Realize your vision

Samsung SDS Database Encryption ST v1.3

Security Target

2020. 02. 18

Samsung SDS

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

SAMSUNG SDS SAMSUNG

Revision history

Document name		Samsung SDS Database Encryption ST v1.3 (Security Target)	
Version	Date	Content	Prepared by
1.0	2019.10.01	Draft	D.J. Moon
1.1	2020.01.13	Update chapter 6. TOE Summary Specification	K.Y Kim
1.2	2020.01.23	Modification of obsolete standard documents defined in "5.1.2 Cryptographic Support".	K.Y Kim
1.3	2020.02.18	Update API-type operational environment	K.Y Kim

Contents

1 ST Introduction

1.1 ST Reference

Classification	Description
Title	Samsung SDS Database Encryption ST
Version	v1.3
Author	Samsung SDS Co., Ltd
Publication Date	February 18, 2020
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria Version	V3.1 r5
Evaluation Assurance Level	EAL 1+ (ATE_FUN.1)
Keyword	Database Encryption, Encryption

1.2 TOE Reference

Classification	Identifier Information
TOE	Samsung SDS Database Encryption v1.0
Detail Version	v1.0.2
TOE Components	Samsung SDS Database Encryption Server v1.0.2
	Samsung SDS Database Encryption Client v1.0.2
Guidance	Samsung SDS Database Encryption PRE v1.3
	Samsung SDS Database Encryption OPE v1.1

1.3 **TOE Overview**

Samsung SDS Database Encryption v1.0 (hereinafter referred to as 'TOE') is a product that encrypts protected databases to prevent unauthorized disclosure of the information to be protected. TOE consists of Samsung SDS Database Encryption Server v1.0.2 (hereinafter referred to as 'Management Server') and Samsung SDS Database Encryption Client v1.0.2 (hereinafter referred to as 'Client Module').

1.3.1 TOE usage and major security features

The TOE is used to encrypt the user data according to the policy set by the authorized administrator to prevent the unauthorized disclosure of the confidential information. In order that the authorized administrator can operate the TOE securely in the operational environment of the organization, the TOE provides various security features such as 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 the user data and protects the residual information; identification and authentication function such as verifying 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 functions 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-test; and TOE access function to manage the access session of the authorized administrator.

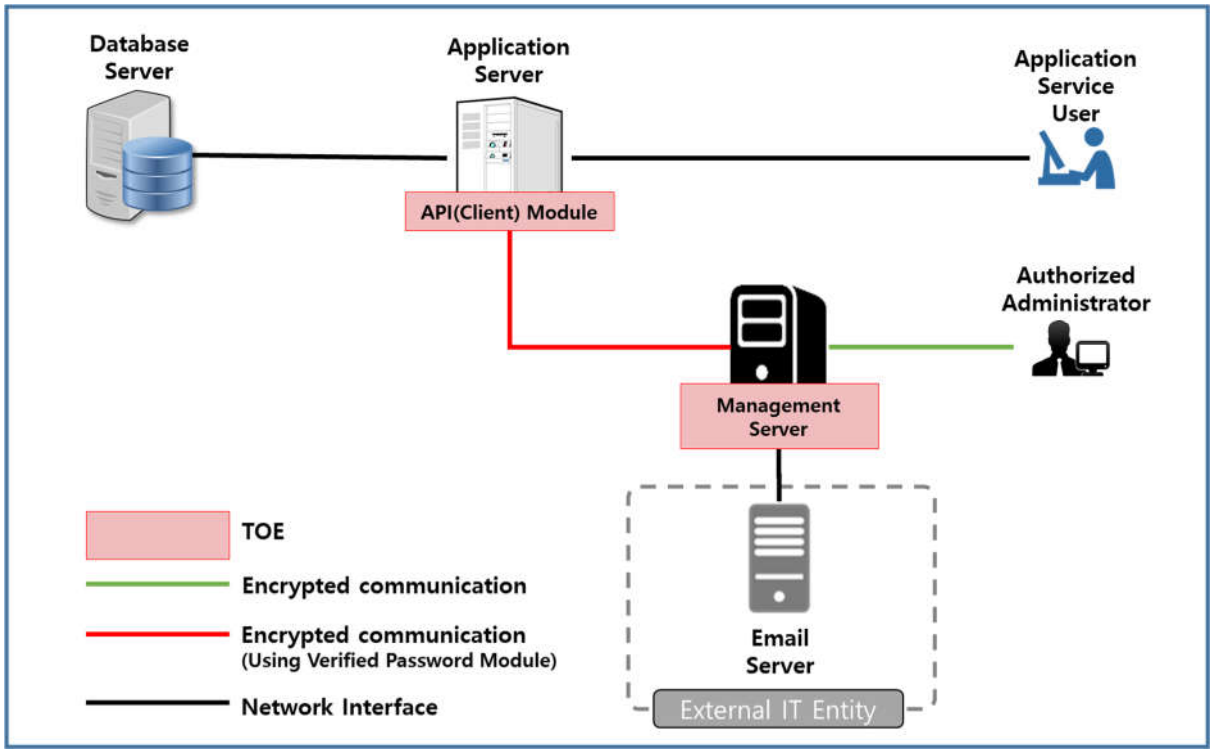
1.3.2 TOE type and scope

The TOE is provided as software and provide the encryption/decryption function for the user data by each column. The TOE type defined in this ST can be grouped into the 'API type', depending on the TOE operation type and TOE consist of management server and Client module.

The application, which is installed in the application server and provides application services, is developed using the API provided by client module in order to use the cryptographic function of the TOE. The client module is installed in the application server and performs encryption/decryption of the user data in accordance with the policies configured by authorized administrator. The user data entered by the application service user is encrypted by the client module, which is installed in the application server, and sent to the database server. The encrypted user data received from the

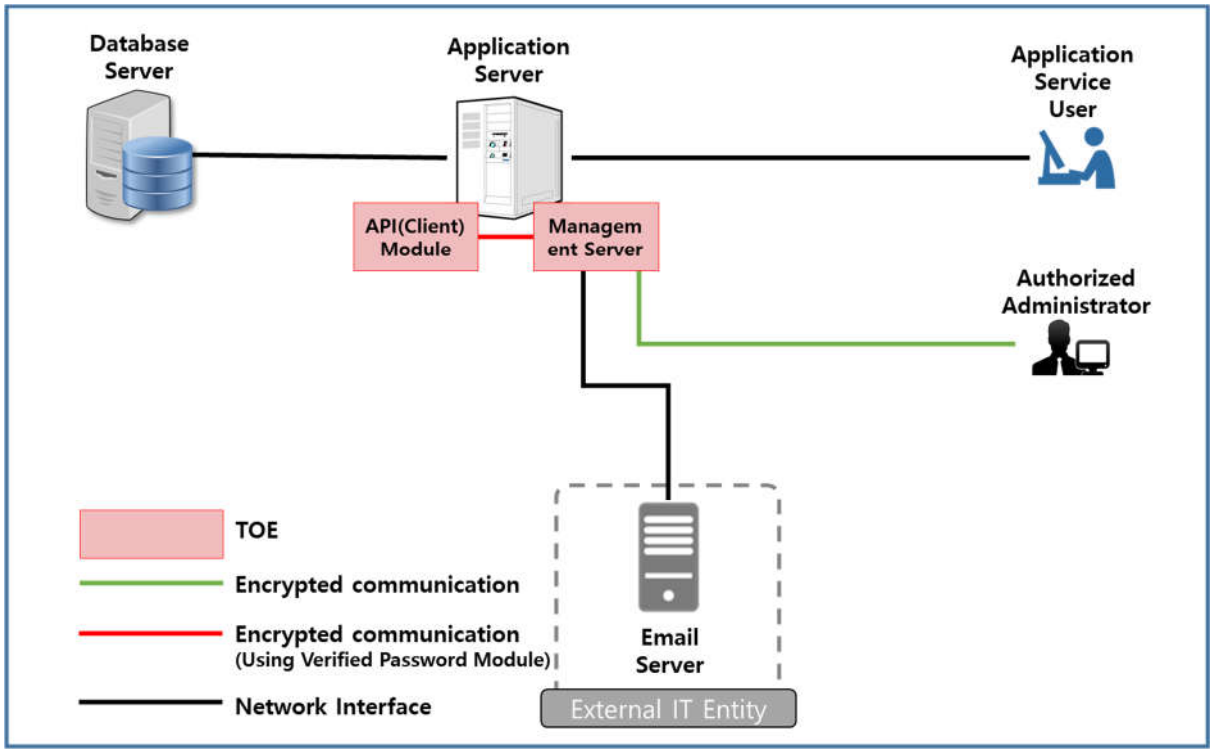
database server is decrypted by the client module, which is installed in the application server, and sent to the application service user. The authorized administrator performs security management through access to the management server, and the management server performs the encryption/decryption of the user data, security management function, and cryptographic key management function. The management server can be installed in the application server along with the agent, or installed separately from the API module.

[Figure 1] shows the operating environment of 'API Module, Separate Management Server separate type', 'API Module, Separate Management Server separate type' means that the client module is installed in the application server and the management server is physically separated.



[Figure 1] API-type operational environment (API module, management server separate type)

[Figure 2] shows the operating environment of 'API module, management server integrated type'. ' API module, management server integrated type' installs client module and management server together in Application Server.



[Figure 2] API-type operational environment (API module, management server integrated type)

The communication among the TOE components shall be based on the encrypted communication using the approved cryptographic algorithm of the validated cryptographic module. Even though the TOE is operated as an integrated type, the TSF data shared among the TOE components through the encrypted communication using the validated cryptographic module.

The external IT entity needed to operate the TOE includes email server to notify the authorized administrator in case of audit data loss.

1.3.3 Non-TOE operational environment

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

Classification	Item		Specification
Management Server	H/W	CPU	Intel Core i7-4710HQ 2.5 GHz or higher
		RAM	8 GB Memory or higher
		HDD	Space required for TOE Installation is 20 GB or higher
		NIC	10/100/1000 Mbps NIC * 1 EA or higher
	S/W	OS	Microsoft Windows Server 2016 Standard 64 bit CentOS 6.10 64bit (Kernel 2.6)

			CentOS 7.7 64bit (Kernel 3.10)
		JRE	JRE 8
		DBMS	PostgreSQL 10.10
		WAS	Tomcat 8.5.49
Client Module	H/W	CPU	Intel Core i7-4710HQ 2.5 GHz or higher
		RAM	8 GB Memory or higher
		HDD	Space required for TOE Installation is 10 GB or higher
		NIC	10/100/1000 Mbps NIC * 1 EA or higher
	S/W	OS	Microsoft Windows Server 2016 Standard 64 bit CentOS 6.10 64bit (Kernel 2.6) CentOS 7.7 64bit (Kernel 3.10)
		JRE	JRE 7, JRE 8

The minimum specifications for hardware and software required for authorized administrator's PC are as follows.

Classification		Item	Specification
Administrator PC	H/W	CPU	Intel Core i7-4710HQ 2.5 GHz or higher
		RAM	4 GB Memory or higher
		HDD	Space required is 10 GB or higher
		NIC	10/100/1000 Mbps NIC * 1 EA or higher
	S/W	OS	Microsoft Windows 10 Enterprise 64 bit
		Browser	Internet Explorer 11 Chrome 79 Firefox 72

External IT entities required for the operation of the TOE are as follows.

Classification	Description
Mail Server	Server for sending mail to authorized administrators when a potential security breach is detected.

1.4 TOE Description

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

1.4.1 Physical scope of the TOE

The TOE consists of Management Server, Client Module, Preparative Procedures and Operational Guidance. The Management Server provides the functions to manage administrator roles, encryption keys, audit records and system configurations and the Client Module provides the functions for encryption and decryption for user data. The hardware, OS and software on which the TOE is installed are not included in the scope of the TOE.

[Table 1] Physical scope of TOE

Classification	Contents		Type	Distribution
TOE Component	Management Server	Samsung SDS Database Encryption Server v1.0.2 · SDBE-Server-v1.0.2-CentOS-jre8.zip · SDBE-Server-v1.0.2-Windows-jre8.zip	S/W	CD
	Client Module	Samsung SDS Database Encryption Client v1.0.2 · SDBE-Client-v1.0.2-CentOS-jre7.zip · SDBE-Client-v1.0.2-CentOS-jre8.zip · SDBE-Client-v1.0.2-Windows-jre7.zip · SDBE-Client-v1.0.2-Windows-jre8.zip	S/W	CD
Guidance Documents	Preparative Procedure	Samsung SDS Database Encryption PRE v1.3 · SDBE-v1.3-PRE.pdf	PDF	CD
	Operation Guide	Samsung SDS Database Encryption OPE v1.1 · SDBE-v1.1-OPE.pdf		

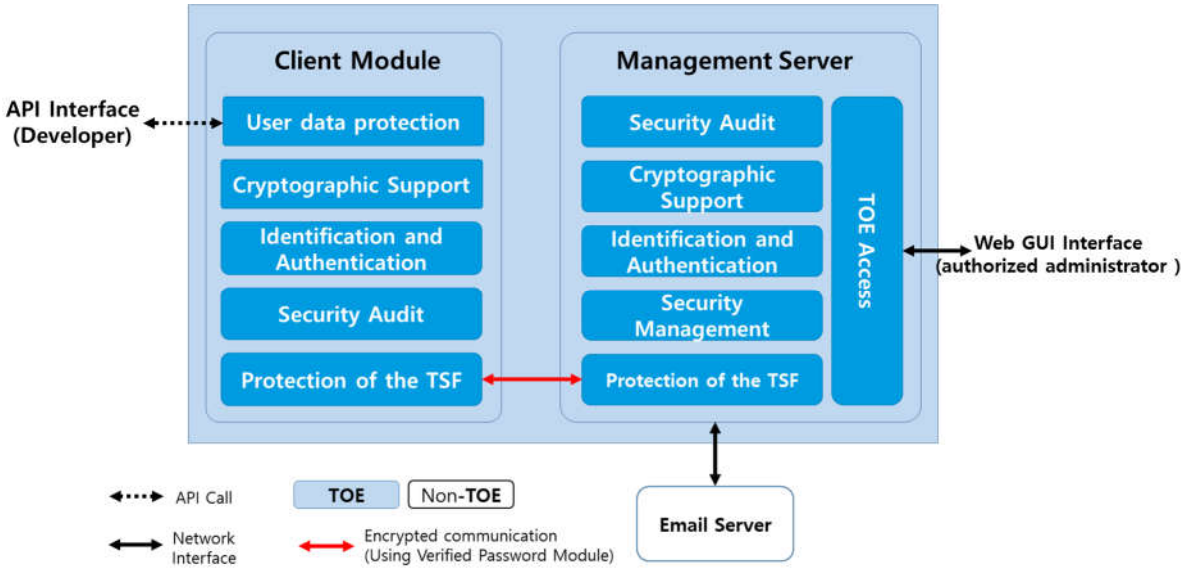
In addition, the verified cryptographic modules required to perform the encryption / decryption functions provided by the TOE are as follows and are included in the scope of the TOE.

Classification	Contents
Crypto Module Name	MagicJCrypto V2.0.0.0
Verification Number	CM-131-2022.10

Developer	Dreamsecurity Co.,Ltd.
Verification Date	2017-10-16
Expiration date	2022-10-16

1.4.2 Logical scope of the TOE

The logical scope of the TOE is shown in following [Figure 3].



[Figure 3] TOE Logical scope and boundary

Security Audit

When auditable events occur in the client module and the management server, the management server writes an audit record to the audit trail storage and sends a warning mail to the system administrator if the audit event is a potential security violation. Audit record contains information about the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. All generated audit data is securely managed to provide the ability for authorized administrators to search and review, and to prevent unauthorized deletion of audit data. Based on the type of event and outcome of the event, it is possible to select the set of events to be audited from the set of all auditable events. If the audit trail storage exceeds 90%, an alert mail is sent to the administrator. It also provides the ability to send alert mail to administrators when the audit trail is full and to prevent the loss of audit data by overwriting the oldest stored audit records.

Cryptographic Support

The TOE, to protect user data and transmitted data between TOE components, generates and distributes all cryptographic keys and performs cryptographic operations using the approved cryptographic algorithm of the validated cryptographic module 'MagicJCrypto V2.0.0.0' whose safety and implementation conformance are validated by the Korea Cryptographic Module Validation

Program (KCMVP). The cryptographic key is overwritten with “0” for destruction.

User data protection

The Client Module performs encryption and decryption for important data in user database by each column accordance with the policies that authorized administrator set. The origin data is removed after the performances of encryption or decryption without being stored to prevent reuse.

Identification and Authentication

Management Server and Client Module the physically separated TOE components communicate with each other performing a mutual authentication through the validated cryptographic module “MagicJCrypto V2.0.0.0" and a standard protocol.

The management server performs identification and authentication based on ID / password before all actions of the administrator who wants to use the security management function, and provides a function to protect authentication feedback on authentication data input. The password should be set to 9 or more and less than 15 digits combining all three types of alphabets, numbers and special characters. If the number of consecutive authentication failures reaches the defined number (default : 5 count), the management server would block account access for five minutes in the case of a system administrator accounts. Whereas in the case of account of policy administrator or audit administrator, it would change the account status to 'locked' and prevent further attempts until system administrator changes the account's status back as 'unlocked'. The management server blocks attempts to reuse of authentication data by generating a new session ID and keeping it as an authentication session when authentication and identification of an authorized administrator has been successfully completed.

Security Management

TOE provides the function of changing password when the first access of authorized administrator and offers the functions to manage security functions and a list of TSF data. There are three types of authorized administrator; system administrator, policy administrator, audit administrator.

Protection of the TSF

TOE performs a suite of self tests and integrity checks during initial start-up, periodically during normal operation to demonstrate the correct operation of TOE process, TSF data and executable TSF codes and sends an alarm mail to system administrators once the self tests and integrity checks fails. TOE performs a test on the external entities at start-up or at the request of an authorized

administrator. TOE uses the validated cryptographic module "MagicJCrypto V2.0.0.0" to protect TSF data and TOE configurations (security policies, system settings and critical security arguments) transmitted between TOE components from the unauthorized disclosure, modification.

TOE Access

When an authorized administrator has logged in, TOE provides a function to check whether the number of sessions per administrator role exceeds the maximum concurrent session and maintain the number of concurrent sessions through terminating previous connection. The TOE also provides a function to terminate with forced inactive sessions remain above the allowed time(default : 10 min) and deny attempted the administrator access from unacceptable remote addresses.

1.5 **Terms and definitions**

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

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

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

Approved mode of operation
The mode of cryptographic module using approved cryptographic algorithm.

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

Assignment
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].

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

Audit Administrator
One of the authorized administrators authorized to operate and manage a TOE safely, who only has privilege of audit records searching.

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

Authentication Data
Information used to verify the claimed identity of a user.

Authorized Administrator
Authorized user to operate and manages the TOE securely.

Authorized User
The TOE user who may, in accordance with SFRs, perform an operation.

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

Class
Set of CC families that share a common focus.

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

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

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

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.

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

Data Encryption Key (DEK)
Key that encrypts and decrypts data.

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

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

Dependency
Relationship between components such that if a requirement based on the depending component is included in 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

Element
Indivisible statement of a security need.

Encryption
The act that coverts the plaintext into the ciphertext using the encryption key.

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

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

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

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

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

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

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

Master Key
Key generated by verified cryptographic module to protect KEK, which is stored in the form of file encrypted by master key encryption key.

Master Key Encryption Key
Key derived from password that encrypts and decrypts Master Key. (PBKDF2)

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

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

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

Organizational Security Policy
A set of security rules, procedures, practices, and guidelines considered currently granted to the operating environment by an entity or a hypothetical organization or expected to be granted.

Policy Administrator
One of the authorized administrators authorized to operate and manage a TOE safely, who has privileges such as policy management, and audit records searching.

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

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

Public Key
A cryptographic key which is used in an 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.

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.

Recommend/be recommended
The ‘recommend’ or ‘be recommended’ presented in Application notes is not mandatorily recommended but required to be applied for secure operations of the TOE.

Refinement
Addition of details to a component.

Role
Predefined set of rules establishing the allowed interactions between a user and the TOE.

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

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

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

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

SSL (Secure Sockets Layer)
This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network.

Subject
Active entity in the TOE that performs operations on objects

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

System Administrator
One of the administrators authorized to operate and manage a TOE safely, who has privileges such as system settings, account management, and audit records searching.

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

Threat Agent
An unauthorized external entity that poses threats such as illegal access, modification, or deletion of assets.

.

TLS (Transport Layer Security)
This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246.

TOE Security Functionality (TSF)
Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

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

TSF Data Encryption Key
Key that encrypts and decrypts TSF data.

User
Refer to “External entity”.

User Data
Data for the user that does not affect the operation of the TSF.

1.6 **Conventions**

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**.

This ST clarifies the meaning of the requirements, provides information of selected item at implementation and offers the "Caution for application" to decide the requirements is suitable or not. "Precautions for application" is provided with the applicable requirements, if necessary.

2 Conformance claim

2.1 CC, PP and Package conformance claim

Item	Description
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 · Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) · Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) · Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
PP	Korean National Protection Profile for Database Encryption V1.1
Part 2 Security functional components	Extended: FCS_RBG.1, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
Part 3 Security assurance components	Conformant
Package	Augmented: EAL1 augmented (ATE_FUN.1)

2.2 Conformance claim rationale

This Security Target declares “strict PP conformance” with ‘the Korean National PP for Database Encryption V1.1’. By strict compliance method, the TOE type, security objectives for the operating environment, and security requirements were all complied with.

3 Security objectives

3.1 Security objectives for the operational environment

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.

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

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

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

OE. LOG_BACKUP
The authorized administrator of the TOE shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

OE.OPERATION_SYSTEM_RE-INFORCEMENT
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 trusted time stamps provided by the TOE operation environment.

OE.AUDIT_DATA_PROTECT
Audit records stored in the audit trail such as the DBMS that interact with the TOE shall be protected from unauthorized deletion or modification.

4 Extended components definition

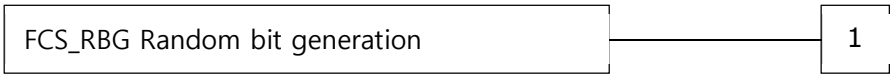
4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

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

Component leveling



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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

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

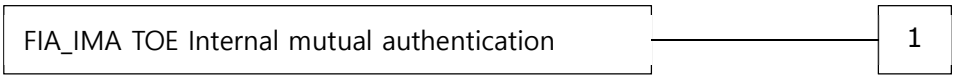
4.2 Identification and authentication

4.2.1 TOE Internal mutual authentication

Family Behaviour

This family defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.

Component leveling



FIA_IMA.1 TOE Internal mutual authentication requires that the TSF provides mutual authentication function between TOE components in the process of user identification and authentication.

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

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

a) Minimal: Success and failure of mutual authentication

b) Minimal: Modification of authentication protocol

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

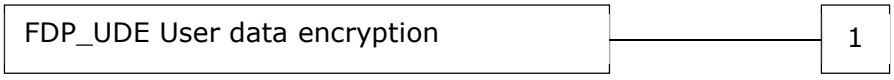
4.3 **User data protection**

4.3.1 User data encryption

Family Behaviour

This family provides requirements to ensure confidentiality of user data.

Component leveling



FDP_UDE.1 User data encryption requires confidentiality of user data.

Management: FDP_UDE.1

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

a) Management of user data encryption/decryption rules

Audit : FDP_UDE.1

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

a) Minimal : Success and failure of user data encryption/decryption

FDP_UDE.1	User data encryption Hierarchical to: No other components. Dependencies: FCS_COP.1 Cryptographic operation
FDP_UDE.1.1	FDP_UDE.1.1 TSF shall provide TOE users with the ability to encrypt/decrypt user data according to [assignment: *the list of encryption/decryption methods*] specified.

4.4 **Security Management**

4.4.1 ID and password

Family Behaviour

This family defines the capability that is required to control ID and password management used in the TOE, and set or modify ID and/or password by authorized users.

Component leveling

FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management: FMT_PWD.1

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

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

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

a) Minimal: All changes of the password.

FMT_PWD.1	Management of ID and password Hierarchical to: No other components. Dependencies: FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*]. 1. [assignment: *password combination rules and/or length*] 2. [assignment: *other management such as management of special characters unusable for password, etc.*]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*]. 1. [assignment: *ID combination rules and/or length*] 2. [assignment: *other management such as management of special characters unusable for ID, etc.*]
FMT_PWD.1.3	The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

4.5 **Protection of the TSF**

4.5.1 Protection of stored TSF data.

Family Behaviour

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

Component leveling

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

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

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

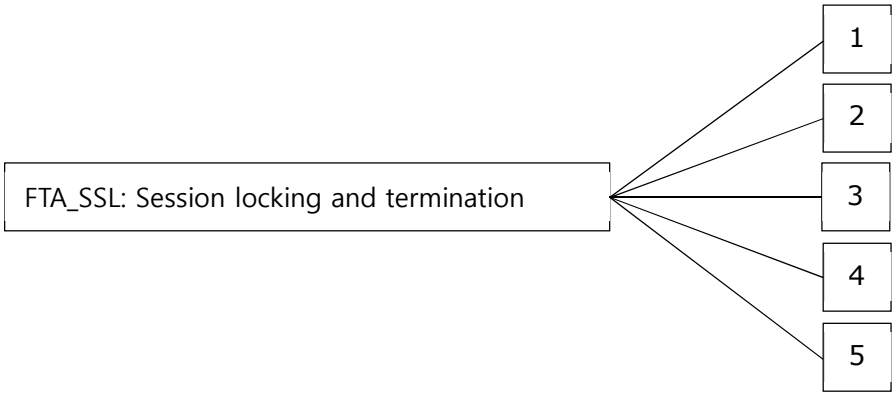
4.6 **TOE Access**

4.6.1 Session locking and termination

Family Behaviour

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Component leveling



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

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

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

Management: FTA_SSL.5

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

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

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

Audit: FTA_SSL.5

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

a) Minimal: Locking or termination of interactive session

FTA_SSL.5	Management of TSF-initiated sessions Hierarchical to: No other components. Dependencies: [FIA_UAU.1 authentication or No dependencies.]
FTA_ SSL.5.1	The TSF shall [selection: • *lock the session and re-authenticate the user before unlocking the session,* • *terminate*] an interactive session after a [assignment: *time interval of user inactivity*].

5 Security requirements

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

5.1 Security functional requirements

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

The following [Table 2] summarizes the security functional requirements used in the ST.

[Table 2] Security functional requirements

Security functional class	Security functional component		note
FAU	FAU_ARP.1	Security alarms	DB-PP
	FAU_GEN.1	Audit data generation	
	FAU_SAA.1	Potential violation analysis	
	FAU_SAR.1	Audit review	
	FAU_SAR.3	Selectable audit review	
	FAU_SEL.1	Selective audit Optional SFR	
	FAU_STG.3	Action in case of possible audit data loss	
	FAU_STG.4	Prevention of audit data loss	
FCS	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)	DB-PP
	FCS_CKM.1(2)	Cryptographic key generation (User data encryption)	
	FCS_CKM.1(3)	Cryptographic key generation (TSF data encryption)	
	FCS_CKM.1(4)	Cryptographic key generation (TSF data encryption)	

	FCS_CKM.2(1)	Cryptographic key distribution	
	FCS_CKM.2(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 (User data encryption)	
	FCS_COP.1(3)	Cryptographic operation (TSF data encryption)	
	FCS_COP.1(4)	Cryptographic operation (TSF data encryption)	
	FCS_COP.1(5)	Cryptographic operation (TSF data encryption)	
	FCS_RBG.1(Extended)	Random bit generation	
FDP	FDP_UDE.1(Extended)	User data encryption	DB-PP
	FDP_RIP.1	Subset residual information protection	
FIA	FIA_AFL.1	Authentication failure handling	DB-PP
	FIA_IMA.1(Extended)	TOE Internal mutual authentication	
	FIA_SOS.1	Verification of secrets	
	FIA_UAU.2	User authentication before any action	
	FIA_UAU.4	Single-use authentication mechanisms	
	FIA_UAU.7	Protected authentication feedback	
	FIA_UID.2	User identification before any action	
FMT	FMT_MOF.1	Management of security functions behaviour	DB-PP
	FMT_MTD.1	Management of TSF data	
	FMT_PWD.1(Extended)	Management of ID and password	
	FMT_SMF.1	Specification of management functions	
	FMT_SMR.1	Security roles	
FPT	FPT_ITT.1	Basic internal TSF data transfer protection	DB-PP
	FPT_PST.1(Extended)	Basic protection of stored TSF data	
	FPT_TEE.1	Testing of external entities	
	FPT_TST.1	TSF testing	
FTA	FTA_MCS.2	Per user attribute limitation on multiple	DB-PP

		concurrent sessions	
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions	
	FTA_TSE.1	TOE session establishment	

5.1.1 Security Audit

FAU_ARP.1	Security alarms Hierarchical to: No other components. Dependencies: FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1	The TSF shall take [sending an alert e-mail to the system 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 the "auditable events" in [Table 3] Audit events, [no other components].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [refer to the contents of "additional audit record" in [Table 3] Audit events, [no other components].

[Table 3] Audit event

Security functional component	Auditable event	Additional audit record
FAU_ARP.1	Actions taken due to potential security violations	Recipient identification of response action

Security functional component	Auditable event	Additional audit record
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
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 (1~4)	Success and failure of the activity	
FCS_CKM.2 (1~2)	Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	
FCS_CKM.4	Success and failure of the activity (only applying to destruction of key related to user data encryption/decryption)	
FCS_COP.1 (1~5)	Success and failure of cryptographic operations, types of cryptographic operations	
FDP_UDE.1	Success and failure of user data encryption/decryption	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_IMA.1	Success and failure of mutual authentication. Modify of authentication protocol	
FIA_UAU.1	All use of the authentication mechanism.	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF selftests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5	Locking or termination of interactive session	

FAU_SAA.1	Potential violation analysis Hierarchical to: No other components. Dependencies: FAU_GEN.1 Audit data generation
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [authentication failure audit event among auditable events of FIA_UAU.1, integrity violation audit event and self-test failure event of validated cryptographic module among auditable events of FPT_TST.1,[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 [[Table 4] methods of selection and/or ordering] of audit data based on [criteria with the following logical relations].

[Table 4] Audit Review Selection Criteria

Type	Selection criteria by type	Ability
Audit	- *Event Period*: Start Date ~ End Date - *Event Type*: Select one of the list of audit event types. - *Event Result Type*: Alternative of Event Result Type (Success / Fail)	Search

	- *Subject identity*: Input Keyword	

FAU_SEL.1	Selective audit Hierarchical to: No other components. Dependencies: FAU_GEN.1 Audit data generation FMT_MTD.1 TSF Management of TSF data
FAU_SEL.1.1	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) [event type] b) [event result type (choice for success, choice for failure)]

FAU_STG.3	Action in case of possible audit data loss Hierarchical to: No other components. Dependencies: FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	The TSF shall [send emails to system administrators] if the audit trail exceeds [90%]].

FAU_STG.4	Prevention of audit data loss Hierarchical to: FAU_STG.3 Action in case of possible audit data loss Dependencies: FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall [overwrite the oldest stored audit records] and [sent alert e-mails to the system administrator] if the audit trail is full.

5.1.2 Cryptographic Support

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 [HASH_DRBG] and specified cryptographic key sizes [128bit, 192bit and 256bit] that meet the following: [KS

	X ISO/IEC 18031].

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 [HASH_DRBG] and specified cryptographic key sizes [128bit] that meet the following: [KS X ISO/IEC 18031].

FCS_CKM.1(3)	Cryptographic key generation (TSF data encryption) Hierarchical to: No other components. Dependencies: [FCS_CKM.2 CryptogtlRkraphic 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 [HASH_DRBG] and specified cryptographic key sizes [256bit] that meet the following: [KS X ISO/IEC 18031].

FCS_CKM.1(4)	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 [PBKDF2] and specified cryptographic key sizes [256bit] that meet the following: [RFC 8018].

FCS_CKM.2(1)	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 distribute cryptographic keys in accordance with a specified cryptographic key distribution method [ID based KEM/DEM] that meets the following: [TTAK.KO-12.0270-Part 1].

FCS_CKM.2(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 distribute cryptographic keys in accordance with a specified cryptographic key distribution method [LEA] that meets the following: [KS X 3246].

FCS_CKM.4	Cryptographic key destruction Hierarchical to: No other components. Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with '0'] that meets the following: [None].

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 [user data encryption] in accordance with a specified cryptographic algorithm [LEA, ARIA] and cryptographic key sizes [128bit, 192bit

	and 256bit] that meet the following: [KS X 3246, KS X 1213-1, KS X 1213-2].

FCS_COP.1(2)	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 [message hash] in accordance with a specified cryptographic algorithm [SHA-256, SHA-512] and cryptographic key sizes [None] that meet the following: [ISO/IEC 10118-3].

FCS_COP.1(3)	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 [TFS data encryption] in accordance with a specified cryptographic algorithm [LEA] and cryptographic key sizes [128bit] that meet the following: [KS X 3246].

FCS_COP.1(4)	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 [TFS data encryption] in accordance with a specified cryptographic algorithm [LEA] and cryptographic key sizes [256bit] that meet the following: [KS X 3246].

FCS_COP.1(5)	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 [message hash] in accordance with a specified cryptographic algorithm [SHA-256] and cryptographic key sizes [None] that meet the following: [ISO/IEC 10118-3].

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 a cryptographic key using the specified random bit generator that meets the following [ISO/IEC 18031].

5.1.3 User Data Protection

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 objects: [user data].

5.1.4 Identification and Authentication

FIA_AFL.1	Authentication failure handling

	Hierarchical to: No other components. Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [*[5], an administrator configurable positive integer within [5]*] unsuccessful authentication attempts occur related to [administrator authentication events].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall [deactivate the identification and authentication function (for 5 minutes for system administrators and until password reset by system administrators for policy administrators and audit administrators) and send alarm e-mails to system administrators].

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 using [ID based KEM/DEM] in accordance with [TTAK.KO-12.0270-Part 1] between [management server and client module].

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 acceptance criteria defined below]. [a) allowed characters - Alphabetic case (52 characters): A to Z, a to z - Numbers (10 characters): 0 to 9 - Special characters (all 32 characters that can be entered via the keyboard): ~, !, @, #, $, %, ^, &, *, (,), _, +, {, }, |, :, ", <, >, ?, `, -, =, [,], ₩, ;, ', , . b) combination rules; - 3 essential combinations of uppercase and lowercase letters, numbers and special characters. c) min / max length

	- 9 to 15 characters (9 to 15 bytes)]

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 user 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 [all authentication scheme].

FIA_UAU.7	Protected authentication feedback Hierarchical to: No other components. Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only [the following list of feedback] to the user while the authentication is in progress. [a) When entering secret information (password), change each character of input window to ' • ' character and display it on the screen. - Administrator passwords create - Administrator passwords change - Administrator identification and authentication b) If identification and authentication fail, a message is displayed except feedback about the reason for the failure. - "Please check your ID/Password."]

FIA_UID.2	User identification before any action Hierarchical to: FIA_UID.1 Timing of identification

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

5.1.5 Security Management

FMT_MOF.1	Management of security functions behaviour Hierarchical to: No other components. Dependencies: FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MOF.1.1	The TSF shall restrict the ability to ***conduct management actions of*** the functions [[Table 5] security function lists] to [authorized administrator].

[Table 5] security function lists

Security Function	Ability				Authorized administrator
	Decide	Stop	Start	Update	
User data encryption method management	O	O	O	-	Policy
Audit function enable / disable management	O	O	O	-	System

※ - Not supported, O Supported

FMT_MTD.1	Management of TSF data Hierarchical to: : No other components Dependencies: : FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1	The TSF shall restrict the ability to ***manage*** [following [Table 6] TSF data lists] to [the authorized administrators].

[Table 6] TSF data lists

TSF data	Ability						
	Query	Update	Delete	Clear	Create	Admin Type	Note
Audit record	O	-	-	-	-	System	

TSF data	Ability						
	Query	Update	Delete	Clear	Create	Admin Type	Note
						Policy Audit	
Encryption Policy	O	O	O	O	O	Policy	Only policy in DRAFT status can be updated / deleted / cleared
Key encryption key	O	O	-	-	O	Policy	
User data encryption key	O	O	-	-	O	Policy	
Administrator Identification and Credentials	O	O	O	-	O	System	In case of system administrator, password information of policy administrator and audit administrator can be changed.
	O	O	-	-	-	Policy	
	O	O	-	-	-	Audit	
Maximum number of auditor sessions allowed	O	O	-	-	-	System	
User inactivity period during which session termination occurs	O	O	-	-	-	System	
Failed Authentication Attempt Threshold Setting	O	O	-	-	-	System	
Access IP Configuration setting	O	O	O	O	O	System	Delete / Clear except localhost IP address
Email server Setting	O	O	-	-	-	System	
Self-test Time Interval Setting	O	O	-	-	-	System	

FMT_PWD.1	Management of ID and password (extended) Hierarchical to: No other components Dependencies: FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [None]. 1. [None] 2. [None]
FMT_PWD.1.2	FMT_PWD.1.2 The TSF shall restrict the ability to manage ID of [None]. 1. [None] 2. [None]
FMT_PWD.1.3	The TSF shall provide the capability for *changing the ID and password when the authorized 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: [List of management functions to be provided by the TSF]. [a) List of security functions specified in FMT_MOF.1 b) TSF data management list specified in FMT_MTD.1 c) Security attributes related to ID and password generation specified in FMT_PWD.1.]

FMT_SMR.1	Security roles Hierarchical to: No other components. Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [authorized identified roles in [Table 7]].
FMT_SMR.1.2	TSF shall be able to associate users and their **roles defined in FMT_SMR.1.1.**

[Table 7] Authorized administrator role

<table>
<tr><th colspan="2">Role</th><th>Management function and data(Ability)</th></tr>
<tr><td rowspan="2">Authorized Administrator</td><td rowspan="2">System Administrator</td><td>Security function management
<table>
<tr><th>Security function</th><th>Ability</th></tr>
<tr><td>Audit function enable / disable management</td><td>Decide / Stop / Start</td></tr>
</table>
TSF data management
<table>
<tr><th>TSF data</th><th>Ability</th></tr>
<tr><td>Audit record</td><td>query</td></tr>
<tr><td>Administrator Identification and Credentials</td><td>query, modify, delete, create</td></tr>
<tr><td>Maximum number of auditor accounts / sessions</td><td>query, modify</td></tr>
<tr><td>User inactivity period during which session termination occurs</td><td>query, modify</td></tr>
<tr><td>Failed Authentication Attempt Threshold Setting</td><td>query, modify</td></tr>
<tr><td>Access IP Configuration</td><td>query, modify, delete, clear, create</td></tr>
<tr><td>Email server settings</td><td>query, modify</td></tr>
<tr><td>Self-test Time Interval Setting</td><td>query, modify</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>Policy Administrator</td><td>Security function management
<table><tr><th>Security function</th><th>Ability</th></tr><tr><td>User data encryption method management</td><td>Decide / Stop / Start</td></tr></table>
TSF data management
<table><tr><th>TSF data</th><th>Ability</th></tr><tr><td>Audit record</td><td>query</td></tr><tr><td>Password Policy Setting</td><td>query, modify, delete, clear, create</td></tr><tr><td>Key encryption key</td><td>query, modify, create</td></tr><tr><td>User Data Encryption Key</td><td>query, modify, create</td></tr><tr><td>Administrator Identification and Credentials</td><td>query, modify</td></tr></table></td></tr>
<tr><td></td><td>Audit Administrator</td><td>TSF data management
<table><tr><th>TSF data</th><th>Ability</th></tr><tr><td>Audit record</td><td>query</td></tr><tr><td>Administrator Identification and Credentials</td><td>query, modify</td></tr></table></td></tr>
</table>

5.1.6 Protection of the TSF

FPT_ITT.1	Basic internal TSF data transfer protection Hierarchical to: No other components. Dependencies: No dependencies.
FPT_ITT.1.1	The TSF shall protect the TSF data from *disclosure, modification* 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 [administrator password, encryption key, account information and TOE configurations] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

FPT_TEE.1	Testing of external entities Hierarchical to: No other components. Dependencies: No dependencies.
FPT_TEE.1.1	The TSF shall run a suite of tests [*during initial start-up, at the request of the authorized* ***administrator***] to check the fulfillment of [E-mail server connectivity].
FPT_TEE.1.2	If the test fails, the TSF shall [take the following actions]. [a) When the mail server test linked with the TOE fails -Shown on the main page dashboard]

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 [***all TSF process***].
FPT_TST.1.2	The TSF shall provide **authorized administrators** with the capability to verify the integrity of *TSF data*.
FPT_TST.1.3	The TSF shall provide **authorized administrators** with the capability to verify the integrity of [***stored TSF execution code***].

5.1.7 TOE Access

FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions Dependencies: FIA_UID.1 Timing of identification
FTA_MCS.2.1	The TSF shall restrict the maximum number of concurrent sessions [belonging to the same administrator according to the rules for the list of management functions defined in FMT_SMF1.1]

	a) limit the maximum number of concurrent sessions to 1 for management access by the same administrator who has the right to perform FMT_MOF.1.1 "Management actions" and FMT_MTD.1.1 "Management." b) limit the maximum number of concurrent sessions to {what is determined by the ST author} for management access by the same administrator who doesn't have the right to perform FMT_MOF.1.1 "Management actions" but has the right to perform a query in FMT_MTD.1.1 "Management" only c) [None]
FTA_MCS.2.2	The TSF shall enforce a limit of [1] session per administrator by default.

FTA_SSL.5	Management of TSF-initiated sessions(Extended) Hierarchical to: No other components. Dependencies: FIA_UAU.1 authentication or No dependencies.
FTA_ SSL.5.1	The TSF shall [*terminate*] the administrator's interactive session after a [time interval(60sec ~ 3600sec, default is 600sec) of the administrator inactivity].

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 Protection Profile are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

[Table 8] Security assurance requirements

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational

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

5.2.1 Security Target evaluation

ASE_INT.1	introduction Dependencies: No dependencies.
	Developer action elements
ASE_INT.1.1D	The developer shall provide an ST introduction.
	Content and presentation
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.
	Evaluator action elements
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all

	requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1	Conformance claims Dependencies: ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements
	Developer action elements
ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
	Content and presentation elements
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of

	security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
	Evaluator action elements
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1	Security objectives for the operational environment Dependencies: No dependencies.
	Developer action elements
ASE_OBJ.1.1D	The developer shall provide a statement of security objectives.
	Content and presentation elements
ASE_OBJ.1.1C	The statement of security objectives shall describe the security objectives for the operational environment.
	Evaluator action elements
ASE_OBJ.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1	Extended components definition Dependencies: No dependencies.
	Developer action elements
ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
	Content and presentation elements
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements

	such that conformance or nonconformance to these elements can be demonstrated.
	Evaluator action elements
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

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

ASE_TSS.1	TOE summary specification Dependencies: ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
	Developer action elements
ASE_TSS.1.1D	The developer shall provide a TOE summary specification

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

5.2.2 Development

ADV_FSP.1	Basic functional specification Dependencies: No dependencies.
	Developer action elements
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
	Content and presentation elements
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
	Evaluator action elements
ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance documents

AGD_OPE.1	Operational user guidance

	Dependencies: ADV_FSP.1 Basic functional specification
	Developer action elements
AGD_OPE.1.1D	The developer shall provide operational user guidance.
	Content and presentation elements
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
	Evaluator action elements
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1	Preparative procedures Dependencies: No dependencies.
	Developer action elements
AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
	Content and presentation elements
AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure

	acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
	Evaluator action elements
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1	TOE Labelling of the TOE Dependencies: ALC_CMS.1 TOE CM coverage
	Developer action elements
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
	Content and presentation elements
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
	Evaluator action elements
ALC_CMC.1.1E	The evaluator shall confirm that the information provided meet requirements for content and presentation of evidence.

ALC_CMS.1	TOE CM coverage Dependencies: No dependencies.
	Developer action elements
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
	Content and presentation elements
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
	Evaluator action elements

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

5.2.5 Tests

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

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

	requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability assessment

AVA_VAN.1	Vulnerability survey Dependencies: ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
	Developer action elements
AVA_VAN.1.1D	The developer shall provide the TOE for testing
	Content and presentation elements
AVA_VAN.1.1C	The TOE shall be suitable for testing.
	Evaluator action elements
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Security requirements rationale

5.3.1 Dependency rationale of security functional requirements

The following [Table 9] shows dependency of security functional requirements.

[Table 9] Rationale for the dependency of the security functional requirements

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	Rationale(1)
3	FAU_SAA.1	FAU_GEN.1	2

4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_SEL.1	FAU_GEN.1	2
		FMT_MTD.1	32
7	FAU_STG.3	FAU_STG.1	Rationale(2)
8	FAU_STG.4	FAU_STG.1	Rationale(2)
9	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	13,14,16,17
		FCS_CKM.4	15
10	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	13,14,18,19,20
		FCS_CKM.4	15
11	FCS_CKM.1(3)	[FCS_CKM.2 or FCS_COP.1]	13,14,18,19,20
		FCS_CKM.4	15
12	FCS_CKM.1(4)	[FCS_CKM.2 or FCS_COP.1]	13,14,18,19,20
		FCS_CKM.4	15
13	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9, 10, 11, 12
		FCS_CKM.4	15
14	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9, 10, 11, 12
		FCS_CKM.4	15
15	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9, 10, 11, 12
16	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9
		FCS_CKM.4	15
17	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Rationale(5)
		FCS_CKM.4	Rationale(5)
18	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	10, 11, 12
		FCS_CKM.4	15
19	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	10, 11, 12
		FCS_CKM.4	15
20	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Rationale(6)
		FCS_CKM.4	Rationale(6)
21	FCS_RBG.1	-	-
22	FDP_UDE.1	FCS_COP.1	16,17
23	FDP_RIP.1	-	-
24	FIA_AFL.1	FIA_UAU.1	27

			Rationale(3)
25	FIA_IMA.1	-	-
26	FIA_SOS.1	-	-
27	FIA_UAU.2	FIA_UID.1	30 Rationale(4)
28	FIA_UAU.4	-	-
29	FIA_UAU.7	FIA_UAU.1	27 Rationale(3)
30	FIA_UID.2	-	-
31	FMT_MOF.1	FMT_SMF.1	34
		FMT_SMR.1	35
32	FMT_MTD.1	FMT_SMF.1	34
		FMT_SMR.1	35
33	FMT_PWD.1	FMT_SMF.1	34
		FMT_SMR.1	35
34	FMT_SMF.1	-	-
35	FMT_SMR.1	FIA_UID.1	30 Rationale(4)
36	FPT_ITT.1	-	-
37	FPT_PST.1	-	-
38	FPT_TEE.1	-	-
39	FPT_TST.1	-	-
40	FTA_MCS.2	FIA_UID.1	30 Rationale(4)
41	FTA_SSL.5	FIA_UAU.1	27 Rationale(3)
42	FTA_TSE.1	-	-

Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1, but the TOE accurately records security-related events using the trusted timestamp provided by the TOE operating environment. Therefore, FAU_GEN.1 depends on the operation environment instead of FPT_STM.1. Dependencies of FAU_GEN.1 are satisfied by security objective OE.TIMESTAMP.

Rationale (2): FAU_STG.3, FAU_STG.4 has a dependency on FAU_STG.1, but the TOE protects against

unauthorized deletion or modification of audit records stored in audit trail, such as DBMS, which interacts with TOE in production environment. However, the dependency of FAU_STG.1 is satisfied by OE.AUDIT data protection for the operational environment instead of FAU_STG.1.

Rationale (3): FIA_UAU.2 has a hierarchical relationship with FIA_UAU.1 and has a limited strength to satisfy the dependency.

Rationale (4): FIA_UID.2 has a hierarchical relationship with FIA_UID.1 and has a limited strength to satisfy the dependency.

Rationale (5): FCS_COP.1 (2) depends on FCS_CKM.1 and FCS_CKM.4, but does not require encryption key because it performs one-way encryption algorithm (SHA-256 / 512) operation when encrypting user data. . Therefore, the dependency of FCS_CKM.1 and FCS_CKM.4 is satisfied.

Rationale (6): FCS_COP.1 (5) has a dependency on FCS_CKM.1 and FCS_CKM.4, but does not require an encryption key because it performs one-way encryption algorithm (SHA-256) operation when encrypting TSF data. Therefore, the dependency of FCS_CKM.1 and FCS_CKM.4 is satisfied.

5.3.2 Dependency of SARs of the TOE

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

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

6 TOE Summary Specification

This chapter describes SFRs implemented in the TOE.

6.1 Security Audit (FAU)

6.1.1 Audit Data Generation and Selective audit

TOE generates audit data for auditable events that occur during operations. Auditable events are created and stored based on event time, event type, event result type (success or failure) and subject identity. The audit function works when the management server is running and is generated including audit events for startup / shutdown. TOE can selectively generate audit data according to the audit event type (see '[Table 10] Audit Events available to sets) when generating audit data. The default value is set to generate audit logs for all audit data.

[Table 10] Audit Events available to set

Types of Audit Event	Details of Audit Event
Start-up Server	Type of audit event for the server startup-up
Shutdown Server	Type of audit event for the server shutdown
Audit Data Capacity Exceeded	Type of audit event for the audit data capacity that exceeded the threshold
Data Encryption Key Distribution	Type of audit event for the data encryption key distribution
Data Decryption Key Distribution	Type of audit event for the data decryption key distribution
User Data Encryption	Type of audit event for the user data encryption performed by client
User Data Decryption	Type of audit event for the user data decryption performed by client
Lock Account with Excessive Login Attempts	Type of audit event for the account lockout with excessive login attempts that exceed the maximum allowed number of times.
Unlock Account	Type of audit event for the account unlock
Mutual Authentication for Policy Server	Type of audit event for the mutual authentication with policy server
Send Random Value at Login	Type of audit event for the transmission of random value from server to browser when login
Result of Server Login	Type of audit event for the admin authentication when login

Access Menu	Type of audit event for the access to menu
Create Policy	Type of audit event for the creation of encryption policy
Update Policy	Type of audit event for the modification of encryption policy
Delete Policy	Type of audit event for the deletion of encryption policy
Confirm Policy	Type of audit event for the confirmation of encryption policy
Create System User	Type of audit event for the creation of the account of authorized administrator
Update System User	Type of audit event for the modification of the account of authorized administrator
Update System User Password	Type of audit event for the change of the password of authorized administrator
Delete System User	Type of audit event for the deletion of the account of authorized administrator
Create System Configuration	Type of audit event for the creation of system configuration information
Update System Configuration	Type of audit event for the modification of system configuration information
Generate Data Encryption Key(DEK)	Type of audit event for the generation of data encryption key (DEK)
Generate Key Encryption Key(KEK)	Type of audit event for the generation of key encryption key (KEK)
Create Audit Configuration	Type of audit event for the creation of audit configuration information
Update Audit Configuration	Type of audit event for the modification of audit configuration information
Create Accessible IP Address	Type of audit event for the creation of remote address that allowed to access to server
Create Accessible IP Address	Type of audit event for the modification of remote address that allowed to access to server
Delete Accessible IP Address	Type of audit event for the deletion of remote address that allowed to access to server
Results of Server Self Test	Type of audit event for the execution of server self-test
Results of Client Self Test	Type of audit event for the execution of client self-test
Disconnect Existing Login Session	Type of audit event for the termination of oldest login session when the count of concurrent sessions is

	exceeded the maximum set by authorized administrator type or by system
Termination of Interactive Session	Type of audit event for the termination of login session existing over timeout
Security Alarm	Type of audit event for the transmission of security alarm
Add Client Access	Type of audit event for the creation of client access information
Add Client Access	Type of audit event for the modification of client access information
Delete Client Access	Type of audit event for the deletion of client access information
Add Client Permission	Type of audit event for the creation of client encryption-permission information (as sub-information of client access information)
Update Client Permission	Type of audit event for the modification of client encryption-permission information (as sub-information of client access information)
Delete Client Permission	Type of audit event for the deletion of client encryption-permission information (as sub-information of client access information)
Add Client Datasource Information	Type of audit event for the creation of datasource information (as sub-information of client access information)
Update Client Datasource Information	Type of audit event for the modification of datasource information (as sub-information of client access information)
Delete Client Datasource Information	Type of audit event for the deletion of datasource information (as sub-information of client access information)
Allocation Audit Storage Capacity	Type of audit event for the re-allocation of audit storage
Verify License	Type of audit event for the execution of software license validation

SFR to be satisfied : FAU_GEN.1, FAU_SEL.1

6.1.2 Security alarms

TOE sends an alert mail to all the system administrators via whose registered email address in the

cases that audit log such as continuous authentication failure, integrity violation and the failure of self-test for KCMVP module of the indicates a potential security violation.

SFR to be satisfied : FAU_ARP.1, FAU_SAA.1

6.1.3 Audit review

TOE stores audit data in an audit repository (DBMS) and provides audit records to suit the authorized administrator's interpretation of the information. The authorized administrators (System/Policy/Audit Administrator) is able to search and review the audit data based on the combination of conditions such as the time of event occurrence, event type, type of event result and subject of the audit data through web-based interface.

SFR to be satisfied : FAU_SAR.1, FAU_SAR.3

6.1.4 Prevention of audit data loss

To prevent the loss of audit data, the TOE shall take the following actions:

- Once audit data volume has reached to the predefined threshold (90%), to generate audit log that indicates audit data volume is exceeded the threshold and to send an alert email to all system administrators
- Once audit data volume has reached to the saturation point (100%), to overwrite oldest audit data for saving recent audit log, to generate audit log that indicates audit storage is full and to send an alert email to all system administrators.

SFR to be satisfied : FAU_STG.3, FAU_STG.4

6.2 **Cryptographic Support (FCS)**

Classification	Key Generate Method	Cryptographic Algorithm	Key Length (bit)	Standard	Usage
Master Key	HASH_DRBG (SHA-256)	LEA	256	- Generate Method: KS X ISO/IEC 18031 - Algorithm: TTAK.KO-12.0223	To encrypt KEK

Master Key Encryption Key		Derivation from password (PBKDF2)	LEA	256	- Generate Method: RFC 8018 - Algorithm: TTAK.KO-12.0223	To encrypt master key
Data Encryption Key (DEK)		HASH_DRBG (SHA-256)	LEA ARIA	128 192 256	- Generate Method: KS X ISO/IEC 18031 - Algorithm: KS X 3246, KS X 1213-1, KS X 1213-2	To encrypt user data
Key Encryption Key (KEK)		HASH_DRBG (SHA-256)	LEA	256	- Generate Method: KS X ISO/IEC 18031 - Algorithm: KS X 3246	To encrypt DEK and configuration database encryption key
Configuration Database Encryption Key		HASH_DRBG (SHA-256)	LEA	128	- Generate Method: KS X ISO/IEC 18031 - Algorithm: KS X 3246	To encrypt TSF data in database
Configuration File Encryption Key		HASH_DRBG (SHA-256)	LEA	128	- Generate Method: KS X ISO/IEC 18031 - Algorithm: KS X 3246	To encrypt configuration file items
Mutual Authentication	Key Exchange	-	-	128	- Key Exchange: TTAK.KO-12.0270-Part 1	To exchange key through the mutual authentication
	Data Encryption Key	HASH_DRBG (SHA-256)	LEA	128	- Generate Method: KS X ISO/IEC 18031 - Algorithm: KS X 3246	To encrypt data of encryption policy and data of audit

6.2.1 Cryptographic Key Generation

TOE uses a random number generator of the verified cryptographic module for generating encryption keys. DEK is generated based on the cryptographic algorithm (LEA, ARIA) and encryption

key length (128, 192, 256 bit) specified in the encryption policy that policy manager created, KEK and master key are generated as 256 bits key length using the LEA cryptographic algorithm. And master key encryption key is generated as 256 bits key length induced by password in accordance with the standard PKCS#5 (PBKDF2). Configuration Database Encryption Key and Configuration File Encryption Key are generated as 128 bit key size using LEA cryptographic algorithm and Data Encryption Key for the distribution of user data encryption key is generated as 128 bits key length using LEA according to the mutual authentication mechanism.

Information of the verified cryptographic module is as follows.

- Validation No. : CM-131-2022.10
- Validation Date : 2017.10.16
- Cryptographic module name : MagicJCrypto V2.0.0
- Module type : S/W(Library)
- Developed Company : Dreamsecurity Co.,Ltd.

SFR to be satisfied : FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4)

6.2.2 Cryptographic Key Distribution

TOE is distributed safely through the ID based 'KEM/DEM' corresponding to the standard specified at 'TTAK.KO-12.0270-Part 1' that computes the session key by using the parameter generated by 'HASH_DRBG' algorithm. The deployed session key protects encryption the policy data and the audit data transmitted between TOE components, through encryption of them using 128-bit LEA algorithm.

SFR to be satisfied : FCS_CKM.2(1), FCS_CKM.2(2)

6.2.3 Cryptographic Key Destruction

The TOE deletes all encryption keys and key security parameters loaded into memory during creation, distribution, and operation by overwriting them with zero after use of them.

SFR to be satisfied : FCS_CKM.4

6.2.4 Cryptographic Operation

TOE uses a verified cryptographic module for cryptographic operation. The encryption keys of TOE

are divided into user data encryption key (DEK), key encryption key (KEK), master key, TSF data encryption key, session key for distribution of encryption keys.

The DEK that protects user data is generated based on the cryptographic algorithm (LEA, ARIA) and encryption key length (128, 192, 256 bit) specified in the encryption policy that policy manager created. KEK (LEA, 256 bit) protects the DEK and master key (LEA, 256 bit) protects the KEK. Master key is encrypted by master key encryption key (LEA, 256 bit) derived from user passwords. TSF data is encrypted and protected by TSF data encryption key (LEA, 128 bit) and transmission data between TOE components is encrypted by session key (LEA, 128 bit).

SFR to be satisfied : FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5)

6.2.5 Random bit Generation

TOE generates random numbers by using the random number generator that complies with ISO/IEC 18031 standard of the verified cryptographic module.

Information of the verified cryptographic module is as follows.

- Validation No. : CM-131-2022.10
- Validation Date : 2017.10.16
- Cryptographic module name : MagicJCrypto V2.0.0
- Module type : S/W(Library)
- Developed Company : Dreamsecurity Co.,Ltd.

SFR to be satisfied : FCS_RBG.1(Extended)

6.3 **User data Protection (FDP)**

6.3.1 User data Protection

The client module encrypts and decrypts user data by column based the encryption policy managed by the management server. It also protects user data by deleting the original data to be encrypted from DBMS as overwriting with null when encrypting and decrypting user data.

SFR to be satisfied : FDP_UDE.1(Extended), FDP_RIP.1

6.4 **Identification and Authentication (FIA)**

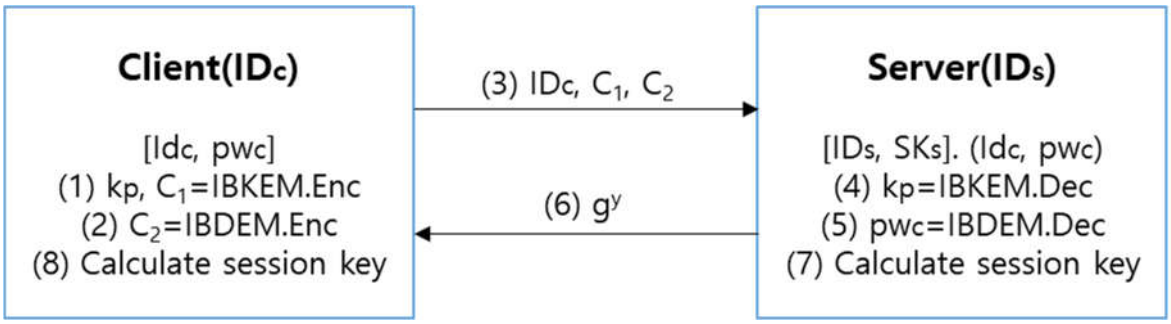
6.4.1 Identification and Authentication

TOE provides security management functions after identification and authentication with the administrator's ID and password prior to any acts by an authorized administrator. In the case when an authorized administrator fails to authentication continually over maximum count allowed (within 1 to 5 times / default 5 times) the TOE disables identification and authentication function (for 5 minutes for system administrator / until unlocking by any system administrator for policy administrator and audit administrator) and sends an email all system administrators.

SFR to be satisfied : FIA_AFL.1, FIA_UAU.2, FIA_UID.2

6.4.2 TOE Internal Mutual Authentication

TSF operates mutual authentication between the management server and the client module through ID based 'KEM/DEM' that complies with the standards specified in 'TTAK.KO-12.0270-Part 1'.
The detailed mechanisms are as follows.



(1) The client performs IBKEM.Enc(params,ID_S) using the 'params' which is the system public parameter and 'ID_S' which is the identity of the server. The IBKEM.Enc algorithm selects the temporary private key $x \in Zq$ and uses it to generate the one-time encryption key k_p and the cipher text C_1.
(2) The client performs IBDEM.Enc (params,kp,pw_c) using params which is the system public parameter, the one-time encryption key k_p and its own 'pw_c' in order to generate the cipher text C_2.
(3) The client sends ID_c correspondng to its ID, ciphertext C_1 and ciphertext C_2 to the server.
(4) The server performs IBKEM.Dec(SK_s,params,C_1) using the private key SK_S corresponding to its ID, 'params' the system public parameter, and the cipher text C_1 in order to obtain the one-time encryption key k_p.
(5) The server obtain the password pw_c by performing IBDEM.Dec(params,k_p,C_2) using the system public parameters 'params', the one-time encryption key k_p and cipher text C_2 and then verifies it

against pw_C which is the password corresponding to the client ID_C in the server.
(The server can store the hash value for client's password to perform verification comparing with that hash value).
(6) After verification of the client's password is completed, the server selects the temporary private key $y \in Zq$ to calculate the g^y and sends it to the client.
(7) The server calculates $g^{xy}=(g^x)^y$ using the client's temporary public key g_x and server's temporary private key y. Next, the server calculates the session key $KDF(ID_C,ID_S,C_1,C_2,k_P,g^y,g^{xy})$ using ID_S corresponding to its ID, ID_C corresponding to the client's ID, cipher text C_1, cipher text C_2, one-time encryption key k_P and server's temporary public key g^y. .
(8) The client calculates $g^{xy}=(g^y)^x$ using the temporary private key x generated during the performance of the IBKEM.Enc algorithm and the server's temporary public key g^y sent from the server. Next, the server calculates the session key $KDF(ID_C,ID_S,C_1,C_2,k_P,g^y,g^{xy})$ using ID_S corresponding to its ID, cipher text C_1, cipher text C_2, one-time encryption key k_P and the server's temporary public key g^y.

SFR to be satisfied : FIA_IMA.1(Extended)

6.4.3 Verification of Secrets

The password required for authentication must consist of three combinations of alphabets, numbers and special characters ranging from 9 to 15 digits in accordance with predefined rules. TOE forces the default-provided system administrator account and the newly created authorized administrator account to change the password on its initial access , and checks the password at all the time of creation and modification of which with the validation-rules.

SFR to be satisfied : FIA_SOS.1

6.4.4 Single-use Authentication Mechanisms

The management server of the TOE authenticates and identifies the authorized administrator with the following procedure.
(1) Authorized administrator requests login (authentication and identification) to administrator PC.
(2) The management server generates and transmits a random number that has hashed value (SHA-256) of the session value between the management server and the authorized administrator PC.
(3) The administrator PC concatenates the random number transmitted from the management server

with hash value of the password the authorized administrator inputted and then sends it to the management server after hashing (SHA-256) it again.
(4) The management server determines whether to authenticate and identify through concatenating the hash value that transmitted to the administrator PC with the hashed and encrypted value of the authorized administrator's password that requested the login, hashes it again (SHA-256), and comparing it with the value received from the administrator PC.

The management server blocks the attempt to reuse authentication information for the logged-in administrator by creating a new session ID every time it is connected and maintaining it as an authentication session for secure authentication and identification of the authenticated administrator.

SFR to be satisfied : FIA_UAU.4

6.4.5 Protection of Authentication Feedback

The TOE blocks the exposure of information through the masking ('•') of confidential information such as the password entered during authorized administrator authentication. The message generated when the authentication fails does not provide the exact reason for the authentication failure, so no password can be inferred.

SFR to be satisfied : FIA_UAU.7

6.5 **Security Management (FMT)**

6.5.1 Management of Security functions behaviour

As the TOE can authenticate based on ID and PW, only the authenticated administrator who has logged in can perform the security management function. TOE provides security function management, TSF data management and ID and password management functions and only authorized administrators can play a role.
For security functions that an authorized administrator can manage, refer to "[Table 5] Security Function List" and "[**Table 7**] Authorized Administrator Role".

SFR to be satisfied : FMT_MOF.1, FMT_SMF.1, FMT_SMR.1

6.5.2 Management of TSF Data

Refer to "[Table 6] TSF Data Lists" for the TOE administrator's ability to manage TSF data.

SFR to be satisfied : FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.5.3 Management ID and Password

The management server controls by force for the authorized administrator to change the password at the first access. The password to set is validated by as follows.

1) The allowed type of characters (the combination of three conditions as follows)
   - alphabet (A-Z, a-z)
   - numbers (0 – 9)
   - special characters (!, @, #, $, %, ^, &, *, (,), -, +, =, {. }. [,], ~, ;, :, /, <, >, ?, ₩, ', ", |, .)
2) The allowed length : not less than 9 and no more than 15

SFR to be satisfied : FMT_PWD.1(Extended)

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

6.6.1 Basic internal TSF data transfer protection

The TOE ensures the confidentiality and integrity of TSF data between components through cryptographic communication which is performed using shared session key (LEA, 128bit) through TTAK.KO-12.0270-Part 1 (key exchange protocol using password and IBC*).

Refer "6.4.2 Mutual Authentication between TOE components".

IBC* : ID-based password system

SFR to be satisfied : FPT_ITT.1

6.6.2 Basic Protection of Stored TSF Data

TOE stores encrypted data into the DB to manage and protect the stored Data. TSF data includes passwords for administrator, crypto key and TOE configurations. The administrator password encryption is performed using the hash (SHA-256) and encryption (LEA, 128bit), and the TOE setting values are stored after encryption with the TSF data encryption key.

The encryption key of the TOE is divided into a User Data DEK, a TSF Data DEK, and a Key Encryption Key (KEK). Each DEK is encrypted with KEK (LEA, 256bit), and the KEK is protected by encrypting

(LEA, 256bit) using the master key. The master key is encrypted (LEA, 256bit) using a master key encryption key derived from a password.

SFR to be satisfied : FPT_PST.1(Extended)

6.6.3 TSF testing and Testing of external entities

To ensure that the TOE remains secure and that the security functions operate normally, the management server and client modules perform their own tests verifying the integrity checks (hash value verification) of all TOE processes, TSF data, and TSF executable code at the start-up and at a set interval time(default: 60 minutes). The TOE checks the connection to email server through the authentication of email server at start-up and at the request of an authorized administrator.

SFR to be satisfied : FPT_TEE.1, FPT_TST.1

6.7 **TOE Access (FTA)**

6.7.1 Limitation of Concurrent Sessions and Session Management and Settings

When an authorized administrator has logged in, TOE provides a function to check whether the sum of sessions by administrator role or entire system is exceeded the maximum concurrent session allowed or not and to keep the count of concurrent sessions through eliminating the oldest session first in the case of excess. AS well TOE terminates by force inactive sessions held beyond the allowed time defined (time-range: 60~3600 seconds, default set: 600 seconds) and denies the administrator access attempted at an unacceptable remote address.

SFR to be satisfied : FTA_MCS.2, FTA_SSL.5(Extended), FTA_TSE.1