17	FIA_AFL.1	FIA_UAU.1	20
18	FIA_IMA.1	-	-
19	FIA_SOS.1	-	-

20	FIA_UAU.2	FIA_UID.1	23
21	FIA_UAU.4	-	-
22	FIA_UAU.7	FIA_UAU.1	20
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
29	FPT_ITT.1	-	-
30	FPT_PST.1	-	-
31	FPT_TST.1	-	-
32	FTA_MCS.2	FIA_UID.1	23
33	FTA_SSL.5	FIA_UAU.1	20
34	FTA_TSE.1	-	-

[Table 5-13] Rationale of the dependencies

FAU_GEN.1 has a dependency on FPT_STM.1. However, reliable time stamps provided by the security objective OE.TIME_STAMP for the operational environment of this ST are used, thereby satisfying the dependency.

the hash algorithm is an algorithm characteristic, and encryption key generation and destruction are not applied in FCS_CKM.2

FIA_AFL.1, FIA_UAU.7 and FTA_SSL.5 are dependent on FIA_UAU.1, which is satisfied by FIA_UAU.2 in its hierarchical relationship with FIA_UAU.1.

FIA_UAU.2, FMT_SMR.1, FTA_MCS.2 have dependencies on FIA_UID.1, which is satisfied by FIA_UID.2 in its hierarchical relationship with FIA_UID.1.

5.4 Assurance Requirements Rationale

The dependency of the EAL1 assurance package provided in Common Criteria for Information Technology Security Evaluation is already satisfied, therefore details into its rationale are excluded.

ATE.FUN.1, which is an augmented assurance requirement, includes ATE_COV.1 by dependency.

ATE_FUN.1 was added to ensure that the developer accurately tests the testing items and records them in the test paper. ATE_COV.1 was not added to this ST, as the proof of consistency between the testing items and the TSFI was not deemed strictly necessary.

6. TOE Summary Specification

This chapter provides detailed explanation on the security functions of the TOE and how the TOE satisfies the SFRs. [Table 6-1] below shows all the security functional components of the TOE.

Security Functional Class	Security Functional Component	
Security Audit (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
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(Extended)	Random bit generation
User Data Protection (FDP)	FDP_UDE.1(Extended)	User data encryption
	FDP_RIP.1	Subset residual information protection
Identification and Authentication (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
Security Management (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
Protection of the TSF (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
TOE Access (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 6-1] List of security functions of the TOE

6.1 Security audit

6.1.1 Audit data generation

The TOE can generate audit data by combining success and failure, and form successful encryption events or unsuccessful decryption events, etc. (FAU_GEN.1).

The default value is set to generate logs on all successful and unsuccessful encryption and decryption events. The authorized administrator can set the condition for audit data generation, based on whether encryption/decryption is successful.

Security Functional Component	Auditable Event
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
FCS_CKM.2	Success and failure of the activity (applied only to distribution of key related to encryption/decryption of user data)
FCS_CKM.4	Success and failure of the activity (applied only to the destruction of key related to encryption/decryption of user data)
FCS_COP.1(1)	Success and failure of cryptographic operation, type of cryptographic operation
FDP_UDE.1	Success and failure of encryption/decryption of user data
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/failure of mutual authentication, modification of authentication

	protocol
FIA_UAU.2	User authentication before any action
FIA_UAU.4	Single-use authentication mechanisms
FIA_UID.2	User identification before any action
FMT_MOF.1	All modification in the behavior of the functions in the TSF
FMT_MTD.1	All modifications to the 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
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

[Table 6-2] Auditable events of the TOE

All TOE components generate audit data on the auditable events listed in [Table 6-2], including audit records such as date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event (FAU_GEN.1).

Regarding audit events shown in [Table 6-3], the TOE generates audit data in [Table 6-2] and additional audit records in [Table 6-3] (FAU_GEN.1).

Audit Event	Additional Audit Record
All modification on TSF data	Modified value of TSF data
Execution of TSF self-tests and the result	Modified TSF data or executable code in case of integrity violation

[Table 6-3] Additional audit record for certain audit events

※ SFR to be satisfied

FAU_GEN.1

6.1.2 Audit data review

The authorized administrator can review audit data stored in the audit storage in the local DB in the "View Log" menu of the administrator's page. Audit data files generated in all TOE components store data in the local DB by the Policy Server located on the same physical server as TOE components. If the authorized administrator requests audit data stored in the local DB through the security management interface provided by the Policy Server, the Policy Server searches audit data stored in the local DB and provides the function of review or selective review of audit data collected from the entire data. The authorized administrator can view audit data by using the selective searching on the basis of keywords or a combination of the criteria that have logical relations (identity of the subject, object, date and time of the event, and type of the event). Search results of audit data are sorted and provided in a descending order according to the date and time of the event.

※ SFR to be satisfied

FAU_SAR.1, FAU_SAR.3

6.1.3 Potential violation analysis and action

Audit data in all TOE components generated as described in FAU_GEN.1 are stored in the local DB by the Policy Server. The Policy Server generates a security alarm if the administrator authentication fails; if the authentication fails for a defined number of times; if the audit trail storage capacity is full or exceeds the predefined threshold; if the verification of the integrity of TOE configuration files fails; if the verification of major security functional processes fails; or if self-tests of the validated cryptographic module fail.

If the Policy Server receives the audit of integrity violation among auditable events in FPT_TST.1, it shall view the event immediately (FAU_SAA.1).

In case of the audit of potential violation, the Policy Server sends a security alarm email to the email address designated by the authorized administrator and generates audit data. In the Agent Server, an error message on an audit event of a potential violation that can occur during initial start-up is displayed on the screen (FAU_ARP.1).

※ SFR to be satisfied

FAU_ARP.1, FAU_SAA.1

6.1.4 Protected audit trail storage and action in case of possible audit data loss

The Policy Server periodically monitors the threshold of the number of audit data and the space used in the local DB to store audit data (FAU_STG.3, FAU_STG.4).

If the threshold of the number of audit data or the space used in the local DB checked by the Policy Server exceeds a defined limit, it sends a security alarm to the email address designated by the administrator and generates audit data.

The authorized administrator can set the limit ranging from at least 60% up to 90% for the threshold of the number of audit data and the DB table space (FAU_STG.3).

If the number of audit data in the local DB or the space used in the local DB exceeds the threshold of 90%, the Policy Server overwrites the oldest audit records, sends a security alarm email and generates audit data (FAU_STG.4).

※ SFR to be satisfied

FAU_STG.3, FAU_STG.4

6.2 Cryptographic support

The TOE generates random bits necessary for cryptographic key generation by using HASH_DRBG (256 bits) algorithm through the random bit generator of MagicCrypto V2.2.0, the validated cryptographic module whose security and implementation conformance have been validated by the cryptographic module validation scheme.

Cryptographic support of the TOE is possible through the cryptographic key and DB encryption policy established by the authorized administrator for the purpose of the protection of the TSF data. Encryption/decryption of user data according to the DB encryption policy established by the authorized administrator is performed through the plug-in provided in the Agent Server, and is destructed safely by using the zeroization function immediately after the use.

Random bit generation and all cryptographic support functions are performed by using the encryption algorithm of the validated cryptographic module as shown in [Table 6-4].

Validated Cryptographic Module	Cryptographic module name	MagicCrypto V2.2.0
	Developer (institutions)	Dream Security
	Validation date	March 3, 2020
	Validation level	VSL1
	Validation number	CM-162-2025.3
	Library	libMagicCrypto.so

[Table 6-4] Validated cryptographic module

6.2.1 Cryptographic key generation

A user data key (key for the user data encryption) is generated on the Policy Server in accordance with the approved cryptographic algorithm in [Table 6-5] and the key size in [Table 6-5] if the authorized administrator generates it through the administrator's page (FCS_CKM.1(1)).

Standard List	Cryptographic Algorithm	Key Size	Use

ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- Generation of cryptographic key for user data

[Table 6-5] Cryptographic key generation algorithm for user data encryption

TSF data such as security policies and encryption keys are encrypted by using the cryptographic algorithm of the validated cryptographic module.

A cryptographic key for TSF data encryption is generated in accordance with the cryptographic algorithm in [Table 6-6] and the key size in [Table 6-6] that meet the list of standards in [Table 6-6] (FCS_CKM.1(2)).

Standard List	Cryptographic Algorithm	Key Size	Use
ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- KEK generation - Generation of cryptographic key for TSF data

[Table 6-6] Cryptographic key generation algorithm for TSF data encryption

※ SFR to be satisfied

FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1(Extended)

6.2.2 Cryptographic key distribution

The Policy Server distributes an encryption key required by each component so that the TOE can protect TSF data and user data accurately.

Cryptographic key distribution between TOE components follows the policy in [Table 6-7] (FCS_CKM.2).

Standard List	TOE (Sender)	TOE (Receiver)	Cryptographic Key	Distribution Method
ISO/IEC 10118-3, TTAS.KO-12.0004/R1	Agent server	Policy Server	Key Encryption Key (KEK)	KEK is encrypted by using a session key, and distributed from the Agent Server to the Policy Server.
ISO/IEC	Policy Server	Agent server	User Data	User data encryption key is

10118-3, TTAS.KO-12.0004/R1			Encryption Key	encrypted by using a session key, and distributed from the Policy Server to the Agent Server. .

[Table 6-7] Cryptographic key distribution method

※ SFR to be satisfied

FCS_CKM.2

6.2.3 Cryptographic key destruction

At the time of the destruction of a cryptographic key (immediately after the user data encryption/decryption operation or immediately after the mutual authentication is removed), the TOE initializes the allocated cryptographic key with "0" and deallocates the used memory area to destruct the cryptographic key (FCS_CKM.4).

※ SFR to be satisfied

FCS_CKM.4

6.2.4 Cryptographic operation

In cryptographic operation provided by the TOE, the operation on user data in [Table 6-8] is performed in accordance with the cryptographic algorithm in [Table 6-8] and cryptographic key size in [Table 6-8]. In the list of standards in [Table 6-8], cryptographic algorithms in the validated cryptographic module are used (FCS_COP.1 (1)).

Standard List	Cryptographic Algorithm	Key Size	Operation Mode	Padding	Operation
KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	- Encryption/decryption of user data
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	- Encryption/decryption of user data
ISO/IEC 10118-3	SHA512	None	None	None	- Encryption of user data

[Table 6-8] Cryptographic operation of user data

In cryptographic operation provided by the TOE, the operation on the TSF data in [Table 6-9] is performed in accordance with the cryptographic algorithm in [Table 6-9] and cryptographic key size in [Table 6-9]. In the list of standards in [Table 6-9], cryptographic algorithms in the validated cryptographic module are used (FCS_COP.1 (2)).

Standard List	Cryptographic Algorithm	Key Size	Operation Mode	Padding	Operation
KS X 1213-1	ARIA	256 bits	CBC	PKCS#5	- Inter-TSF cryptographic communication - Encryption/decryption of environment configuration file - Encryption/decryption of TSF data
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	- Encryption/decryption of KEK
ISO/IEC 10118-3	SHA512	None	None	None	- Integrity check of the TOE - Generation of SALT value of KEK - Generation of SALT value of session key - Mutual verification of session key - Inter-TSF cryptographic communication - Encryption of administrator password
ISO/IEC 18033-2	RSAES (SHA-256)	2048 bits	None	None	- Inter-TSF mutual authentication
ISO/IEC 14888-2	RSA-PSS (SHA-256)	2048 bits	None	None	- Inter-TSF mutual authentication
ISO/IEC 11770-3	ECDH (SHA-256)	256 bits	None	None	- Inter-TSF mutual authentication
TTAS.KO-12.0334	PBKDF2 (SHA-256)	256 bits	None	None	- KEK generation

[Table 6-9] Cryptographic operation of TSF data

The usage of cryptographic key generation algorithm, hash, block cipher, public key cryptography, electronic signature, key derivation and key setting are shown in [Table 6-10] below.

Classification	Standard List	Cryptographic Algorithm	Key Size	Use
Cryptographic key generation	ISO/IEC 18031	Hash-DRBG(SHA256)	128/256 bits	- KEK generation - Generation of cryptographic key for TSF data - Generation of cryptographic key for user data
Hash	ISO/IEC 10118-3	SHA512	None	- Integrity monitoring of the TOE - Generation of SALT value of KEK - Generation of SALT value of session key - Mutual verification of session key - User data encryption - Inter-TSF cryptographic communication - Encryption of administrator password
Block cipher (CBC mode)	KS X 1213-1	ARIA	256 bits	- Encryption/decryption of user data - Inter-TSF cryptographic communication - Encryption/decryption of environment configuration file

				- Encryption/decryption of TSF data
	TTAS.KO-12.0004/R1	SEED	128 bits	- Encryption/decryption of KEK - Encryption/decryption of user data
Public key cryptography	ISO/IEC 18033- 2	RSAES (SHA-256)	2048 bits	- Inter-TSF mutual authentication
Electronic signature	ISO/IEC 14888-2	RSA-PSS (SHA-256)	2048 bits	- Inter-TSF mutual authentication
Key setting	ISO/IEC 11770-3	ECDH (SHA-256)	256 bits	- Inter-TSF mutual authentication
Key derivation	TTAS.KO-12.0334	PBKDF2 (SHA-256)	256 bits	- KEK generation

[Table 6-10] Usage of key applied to the TOE

※ SFR to be satisfied

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

6.3 User data protection

The TOE provides the function of column-level encryption/decryption of the data stored in the DBMS to be protected through the validated cryptographic module MagicCrypto V2.2.0. The same ciphertext is not generated for the same plaintext when encrypting the user data.

In addition, it deletes all the original user data in plaintexts after user data encryption/decryption in order to protect the user data.

The authorized administrator sets the DB encryption policy in the Policy Server. The Agent Server performs two-way encryption and one-way encryption of user data in accordance with the DB encryption/decryption policy set in the Policy Server (FDP_UDE.1 (Extended)).

Cryptographic algorithms listed in FCS_COP.1(1) are used for the encryption/decryption of user data. SHA-512 is provided for one-way cryptographic algorithm (FDP_UDE.1 (Extended)).

After the encryption/decryption is completed, the memory area is initialized with "0" value and the used memory area is deallocated so that the user data are unrecoverable in the memory (FDP_RIP.1).

※ SFR to be satisfied

FDP_UDE.1(Extended), FDP_RIP.1

6.4 Identification and authentication

The identification and authentication function offered by the TOE is to provide mutual authentication between TOE components and the identification and authentication of the administrator in order to access the administrator's page on the Policy Server.

6.4.1 Identification and authentication of the administrator

The identification and authentication shall be performed successfully before allowing access to and control of the administrator's page provided by the Policy Server (FIA_UAU.2).

The TOE satisfies the hierarchical levelling of FIA_UAU.2 by performing the identification and authentication based on the administrator ID/password (FIA_UAU.1).

During the authentication of the administrator, the password entered is masked (*) to make it unrecognizable on the screen. If the authentication fails, only the authentication failure message that states "You are not a registered user or your password does not match" is provided (FIA_UAU.7).

The Policy Server blocks access attempts for the account for 10 minutes (fixed value), and if authentication attempts fail consecutively (default value: 5 times) for the defined number of times, it stores audit records on the authentication failure (FIA_AFL.1).

For the administrator password, the verification mechanism is provided to satisfy the allowable criteria as defined below (FIA_SOS.1).

- Password length: at least 9 digits up to 20 digits
- Password combination rule: A combination of alphabetic characters (52 characters: a~z, A~Z), numeric characters (10 characters: 0-9) and special characters (32 characters: :`~! @ # $ % ^ & * () -_ + = [] {} ₩ |; : '",. <> /?)

In addition, the reuse of authentication data is prevented by using time stamps in order to ensure the uniqueness of session ID of the administrator (FIA_UAU.4).

When the Policy Server is installed, an account (ID and password) and allowed IP are registered for the authorized administrator to generate the his/her information. Before the authorized administrator performs the security management function on the Policy Server,

the unique session ID authenticated to be the administrator needs to be checked to confirm whether he/she was authenticated as the administrator (FIA_UID.2).

※ SFR to be satisfied

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

6.4.2 Mutual authentication

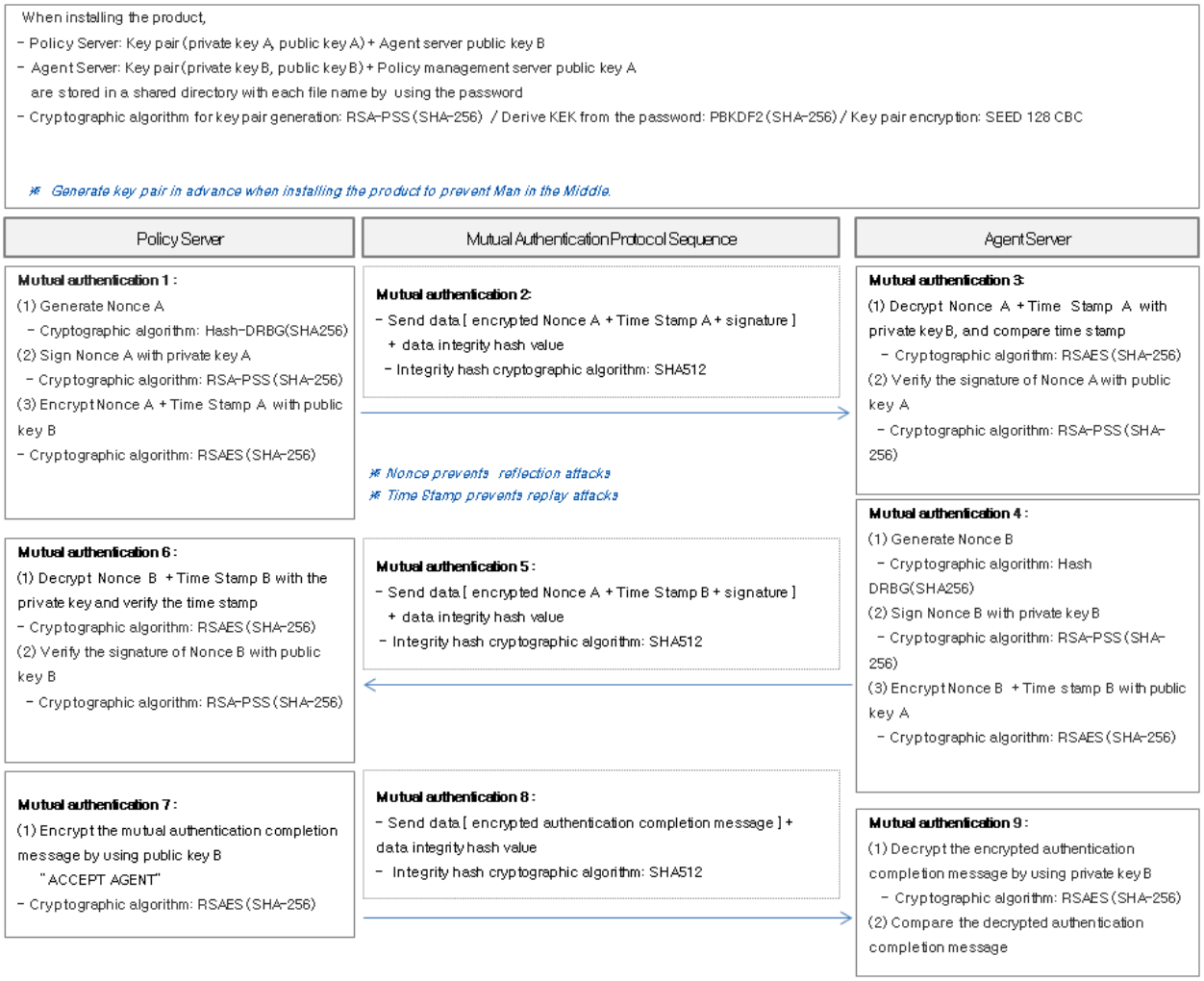
Ahead of the communication between TOE components, the TOE performs the mutual authentication through the mutual signature verification by using a private key and a public key issued between the Policy Server and the Agent Server in real time. The process of the mutual authentication between TOE components is shown in [Table 6-11] below.

Step	Sender	Receiver	Mutual Authentication Procedure
1	Policy Server	-	(1) Generate Nonce A based on the cryptographic algorithm Hash-DRBG(SHA256). (2) Sign Nonce A with the private key of the Policy Server based on cryptographic algorithm RSA-PSS (SHA-256). (3) Encrypt Nonce A and the time stamp of the Policy Server by using the public key of the Agent Server based on cryptographic algorithm RSAES (SHA-256).
2	Policy Server	Agent server	Send the data encrypted in step 1 and data hash value based on the cryptographic algorithm SHA 512.
3	-	Agent server	(1) Decrypt Nonce A and the time stamp by using the private key of the Agent Server based on cryptographic algorithm RSAES (SHA-256). (2) Compare the time stamp with the time stamp of the Agent Server by applying Clock Skew. (3) Verify the signature of Nonce A with the

			public key of the Policy Server based on cryptographic algorithm RSA-PSS (SHA-256).
4	-	Agent server	(1) Generate Nonce B based on cryptographic algorithm Hash-DRBG(SHA256). (2) Sign Nonce B with the private key of the Agent Server based on cryptographic algorithm RSA-PSS (SHA-256). (3) Encrypt Nonce B and the time stamp of the Agent Server by using the public key of the Policy Server based on cryptographic algorithm RSAES (SHA-256).
5	Agent server	Policy Server	Send the data encrypted in step 4 and data hash value based on the cryptographic algorithm SHA 512.
6	-	Policy Server	(1) Decrypt Nonce B and the time stamp by using the private key of the Policy Server based on cryptographic algorithm RSAES (SHA-256). (2) Compare the time stamp with the time stamp of the Policy Server by applying Clock Skew. (3) Verify the signature of Nonce B with the public key of the Agent Server based on cryptographic algorithm RSA-PSS (SHA-256).
7	-	Policy Server	Encrypt the mutual authentication completion message by using the public key of the Agent Server based on cryptographic algorithm RSAES (SHA-256).
8	Policy Server	Agent server	Send the data encrypted in step 7 and data hash value based on the cryptographic algorithm SHA 512.
9	-	Agent server	Decrypt the mutual authentication completion message by using the private key of the Agent Server based on cryptographic

			algorithm RSAES (SHA-256), and check the mutual authentication completion message.
After the mutual authentication is completed, a session key is generated based on cryptographic algorithm ECDH (SHA-256), and message encryption communication is performed based on cryptographic algorithm ARIA 256 CBC.			

[Table 6-11] TOE internal mutual authentication procedure



[Figure 6-1] Diagram of TOE internal mutual authentication procedure

※ SFR to be satisfied

FIA_IMA.1

6.5 Security management

6.5.1 Security roles

The administrator is entitled to be the top administrator in charge of all security roles in the Policy Server of the TOE (FMT_SMR.1).

※ SFR to be satisfied

FMT_SMR.1

6.5.2 Management of security functions behaviour

The security functions that the TOE provides for the administrator is shown in [Table 6-12]. The basic setting items in [Table 6-12] are set as default when the TOE is installed.
(FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1)

Security functions (Policy Server)	Management Type				
	Basic	Query	Insert	Modify	Delete
Set the administrator's email address for the detection of a potential violation	○	○		○	
Apply a set of rules to audit events	○				
View audit records	○	○			
Maintain the threshold on audit data	○	○		○	
Manage actions to be taken in case of imminent audit storage failure	○				
Manage the policy to overwrite the oldest records in case of audit storage failure	○				
Manage the rule for user data encryption/decryption		○	○	○	○
Manage the threshold for unsuccessful authentication attempts	○	○		○	

Manage the authentication protocol for mutual authentication	○				
Manage the quality metrics used to verify passwords	○				
Manage the group of roles that can interact with the functions in the TSF	○				
Manage the group of roles that can interact with TSF data	○				
Manage the rules for ID and password setting	○				
Manage the group of users that are part of a role	○				
Manage the types of modification against which the TSF should protect	○				
Manage the mechanism used to provide the protection of the data in transit between different parts of the TSF	○				
Self-tests and integrity verification on TSF	○				
Terminate a session in case of the administrator inactivity	○				
Number of concurrent sessions of administrator access	○				

[Table 6-12] Security function behavior of administrator

※ SFR to be satisfied

FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.5.3 Management of ID and password

The TOE has only one administrator, and generates an account of the authorized administrator (ID and password) in installing the Policy Server.

The authorized administrator can modify the password of the administrator through the security management interface after the identification and authentication in the Policy Server. The administrator password has at least 9 up to 20 digits in length, and consists of a combination of alphabetic characters (52 characters: a~z, A~Z), numeric characters (10 characters: 0-9) and special characters (32 characters: :`~! @ # $ % ^ & * () -_ + = [] {} ₩ |; : '",. <>) (FMT_PWD.1).

※ SFR to be satisfied

FMT_PWD.1

6.6 Protection of the TSF

The TOE protects TSF by using the cryptographic algorithm of "MagicCrypto V2.2.0" which is the validate cryptographic module.

6.6.1 Basic internal TSF data transfer protection

For the encrypted transmission of the TSF data between TOE components, the TSF data are protected from unauthorized disclosure and modification by encrypting/decrypting the data in transit (TSF data + SHA512HASH value of the TSF data) with ARIA-256-CBC cryptographic algorithm. If the integrity violation is detected regarding the hash value of the received TSF data, the TSF ignores the received data ad generates audit data on this event (FPT_ITT.1).

※ SFR to be satisfied

FPT_ITT.1

6.6.2 Basic protection of stored TSF data

The TOE protects stored TSF data by performing the protection in [Table 6-13] to protect TSF data in [Table 6-13] stored in TOE component in [Table 6-13].

The encryption to protect the TSF data is conducted by using "MagicCrypto V2.2.0" which is the validated cryptographic module (FPT_PST.1 (Extended)).

TOE Component	TSF Data	Protection Method
Policy Server	Administrator password	SHA-512 hash
	DBMS access information	ARIA-256-CBC encryption
	Authentication authority key	ARIA-256-CBC encryption
	Mutual authentication session key	ARIA-256-CBC encryption
Agent server	Key encryption key (KEK)	SEED-128-CBC encryption
	User data key	ARIA-256-CBC encryption
	Mutual authentication session key	ARIA-256-CBC encryption

[Table 6-13] TSF data protection method

※ SFR to be satisfied

FPT_PST.1 (Extended)

6.6.3 Self tests

The TOE runs a suite of self tests (self tests of the validated cryptographic module, integrity verification of executable files and configuration of TOE components, and process status check) upon initial start-up of each component. Self tests are carried out periodically after initial start-up, and the results of self tests are stored in the DB. If self tests fail, the TOE component is disabled, and an alarm is sent to the email address set by the authorized administrator. In addition, the authorized administrator can access the Policy Server through a web browser, and verify the integrity of executable files and configuration files of TOE components.

If self tests fail, an alarm email is sent and the failure is recorded as audit data. Then, the process is disabled immediately. The authorized administrator can carry out self tests on the administrator's page, if necessary.

Self test items for each TOE component are listed in [Table 6-14], TSF data integrity verification items for the TOE in [Table 6-15], and TSF integrity verification items for the TOE in [Table 6-16]. Self tests are performed in the same manner regardless of the operational environment of the physical server where the TOE is installed (FPT_TST.1).

TOE Component	Timing of Self Tests	Verification Item
Policy Server	- When the process starts - At 1-hour interval after the initial start-up - At the request on the administrator's page	- Library module - Validated cryptographic module - Process
Agent server	- When the process starts - At 1-hour interval after the initial start-up	- Library module - Validated cryptographic module - Process

[Table 6-14] Self test items for each TOE component

TOE Component	Timing of Integrity Verification	Verification Item
Policy Server	- When the process starts - At 1-hour interval after the initial start-up - At the request on the administrator's page	- TSF data (Local Key)
Agent server	- When the process starts - At 1-hour interval after the initial start-up	- TSF data (Local Key)

[Table 6-15] TSF data integrity verification items

TOE Component	Timing of Integrity Verification	Verification Item
Policy Server	- When the process starts - At 1-hour interval after the initial start-up - At the request on the administrator's page	- Policy Server binary data
Agent server	- When the process starts - At 1-hour interval after the initial start-up	- Agent server binary data

[Table 6-16] TSF integrity verification items

※ SFR to be satisfied

FPT_TST.1

6.7 TOE access

6.7.1 Limitation on multiple concurrent sessions

The maximum number of concurrent session by the authorized administrator to the Policy Server is limited to one in order to block concurrent access sessions that belong to the same administrator.

If the same account makes new access, the existing session is terminated (FTA_MCS.2).

※ SFR to be satisfied

FTA_MCS.2

The TOE allows the management sessions made only from a device (2 or less) whose IP was designated and allowed to access, and generates audit data on the result of the limitation of sessions by the security management interface.

6.7.2 Session management and establishment

The TOE restricts TOE access to ensure that access to the management interface is made only from the registered IP addresses. If the authorized administrator remains inactive for 10 minutes, the session is automatically terminated (FTA_SSL.5 (Extended), FTA_TSE.1).

In installing the TOE, the number of accessible IPs of an administrator device is set as 2 or less, and the management access session is denied if access is made from an unauthorized IP (FTA_TSE.1).

※ SFR to be satisfied

FTA_SSL.5 (Extended), FTA_TSE.1