Data Security Solutions

Security Target

PrivacyDB V2.1

V1.7

OWL Systems Inc.

Dec 04, 2022

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

Revision History

Ver	Date	Author	Revision
V1.0	Nov 22, 2021	Sihun Lim	Initial release
V1.1	Apr 6, 2022	Sihun Lim	Complement content revisions based on full document indexes
V1.2	May 9, 2022	Sihun Lim	Modification and supplementation after the first review of CC re-verification
V1.3	May 27, 2022	Sihun Lim	Modification and supplementation after the second review of CC re-verification
V1.4	July 8, 2022	Sihun Lim	Modification and supplementation after the third review of CC re-verification
V1.5	July 29, 2022	Sihun Lim	Modification and supplementation after the fourth review of CC re-verification
V1.6	Nov 10, 2022	Youngmin Kim	Modification and supplementation
V1.7	Dec 04, 2022	Youngmin Kim	Modification and supplementation

< Table of Contents >

1. ST Introduction 6

1.1. ST Reference 6

1.2. TOE Reference 6

1.3. TOE Overview 7

1.4. TOE Description 11

1.5. Terms and Definitions 18

1.6. Conventions 24

2. Declaration of compliance 25

2.1. Declaration of compliance of CC, PP, Package 25

2.2. Rationale for PP Declaration of compliance 25

3. Security objectives 28

3.1. Security objectives for the operational environment 28

4. Extended Components Definition 29

4.1. Cryptographic support (FCS) 29

4.2. Identification & authentication (FIA) 29

4.3. User data protection (FDP) 30

4.4. Security Management(FMT) 31

4.5. Protection of the TSF(FPT) 32

4.6. TOE Access(FTA) 33

5. Security Requirements 35

5.1. Security Functional Requirements 35

5.2. Assurance requirements 49

5.3. Security Requirements Rationale 58

6. TOE Summary Specification 60

6.1. Security Audit (FAU) 60

6.2. Cryptographic Support (FCS) 61

6.3. User data protection (FDP) 63

6.4. Identification and Authentication (FIA) 63

6.5. Security Management (FMT) 64

6.6. Protection of the TSF 66

6.7. TOE Access 67

< List of Figures >

[Figure-1] Plug-in type operational environment (EOC, KMS separate type) 8
[Figure-2] Plug-in type operational environment (EOC, KMS integrated type) 9
[Figure-3] API-type operational environment (EOC, KMS separate type) 10
[Figure-4] API-type operational environment (EOC, KMS Integrated type) 10
[Figure-5] TOE Physical Configuration - Plug-in (EOC, KMS separate type) 12
[Figure-6] TOE Physical Configuration - Plug-in (EOC, KMS Integrated type) 12
[Figure-7] TOE Physical Configuration - API (EOC, KMS separate type) 13
[Figure-8] TOE Physical Configuration - API (EOC, KMS Integrated type) 13
[Figure-9] Logical Scope of the TOE 15

< List of Tables >

[Table 1] ST Reference 6
[Table 2] TOE Reference 7
[Table 3] Non-TOE Hardware required by the TOE 11
[Table 4] Non-TOE Software required by the TOE 11
[Table 5] Physical scope of the TOE 14
[Table 6] TOE Libraries 15
[Table 7] KCMVP 15
[Table 8] CC Declaration of compliance 25
[Table 9] Rationale for PP Declaration of compliance 27
[Table 10] Summary of Security Functional Components 36
[Table 11] Audit event 38
[Table 12] Audit Data Type and Selection Criteria 39
[Table 13] TSF Data Encryption Key Generation Standards and Algorithms 40
[Table 14] Cryptographic operation standards and algorithms 41
[Table 15] Cryptographic algorithm List 42
[Table 16] Standard random number generator algorithm 42
[Table 17] List of Security Functions Behavior of Administrator 46
[Table 18] List of TSF Data and Management Ability 47
[Table 19] Assurance Component Summary 50
[Table 20] Dependencies of the SFRs of the TOE 59
[Table 21] Audit data search 61
[Table 22] KCMVP 61
[Table 23] TOE Cryptographic Operation 63
[Table 24] List of Security Functions Behavior of Administrator 65
[Table 25] List of TSF Data and Management Ability 66

1. ST Introduction

This chapter introduces the Security Target (ST) of PrivacyDB V2.1 of OWL Systems Inc.

1.1. ST Reference

Classification	Description
Title	PrivacyDB V2.1 Security Target
Version	V1.7
Author	Hankoo Cho of OWL Systems Inc.
Publication Date	Dec 04, 2022
Common Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria Version	CC V3.1 r5
Evaluation Assurance Level	EAL 1+ (ATE_FUN.1)
Keywords	DB encryption, Encryption

[Table 1] ST Reference

1.2. TOE Reference

The components of this TOE are divided into the following four S/W.

Classification		Contents	Type	Distribution type
TOE Identification		PrivacyDB V2.1	-	
TOE Version		PrivacyDB V2.1.0.44	-	
TOE Component	PrivacyKMS	PrivacyKMS V2.1.0.11 - PrivacyKMS_linux_64bit_V2.1.0.11.tar	S/W	Distributed as a CD
	PrivacyConsole	PrivacyConsole V2.1.1.11 - PrivacyConsole_x64_V2.1.1.11.zip	S/W	
	PrivacyEOC_API	PrivacyEOC_API V2.1.0.11 - PrivacyEOC_API_linux_64bit_V2.1.0.11.tar	S/W	
	PrivacyEOC_Plug-in	PrivacyEOC_Plug-in V2.1.0.11 - PrivacyEOC_Plug-in_linux_64bit_V2.1.0.11.tar	S/W	
Guidance		PrivacyDB V2.1 Preparative Procedures V1.7	Electro	

	- PrivacyDB V2.1 Preparative Procedures V1.7.pdf PrivacyDB V2.1 User Operational Guidance V1.7 - PrivacyDB V2.1 User Operational Guidance V1.7.pdf	nic docum ents (PDF)	

[Table 2] TOE Reference

1.3. TOE Overview

PrivacyDB V2.1(hereinafter referred to as the 'TOE') encrypts the database (hereinafter referred to as the 'DB') to prevent unauthorized exposure of the information you want to protect. Cryptographic keys are used to encrypt user data that is managed by the key management server and stored in the DB.
TOE's encryption target is a DB that is managed by the database management system (hereinafter 'DBMS') in the operating environment. This security target defines all data as user data before and after encryption is stored in the DB. Depending on the security policy of the organization that operates the TOE, some or all of the user's data can be encrypted.

1.3.1. TOE Type and Scope

TOE is provided in the form of software and provides an encryption/decryption function for each column of user data. TOE is a DB encryption product that supports both methods and is divided into "plug-in method" and "API method" according to the location of encryption and decryption of user data.
The components of TOE consist of the key management server PrivacyKMS (hereinafter referred to as 'KMS') for encryption and policy management, API for performing encryption and decryption, PrivacyEOC_API and PrivacyEOC_Plug-in (hereinafter referred to as 'EOC') and management tools for setting administrator policies.

1.3.2. TOE Usage and Major Security Features

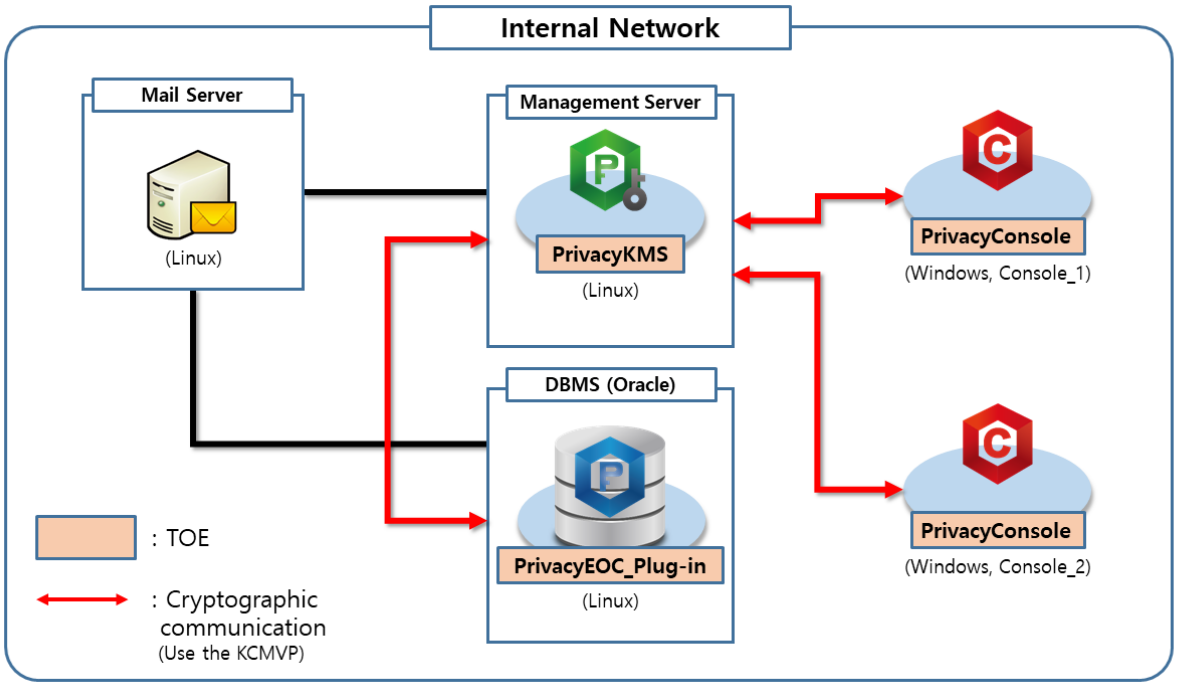
TOE provides the ability to encrypt and decrypt in accordance with security policies set by authorized administrators to prevent unauthorized exposure to the information you want to protect.
The TOE is required to use a validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP)
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.

The data encryption key (DEK) used to encrypt and decrypt user data is protected by encryption with the key encryption key (KEK). In addition, to protect stored TSF data and communication between TOE components. It shall be performed using the approved cryptographic algorithm of the validated cryptographic module of which safety and implementation suitabilities are validated using the Korea Cryptographic Module Validation Process (KCMVP).

1.3.3. TOE Operational Environment

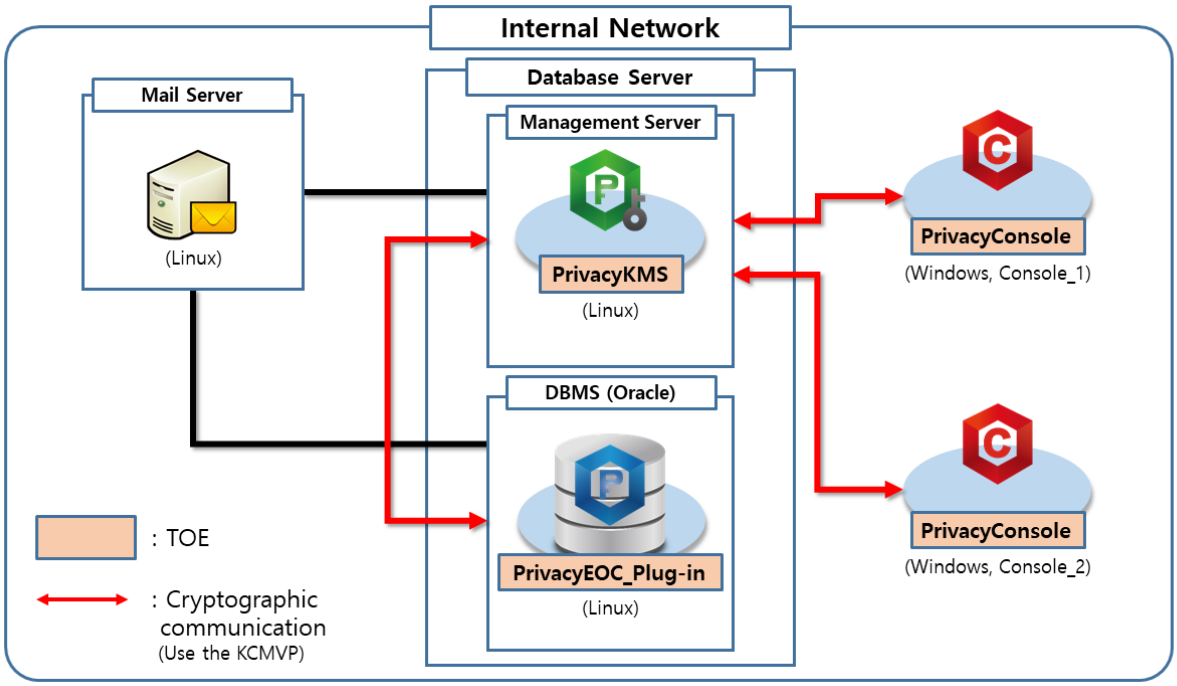
The operational environment of the TOE can be divided into 'plug-in' and 'API' as shown in the following figure. The operational environment of the TOE includes a mail server for authorized administrator notifications in potential violation analysis and audit data loss.

[Figure-1], [Figure-2] is a general plug-in operating environment. The EOC is installed within the Database Server where the protected DB resides and encrypts the user data received from the Application Server before storing it as DB in accordance with the security policy of an authorized administrator. EOC Performs the decryption of encrypted user data from the Database Server to the Application Server.



[Figure-1] Plug-in type operational environment (EOC, KMS separate type)

An authorized administrator accesses the KMS through the console to perform security management. An KMS can be installed with an EOC on a Database Server or physically separate from an EOC.

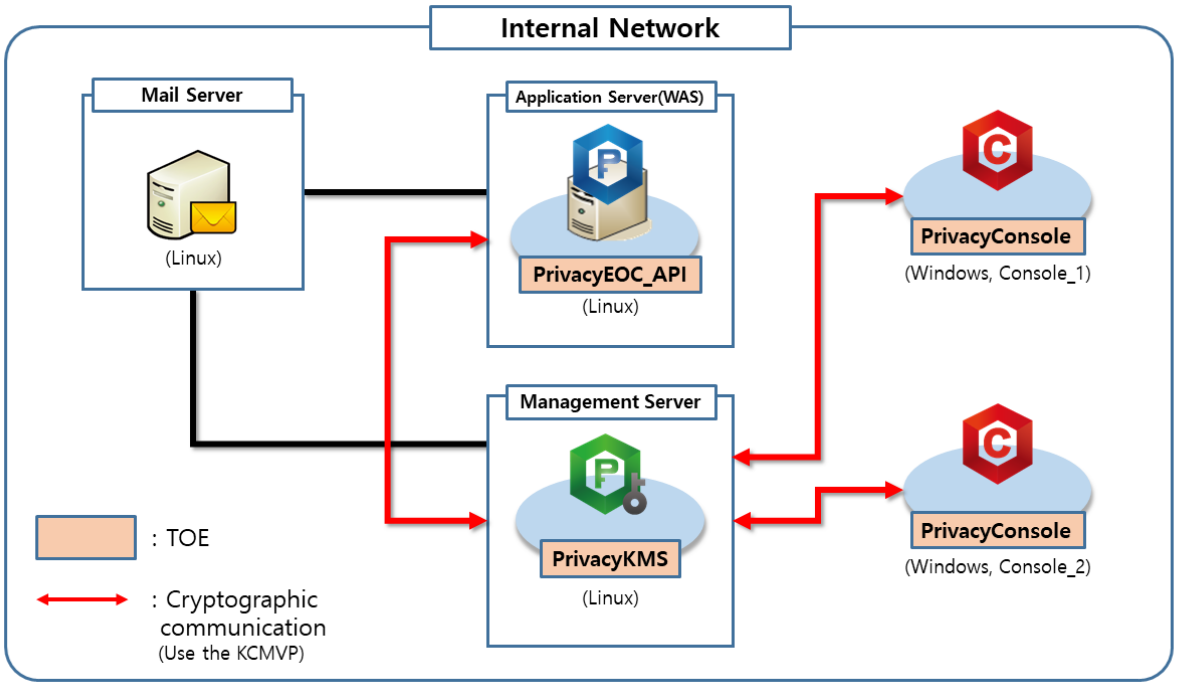


[Figure-2] Plug-in type operational environment (EOC, KMS integrated type)

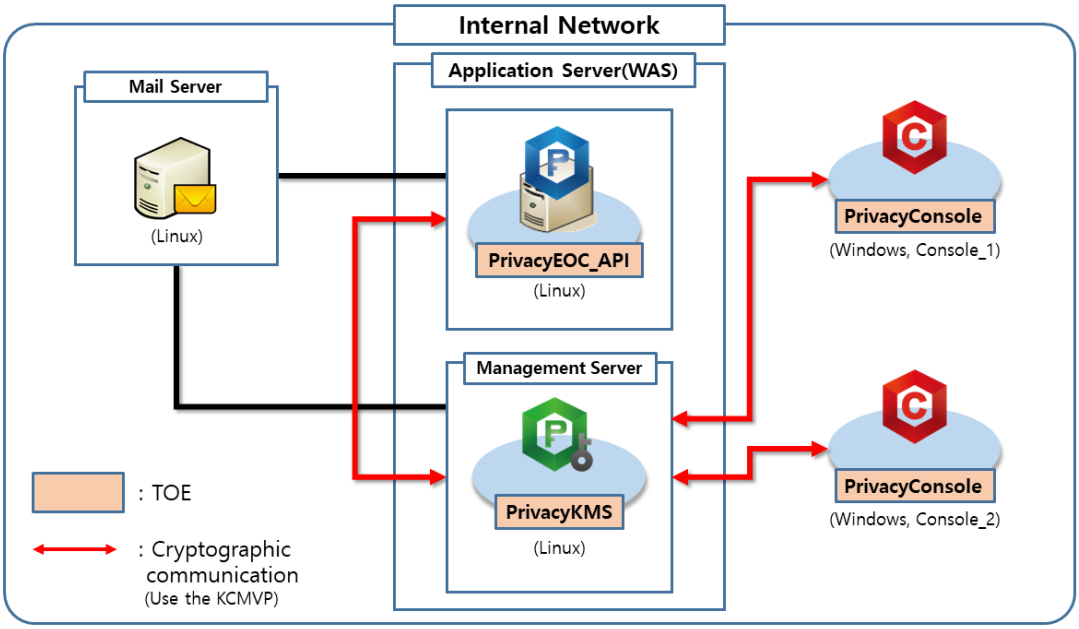
[Figure-3], [Figure-4] is an API-based operating environment. Applications that are installed in Application Server and provide application services are developed using the EOC to use the encryption and decryption function of the TOE.

The EOC is installed in Application Server and perform encryption and decryption of user data in accordance with the security policies of an authorized administrator. The user data entered by the application user is encrypted by the EOC installed on the Application Server and sent to the Database Server. Encrypted user data from the Database Server is decrypted by the EOC installed on the Application Server and sent to the application user.

An authorized administrator accesses the KMS to perform security management. The KMS can be installed with the EOC in an Application Server or physically separate from the EOC.



[Figure-3] API-type operational environment (EOC, KMS separate type)



[Figure-4] API-type operational environment (EOC, KMS Integrated type)

1.3.4. Non-TOE environment required by TOE

In addition, the external IT entities required for TOE operations are:

- SMTP Server used to send alert mail to administrators

The hardware required for the TOE to be installed is as follows.

TOE Component	Contents
PrivacyKMS	CPU: Intel Dual core 2.4 GHz or higher
PrivacyEOC_API	Memory: 8 GB Memory or higher
PrivacyEOC_Plug-in	HDD: Space required for TOE installation is 30 GB or higher
PrivacyConsole	NIC : 10/100/1000 Mbps * 1 EA or higher

[Table 3] Non-TOE Hardware required by the TOE

The 3rd Party software required for operation of the TOE is not included in the scope of the TOE, as follows:

TOE Component	Type	Contents	Notes
PrivacyKMS	OS	Ubuntu 16.04.6 LTS 64 bit (GNU/Linux 4.4.0-142-generic x86_64)	
	DBMS	PostgreSQL 12.13	Audit Storage
PrivacyEOC_API	OS	Ubuntu 16.04.6 LTS 64 bit (GNU/Linux 4.4.0-142-generic x86_64)	
PrivacyEOC_Plug-in	OS	Ubuntu 16.04.6 LTS 64 bit (GNU/Linux 4.4.0-142-generic x86_64)	
	DBMS	Oracle Database 11g Release 2 (11.2)	
PrivacyConsole	OS	Windows 10 Pro 64 bit	
	JRE	Java JRE 8u351	

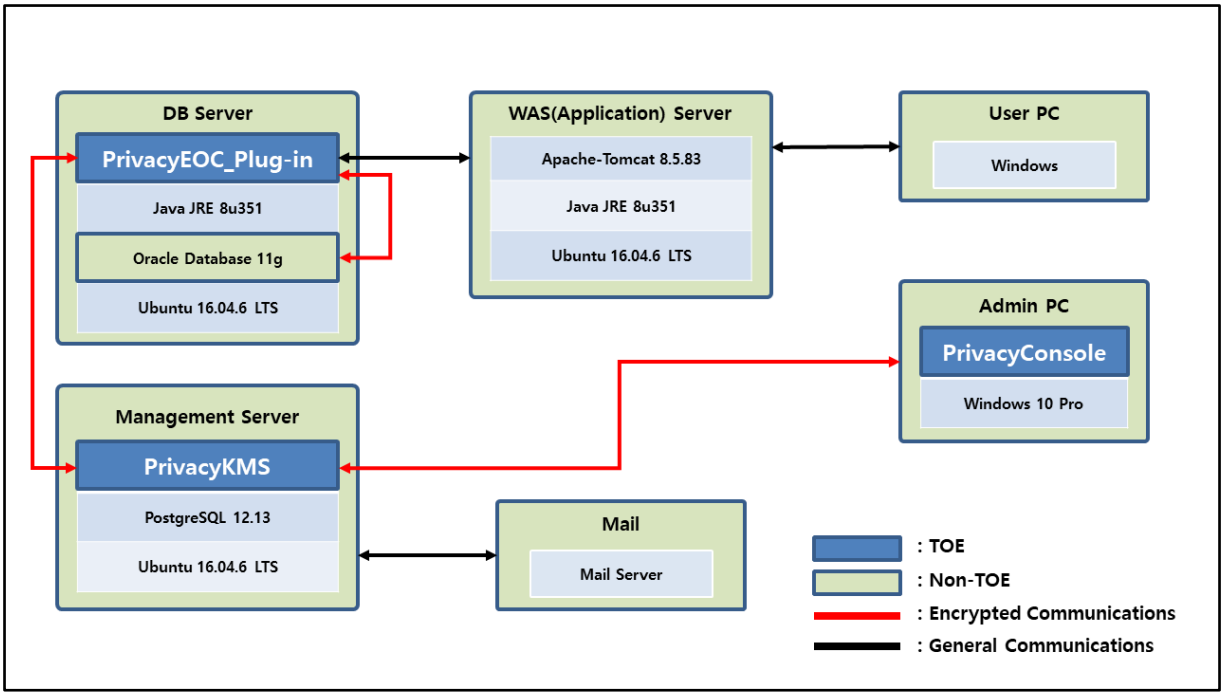
[Table 4] Non-TOE Software required by the TOE

1.4. TOE Description

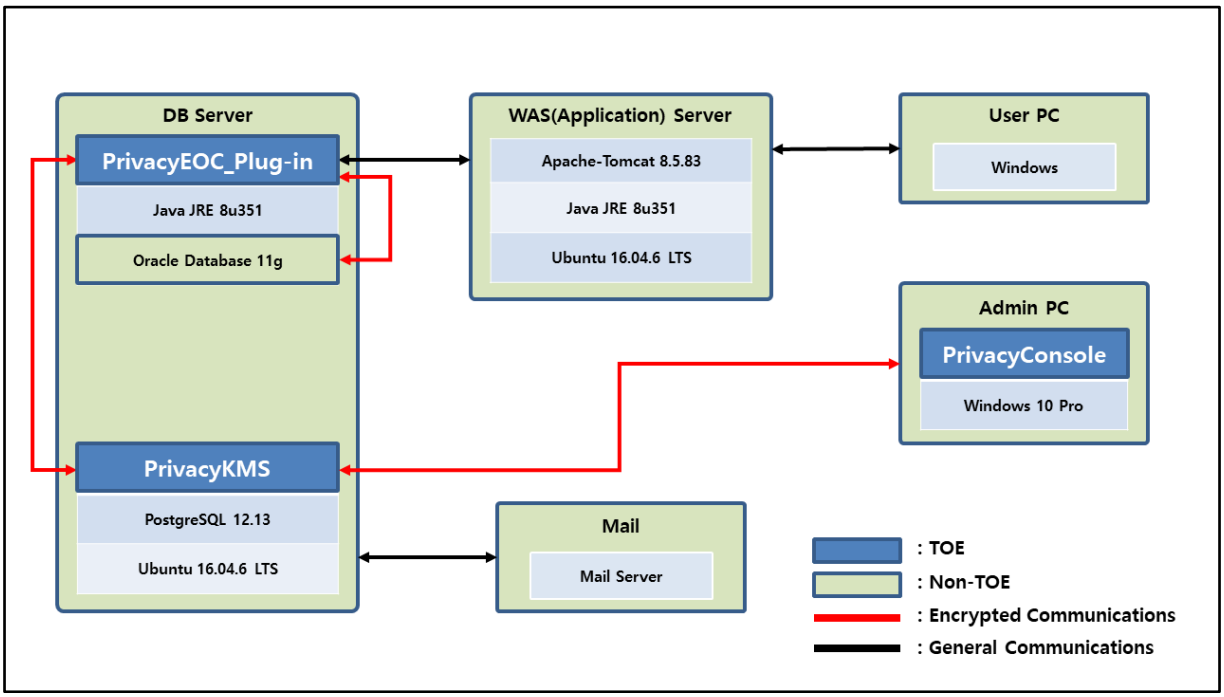
This section describes the physical and logical ranges of the TOE.

1.4.1. Physical Scope of the TOE

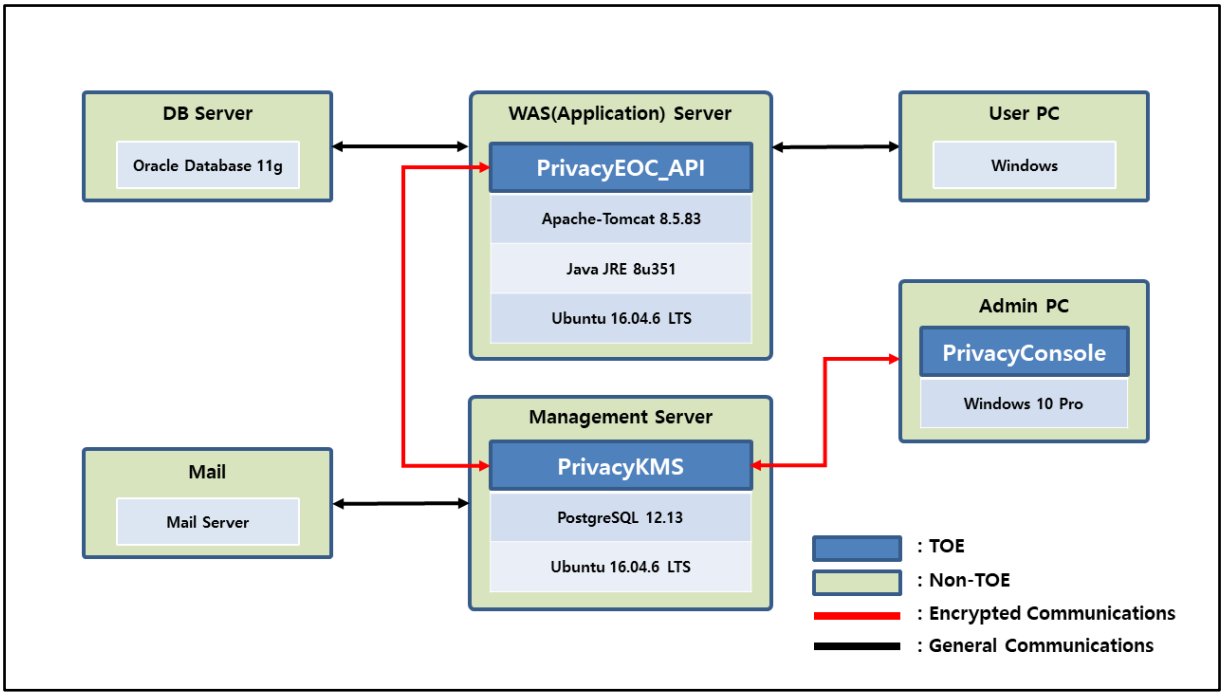
The TOE consists of KMS, which is security policy establishment and management server, Console, which is an administrator tool, and EOC that encrypts and decrypts data in a DB or an application by receiving a DB cryptographic key and an encryption policy stored in KMS.
The EOC is installed on the WEB/WAS server for the API method and on the target DB server for the Plug-in method.



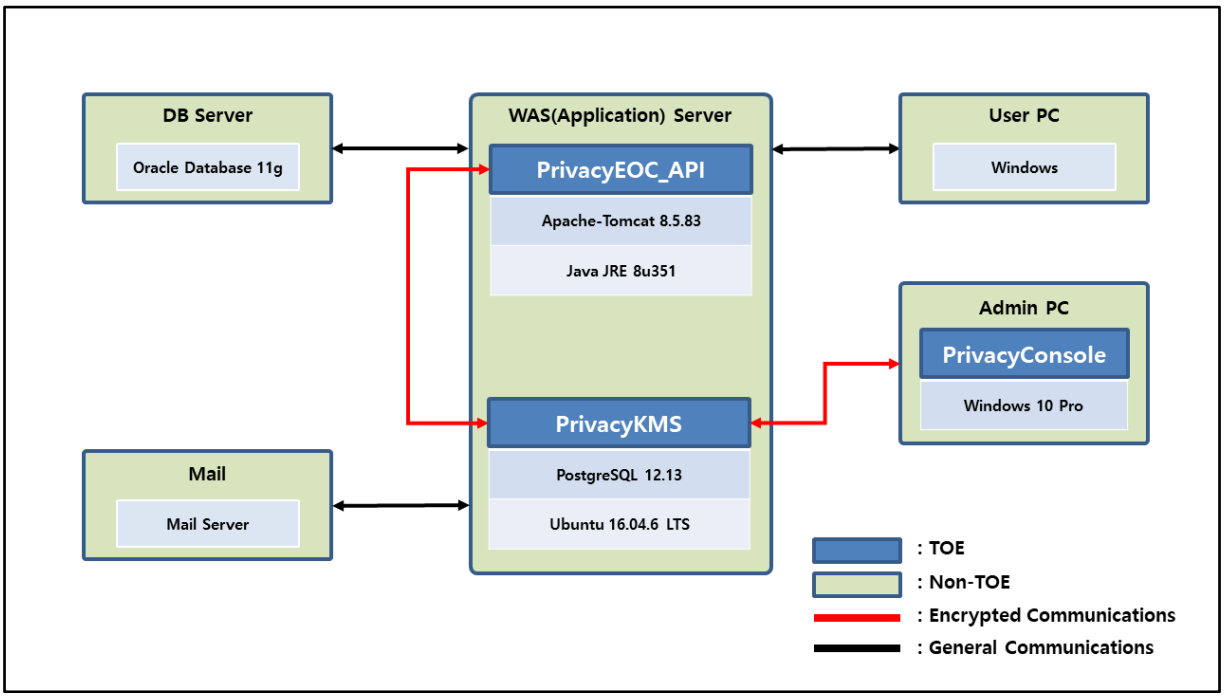
[Figure-5] TOE Physical Configuration - Plug-in (EOC, KMS separate type)



[Figure-6] TOE Physical Configuration - Plug-in (EOC, KMS Integrated type)



[Figure-7] TOE Physical Configuration - API (EOC, KMS separate type)



[Figure-8] TOE Physical Configuration - API (EOC, KMS Integrated type)

The TOE consists of KMS, EOC, Console and User Operational Guidance and Preparation Procedure.

Classification	Contents	Type	Distribution type
TOE Identification	PrivacyDB V2.1	-	
TOE Version	PrivacyDB V2.1.0.44	-	

TOE Component	PrivacyKMS	PrivacyKMS V2.1.0.11 - PrivacyKMS_linux_64bit_V2.1.0.11.tar	S/W	Distributed as a CD
	PrivacyConsole	PrivacyConsole V2.1.1.11 - PrivacyConsole_x64_V2.1.1.11.zip	S/W	
	PrivacyEOC_API	PrivacyEOC_API V2.1.0.11 - PrivacyEOC_API_linux_64bit_V2.1.0.11.tar	S/W	
	PrivacyEOC_Plug-in	PrivacyEOC_Plug-in V2.1.0.11 - PrivacyEOC_Plug-in_linux_64bit_V2.1.0.11.tar	S/W	
Guidance		PrivacyDB V2.1 Preparative Procedures V1.7 - PrivacyDB V2.1 Preparative Procedures V1.7.pdf PrivacyDB V2.1 User Operational Guidance V1.7 - PrivacyDB V2.1 User Operational Guidance V1.7.pdf	Electronic documents (PDF)	

[Table 5] Physical scope of the TOE

TOE Conponent	Type	Purpose	Version
PrivacyKMS	Key# Crypto v1.4	Raonsecure Encryption Module	V1.4.0.7
	PostgreSQL	PostgreSQL Library	V12.13
PrivacyEOC_API	Key# Crypto v1.4	Raonsecure Encryption Module	V1.4.0.7
PrivacyEOC_Plug-in	Key# Crypto v1.4	Raonsecure Encryption Module	V1.4.0.7
PrivacyConsole	Key# Crypto v1.4	Raonsecure Encryption Module	V1.4.0.7
	zlib1	Data Compression Library	V1.2.6.0

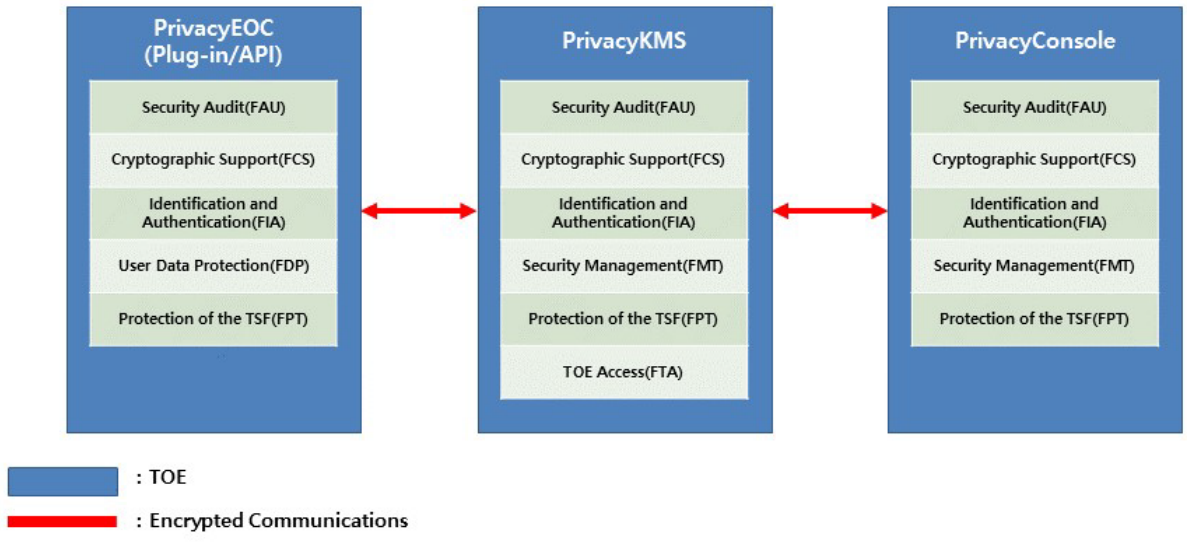
[Table 6] TOE Libraries

Classification	Description
Cryptographic module name	Key# Crypto v1.4
Developed company	Raonsecure Co., Ltd.
Validation No.	CM-180-2026.1
Module type	S/W(Library)
Validation Date	Jan 20, 2021
Effective Expiration Date	Jan 20, 2026

[Table 7] KCMVP

1.4.2. Logical Scope of the TOE

The logical scope of the TOE consists of security audits, cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, and TOE access, as shown in the [Figure-6] Logical scope of the TOE, as follows.



[Figure-9] Logical Scope of the TOE

■ Security Audit

TOE generates audit data using trusted time information for major audit cases and notifies authorized managers by e-mail if potential security violations occur.

Privacy KMS notifies authorized managers by e-mail when audit trail exceeds 90% of the threshold, overwrites the oldest log when audit trail is saturated, and notifies authorized managers by e-mail. Only authorized managers are allowed to inquire audit data through Privacy Console, and optional inquiry functions are supported when inquiring audit data.

■ Cryptographic Support

TOE generates audit data using trusted time information for major audit cases and notifies authorized managers by e-mail if potential security violations occur.

Privacy KMS notifies authorized managers by e-mail when audit trail exceeds 90% of the threshold, overwrites the oldest log when audit trail is saturated, and notifies authorized managers by e-mail. Only authorized managers are allowed to inquire audit data through Privacy Console, and optional inquiry functions are supported when inquiring audit data.

■ User data protection

PrivacyEOC encrypts and stores user data stored in the protected DBMS using a verified encryption module. Encryption and decryption are performed through block encryption algorithms (ARIA-128, 192, 256, SEED-128) according to the security policy set by the authorized administrator. Additionally, unidirectional encryption is supported through hash algorithms SHA-256, 384, and 512.

PrivacyEOC provides a function of encrypting and decrypting user data for each column. In addition, when encrypting user data, the same ciphertext is not generated for the same plaintext. After encryption of user data is performed, complete deletion is performed so that the original data is not available.

■ Identification and Authentication

Privacy KMS uses Privacy Console to identify and authenticate the identity of the accessed administrator based on ID and PW, and locks the administrator account for a certain period of time when the threshold of the number of consecutive authentication failures of the administrator is reached. To prevent reuse of administrator authentication data, the only session ID provides a function to verify use.

PrivacyConsole marks PW as '*' during administrator authentication and does not provide a reason for authentication failure.

Create administrator account of Privacy KMS, authenticate administrator of Privacy Console, and verify whether it meets defined security criteria (length and combination rules) when changing PW.

Privacy KMS and Privacy Console, Privacy KMS and Privacy EOC perform mutual authentication.

■ Security Management

Only authorized administrators who have passed the identification and authentication of Privacy KMS can

perform security management functions such as setting security functions, setting security policies, and generating encryption keys. When the administrator accesses for the first time, it is forced to change the password for the administrator, and the administrator can only perform security management through Privacy Console.

■ Protection of the TSF

PrivacyKMS encrypts and protects critical TSF data stored in TSF-controlled repositories. TSF data transmitted between TOE components is protected through encryption and message integrity verification. The TOE periodically performs self-testing on major processes during operation when the TOE is running, and periodically performs integrity checks on the TOE configuration file and the TOE during operation when the TOE is running.

■ TOE Access

Privacy KMS allows only management access sessions of terminals designated as access permission IP, and rejects management access sessions of terminals other than access permission IP. If there is no activity for a certain period of time after logging in, the authorized administrator provides a function to end the session, and maintains only one session so that the same administrator cannot log in repeatedly.

1.5. Terms and Definitions

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

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

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

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

Self test
Pre-operational and conditional testing performed by the cryptographic module.

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

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

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

Authorized Administrator
Authorized user to securely operates and manages the TOE

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

Authorized User

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

Can/could

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

column

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

Component

Smallest selectable set of elements on which requirements may be based

Critical Security Parameters(CSP)

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

Class

Set of CC families that share a common focus

Database(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

Database Management System(DBMS)

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

Data Encryption Key(DEK)

Key that encrypts and decrypts data.

DB encryption key

Key to encrypt and decrypt real table columns

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

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

Element
Indivisible statement of a security need

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

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

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

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 encryption key
This is the key to encrypt master key

Master key
Key to encrypt the Encryption key when saving it to a file

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

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 an unique entity (the subject using the public key), it can be disclosed

Public Key (Asymmetric) Cryptographic Algorithm
A cryptographic algorithm that uses a pair of public and private keys

Random Bit Generator(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

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

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

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

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

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

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

Session Key
Encryption key to encrypt and decrypt data in the communications section

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

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

Subject

Active entity in the TOE that performs operations on objects

Target of Evaluation(TOE)

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

TLS(Transport Layer Security)

An SSL-based cryptographic authentication communication protocol between servers and clients, 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

User

Refer to "External entity"

User Data

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

1.6. Conventions

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

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

Iteration

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

Assignment

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

Selection

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

Refinement

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

2. Declaration of compliance

2.1. Declaration of compliance of CC, PP, Package

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

Classification	Compliance
Declaration of compliance with the Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 - Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
Declaration of compliance with the Common Criteria Part 2	Extended: FCS_RBG.1, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
Declaration of compliance with the Common Criteria Part 3	*Conformant*
Conformance Claim Package	Augmented: EAL1+ *augmented* (ATE_FUN.1)
Protection Profile	Korean National PP for Database Encryption V1.1

[Table 8] CC Declaration of compliance

2.2. Rationale for PP Declaration of compliance

This ST complied with the same type of TOE and security requirements by strict compliance with the Korean National PP for Database Encryption V1.1

Classification	PP	ST	Rationale
Type of TOE	Database Encryption	Database Encryption	Same as PP
Security Function Requirement (SFR)	FAU_ARP.1	FAU_ARP.1	Same as PP
	FAU_GEN.1	FAU_GEN.1	Same as PP
	FAU_SAA.1	FAU_SAA.1	Same as PP
	FAU_SAR.1	FAU_SAR.1	Same as PP

	FAU_SAR.3	FAU_SAR.3	Same as PP
	FAU_SEL.1	FAU_SEL.1	Same as PP
	FAU_STG.3	FAU_STG.3	Same as PP
	FAU_STG.4	FAU_STG.4	Same as PP
	FCS_CKM.1(1)	FCS_CKM.1(1)	Same as PP
	FCS_CKM.1(2)	FCS_CKM.1(2)	Same as PP
	FCS_CKM.2	FCS_CKM.2	Same as PP
	FCS_CKM.4	FCS_CKM.4	Same as PP
	FCS_COP.1(1)	FCS_COP.1(1)	Same as PP
	FCS_COP.1(2)	FCS_COP.1(2)	Same as PP
	FCS_RBG.1(Extended)	FCS_RBG.1(Extended)	Same as PP
	FDP_UDE.1(Extended)	FDP_UDE.1(Extended)	Same as PP
	FDP_RIP.1	FDP_RIP.1	Same as PP
	FIA_AFL.1	FIA_AFL.1	Same as PP
	FIA_IMA.1(Extended)	FIA_IMA.1(Extended)	Same as PP
	FIA_SOS.1	FIA_SOS.1	Same as PP
	FIA_UAU.1	FIA_UAU.1	Same as PP
	FIA_UAU.4	FIA_UAU.4	Same as PP
	FIA_UAU.7	FIA_UAU.7	Same as PP
	FIA_UID.1	FIA_UID.1	Same as PP
	FMT_MOF.1	FMT_MOF.1	Same as PP
	FMT_MTD.1	FMT_MTD.1	Same as PP
	FMT_PWD.1(Extended)	FMT_PWD.1(Extended)	Same as PP
	FMT_SMF.1	FMT_SMF.1	Same as PP
	FMT_SMR.1	FMT_SMR.1	Same as PP
	FPT_ITT.1	FPT_ITT.1	Same as PP
	FPT_PST.1(Extended)	FPT_PST.1(Extended)	Same as PP
	FPT_TST.1	FPT_TST.1	Same as PP
	FTA_MCS.2	FTA_MCS.2	Same as PP
	FTA_SSL.5(Extended)	FTA_SSL.5(Extended)	Same as PP
	FTA_TSE.1	FTA_TSE.1	Same as PP
Security Assurance Requirement (SAR)	AGD_OPE.1	AGD_OPE.1	Same as PP
	AGD_PRE.1	AGD_PRE.1	Same as PP
	ALC_CMC.1	ALC_CMC.1	Same as PP
	ALC_CMS.1	ALC_CMS.1	Same as PP
	ASE_CCL.1	ASE_CCL.1	Same as PP
	ASE_ECD.1	ASE_ECD.1	Same as PP
	ASE_INT.1	ASE_INT.1	Same as PP

	ASE_OBJ.1	ASE_OBJ.1	Same as PP
	ASE_REQ.1	ASE_REQ.1	Same as PP
	ASE_TSS.1	ASE_TSS.1	Same as PP
	ATE_FUN.1	ATE_FUN.1	Same as PP
	ATE_IND.1	ATE_IND.1	Same as PP
	AVA_VAN.1	AVA_VAN.1	Same as PP

[Table 9] Rationale for PP Declaration of compliance

3. Security objectives

3.1. Security objectives for the operational environment

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

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

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

OE.OPERATION_SYSTEM_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.AUDIT_DATA_PROTECTION
Audit records with stored audit evidence, such as DBMS that interact with TOE, shall be protected from unauthorized deletion or modification.

OE.TIME_STAMP
The TOE shall accurately record security-relevant events by using reliable time stamps provided by the TOE operational environment.

4. Extended Components Definition

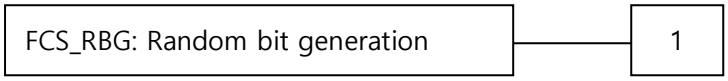
4.1. Cryptographic support (FCS)

4.1.1. Random Bit Generation

Family Behavior

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

Component Leveling



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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

4.1.1.1. FCS_RBG.1 Random bit generation

Hierarchical to No other components

Dependencies No dependencies

FCS_RBG.1.1 The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

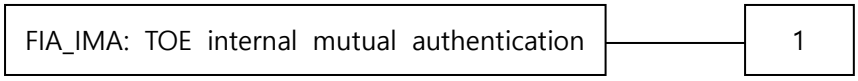
4.2. Identification & authentication (FIA)

4.2.1. Mutual authentication between TOE components

Family Behavior

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: Change of authentication protocol

4.2.1.1. FIA_IMA.1 Mutual authentication between TOE components

FIA_IMA.1	TOE internal mutual authentication	
	Hierarchical to	No other components
	Dependencies	No dependencies

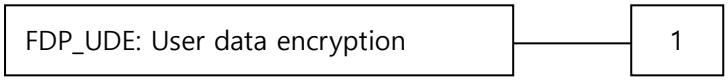
FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE]* using the [assignment: authentication protocol] that meets the following: [assignment: *list of standards*].

4.3. User data protection (FDP)

4.3.1. User data encryption

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

Component Leveling



FDP_UDE.1 User Data Encryption(FDP) 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

4.3.1.1. FDP_UDE.1 User data encryption

Hierarchical to	No other components
Dependencies	FCS_COP.1 Cryptographic operation

FDP_UDE.1.1 TSF shall provide TOE users with the ability to encrypt/decrypt user data according to [assignment: *the list of Encryption/decryption methods*] specified.

4.4. Security Management(FMT)

4.4.1. ID and Password

Family Behavior
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

4.4.1.1. 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 roles*].
1.[assignment *password combination rules and/or length*]
2.[assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
1.[assignment : *ID combination rules and/or length*]
2.[assignment : *other management such as management of special characters unusable for ID, etc.*]

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

4.5. Protection of the TSF(FPT)

4.5.1. Protection of stored TSF data

Family Behavior

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.

4.5.1.1. 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*].

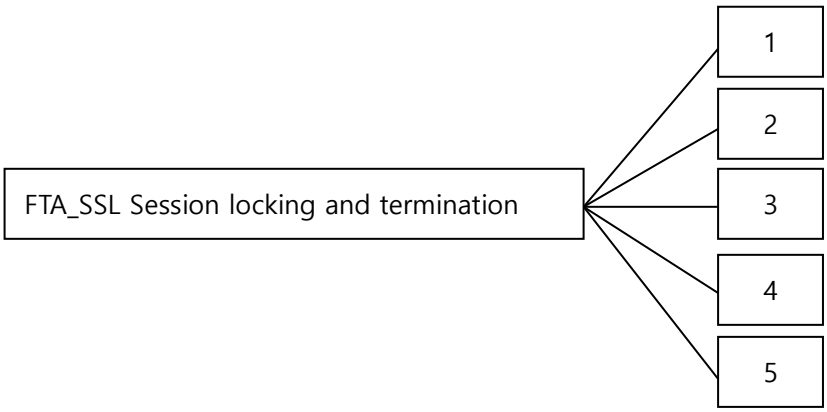
4.6. TOE Access(FTA)

4.6.1. Session Locking and Termination

Family Behavior

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 terminating family consists of four components. In this PP, as one component is further expanded as follows, it consists of five components.

※ The description of the four components included in Part 2 of CC 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 of the time period of user inactivity that results in session locking or 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 sessions

4.6.1.1. 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 describe security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to this ST.

5.1. Security Functional Requirements

The security function requirements defined in this ST are expressed by selecting the relevant security function components from CC Part 2 to satisfy the security objectives identified in Chapter 4.
The following [Table 10] provides a summary of the security function components used in this ST.

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation(TSF data encryption)
	FCS_RBG.1(Extended)	Random bit generation
User Data Protection (FDP)	FDP_UDE.1(Extended)	User data encryption
	FDP_RIP.1	Protect the residual information Protection
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Certified
	FIA_UAU.4	Single-use authentication mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	User identification

Security Management (FMT)	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF testing
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

[Table 10] Summary of Security Functional Components

5.1.1. Security Audit (FAU)

5.1.1.1. FAU_ARP.1 Security alarms

Hierarchical to No other components

Dependencies FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [an email notification to an authorized administrator] upon detection of a potential security violation.

5.1.1.2. FAU_GEN.1 Audit data generation

Hierarchical to No other components

Dependencies FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions.
b) All auditable events for the *not specified* level of audit, and
c) [Refer to "auditable event" in [Table 11] Auditable Event. [None]

Security Functional Component	Auditable Event	Additional Audit Record
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	

FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	
FCS_CKM.4	Success and failure of the activity (only applying to destruction of key related to user data encryption/decryption)	
FCS_COP.1	Success and failure of cryptographic operation	
FDP_UDE.1	Success and failure of user data encryption/decryption	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the action 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 uses of authentication mechanisms	
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 behavior of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5	Locking or termination of interactive session	

FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

[Table 11] Audit event

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable) and the outcome (success of failure) of the event: and
b) For each audit event type, based on the auditable event definitions of the functional components include in the ST, [refer to "Additional Audit Record" in [Table 11] Auditable Event, (*None*)]

5.1.1.3. FAU_SAA.1 Potential violation analysis

Hierarchical to No other components
Dependencies FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs**.**

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [
- Authentication failure audit event among auditable event in FIA_UAU.1
- Integrity violation event among auditable events in FPT_TST.1
- Self-test failure of the KCMVP, cumulative or combination of [None]

b) [None]

5.1.1.4. 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.

5.1.1.5. FAU_SAR.3 Selectable audit review

Hierarchical to No other components

Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the capability to apply [the following conditions (AND)] of audit data based on [the following conditions (AND) or sequencing methods]**.**

Audit Data Type	Selection Criteria (AND)	Allowable Ability
Administrator log	Date and time	The search results that meet the selected search conditions are sorted in descending order in chronological order.
	Data type	
	Type of action	
	Result code	
	Security name	

[Table 12] Audit Data Type and Selection Criteria

5.1.1.6. FAU_STG.3 Selective audit

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) [None]

Application notes : This requirement is applied to the encryption / decryption success log and whether to include cipher text in the log.

5.1.1.7. FAU_STG.3 Action in case of possible audit data loss

Hierarchical to No other components
Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [notification to the authorized administrator, [None]] if the audit trail exceeds [90 Percentage of DB table-wide rows].

5.1.1.8. 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 oldest audit records* and [Notify authorized administrators] if the audit trail is full.

5.1.2. Cryptographic Support (FCS)

5.1.2.1. 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 the specified cryptographic key generation algorithm [HASH_DRBG(SHA 256)] and the specified cryptographic key length [128, 192, 256 Bit] in accordance with the following [TTAK.KO-12.0331]

5.1.2.2. 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 the specified encryption key generation algorithm [key generation algorithm of [Table 13]] and the cryptographic key length [cryptographic key length of [Table 13]] in accordance with the following [Stanard List of [Table 13]].

Standard List	Key generation algorithm	Cryptographic key length	Encryption key usage
TTAK.KO-12.0331	HASH_DRBG (SHA 256)	256	Encryption and decryption of configuration Encryption and decryption of security policy file, transport data, and DB encryption key, Session key distribution
PKCS#5-RFC 2898	PBKDF2	256	Encryption and decryption Master key

[Table 13] TSF Data Encryption Key Generation Standards and Algorithms

Note for application: When generating a key (KEK) for key encryption by deriving it from a password, the pseudo-random function uses HMAC-SHA2 and the authorization count is 100,000.

5.1.2.3. FCS_CKM.2 Cryptographic key distribution

Hierarchical to No other components
Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data without security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute encryption keys in accordance with the stated cryptographic method [public key and symmetric key encryption methods] consistent with the following [None]

5.1.2.4. 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 without security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy the encryption key in accordance with the stated cryptographic method [overwrite with "0" three times] that conforms to the following [None]:

5.1.2.5. 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 following TSF shall perform [Standard List of [Table 14]] according to the stated cryptographic algorithm [Cryptographic Algorithm List of [Table 14]] and the specified cryptographic key length [Cryptographic Key Length of [Table 14]] in accordance with the following [Operation list of [Table 14]].

Standard List	Cryptographic Algorithms	Cryptographic Key length	Operation mode	Operation list
KS X 1213-1	ARIA	128, 192, 256	CBC, OFB, CFB, CTR,	Encrypt and decrypt user data stored in DB
TTAS.KO-12.0004/R1	SEED	128	CBC, OFB, CFB, CTR	
ISO/IEC 10118-3	SHA256, SHA-384, SHA-512	N/A	N/A	Encrypt user data stored in DB

[Table 14] Cryptographic operation standards and algorithms

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

Hierarchical to No other components

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 TSF shall perform [Standard List of [Table 15]] according to the stated cryptographic algorithm [Cryptographic Algorithm of [Table 15]] and the specified cryptographic key length [Cryptographic key length of [Table 15]] that complies with the following [Operation List of [Table 15]].

Standard List	Cryptographic Algorithm	Cryptographic key length	Operation mode	Operation List
KS X 1213-1	ARIA	256	CBC	Encryption and decryption of security policy file, transport data, and DB encryption key
ISO/IEC 18033-2	RSAES	2048	N/A	Encryption key distribution
ISO/IEC 14888-2	RSA-PSS	2048	N/A	Mutual authentication, Integrity verification, Encryption of authentication data
ISO/IEC 10118-3	SHA256	N/A	N/A	Integrity verification

[Table 15] Cryptographic algorithm List

5.1.2.7. FCS_RBG.1 Random bit generation (extended)

Hierarchical to No other components
Dependencies No dependencies
FCS_RBG.1.1 The TSF shall generate random numbers using a specified random number generator conforming to the following [Standard of [Table 16]].

Standard	Cryptographic Algorithm	Random number lenght
TTAK.KO-12.0331-Part2	HASH-DRBG (SHA 256)	256

[Table 16] Standard random number generator algorithm

5.1.3. User data protection(FDP)

5.1.3.1. FDP_UDE.1 User data protection (extended)

Hierarchical to No other components
Dependencies cryptographic operational.

FDP_UDE.1.1 TSF should provide TOE users with the ability to encrypt and decrypt user data

according to the [Column-specific encryption method, [None]] stated.

5.1.3.2. 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 form* the following objects. [user data].

5.1.4. Identification and authentication(FIA)

5.1.4.1. FIA_AFL.1 Authentication failure handling

Hierarchical to No other components

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [*Administrator Authentication Attempts*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [lock the screen for 5 minutes and notify the administrator of mail].

5.1.4.2. FIA_IMA.1 TOE Internal mutual authentication (extended)

Hierarchical to No other components

Dependencies No dependencies

FIA_IMA.1.1 TSF shall perform mutual authentication using [Self-authentication protocol] in accordance with [None] between [PrivacyConsole and PrivacyKMS, PrivacyKMS and PrivacyEOC].

5.1.4.3. FIA_SOS.1 Verification of secrets

Hierarchical to No other components

Dependencies No dependencies

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

[Password combination rules]

- Digits : 10 ~ 40
- Three combinations of letters, special characters, and numbers
- Number(10) : 0~9,

- English capital letter(26) : A~Z,
- English small letter (26) : a~z,
- Special character(32) : `~!@#$%^&*()-_+=[]{}₩|;:'",.<>/?

FIA_UAU.1 **User authentication**

Hierarchical to No other components

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [certificate generation] to be performed on behalf of the authorized manager before the authorized manager is authenticated.

FIA_UAU.1.2 The TSF shall successfully certify the accredited manager before allowing any other actions mediated by the TSF on behalf of the accredited manager other than those specified in FIA_UAU.1.1.

5.1.4.5. FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components

Dependencies No dependencies

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

5.1.4.6. FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components

Dependencies FIA_UAU.1 Timing of identification

FIA_UAU.7.1 The TSF shall provide only ['*', a message that cannot infer the reason for failure in the event of authentication failure] to the user while the authentication is in progress

5.1.4.7. FIA_UID.1 User identification before any action

Hierarchical to No other components

Dependencies No dependencies

FIA_UID.1.1 The TSF shall allow [certificate generation] to be performed on behalf of the authorized manager before identifying the authorized manager.

FIA_UID.1.2 The TSF must successfully identify each accredited manager before allowing any other actions mediated by the TSF on behalf of the accredited manager other than those specified in FIA_UID.1.1.

5.1.5. Security Management(FMT)

5.1.5.1. FMT_MOF.1 Management of security functions behavior

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 administrative actions of the functions of security function of [Table 17] to [Authorised Managers].

Administrator Type	Classification	Security Function	Ability			
			Determine the behavior	Not use	use	Modify the behavior
Authorized Administrator	Encryption key management	Generate encryption and decryption key	○	-	○	-
	Security management	Encryption target type	○	○	○	○
		Type of encryption algorithm	○	○	○	○
		User data integrity check feature	○	○	○	○
		Double encryption	○	○	○	○
		Encryption pattern	○	○	○	○
	Access control	User access right	○	○	○	○
	Environmental management	User access right (Permit and deny policy)	○	○	-	○
		Administrator IP setting	-	○	○	○
		Mail server setting	-	○	○	○
	Audit log	Selecting of audit targets (plain text, cipher text)	○	○	○	○
		Creating a success log	○	○	○	○

[Table 17] List of Security Functions Behavior of Administrator

5.1.5.2. 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 [data type of [Table 18]] to [Authorized Administrators].

Administrator Type	Classification	TSF Data	Ability				
			Modify Default	Query	Update	Create	Delete
Authorized Administrator	Key management	Encryption and Decryption of user data key management	-	○	-	○	○
		Master key management	-	-	○	○	-
	User management	DB user management	-	○	○	○	○
	Security management	User data security policy management	○	○	○	○	○
	Access Control	Access time management	○	○	-	○	○
		Manage access user	○	○	-	○	○
		Access IP management	-	○	○	○	○
		Manage access program	-	○	○	○	○
	Environmental management	Administrator IP	–	○	○	○	○
		Mail Server management	–	○	○	○	○
	Audit log	Admin log	-	○	-	-	-
		Encryption log	-	○	-	-	-

	Certified information	Password log	-	-	○	○	-

[Table 18] List of TSF Data and Management Ability

5.1.5.3. 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 The TSF shall restrict the ability to manage ID of [None].
1. [None]
2. [None]

FMT_PWD.1.3 The TSF shall provide the ability to set the ID and password during the installation process.

5.1.5.4. 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]
- Management functions of the TSF: Management functions specified in FMT_MOF.1
- Management of TSF data: Management functions specified in FMT_MTD.12
- Management of security role: Management functions specified in FMT_SMR.1

5.1.5.5. 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 [Authentication Administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with **roles defined in FMT_SMR.1.1**

5.1.6. Protection of the TSF(FPT)

5.1.6.1. FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical No other components

Dependencies No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE **through the encryption and message integrity verification**.

5.1.6.2. 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 [the following TSF data] stored in the containers controlled by the TSF from unauthorized *disclosure, modification*.

- Administrator authentication data
- Database access account information
- Encryption key
- TOE setting value (configuration, security policy settings, etc.)

5.1.6.3. FPT_TST.1 TSF testing

Hierarchical to No other components

Dependencies No dependencies

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

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

FPT_TST.1.3 The TSF shall provide the **authorized administrator** with the capability to verify the integrity of *TSF*

Components of the product performing the encryption/decryption function shall receive the results of the self-test of the verified cryptographic module and notify the authorized manager in the event of failure.

5.1.7. TOE Access(FTA)

5.1.7.1. FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF has a list of management functions defined in [FMT_SMF.1.1:
a) Limit the maximum number of concurrent sessions to 1 for administrative access by the same administrator who have the authority to perform "management behavior" in FMT_MOF.1.1 and "management" in FMT_MTD.1.1.
b) 'Management behavior' in FMT_MOF.1.1 cannot be performed and 'manage' in FMT_MTD.1.1 maximum number of sessions for the same administrator with the right to perform query only 0 person.
c) Limit the maximum number of concurrent sessions belonging to the same **Administrator** according to the [None] rule.

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

5.1.7.2. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to No other components
Dependencies FIA_UAU.1 Timing of authentication

FTA_SSL.5.1 The TSF shall *terminate* an interactive session after [10 minutes].

5.1.7.3. FTA_TSE.1 TOE session establishment

Hierarchical to No other components
Dependencies No dependencies

FTA_TSE.1.1 The TSF shall be able to deny the administrator's management access session establishment based on [assess IP, *whether or not management access session of the same account is activated*]
An administrator IP address accessible to TOE may be designated exceptionally for an administrator having only read authority such as monitoring. However, when setting up accessible IP for administrators, it is not allowed to specify an IP address range (e.g., 192.168.10.2 to 253) and add one IP address individually. In addition, the IP addressing does not allow settings for 0.0.0.0 or 192.168.10.* or any, which means the entire network range.

5.2. Assurance requirements

Security assurance requirements of this ST are composed of assurance components in Common Criteria (CC V3.1) Part 3 and the evaluation assurance level is EAL1+.
The table below summarizes assurance components.

Assurance Class	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 defination
	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	Labeling of the TOE
	ALC_CMS.1	TOE configuration management coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

[Table 19] Assurance Component Summary

5.2.1. Security Target Evaluation

5.2.1.1. ASE_INT.1 ST introduction

Dependencies No dependencies

Developer action elements

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

Content and presentation elements

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

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

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

ASE_INT.1.4C The TOE overview shall 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.

5.2.1.2. 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

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.

5.2.1.3. 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.

5.2.1.4. 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.

5.2.1.5. ASsssE_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.2.2D 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.

5.2.1.6. ASE_TSS.1 TOE summary specification

Dependencies ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

TOE overview and the TOE description.

5.2.2. Development

5.2.2.1. ADV_FSP.1 Basic functional specification

Dependencies No dependencies

Developer action elements

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

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

Content and presentation elements

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

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

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

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

Evaluator action elements

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3. Guidance Documents

5.2.3.1. 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 privilege that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions

and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The operational user guidance shall be clear and reasonable.

5.2.3.2. 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

5.2.4.1. ALC_CMC.1 Labeling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action elements

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

Content and presentation elements

5.2.4.2. ALC_CMS.1 TOE CM coverage

Dependencies No dependencies

Developer action elements

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

Content and presentation elements

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

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

Evaluator action elements

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

5.2.5. Tests

5.2.5.1. ATE_FUN.1 Functional testing

Dependencies ATE_COV.1 Evidence of coverage

Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

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

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

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

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

Evaluator action elements

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

5.2.5.2. ATE_IND.1 Independent testing: sample

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

5.2.6.1. 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 preparation of evidence

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

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

processing Basic attack potential.

5.3. Security Requirements Rationale

5.3.1. Dependency of the SFRs of the TOE

The [Table 20] below shows dependencies of functional components.

NO.	SFR	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FTP_STM.1	OE.TMIE_STAMP
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_SEL.1	FAU_GEN.1	2
		FMT_MTD.1	26
7	FAU_STG.3	FAU_STG.1	OE.AUDIT_DATA _PROTECTION
8	FAU_STG.4	FAU_STG.1	OE.AUDIT_DATA _PROTECTION
9	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	11, 13
		FCS_CKM.4	12
10	FCS.CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	11, 14
		FCS_CKM.4	12
11	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9, 10
		FCS_CKM.4	12
12	FCS.CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9, 10
13	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9
		FCS_CKM.4	12
14	FCS_COP.1(2)	FDP_ITC. or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	10
		FCS_CKM.4	12
15	FCS_RBG.1(Extended)	-	-
16	FDP_UDE.1(Extended)	FCS_COP.1	13
17	FDP_RIP.1	-	-
18	FIA_AFL.1	FIA_UAU.1	21
19	FIA_IMA.1(Extended)	-	-
20	FIA_SOS.1	-	-
21	FIA_UAU.1	FIA_UID.1	24
22	FIA_UAU.4	-	-
23	FIA_UAU.7	FIA_UAU.1	21
24	FIA_UID.1	-	-
25	FMT_MOF.1	FMT_SMF.1	28

		FMT_SMR.1	29
26	FMT_MTD.1	FMT_SMF.1	28
		FMT_SMR.1	29
27	FMT_PWD.1(Extended)	FMT_SMF.1	28
		FMT_SMR.1	29
28	FMT_SMF.1	-	-
29	FMT_SMR.1	FIA_UID.1	24
30	FPT_ITT.1	-	-
31	FPT_PST.1(Extended)	-	-
32	FPT_TST.1	-	-
33	FTA_MCS.2	FIA_UID.1	24
34	FTA_SSL.5(Extended)	FIA_UAU.1	21
35	FTA_TSE.1	-	-

[Table 20] Dependencies of the SFRs of the TOE

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

FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1, which is satisfied by the operating environment of OE.DBMS.

5.3.2. Dependency of SARs of the TOE

The dependency of each assurance package provided in Common Criteria for Information Technology Security Evaluation is already satisfied.

6. TOE Summary Specification

This chapter provides brief and clear description of how the SFRs are implemented in the TOE.

6.1. Security Audit (FAU)

6.1.1. Audit Data Generation

TOE generates audit data for each component (Console, EOC, KMS) and sends it to KMS. KMS collects audit data and stores it in DBMS. When saving KMS audit data, save the data in the DBMS audit data table for each record and the audit record includes the event period, event type, identity of the subject, and the event result.

The TOE can selectively generate audit data according to the type of event (Whether ciphertext is included, encryption / decryption success log) when generating audit data. The default value is to generate audit log for all audit data.

For specific types of audit data, refer to the [Table 11] Audit event.

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

6.1.2. Security alarms

TOE sends an alert mail to the administrator via registered mail if a log of the administrator continuous authentication failure, integrity violation event, and failure of selftest of the KCMVP 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 a database format in DBMS and only authorized administrators can view audit data through Console. When inquiring audit data, the Console can perform mutual authentication with KMS and then inquire audit data stored in DBMS through KMS.

Audit data can be viewed in detail within the log through the security audit function of the Console, and authorized administrators can selectively check the accumulated audit data for each audit data type. The following table shows how to select/order audit data by type and condition.

Audit data type	Condition (AND)	To select or order
Administrator log	Date and time	The search results that meet the selected search conditions are sorted in descending order in chronological order.
	Data type	
	Action type	
	Result code	
	Security policy name	

[Table 21] Audit data search

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

6.1.4. Prevention of audit data loss

The TOE periodically monitors the audit data store to generate an audit log for exceeding the threshold when 90% of the specified audit logs are reached and sends an alert email to the authorized administrator. If the audit data store is 100% saturated, an audit log for the storage saturation is generated and an alert mail is sent to the authorized administrator via email. TOE provides a function to store the latest audit data by overwriting the oldest audit data.

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

6.2. Cryptographic Support (FCS)

6.2.1. Cryptographic Key Generation

TOE generates random numbers from the random number generator (HASH_DRBG 256) via the Korea Cryptographic Module Validation Program (KCMVP) and optionally generates 128, 192, 256 bits depending on the length of the encryption key selected by the administrator. The KEK generation generates 256 bit keys through password-based encryption key guidance (PBKDF2) according to the PKCS#5 standard. TOE also generates a public key (2048 bit)/ private key pair via the Korea Cryptographic Module Validation Program (KCMVP).
For key generation, use the following by KCMVP.

Classification	Description
Cryptographic module name	Key# Crypto v1.4
Developed company	Raonsecure Co., Ltd.
Validation No.	CM-180-2026.1
Module type	S/W(Library)
Validation Date	Jan 20, 2021
Effective Expiration Date	Jan 20, 2026

[Table 22] KCMVP

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

6.2.2. Cryptographic Key Distribution

TOE distributes session keys for protection of transmission data between TOE components. The distributed

session keys perform data protection through ARIA-256. The distribution of session keys is safely distributed using the public key encryption algorithm (RSAES-2048) and the symmetric key encryption algorithm (ARIA-256).
Cryptographic keys used in EOC to encrypt and decrypt user data are safely distributed using the public key encryption algorithm (RSAES-2048) and the symmetric key encryption algorithm (ARIA-256) to send cryptographic keys stored in KMS to EOC.

SFR to be satisfied: FCS_CKM.2

6.2.3. Cryptographic Key Destruction

At the end of the process, the TOE uses the encryption key at the end of the session between components and overwrites the encryption key memory area with '0' three times, releases the memory, and safely destroys it. The password used to generate KEK is also safely destroyed by overwriting it with '0' three times in the memory area.

SFR to be satisfied: FCS_CKM.4

6.2.4. Cryptographic Operation

When attempting to encrypt and decrypt user data stored within the DBMS to protect TOE, cryptographic operations are performed using KCMVP's ARIA-128, 1926, and SEED-128. It also provides user data encryption using one-way cryptographic algorithms such as SHA-256, 384, and 512. When encrypting stored TSF data and encrypting transmission data, encryption and decoding are performed using the ARIA-256 algorithm of KCMVP, TSF storage data encryption can be encrypted with ARIA-128, 192, 256 or SEED-128, depending on the administrator's choice. The SHA-256 algorithm also generates integrity data.
The following table provides a summary of the standards, algorithms, cryptographic keys, operating modes, and computational lists used in cryptographic operations.

Division	Standard	Cryptographic algorithms	Encryption key length	Operational mode	Operation mode
Encrypt user data	KS X 1213-1	ARIA	128, 192, 256	CBC, OFB, CFB, CTR	DB Storage User Data Encryption Decryption
	TTAS.KO-12.0004/R1	SEED	128	CBC, OFB, CFB, CTR	
	ISO/IEC 10118-3	SHA-256, SHA-384, SHA-512	N/A	N/A	DB Storage User Data Encryption Decryption
Encrypt TSF data	KS X 1213-1	ARIA	256	CBC	Policy file, Transmission data, DB Encryption key Encryption Decryption

	ISO/IEC 18033-2	RSAES	2048	N/A	Encryption key distribution
	ISO/IEC 14888-2	RSA-PSS	2048	N/A	Mutual authentication, Integrity verification, authentication data Encryption

[Table 23] TOE Cryptographic Operation

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

6.2.5. Random number generation

In the case of using a random number in an SFR that requires the use of a verification target encryption algorithm of a verified encryption module such as generation of an encryption key, a random number is generated using the random number generator algorithm HASH_DRBG (SHA256).

SFR to be satisfied: FCS_RBG.1(Extended)

6.3. User data protection (FDP)

6.3.1. Encrypt and decrypt user data

It provides column-by-column encryption and decryption of user data stored within the DBMS to protect TOE and performs encryption and decryption on web application servers or DBMS according to API and Plug-In methods. After TOE performs to encrypt and decrypt user data, it completely destroys the remaining information and files in memory as follows to protect the residual information for the original data. The remaining information in the memory is overwritten with a '0' to be unpacked.

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

6.4. Identification and Authentication (FIA)

6.4.1. Administrator identification and authentication

TOE provides administrator ID and PW-based identification and authentication through the Console and further authentication through registered certificates.
If the administrator fails a continuous authentication failure (default value: five consecutive times) during authentication, the TOE will perform a (default value: five-minute) lock to prevent further authentication.
TOE processes a masking ('*') on secret information, such as passwords that are entered during administrator authentication, and blocks information that is exposed to the screen. A pop-up message generated in the event of a failed authentication does not provide an exact reason for the authentication

failure so that passwords cannot be inferred.
Passwords required for administrator authentication must consist of at least 10 digits according to predefined combination rules and three combinations of alphabetic, numeric, and special characters for successful authentication. In addition, to prevent reuse of authentication data while the administrator is certified, the re-used data is verified and prevented using sequence numbers and random numbers.

SFR to be satisfied: FIA_AFL.1, FIA_SOS.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7

6.4.2. Mutual authentication between TOE components (extended)

TOE provides communication relative to component KMS, EOC and Console.

SFR to be satisfied: FIA_IMA.1(Extended)

6.5. Security Management (FMT)

6.5.1. Management of Security Functions Behavior

The Console enables TOE to successfully authenticate based on ID and PW so that only logged in authorized administrators can perform security management functions. TOE provides security function management, TSF data management, ID and password management functions, and only authorized administrators play roles.

The administrator ID and password must be set when KMS is first operated, and the administrator password must be changed when the console is first logged in.

The security functions and administrative actions that an authorized administrator can manage are as follows:

Administrator Type	Classification	Security Function	Ability			
			Determine the behavior	Not use	use	Modify the behavior
Authorized Administrator	Encryption key management	Generate encryption and decryption key	○	–	○	–
	Security management	Encryption target type	○	○	○	○
		Type of encryption algorithm	○	○	○	○
		User data integrity	○	○	○	○

		check feature				
		Double encryption	○	○	○	○
		Encryption pattern	○	○	○	○
	Access control	User access right	○	○	○	○
	Environmental management	User access right (Permit and deny policy)	○	○	–	○
		Administrator IP setting	-	○	○	○
		Mail server setting	-	○	○	○
	Audit log	Selecting of audit targets (cipher text)	○	○	○	○
		Creating a success log	○	○	○	○

[Table 24] List of Security Functions Behavior of Administrator

In addition, the types and management abilities of TSF data managed by an authorized administrator are as follows:

Administrator Type	**Classification**	**TSF Data**	**Ability**				
			Modify Default	**Query**	**Update**	**Create**	**Delete**
Authorized Administrator	Key management	Encryption and Decryption of user data key management	–	○	–	○	○
		Master key management	–	–	○	○	–
	User management	DB user management	–	○	○	○	○
	Security management	User data security policy management	○	○	○	○	○
	Access Control	Access time management	○	○	–	○	○

		Manage access user	○	○	–	○	○
		Access IP management	–	○	○	○	○
		Manage access program	–	○	○	○	○
	Environmental management	Administrator IP	–	○	○	○	○
		Mail Server management	–	○	○	○	○
	Audit log	Admin log	–	○	–	–	–
		Encryption log	–	○	–	–	–
	Certified information	Password log	–	–	○	○	–

[Table 25] List of TSF Data and Management Ability

The password is a combination of alphabetic, numeric, and special characters that will be set to a minimum length of 10 digits, forcing a popup reset if this rule is violated.

[Password combination rules]
- Digits: 10 or more digits ~ 40 or less
- Three combinations of English capital/small letters, special characters, and numbers.
- Number (10): 0~9,
- English capital (26): A~Z,
- English small (26): a~z,
- Special characters (32): `~!@#$%^&*()-_+=[]{}₩|;:'",.<>/?

SFR to be satisfied: FMT_MOF.1, FMT_MTD.1, FMT_PWD.1(Extended), FMT_SMF.1, FMT_SMR.1

6.6. Protection of the TSF

6.6.1. Basic protection of internal transport TSF data

TSF data transmitted between components is verified for message integrity using SHA-256, and data is encrypted and protected through ARIA-256.
Before transmitting data, data encrypted with an algorithm for message integrity verification (SHA-256) is encrypted with a data encryption algorithm (ARIA-256) along with a TSF data source, and encrypted data is transmitted using the received session key. Upon receiving the data, the data is decrypted via the data

encryption algorithm (ARIA-256) and then the TSF data source is encrypted with the message integrity verification algorithm (SHA-256) to verify the integrity of the received data by comparing it with the enclosed hash value.

SFR to be sarisfied: FPT_ITT.1

6.6.2. Basic Protection of Stored TSF data

Among stored TSF data, the DB encryption key is securely encrypted (ARIA-256) by the master key protected in the KMS. The master key is encrypted with ARIA-256 using a cryptographic key derived from the user password and is used to encrypt and store security policy files.
The administrator password is encrypted with RSA-PSS and stored in KMS, and the encryption key and key security parameters loaded in memory do not exist in plain text in memory at the time of operation, and are safely destroyed three times with '0' at the end of operation.

SFR to be satisfied: FPT_PST.1(extended)

6.6.3. TSF Self Tests and Integrity Tests

TOE performs the KCMVP's self-test on drive and on a periodic basis (24-hour cycle), and a self-test of the main TOE process.
Perform a self-test if the process of the TOE is running normally at regular intervals (every 24 hours).
TOE also performs integrity verification function using RSA-PSS algorithm for binary files such as executable files and library files on a regular (24-hour cycle) basis.
For critical TSF data, such as configuration files and policy files, the integrity check function is performed periodically (24-hour cycles) at startup.

SFR to be satisfied: FPT_TST.1

6.7. TOE Access

6.7.1. Admin Session Management

TOE can perform security management functions only by an authorized and identified administrator through the Console. TOE's access limits the number of concurrent sessions to one authorized administrator based on the unique identification and certificate of the administrator PC where the console is installed.
If an authorized administrator logged in through the console does not have input for 5 minutes (default value), the session between KMS and the console ends and the administrator logout is performed automatically. TOE can be managed by one authorized administrator by default and is accessible only by the allowed access IP. TOE also blocks new access if an authorized administrator attempts to access it simultaneously.

SFR to be satisfied: FTA_MCS.2, FTA_SSL5(extended), FTA_TSE.1