SOFTCAMP

Document Security V5.0

Security Target Lite

V1.4

SoftCamp Co., Ltd.
2F, Elentec-dong, 17, Pangyo-ro 228beon-gil,
Bundang-gu, Seongnam-si, Gyeonggi-do, 13487
Republic of Korea
Phone: 1644-9366
Fax: 031-697-4599
www.softcamp.co.kr

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

Table of Contents

Revision History

Version	Revision	Author	Date revised
V1.0	Initial release	Eun Seung-hyun	2018-09-13
V1.1	Reflect Observation Report Contents - Modify TOE overview, SFR, etc	Eun Seung-hyun	2019-07-12
V1.2	Modify, Add terms and definitions, etc	Eun Seung-hyun	2019-09-19
V1.3	Reflect content after the ITSCC review - Specify 6.2 Cryptographic support(FCS) - Specify 6.3 User data protection(FDP)	Eun Seung-hyun	2019-10-15
V1.4	Reflect content after the ITSCC review - Add a Word processing program to the 1.3.3 Requirement specification of Client's hardware and 3rd party software	Eun Seung-hyun	2019-10-15

1. ST Introduction

This document is the Security Target, or referred to as ST, of Document Security V5.0, an electronic document encryption product from SoftCamp Co., Ltd. It defines the security functional requirements and security assurance requirements of the TOE, describes security objectives, IT security requirements, and the TOE summary specification, and provides the relevant rationale.

This ST consists of the following.

Chapter 1.: It provides the basic information of the TOE in ST, and identifies the TOE through TOE reference, TOE overview, and TOE description.
Chapter 2.: It describes the TOE's conformance with Common Criteria, Protection Profile and Package, and provides the relevant rationale.
Chapter 3.: It describes the security objectives for the TOE and for the environment, and provides the relevant rationale.
Chapter 4.: It explains the definition of extended components.
Chapter 5.: It describes the security requirements and the security assurance requirements for the TOE, and provides the relevant rationale.
Chapter 6.: It describes the TOE summary specification defined in Chapter 5., and provides its rationale.

1.1 ST reference

Item	Description
Title	Document Security V5.0 Security Target
ST Version	V1.4
Author	SoftCamp Co., Ltd.
Publication Date	2019.10.15.
Common Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning, Notice No. 2013-51)
Common Criteria Version	V3.1 r5
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keywords	Document, Encryption

[Table 1-1] ST reference

1.2 TOE reference

Information that uniquely identifies and controls the TOE is as follows.

- TOE Identification : Document Security V5.0
- TOE Version : V5.0.0.6
- TOE Components & version

Item	TOE Components	Version
Document Security V5.0	Document Security Server V5.0	V5.0.0.3
	Document Security Client V5.0	V5.0.0.6
	Document Security Console V5.0	V5.0.0.4
Guidance Documents	Document Security V5.0 Preparative Procedures (PRE) V1.2 Document Security V5.0 Manager Guidance (OPE_A) V1.2 Document Security V5.0 User Guidance (OPE_U) V1.3	-

[Table 1-2] TOE Components & version

1.3 TOE overview

Chapter 1.3 explains the usage, major security features and types of the TOE, as well as non-TOE hardware/software/firmware.

1.3.1 TOE usage and major security features

Document Security V5.0 (hereinafter "TOE") encrypts electronic documents to protect important documents managed by the organization according to the policy set by the administrator, and a document is decrypted according to the document user's request and right. The TOE provides security audit function that records and reviews major events while carrying out security function or management function, identification & autehntification function such as identification for administrator and document user, authentication failure processing, and mutual authentication among the TOE components, security management function for the definition of security function, role, and configuration, protecting function to protect data stored in repository controlled by TSF, TSF protection function like TSF's self-test, and TOE access function to manage the access session of the authorized administrator. The TOE also controls the authority for use of documentsd, blocks a non-authorized access, and protects the organization's important documents through encryption, user authentication, and the control of authority for use for each file.

.

The key functions of each TOE component are as follows.

- **Document Security Server V5.0**

Document Security Server V5.0 (hereinafter "Server"), installed in the management server, issues and manages cryptographic keys used in the TOE, creates audit logs related to security policy management, the authentication of administrator and document user, and security management function, and collects the audit logs generated in each component of the TOE. Server stores the key values of policy configuration and audit logs in DBMS interoperated with the Server.

- **Document Security Client V5.0**

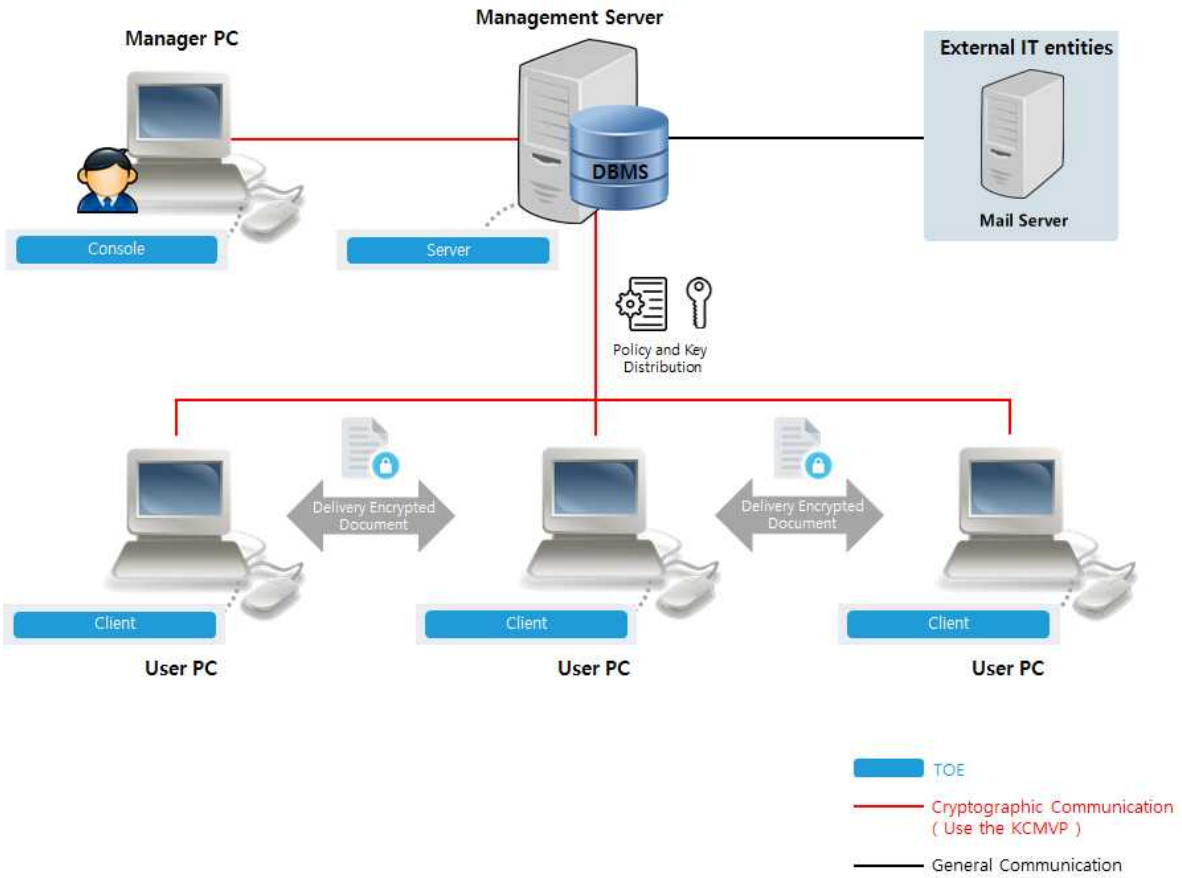
Document Security Client V5.0 (hereinafter "Client") is installed in document user's PC to perform document encryption/decryption according to administrator's policy distributed from Server. Users have to go through document user identification and authentication to use documents. Client receives policy such as document encryption/decryption, document access, print marking and application function restriction set by administrator from Server and applies it to document user.

- **Document Security Console V5.0**

Document Security Console V5.0 (hereinafter "Console") is installed in administrator's PC to provide the TOE's authorized administrator with security management interface. Through Console, administrator creates a user account that can use the Client and sets policy and authorities for the TOE's security functions, such as electronic document encryption policy. The policy set by administrator is transmitted to Server through Console and stored in the Server's DBMS.

1.3.2 TOE type

The TOE is "Electronic Document Encryption" that prevents information leakage by encrypting/decrypting important documents within the organization and is provided as software. The TOE supports "user device encryption" type depending on the operation type.



[Figure 1-1] TOE operational environment of "user device encryption" type

[Figure 1-1] represents the operational environment of "user device encryption" type among other TOE operational environments. In the "user device encryption" type, the TOE is composed of Server that is installed in management server to manage security policy and cryptographic key, Client that is installed in user's PC to perform the encryption/decryption of documents, and Console that is installed in administrator's PC to provide security management interface. Administrator sets policy for each document user through Console, and Server distributes the policies and cryptographic keys set by administrator to Client. Client installed in user PC performans document encryption/decryption by using validated cryptographic module according to the distributed policy, and the encrypted or decrypted document is stored as a file in the user PC. In the event of a potential violation, mail server is used as an external IT entity to notify the authorized administrator.

1.3.3 Non-TOE Hardware/Software/Firmware identification

Although additional hardware and software are required for the operation of the TOE, those are not included in the TOE.

The requirements of hardware and software for the operation of the TOE are as follows.

(1) Requirement specification of Server's hardware and 3rd party software

TOE	Type	Requirement
Doument Security Server V5.0	CPU	Intel(R) Xeon(R) CPU E5-2630L 0 @ 2.00GHz or higher
	HDD	Space required for TOE installation is 20GB or higher
	RAM	8GB or higher
	NIC	10/100/1000 Mbps Ethernet Card 1 Port or higher
	OS	CentOS Linux release 6.10 (Linux Kernel 2.6, 64bit)
	S/W	JRE 1.7 MariaDB 10.3

[Table 1-3] Requirement specification of Server's hardware and software

(2) Requirement specification of Client's hardware and 3rd party software

TOE	Type	Requirement
Doument Security Client V5.0	CPU	Intel(R) Pentium(R) Dual CPU E2200 @ 2.20 GHz or higher
	HDD	Space required for TOE installation is 20GB or higher
	RAM	4GB or higher
	NIC	10/100/1000 Mbps Ethernet Card 1 Port or higher
	OS	Windows 7 Professional SP1 32 bit, 64 bit Windows 8 32 bit, 64 bit Windows 10 Pro 32 bit, 64 bit Windows 10 Enterprise 32 bit, 64 bit
	S/W	Microsoft Visual C++ 2008 redistributable 9.0.30729.4148 MS Notepad, MS Wordpad, MS Paint Microsoft Office 2010, 2013, 2016, 365 Hancom Office 2010, 2014(VP), NEO, 2018 Acrobat Reader DC, Acrobat Pro 2017, DC

[Table 1-4] Requirement specification of Client's hardware and software

(3) Requirement specification of Console's hardware and 3rd party software

TOE	Type	사양
Doument Security Console V5.0	CPU	Intel(R) Pentium(R) Dual CPU E2140 @ 1.60GHz or higher
	HDD	Space required for TOE installation is 10GB or higher
	RAM	4GB or higher
	NIC	10/100/1000 Mbps Ethernet Card 1 Port or higher
	OS	Windows 7 Professional SP1 32 bit, 64 bit Windows 8 32 bit, 64 bit

		Windows 10 Pro 32 bit, 64 bit Windows 10 Enterprise 32 bit, 64 bit
	S/W	Microsoft Visual C++ 2008 redistributable 9.0.30729.4148

[Table 1-5] Requirement specification of Console's hardware and software

(4) Identification and description of 3rd party software

3rd Party Software	Description
MariaDB 10.3	DBMS to store the audit log and policy of TOE
JRE 1.7	Java runtime environment

[Table 1-6] Identification and description of 3rd party software

(5) External IT entity that interacts with other TOE besides the evaluation target TOE

External IT Entity	Description
Mail Server	Server that sends a mail to authorized administrator upon a potential security violation detected

[Table 1-7] External IT Entity

(6) Document type by word processing program supported by electronic document encryption

Word processing program	Main file format (extension)
Hancom Office	hwp
MS Office Word.	doc, docx
MS Office Powerpoint	ppt, pptx
MS Office Excel	xls, xlsx
Adobe Acrobat	pdf
Notepad	txt
Wordpad	rtf
Mspaint	bmp, jpg, png, gif

[Table 1-8] Types of documents supported by electronic document encryption

1.4 TOE description

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

1.4.1 Physical scope of the TOE

The physical scope of the TOE consists of the TOE's components, namely Document Security Server V5.0, Document Security Client V5.0 and Document Security Console V5.0 as well as guidance documents such as Document Security V5.0 Preparative Procedures and Document Security V5.0 Operational Guidance, which are included in the product, Document Security V5.0. The TOE is offered in the form of software.

The hardware platform and operating system on which TOE is installed, and the DBMS required to operate the TOE are excluded from the physical scope of the TOE.

Item	TOE Components	Distribution	
		Type	Method
Document Security V5.0	Document Security Server V5.0 - SCDS_Server_5.0.0.3.bin	bin	CD
	Document Security Client V5.0 - SCDS_Client_5.0.0.6.exe - SCDS_Client_5.0.0.6_x64.exe	exe	
	Document Security Console V5.0 - SCDS_Console_5.0.0.4.exe - SCDS_Console_5.0.0.4_x64.exe	exe	
Guidance Documents	Document Security V5.0_Preparative Procedures (PRE)_V1.2.pdf Document Security V5.0_Manager Guidance (OPE_A) _V1.2.pdf Document Security V5.0_User Guidance (OPE_U) _V1.3.pdf	pdf	CD

[Table 1-9] Physical scope of the TOE

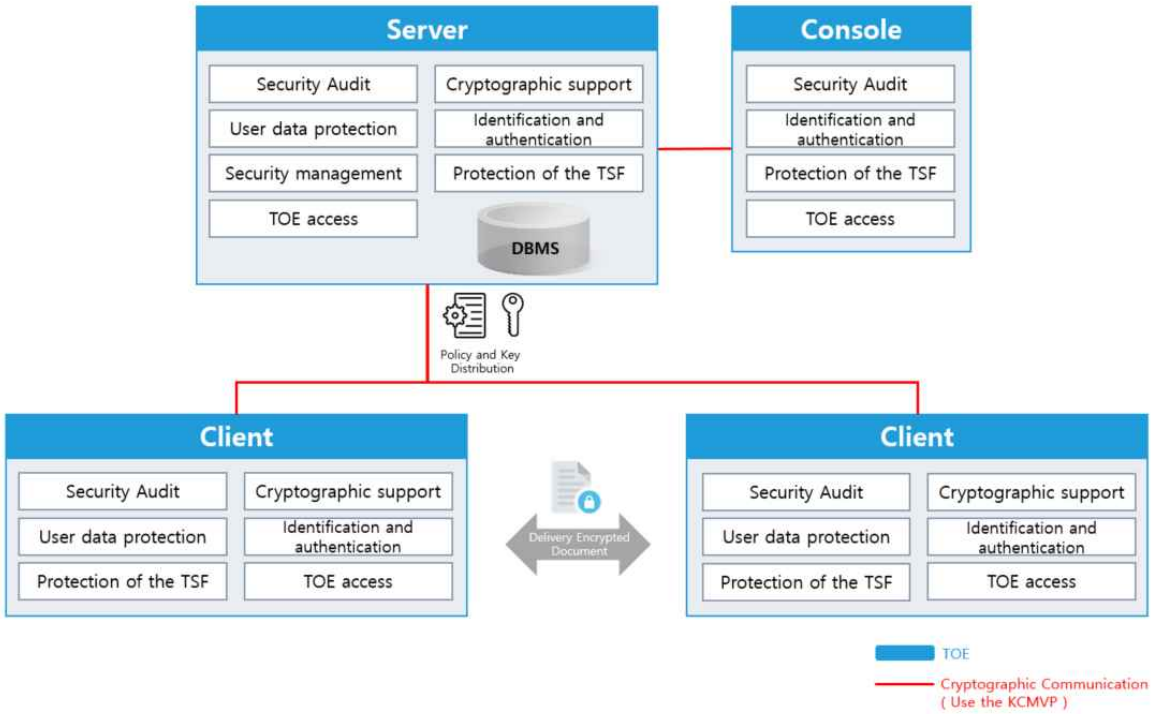
Additionally, the validated cryptographic modules required to perform the encryption/decryption functions provided by the TOE are as follows, and such modules are also within the TOE scope.

Item	Description	
Cryptographic module name	SCCrypto V1.0	XecureCrypto v2.0.1.1
Validation No.	CM-122-2021.9	CM-153-2024.5
Validation Grade	VSL1	VSL1

Developed company	SoftCamp Co., Ltd.	Hancom Secure Inc.
Validation Date	2016-09-22	2019-05-02
Effective Expiration Date	2021-09-22	2025-05-02

[Table 1-10] Validated cryptographic modules

1.4.2 Logical scope of the TOE



[Figure 1-2] Logical scope of the TOE

- Security audit

  The TOE generates and records audit records for defined auditable events. When audit records are generated, the occurrence time, category, subject information, and processing result of the auditable event are recorded. Server stores audit data it generates and those it receives from Client in DBMS. Also, it provides the function for authorized administrator to view audit data.

  When potential security violence is detected, the TOE performs a response action for the relevant act. The TOE provides the function to notify authorized administrator of the relevant information via a mail when the amount of audit trail exceeds the predefined limits. When the audit trail reaches more than 80% of the predefined limit, it sends a warning mail to the administrator, and when the audit trail is full, it sends a warning mail to the administrator

after deleting the oldest stored audit data.

- Cryptographic support

  The TOE provides functions to generate, distribute and destruct cryptographic key, as well as cryptographic operation function for the protection of data transmitted among the TOE components, the protection of TSF data, and document encryption/decryption. The TOE generates and distributes a cryptographic key, and performs the cryptographic operation, by using the TOE cryptographic algorithm of the validated cryptographic modules, namely 'XecureCrypto v2.0.1.1' and 'SCCrypto V1.0', whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).
  If the cryptographic key is not used anymore, it is destructed. The cryptographic key used in document encryption/decryption is destructed when the encrypted or decrypted document is deleted, while the cryptographic keys created for other purposes are destructed through Zeroization where the key is overwritten by 0.

- User data protection

  Through access control policy, the TOE controls read, readable counts, edit, decrypt, print, print marking, authority change, and expiration of documents to be protected according to document user, document user group and category. In the TOE, document user shall go through user identification and authentication and comply with access control policy set by administrator, in order to access to documents and use them.

- Identification and authentication

  The TOE performs mutual verification using Internally Implemented Mutual Authentication Protocol between its components, and verifies the identity of administrator and document user based on ID/password. Password shall be not less than 9 digits in combination of alphabet letter, number, and special character.
  If administrator or document user fails authentication attempts for five consecutive times during identification and authentication, the administrator or user shall try to access after five minutes as the access of the relevant account is blocked for five minutes.
  The TOE shall mask password to make it unrecognizable on the screen for the sake of protected authentication feedback. Also, when user identification or authentication fails, the TOE shall not provide the feedback for the cause of the failure.
  The TOE ensures the uniqueness of a session ID using time stamp to prevent the reuse of authentication data.

- Security management

  The TOE provides security management function for authorized manager to set and manage security policy and key data. Authorized manager performs security management function

through Console, and manages accounts, keys, policies, security management interface setting, password combination rules and password length.

- Protection of the TSF

  The TOE conducts self-tests on the major processes during initial start-up or at regular intervals. It verifies the integrity of the TOE execution files during initial start-up or at regular intervals or upon authorized administrator's request, and if the verification fails, notifies the administrator in real time.

  When TSF data is transmitted between separate parts of the TOE, validated cryptographic module is used to protect the data from disclosure and modification, and to protect the passwords of authorized manager and user, cryptographic key, critical security parameters, TOE configuration values (security policy and configuration parameters) and audit data, which are stored in TSF data storage, from unauthorized disclosure and modification.

- TOE Access

  The TOE controls any access to the TOE by allowing only registered IP (one IP by default) to access the security management interface, and limits the number of cocurrent sessions up to 1 to block simultaneous access to the same account and and the same authority. When there is an attempt at simultaneous access, it blocks new connection and maintains the existing connection.

  The TOE terminates a session if there is no activity during a certain amount of idle time (five minutes by default) after authorized administrator logs in.

1.5 Terms and definitions

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

Private Key

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

Access Control List, ACL

The list including entities who are permitted to access the entity and the types of these Permission

Approved cryptographic algorithm

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

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

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

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

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

Authorized Administrator
Authorized user to securely operates and manages the TOE, In the ST, Server manager(an authorized administrator who be able to perform the operation and management functions of a server.), chief console Manager(a super administrator of the console, an authorized administrator who be able to perform all of the security and management functions provided by the console), middle console manager (who added from the console by the chief console manager, an authorized administrator who be able to perform security and management functions only to the extent permitted by the chief console manager)

Authorized Document User
The TOE user who may, in accordance with the SFRs, perform an operation, In short, document users

Classification
A document identifier of document users for categories and mappings.

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

Category
Permission groups to grant the required level of operation (read, access counts, edit, decrypt,

authority change, access period, auto destruction) to an object (document to be encrypted) by classifications

Category Based Access Control

As the one of the mandatory access control, performing the access control for the entity based on category identity.

Class

Set of CC families that share a common focus

Component

Smallest selectable set of elements on which requirements may be based

Critical Security Parameters, CSP

Security-related information whose disclosure or modification can compromise the security of a cryptographic module (e.g., secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors)

Data Encryption Key : DEK

Key that encrypts and decrypts data, In the ST, there is a DEK used is document encryption key(encryption of document to be encrypted), document header encryption key (encryption of headers of encrypted documents), client configuration encryption key (encrypting the client's environment configuration file), server configuration encryption key (encrypting the server's environment configuration file), communication data encryption key (encryption of packets for secure communication).

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

Document User

Authorized Document User

EAL, Evaluation Assurance Level

Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined

assurance scale, that form an assurance package
Element Indivisible statement of a security need

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

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

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

Group Based Access Control
As the one of the discretionary access control, performing the access control for the entity based on group identity

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

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

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

Key Encryption Key : KEK
Key that encrypts and decrypts another cryptographic key, In the ST, there is a KEK used is server encryption key(Key to encrypt document encryption keys on a per server, kind of master key) user encryption key(Key to encrypt document encryption keys on a per user), group encryption key(Key to encrypt document encryption keys on a per group), category encryption Key(Key to encrypt document encryption keys on a per category), client configuration key encryption key (Key to encrypt client configuration encryption key), server configuration key encryption key (Key to encrypt server configuration encryption key), database encryption Key (Key to encrypt keys stored in the DB), and communication data key encryption key (Key to encrypt communication data encryption key).

Local access

The access to the TOE by using the console port to manage the TOE by administrator, directly

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

PP, Protection Profile

Implementation-independent statement of security needs for a TOE type

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.

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

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 Policy Document Document uploaded to the list of the validated cryptographic module with the module's name and specifying the summary for the cryptographic algorithms and operational environments of the TOE

Security Token

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

Selection

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

Self-tests

Pre-operational or conditional test executed by the cryptographic module

Sensitive Security Parameters, SSP Critical security parameter (CSP) and public security parameter (PSP)

Server Manager

Authorized administrators who can operate and manage server

Shall/must

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

ST, Security Target

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

Subject

Active entity in the TOE that performs operations on objects

Symmetric cryptographic technique

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

TOE, Target of Evaluation

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

TSF Data

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

TSF, TOE Security Functionality

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

Unapproved mode of operation

The mode of cryptographic module which can use both approved cryptographic algorithms and unapproved cryptographic algorithms

User

See "external entity", a user means authorized administrator and authorized document user

User Based Access Control

As the one of the discretionary access control, performing the access control for the entity based on document user identity.

Validated Cryptographic Module

A cryptographic module that is validated and given a validation number by validation authority

Word processing program

Program used to process the important documents, such as generation, modification, manipulation, and print of documents (e.g., Hangul word processor, MS word processor, Acrobat, Excel, PowerPoint, etc.)

1.6 Conventions

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

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

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.**

Security Target (ST) Author

This is used to represent the final decision of attributes being made by the ST author. The ST author's operation is denoted in braces, as in {decided by the ST author}. In addition, operations of SFR not completed in the Protection Profile must be completed by the ST author.

"Application notes" is provided to clarify the intent of requirements, provide the information for the optional items in implementation, and define "Pass/Fail" criteria for a requirement. The application notes is provided with corresponding requirements if necessary.

2. Conformance claim

Conformance claim describes Common Criteria, Protection Profile and Package Conformance Claim which the ST complies with, and how the ST complies with the Protection Profile.

2.1 CC conformance claim

This ST complies with Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning, Notice No. 2013-51) V3.1 R.5-2, and its extended version R.5-3.

- Common Criteria identification
  - 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)

- Common Criteria conformance type
  - Common Criteria for Information Technology Security Evaluation. Part 2 Extended (FCS_RBG.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2, FPT_TUD.1, FTA_SSL.5)
  - Common Criteria for Information Technology Security Evaluation. Part 3 Conformant
  - Package Augmented: EAL1 Augmented (ATE_FUN.1)

2.2 PP conformance

This ST complies with the 'Korean National Protection Profile for Electronic Document Encryption V1.0(KECS-PP-0821-2017)' as "strict PP conformance". According to strict conformance method, TOE types, the purpose of security for the operating environment, and the security requirements are equally conformed.

2.3 Package conformance claim

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

3. Security objectives

This chapter describes the security objectives based on the security issues for the TOE operating 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.

3.1 Security objectives for the operational environment

OE.PHYSICAL_CONTROL

The place where the management server among 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.LOG_BACKUP

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

OE.OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

OE.TIMESTAMP

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

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.

4. Extended components definition

4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

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

Component leveling

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

Management: FCS_RBG.1
There are no management activities foreseen.

Audit: FCS_RBG.1
There are no auditable events foreseen.

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

4.2.1 TOE Internal mutual authentication

Family Behaviour

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

Component leveling

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

Management: FIA_IMA.1
There are no management activities foreseen.

Audit: FIA_IMA.1
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of mutual authentication

4.2.1.1 FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.
Dependencies No dependencies.

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

4.3 Security Management

4.3.1 ID and password

Family Behaviour

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

Component leveling

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

Management: FMT_PWD.1
The following actions could be considered for the management functions in FMT:

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password.

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

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

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

4.4 Protection of the TSF

4.4.1 Protection of stored TSF data

Family Behaviour

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

Component leveling

FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.
FPT_PST.2 Availability protection of TSF data requires the TSF to ensure the defined levels of availability for the TSF data.

Management: FPT_PST.1, FPT_PST.2
There are no management activities foreseen.

Audit: FPT_PST.1, FPT_PST.2
There are no auditable events foreseen.

4.4.1.1 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*].

4.4.1.2 FPT_PST.2 TSF Availability protection of TSF data

Hierarchical to No other components.
Dependencies No dependencies.

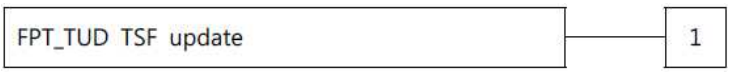
FPT_PST.2.1 The TSF shall [selection: *detect, prevent*] the unauthorized deletion for [assignment: *TSF data*].
FPT_PST.2.1 The TSF shall [selection: *detect, prevent*] the unauthorized termination for [assignment: *TSF data*].

4.4.2 TSF update

Family Behaviour

This family defines TOE firmware/software update requirements.

Component leveling



FPT_TUD.1 TSF security patch update, requires trusted update of the TOE firmware/software including the capability to verify the validity on the update file before installing updates.

Management: FPT_TUD.1
The following actions could be considered for the management functions in FMT:

a) Management of update file verification mechanism

Audit: FPT_TUD.1
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Update file verification result (success, failure)

4.4.2.1 FPT_TUD.1 TSF security patch update

Hierarchical to No other components.
Dependencies No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [assignment: *the authorized identified roles*].
FPT_TUD.1.2 The TSF shall verify validity of the update files using [selection: *hash value comparison, digital signature verification*] before installing updates.

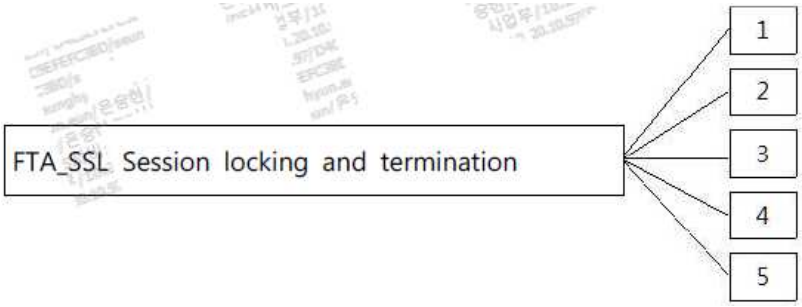
4.5 TOE Access

4.5.1 Session locking and termination

Family Behaviour

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

Component leveling



In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending one additional component as follows.
※ The relevant description for four components contained in CC Part 2 is omitted.

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

Management: FTA_SSL.5
The following actions could be considered for the management functions in FMT:

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

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

Audit: FTA_SSL.5
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive session

4.5.1.1 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

5.1 Security functional requirements

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

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(Electronic document encryption)
	FCS_CKM.1(2)	Cryptographic key generation(TSF data encryption)
	FCS_CKM.1(3)	Cryptographic key generation(Encryption by policy)
	FCS_CKM.1(4)	Cryptographic key generation(Communication encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation(Electronic document encryption)
	FCS_COP.1(2)	Cryptographic operation(TSF data encryption)
	FCS_COP.1(3)	Cryptographic operation(Encryption by policy)
	FCS_COP.1(4)	Cryptographic operation(Communication encryption)
	FCS_RBG.1(Extended)	Random bit generation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (Electronic Document Encryption access control)

	FDP_ACC.1(2)	Subset access control (Document Usage access control)
	FDP_ACF.1(1)	Security attribute based access control (Electronic Document Encryption access control)
	FDP_ACF.1(2)	Security attribute based access control (Document Usage access control)
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	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_PST.2(Extended)	Availability protection of TSF data
	FPT_TST.1	TSF testing
	FPT_TEE.1	Testing of external entities
TOE Access (FPT)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

[Table 5-1] Security functional requirements

5.1.1 Security audit (FAU)

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [Countermeasure in [Table 5-2]] upon detection of a potential security violation.

Security Functional Component	Potential security violation	Countermeasure
FIA_UAU.2	Authentication failure audit event among auditable event	Send a notification email to the authorized administrator
FPT_TST.1	Integrity violation and Failure of self test of the KCMVP event among auditable events	Send a notification email to the authorized administrator
FDP_ACF.1	Control rules violation audit event among auditable event	Show pop-up message to the document user

[Table 5-2] Actions for potential security violation

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [Refer to the "auditable events" in [Table 5-2] Audit events, [None]]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable) and the outcome (success of failure) of the event: and

b) For each audit event type, based on the auditable event definitions of the functional components include in the ST, [refer to "Additional Audit Record" in [Table 5-3] 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(2)	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_ACF.1	Successful request of operation execution regarding the object handled by SFP	Object identification information
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 (Extended)	Success and failure of mutual authentication Modify of authentication protocol	
FIA_UAU.2	All uses of authentication mechanisms	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.2	All use of the User Identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	
FMT_MSA.1	All modifications to the security attributes	
FMT_MSA.3	Modifications to the basic settings of allowance or restriction rules All modifications to the initial values of security attributes	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1 (Extended)	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 (Extended)	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 5-3] Audit event

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [Authentication failure audit event among auditable event in FIA_UAU.2, Control rules violation audit event among auditable event in FDP_ACF.1, Integrity violation and Failure of self test of the KCMVP event among auditable events in FPT_TST.1, None] Known to indicate potential security violation.

b) [None]

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide the [authorized administrator] with the capability to read [all the audit data] from the audit records.

FAU_SAR.1.2 The TSF shall provi de the audit records in a manner suitable for the **authorized administrator** to interpret the information.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the capability to apply [the following methods of selection and/or ordering] of audit data based on [the following criteria with logical relations].

a) Criteria with logical relations (AND)

Log Type, Log name, Search period, Operator name, Operator affiliation, File

name

b) Ascending, descending, per each result field

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 TSF TSF Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from theset of all auditable events based on the following attributes:

a) *event type*

b) [success or failure]

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [send a notification email to the authorized administrator, [None]] if the audit trail exceeds [80% of the total capacity of the audit trail storage].

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] and [send a notification email to the authorized administrator] if the audit trail is full.

5.1.2 Cryptographic support (FCS)

FCS_CKM.1(1) Cryptographic key generation (Electronic document encryption)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(1) Cryptographic operation (Electronic document encryption)
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in [Table 5-4]] and a specified cryptographic key size [Cryptographic key size in [Table 5-4]] that meet the following [List of standards in [Table 5-4]].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
DEK(Document Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128

[Table 5-4] Cryptographic key generation algorithm (Electronic document encryption)

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

Hierarchical to: No other components.

Dependencies: FCS_COP.1(2) Cryptographic operation (TSF data encryption)
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in [Table 5-5]] and a specified cryptographic key size [Cryptographic key size in [Table 5-5]] that meet the following [List of standards in [Table 5-5]].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
DEK(Document Header Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
DEK(Client Configuration Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
KEK(Client Configuration Key Encryption Key)	PKCS#5	PBKDF2 (Password-Based Key Derivation Function 2)	128
DEK(Server Configuration Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
KEK(Server Configuration Key Encryption Key)	PKCS#5	PBKDF2 (Password-Based Key Derivation Function 2)	128
KEK(Database Encryption Key)	PKCS#5	PBKDF2 (Password-Based Key Derivation Function 2)	128

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

FCS_CKM.1(3) Cryptographic key generation (Encryption by policy)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(3) Cryptographic operation (Encryption by policy)
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in [Table 5-6]] and a specified cryptographic key size [Cryptographic key size in [Table 5-6]] that meet the following [List of standards in [Table 5-6]].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
KEK(Server Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
KEK(User Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
KEK(Group Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
KEK(Category Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128

[Table 5-6] Cryptographic key generation algorithm (Encryption by policy)

FCS_CKM.1(4) Cryptographic key generation (Communication encryption)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(4) Cryptographic operation (Communication encryption)
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in [Table 5-7]] and a specified cryptographic key size [Cryptographic key size in [Table 5-7]] that meet the following [List of standards in [Table 5-7]].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
DEK(Communication Data Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128
KEK(Communication Data Key Encryption Key)	ISO/IEC 18033-2	RSAES (SHA256)	2048

[Table 5-7] Cryptographic key generation algorithm (Communication encryption)

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

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

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with the specified cryptographic distribution method [RSAES] that meets the following [ISO/IEC 18033-2].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy the encryption key in accordance with the stated cryptographic method [Cryptographic key destruction method in [Table 5-8]] that conforms to the following [None]:

Cryptographic key(Usage)	Timing of destruction	Cryptographic key destruction method
DEK(Electronic Document Encryption)	When decrypting an encrypted document	The header information of security document is destructed and overwritten by a general document.
	When there is a request for the destruction of an encrypted document	Document is overwritten in order of '0', '0xFF', and 'random value'.
KEK(Key Encryption Key)	When encrypting or decrypting a document	It becomes zero in order of '1' and '0' on memory.
	When there is a request from authorized administrator	It is deleted from encryption key storage.
DEK(Communication Encryption)	When a session is terminated	It becomes zero in order of '1' and '0' on memory.
DEK(TSF Data Encryption)	When TSF data is encrypted or decrypted	It becomes zero in order of '1' and '0' on memory.

[Table 5-8] Cryptographic key destruction

FCS_COP.1(1) Cryptographic operation (Electronic document encryption)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1(1) Cryptographic key generation (Electronic document

encryption)
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform the cryptographic operation list [Cryptographic operation list in [Table 5-9]] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in [Table 5-9]] and a specified cryptographic key size [Cryptographic key size in [Table 5-9]] that meet the following [List of standards in [Table 5-9]]

Cryptographic operation list	List of standards	Cryptographic algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128

[Table 5-9] Cryptographic operation (Electronic document encryption)

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

Hierarchical to: No other components.
Dependencies: FCS_CKM.1(2) Cryptographic key generation (TSF data encryption)
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform the cryptographic operation list [Cryptographic operation list in [Table 5-10]] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in [Table 5-10]] and a specified cryptographic key size [Cryptographic key size in [Table 5-10]] that meet the following [List of standards in [Table 5-10]]

Cryptographic operation list	List of standards	Cryptographic algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128
Hash function	KS X ISO/IEC 10118-3:2001	SHA-256/512	N/A

[Table 5-10] Cryptographic operation (TSF data encryption)

FCS_COP.1(3) Cryptographic operation (Encryption by policy)

Hierarchical to: No other components.
Dependencies: FCS_CKM.1(3) Cryptographic key generation (Encryption by policy)
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform the cryptographic operation list [Cryptographic operation list in [Table 5-11]] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in [Table 5-11]] and a specified cryptographic key size

[Cryptographic key size in [Table 5-11]] that meet the following [List of standards in [Table 5-11]]

Cryptographic operation list	List of standards	Cryptographic algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128

[Table 5-11] Cryptographic operation (Encryption by policy)

FCS_COP.1(4) Cryptographic operation (Communication encryption)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1(4) Cryptographic key generation (Communication encryption)
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform the cryptographic operation list [Cryptographic operation list in [Table 5-12]] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in [Table 5-12]] and a specified cryptographic key size [Cryptographic key size in [Table 5-12]] that meet the following [List of standards in [Table 5-12]]

Cryptographic operation list	List of standards	Cryptographic algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128
public key cipher	ISO/IEC 18033-2	RSAES (SHA256)	2048

[Table 5-12] Cryptographic operation (Communication encryption)

FCS_RGB.1 Random bit generation (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_RGB.1.1 The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following [ISO/IEC 18031].

5.1.3 User data protection (FDP)

FDP_ACC.1(1) Subset access control (Electronic Document Encryption access control)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(1) Security attribute-based access control (Electronic

Document Encryption access control)

FDP_ACC.1.1 TSF shall enforce the [electronic document encryption access control] on [list of subjects(document user), objects(protected document), and operations(read, readable count, edit, decrypt, right modification, access period, auto destruction)].

FDP_ACC.1(2) Subset access control (Electronic Document Usage access control)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(2) Security attribute-based access control (Electronic Document Usage access control)

FDP_ACC.1.1 TSF shall enforce the [Electronic Document Usage access control] on [list of subjects(document user), objects(documents to be protected), and operations(print, printable count, print marking, copy & paste between documents, screen capture)]

FDP_ACF.1(1) Security attribute-based access control (Electronic Document Encryption access control)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(1) Subset access control (lectronic Document Encryption access control)
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce [electronic document encryption access control] on objects based on [List of subjects a) and objects b) controlled by the following SFP, Security attribute c), d) appropriate for SFP regarding each subject and object].

[

a) Subject : document user

b) Object: documents to be protected

c) Security attribute of subject: user ID, group ID, classification ID

d) Security attribute of object: user ID, group ID, category ID, authority information

]

FDP_ACF.1.2 TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) If the security attribute for the subject is included to the security attribute which is permitted to access for the object and the operation is matched with the security attribute of the object, the corresponding operation is allowed.

b) *none]*

FDP_ACF.1.3 TSF shall explicitly authorize access of the subject to objects based on the following additionalrules: [none]

FDP_ACF.1.4 TSF shall explicitly deny access of the subject to objects based on the following additional rules: [none]

FDP_ACF.1(2) Security attribute based access control (Electronic Document usage access control)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(2) Subset access control (Electronic Document usage access control)
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce [electronic Document usage access control] on objects based on [List of subjects a) and objects b) controlled by the following SFP, Security attribute c), d) appropriate for SFP regarding each subject and object].
[
a) Subject : document user
b) Object: documents to be protected
c) Security attribute of subject: user ID, group ID, classification ID
d) Security attribute of object: user ID, group ID, category ID, authority information
]

FDP_ACF.1.2 TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
a) If the security attribute for the subject is included to the security attribute which is permitted to access for the object and the operation is matched with the security attribute of the object, the corresponding operation is allowed.
b) *none]*

FDP_ACF.1.3 TSF shall explicitly authorize access of the subject to objects based on the following additionalrules: [none]

FDP_ACF.1.4 TSF shall explicitly deny access of the subject to objects based on the following additional rules: [none]

5.1.4 Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [5] unsuccessful authentication attempts occur related to [Authentication attempts of server manager, chief console manager, middle console manager, document user].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [Disable identification and authentication feature for 5 minutes].

FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication between [Server and Client, Server and Console] in accordance with a specified [Internally implemented authentication protocol] that meets the following: [None].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_SOS.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined permission criteria].

[

a) Allowed characters

- Alphabet Uppercase, Lowercase (A ~ Z, a ~ z 52 kinds)
- Number (0 ~ 9, 10 kinds)
- Special character (32 kinds): `~!@#$%^&*()-_=+₩|[]{};:'",.<>/?

b) Combination rule

- Uppercase, lowercase, number, and special characters must each contain at least one.
- The same character cannot be used more than 3 times consecutively
- Alphabets and numbers cannot be used in ascending or descending order three or more times in a row

c) Minimum length: 9 characters (9byte)

d) Maximum length: 15 characters (15byte)

]

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [Information masked by the "●" character of the password entered] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies

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

5.1.5 Security management (FMT)

Security functional component	Management function	Management type
FAU_ARP.1	Management of actions (addition, removal, modification) to be taken	Management of security functions
FAU_SAA.1	Maintenance of the rules (addition, removal and	Management of

	modification of the rules in the rule group)	security functions
FAU_SAR.1	Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records	Management of security roles
FAU_STG.3	Maintenance of the threshold	Management of TSF data threshold
	Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure	Management of security functions
FAU_STG.4	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	Management of security functions
FDP_ACF.1	Managing the attributes used to make explicit access based decisions or denial decisions.	Management of security attributes
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Management of TSF data threshold
	Management of actions to be taken in the event of an authentication failure	Management of security functions
FIA_SOS.1	Management of the metric used to verify the secrets	Management of security functions
FIA_UAU.2	Management of the authentication data by an administrator Management of the authentication data by the user associated with this data.	Management of TSF data
FIA_UID.2	Management of the user identities	Management of TSF data
FMT_MOF.1	Management of the group of roles that can interact with the functions in the TSF	Management of security roles
FMT_MSA.1	Management of the group of roles that can interact with the security attributes	Management of security roles
	Management of rules by which security attributes inherit specified values.	Management of security roles
FMT_MSA.3	Management of the group of roles that can specify initial values	Management of security roles
	Management of the configuration that permit or limit the default values in accordance with given access control SFP Management of rules by which security attributes inherit specified values.	Management of security attributes
FMT_MTD.1	Management of the group of roles that can interact with the TSF data	Management of security roles
FMT_PWD.1	Management of ID and password configuration rules	Management of security functions

FMT_SMR.1	Management of the group of users that are part of a role.	Management of security roles
FPT_ITT.1	Management of the types of modification against which the TSF shall protect Management of the mechanism used to provide the protection of the data in transit between different parts of the TSF	Management of security functions
FPT_TST.1	Management of the conditions under which TSF self testing occurs, such as 'during initial start-up', 'regular interval', or 'under specified conditions' Management of the time interval (if appropriate)	Management of TSF data
FTA_MCS.2	Management of the maximum allowed number of concurrent user sessions by an administrator	Management of TSF data threshold
FTA_SSL.5	Specification of the time of user inactivity after which lock-out occurs for an individual user Specification of the default time of user inactivity after which lock-out occurs	Management of TSF data
FTA_TSE.1	Management of the session establishment conditions by the authorized administrator	Management of TSF data

[Table 5-13] Security management action and management type by component

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to conduct **management actions** on the following functions [

a) Chief console manager:
- Integrity verification request
- Basic encryption policy management and force encryption policy management
- Client log-in policy management, APP control management, print marking management

b) Middle console manager:
- Basic encryption policy management and force encryption policy management,
- Client log-in policy management, APP control management, print marking management

c) Document user
- Integrity verification request

] to [**each user's role**].

※ "Management actions" for which refinement is applied include all the abilities to determine, disable, enable and modify the behavior of some of the TSF functions.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of ManagementFunctions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce [electronic document encryption access control, electronic document usage access control] to restrict the ability to *change the default value of, query, modify and delete* the security attributes of [document user ID, group ID, category ID, authority information] to [authorized administrator].

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce [electronic document encryption access control policy, electronic document usage access control policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 TSF Data management

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*** the [following TSF data list] to [**each user's role**]. [

a) Chief console manager
- Management of the threshold for the unsuccessful authentication attempts of

Middle console manager
- Management of the identification and authentication information of Middle console manager
- Management of the identification and authentication data of document user
- Management of session termination time of Middle console manager
- Management of accessible IP for Chief console manager and Middle console manager
- Management of user, group, category, classification, security policy and log

b) Middle console manager
- Management of the identification and authentication data of document user
- Management of user, group and log

c) Server manager
- Creation of a pair of public and private keys
- Mail information setting to send alarm mails

d) Document user
- Management of the authentication data of document user

]

※ By the definition, "Manage" to which a refinement operation is applied includes the ability to change default value, query, modify, delete, clear, and conduct other operations.

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [none] to [the authorized administrator].
1. [None]
2. [None]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [none] to [the authorized administrator].
1. [None]
2. [None]

FMT_PWD.1.3 The TSF shall provide the capability for *changing the ID and password when the authorized administrator accesses for the first time*.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Security function management, TSF data management, security attributes management and environment configuration parameter defined in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1 and FMT_PWD.1]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the role of [Server manager, Chief console manager, Middle console manager, Document user].

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

5.1.6 Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies

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

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 [password of administrator, cryptographic key, critical security parameters**,** TOE setting value (security policy, configuration parameters)] stored in containers controlled by the TSF from unauthorized *disclosure, modification*.

FPT_PST.2 Availability protection of stored TSF data (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PST.2.1 TSF shall *prevent* the unauthorized deletion for [client setting value (security policy, configuration parameters)].

FPT_PST.2.2 TSF shall *prevent* the unauthorized termination for [execution file of client(process)].

FPT_TST.1 TSF self-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 a function that verifies integrity of *TSF data* to the **authorized administrator.**

FPT_TST.1.3 The TSF shall provide a function that verifies integrity of *TSF* to the **authorized administrator**.

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TEE.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation* to check the fulfillment of [SMTP server, DBMS].

FPT_TST.1.2 If the test fails, the TSF shall [The following response actions]

a) Failure of DBMS external entities: Send a notification email to the authorized administrator
b) Failure of SMTP server external entities: Audit data generation

5.1.7 TOE access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [The maximum number of concurrent sessions for administrator management access session restricted to one, prohibition of same user both concurrent connections of management access session and local access session]

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] sessions per user.

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 authentication

FTA_SSL.5.1 The TSF shall *terminate* an interactive session of the **authorized administrator** after a [5 minutes of Administrator inactivity].

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_TSE.1.1 The TSF shall be able to deny **administrator's management access session** establishment based on [connection IP, *whether or not to activate the management access session of administrator account with the same privilege*].

5.2 Security 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.

Security Assurance Class	Security Assurance Component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components 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.1.2	TOE configuration management coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

[Table 5-14] Security assurance requirements

5.2.1 Security Target evaluation

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.

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.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies

Developer action elements

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

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

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

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

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

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

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

Evaluator action elements

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

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

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements

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

ASE_REQ.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.

ASE_TSS.1 TOE summary specification

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies

Developer action elements

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

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

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

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

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

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

specification.

Evaluator action elements

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

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

5.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and 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.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures. Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1 Labeling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements

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

Content and presentation elements

ALC_CMC.1.1C TOE shall be labelled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E The evaluator shall confirm that the information provided meet requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies

Developer action elements

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

Content and presentation elements

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

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

Evaluator action elements

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

5.2.5 Tests

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

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

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

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

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

Evaluator action elements

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

ATE_IND.1 Independent testing: conformance

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and 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 rationale of security functional requirements

The following Table shows the dependencies of security functional requirement.

No	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	Rationale (2)
7	FAU_STG.4	FAU_STG.1	Rationale (2)
8	FAU_SEL.1	FAU_GEN.1	2
		FMT_MTD.1	34
9	FCS_CKM.1(1)	FCS_COP.1(1)	15
		FCS_CKM.4	14
10	FCS_CKM.1(2)	FCS_COP.1(2)	16
		FCS_CKM.4	14
11	FCS_CKM.1(3)	FCS_COP.1(3)	17
		FCS_CKM.4	14
12	FCS_CKM.1(4)	FCS_COP.1(4)	18
		FCS_CKM.4	14
13	FCS_CKM.2	FCS_CKM.1	9,10,11,12
		FCS_CKM.4	14
14	FCS_CKM.4	FCS_CKM.1	9,10,11,12
15	FCS_COP.1(1)	FCS_CKM.1(1)	9

		FCS_CKM.4	14
16	FCS_COP.1(2)	FCS_CKM.1(2)	10
		FCS_CKM.4	14
17	FCS_COP.1(3)	FCS_CKM.1(3)	11
		FCS_CKM.4	14
18	FCS_COP.1(4)	FCS_CKM.1(4)	12
		FCS_CKM.4	14
19	FCS_RBG.1	-	-
20	FDP_ACC.1(1)	FDP_ACF.1(1)	22
21	FDP_ACC.1(2)	FDP_ACF.1(2)	23
22	FDP_ACF.1(1)	FDP_ACC.1(1)	20
		FMT_MSA.3	33
23	FDP_ACF.1(2)	FDP_ACC.1(2)	21
		FMT_MSA.3	33
24	FIA_AFL.1	FIA_UAU.1	Rationale (3)
25	FIA_IMA.1	-	-
26	FIA_SOS.1	-	-
27	FIA_UAU.2	FIA_UID.1	Rationale (4)
28	FIA_UAU.4	-	-
29	FIA_UAU.7	FIA_UAU.1	Rationale (3)
30	FIA_UID.2	-	-
31	FMT_MOF.1	FMT_SMF.1	36
		FMT_SMR.1	37
32	FMT_MSA.1	FDP_ACC.1	20,21
		FMT_SMF.1	36
		FMT_SMR.1	37
33	FMT_MSA.3	FMT_MSA.1	32
		FMT_SMR.1	37
34	FMT_MTD.1	FMT_SMF.1	36
		FMT_SMR.1	37
35	FMT_PWD.1	FMT_SMF.1	36
		FMT_SMR.1	37
36	FMT_SMF.1	-	-
37	FMT_SMR.1	FIA_UID.1	Rationale (4)
38	FPT_ITT.1	-	-
39	FPT_PST.1	-	-
40	FPT_PST.2	-	
41	FPT_TST.1	-	-

42	FPT_TEE.1		
43	FTA_MCS.2	FIA_UID.1	Rationale (4)
44	FTA_SSL.5	FIA_UAU.1	Rationale (3)
45	FTA_TSE.1	-	

[Table 5-15] Dependency of TOE security functional requirements

Rationale (1): FAU_GEN.1 is subordinated to FPT_STM.1, and as FPT_STM.1 is satisfied by OE.time stamp which is for the security of operating environment, the subordinate relationship is satisfied

Rationale (2): FAU_STG.3 and FAU_STG.4 are subordinated to FAU_STG.1, and as FAU_STG.1 is satisfied by OE.DBMS which is for the security of operating environment, the subordinate relationship is satisfied.

Rationale (3): FIA_UAU.2 has a hierarchical relationship with FIA_UAU.1, so it has restrictive strength and satisfies the dependencies.

Rationale (4): FIA_UID.2 has a hierarchical relationship with FIA_UID.1, so it has restrictive strength and satisfies the dependencies.

5.3.2 Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.
The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. but, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE Specificaion summary

6.1 Security audit (FAU)

Audit data created in Client and Console is transmitted to Server through encrypted communication, and Server that received the audit data stores such data in DBMS. Audit data created in Server is also stored in DBMS, and the data stored in DBMS can be retrieved by authorized manager through Console which is security management interface.

Security alarms

The TOE sends an alarm mail to authorized manager when a potential security violation is detected. Potential security violations and the corresponding response actions are shown in [Table 6-2].

Audit data generation

The TOE generates the audit records of the auditable events defined in [Table 5-3].

The TOE records the following information when it generates audit records on the acts of administrator and document user.

Information	
User	Log type, time, PC IP, PC MAC, success/failure, cause, user ID, user name, user team, user position, PC ID
Security document	Log type, time, user ID, user name, user team, user position, PC ID, PC IP, PC MAC, file name, original file name, generator ID, time of generation, category name
Administrator	Log type, time, administrator ID, administrator name, administrator mail, administrator contact information, administrator PC IP, administrator PC MAC, target group, revision history, target ID, target user name, target user position

[Table 6-1] Information recorded upon the generation of TOE audit data

Potential violation analysis and response actions

If one of the potential security violations defined below is detected, the TOE notifies authorized manager of such event via mail in real time, and respond to it according to pre-designated method by the type of security violation. Potential security violation events and the corresponding response actions are as follows.

.

Potential security violation	Countermeasure
Authentication failure audit event among auditable event (FIA_UAU.2)	Send a notification email to the authorized administrator
Integrity violation and Failure of self test of the KCMVP	Send a notification email to the

event among auditable events (FPT_TST.1)	authorized administrator Terminate Violation Process
Control rules violation audit event among auditable event (FDP_ACF.1)	Show pop-up message to the document user

[Table 6-2] Response actions for potential security violation

Audit review

The TOE provides functions to review and selectively review the audit data generated by the TOE and stored in DBMS. Authorized manager can retrieve audit data through Console which is security management interface. Audit data is retrieved from DBMS, the operating environment of the TOE, by executing queries that meet the conditions requested by authorized manager in Console.
Authorized manager can retrieve all audit data, which have been generated, and selective audit data according to logical relationship such as AND condition.

Selective audit

The TOE can selectively generate audit log by type of event defined in [Table 6-3]. It generates audit log for all audit data by default.

Item	Type of event
User log	Log in, log out, password change, program deletion
Security document log	create, read, edit, decrypt, print, auto destruction, authority change, destruction
Administrator log	Administrator log in, security policy change, log policy change, marking image change, position information change, middle console manager change, server profile change, adding user, deleting user, relocating user, user information change, adding group, deleting group, relocating group, group information change, deleting PC(ID)

[Table 6-3] Selectable types of event

Action in case of possible audit data loss and prevention of audit data loss

The TOE does not provide a function to modify or delete audit data through administrator's interface. Also, the TOE provides the function to notify authorized administrator of the relevant information via a mail where the amount of audit trail exceeds the predefined limits. When the audit trail reaches more than 80% of the audit storage capacity, the TOE sends a warning mail to the administrator, and when the trail exceeds 95%, it deletes 5% and then notifies the administrator whether the audit trail has been deleted or not via a mail.

※ Related SFRS

- FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.3, FAU_STG.4

6.2 Cryptographic support (FCS)

The TOE generates a cryptographic key by using the TOE cryptographic algorithm of the validated cryptographic modules shown in [Table 6-4], namely 'XecureCrypto v2.0.1.1' and 'SCCrypto V1.0', whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

Item	Description	
Cryptographic module name	SCCrypto V1.0	XecureCrypto v2.0.1.1
Validation No.	CM-122-2021.9	CM-153-2024.5
Validation Grade	VSL1	VSL1
Developed company	SoftCamp Co., Ltd.	Hancom With Inc.
Validation Date	2016-09-22	2019-05-02
Effective Expiration Date	2021-09-22	2025-05-02

[Table 6-4] validated cryptographic modules

Cryptographic key generation (Electronic document encryption)

Cryptographic key used for the encryption of a document to be used in the TOE is generated when the document is generated in Client. The cryptographic key is generated through the random bit generator (HASH_DRBG) of 'SCCrypto V1.0', a validated cryptographic module used by the TOE.

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size	Cryptographic module
DEK(Document Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128	SCCrypto V1.0

[Table 6-5] Cryptographic key generation algorithm (Electronic document encryption)

Cryptographic key generation (TSF data encryption)

Cryptographic key used for the encryption of the TSF data is generated in Server and Client of the TOE. The cryptographic key is generated through the TOE cryptographic algorithm of 'SCCrypto V1.0' and 'XecureCrypto v2.0.1.1', validated cryptographic modules used in the TOE.

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size	Cryptographic module
DEK(Document Header Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128	XecureCrypto v2.0.1.1
DEK(Client Configuration Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128	SCCrypto V1.0
KEK(Client Configuration Key Encryption Key)	PKCS#5	PBKDB2 (Password-Based Key Derivation Function 2)	128	-
DEK(Server Configuration Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128	XecureCrypto v2.0.1.1
KEK(Server Configuration Key Encryption Key)	PKCS#5	PBKDF2 (Password-Based Key Derivation Function 2)	128	-
KEK(Database Encryption Key)	PKCS#5	PBKDB2 (Password-Based Key Derivation Function 2)	128	-

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

Cryptographic key generation (Encryption by policy)

Cryptographic key used to apply policy according to certain user, group or category in the TOE is generated in Server of the TOE by the relevant policy. The cryptographic key is generated through the TOE cryptographic algorithm of 'XecureCrypto v2.0.1.1', a validated cryptographic module used by the TOE.

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size	Cryptographic module
KEK(Server Encryption Key)	ISO/IEC 18033-2	RSAES (SHA256)	128	XecureCrypto v2.0.1.1
KEK(User Encryption Key)	ISO/IEC 18033-2	RSAES (SHA256)	128	XecureCrypto v2.0.1.1
KEK(Group	ISO/IEC 18033-2	RSAES (SHA256)	128	XecureCrypto

Encryption Key)				v2.0.1.1
KEK(Category Encryption Key)	ISO/IEC 18033-2	RSAES (SHA256)	128	XecureCrypto v2.0.1.1

[Table 6-7] Cryptographic key generation algorithm (Encryption by policy)

Cryptographic key generation (Communication encryption)

Cryptographic key used for the safe encrypted communication between Server and Client, and Server and Console is generated in Server, Console and Client of the TOE. The cryptographic key is generated through the TOE cryptographic algorithm of 'SCCrypto V1.0' and 'XecureCrypto v2.0.1.1', validated cryptographic modules used in the TOE.

.

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size	Cryptographic module
DEK(Communication Data Encryption Key)	ISO/IEC 18031	HASH_DRBG (SHA256)	128	SCCrypto V1.0
KEK(Communication Data Key Encryption Key)	ISO/IEC 18033-2	RSAES (SHA256)	2048	XecureCrypto v2.0.1.1

[Table 6-8] Cryptographic key generation algorithm (Communication encryption)

Cryptographic key distribution

Cryptographic keys of the TOE are transmitted from Server to Client via a safely encrypted communication sector. The TOE distributes cryptographic keys using RSAES, a cryptographic key distribution method that satisfies ISO/IEC 18033-2.

Cryptographic key destruction

Cryptographic key is destructed when authorized administrator deletes a policy, deletes a user or a group, and decrypts an encrypted document. Once deleted, the cryptographic key shall not be restored or reused.

The timing of cryptographic key destruction varies according to each cryptographic key's type. When deleting cryptographic key, it is initialized to "0" to be completely deleted in the location where it is stored, and shall not be reused in any security document to which the key was previously applied.

Cryptographic operation (Electronic document encryption)

The TOE performs cryptographic operation for electronic document encryption using the TOE cryptographic algorithm of 'SCCrypto V1.0', a validated cryptographic module whose security and

implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP). When the cryptographic operation is performed, the validated cryptographic module is operated on the approved mode of operation. The standard, cryptographic key algorithm, and cryptographic key size used for the electronic document encryption are shown in [Table 6-9].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA128	128

[Table 6-9] Cryptographic operation (Electronic document encryption)

Cryptographic operation (TSF data encryption)

The TOE performs cryptographic operation for TSF data encryption using the TOE cryptographic algorithm of 'XecureCrypto v2.0.1.1', a validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP). When the cryptographic operation is performed, the validated cryptographic module is operated on the approved mode of operation. The standard, cryptographic key algorithm, and cryptographic key size used for the TSF data encryption are shown in [Table 6-10].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128
Hash function	KS X ISO/IEC 10118-3:2001	SHA-256/512	N/A

[Table 6-10] Cryptographic operation (TSF data encryption)

Cryptographic operation (Encryption by policy)

The TOE performs cryptographic operation for encryption by policy using the TOE cryptographic algorithm of 'XecureCrypto v2.0.1.1', a validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP). When the cryptographic operation is performed, the validated cryptographic module is operated on the approved mode of operation. The standard, cryptographic key algorithm, and cryptographic key size used for the encryption by policy are shown in [Table 6-11].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128

[Table 6-11] Cryptographic operation (Encryption by policy)

Cryptographic operation (Communication encryption)

The TOE performs cryptographic operation communication encryption using the TOE cryptographic algorithm of 'SCCrypto V1.0' and 'XecureCrypto v2.0.1.1', validated cryptographic modules whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP). When the cryptographic operation is performed, the validated cryptographic module is operated on the approved mode of operation. The standard, cryptographic key algorithm, and cryptographic key size used for the communication encryption are shown in [Table 6-12].

Cryptographic key	List of standards	Cryptographic key generation algorithm	Cryptographic key size
Block cipher	KS X 1213	ARIA	128
public key cipher	ISO/IEC 18033-2	RSAES (SHA256)	2048

[Table 6-12] Cryptographic operation (Communication encryption)

Random Bit Generation

When random numbers are used in SFR where the TOE cryptographic algorithm of validated cryptographic modules, such as main cryptographic key generation like data encryption key (DEK), are required, the TOE uses the random bit generator of 'SCCrypto V1.0' and 'XecureCrypto v2.0.1.1', validated cryptographic modules whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

※ Related SFRS

- FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG.1

6.3 User data protection (FDP)

Electronic document encryption access control

The TOE controls the read, readable count, edit, decrypt, authority change, destruction and auto destruction. of documents to be protected by document user, document user group, category user, and private document user through access control policy such as user-based access control, group-based access control, category-based access control. Descriptions by access control policy are shown in the table below.

Access control policy	Description

User-based access control	Controlling access by applying policies based on included user
Group-based access control	Controlling access by applying policies based on included group
Category-based access control	Controlling access by differentiating access authority to security document by relevant user and group. A user can select only the categories allowed to him/her.

[Table 6-13] Access control policy

The TOE controls the read, readable count, edit, decrypt, authority change, destruction and auto destruction. of documents to be protected by document user, document user group, category user, and private document user.

Type	List
Subject security attribute	User ID, group ID, classification ID
Object security attribute	User ID, group ID, category ID, authority information

[Table 6-14] List of security attributes (Electronic document encryption access control)

Electronic document usage access control

The TOE controls the print, printable counts, print marking, copy and paste between documents, screen capture and menu control of a part word processing program. of documents to be protected by document user, document user group, category user, and private document user through access control policy such as user-based access control, group-based access control, category-based access control.

Access control policy	Description
User-based access control	Controlling access by applying policies based on included user
Group-based access control	Controlling access by applying policies based on included group
Category-based access control	Controlling access by differentiating access authority to security document by relevant user and group. A user can select only the categories allowed to him/her.

[Table 6-15] Access control policy

The TOE controls print, printable counts, print marking, copy and paste between documents, screen capture and menu control of a part word processing program. of documents to be protected by document user, document user group, category user, and private document user.

Type	List
Subject security attribute	User ID, group ID, classification ID
Object security attribute	User ID, group ID, category ID, authority information

[Table 6-16] List of security attributes (Electronic document usage access control)

※ Related SFRS

- FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2)

6.4 Identification and Authentication (FIA)

Identification and authentication

An authorized administrator or an authorized document user of the TOE shall successfully go through authentication before he or she is allowed to access and control all of security functions, and perform electronic document encryption. The TOE provides a password-based authentication mechanism that performs the identification and authentication using ID and password.

The password of administrator and user shall be not less than 9 digits in combination of alphabet letter, number, and special character, which is set by default upon installation. The TOE prevents the reuse of the authentication data using the time stamp value of the authentication.

For the management access of authorized administrator and the identification and authentication of authorized document user, if the administrator or user fails the authentication for five consecutive times, the access of the relevant account is blocked for five minutes and the audit record of such authentication failure is stored.

Protected authentication feedback

When user authentication fails, the TOE shall not provide the feedback for the cause of the failure. The password, which is input during password registration or password change, shall be masked with "●" to make it unrecognizable on the screen. The feedback messages provided upon the log-in failure of administrator or user are as follows.

Type	Message
Where ID does not match	"User authentication failed. Please try again."
Where password does not match	"User authentication failed. Please try again."

[Table 6-17] Feedback message upon log-in failure

TOE Internal mutual authentication

Mutual authentications between Server and Client, and Server and Console use Internally

Implemented Mutual Authentication Protocol. The mutual authentication methods that Client and Console use on Server are identical. For the sake of encrypted communication, Client and Console have communication public key (KEK) which is provided upon installation, and Server has communication public key (KEK) and private key (KEK). When data is transmitted from Client to Server, the data is encrypted using communication data key (DEK) which is temporarily generated, and the communication data key (DEK) is encrypted with communication public key (KEK) before transmitting to Server. Communication data key (DEK) is destructed after receiving the result from Server. The above process is repeated when there is a communication request from Client.

※ Related SFRS

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

6.5 Security management(FMT)

Management of security functions behaviour

The TOE provides chief console manager with the ability to determine, enable, disable and modify behaviors on security functions such as integrity verification request, basic encryption policy management, force encryption policy management, Client log-in policy management, APP control management, print marking and others. For middle console manager, the TOE provides the ability to determine, enable, disable and modify behaviors on security functions such as basic encryption policy management, force encryption policy management, Client log-in policy management, APP control management, print marking and others within the relevant group. For document user, the TOE provides the ability to determine, enable, disable and modify behaviors on security function, namely integrity verification request.

Management of security attributes

The TOE limits the ability to change, query, modify and delete the default value of the security attributes of administrator, user and group through access control policy strictly to authorized administrator. The TOE enforces restrictive basic policy on the electronic document encryption.

TSF Data management

The TOE provides server manager with the management function to create a pair of public and private keys, and to change, query, modify, delete and create the default value for mail information setting to send alarm mails. For chief console manager, the TOE provides the management function to change, query, modify, delete and generate the default value on the management of the threshold for the unsuccessful authentication attempts of middle console manager, the management of the identification and authentication information of middle console manager, the management of the session termination time of middle console manager, and the management of accessible IP

for chief console manager and middle console manager, as well as attributes data such as user, group, category, classification, security policy and log. For middle console manager, the TOE provides the management function to change, query, modify, delete and generate the default value on the management of the identification and authentication data of document user, and attributes data such as user, group and log. For document user, the TOE provides the management function to change, query, modify, delete and generate the default value on the management of authentication data of document user.

Management of ID and password

The TOE provides the function that enforces to change ID and password upon the initial access of authorized administrator after the product installation.

Security roles

The users of the TOE are classified as server manager, chief console manager, middle console manager and document user.

The table below explains user's authorities by role.

Role	Authority
Server manager	Server management such as server start-up
Chief console manager	All of the security functions provided by Console
Middle console manager (Group manager)	Some of the security functions (management of encryption policy on the relevant group) provided by Console according to the authorities set by authorized chief console manager who created the relevant middle console manager account
Document user	Document encryption/decryption by receiving encryption policy in a device where Client is installed

[Table 6-18] Authorities by security role

※ Related SFRS

- FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1

6.6 Protection of the TSF (FPT)

Basic internal TSF data transfer protection

The TOE protects transmitted TSF data such as audit data and sensitive security parameters from disclosure and modification when the TSF data is transmitted between separate parts of the TOE using the TOE encryption algorithm of 'XecureCrypto v2.0.1.1' and 'SCCrypto V1.0', validated encryption modules whose security and implementation conformance are validated by the Korea

Cryptographic Module Validation Program (KCMVP).

Basic protection of stored TSF data

The TOE protects the passwords of authorized manager and user, cryptographic key, critical security parameters, TOE configuration values (security policy and configuration parameters) and audit data, which are stored in TSF data storage, from unauthorized disclosure and modification. In particular, the TSF data such as the passwords of authorized administrator and user, data encryption key (DEK), critical security parameters, TOE configuration values, and DBMS connection information are encrypted and stored by the TOE encryption algorithm of "XecureCrypto v.2.0.1.1", a validated encryption module.

The data encryption key (DEK) shall be encrypted by the TEO encryption algorithm that is provided by the validated encryption module using key encryption key (KEK) before stored. The encryption key and the critical security parameters loaded on memory shall not exist as plaintext when they are no more in use as encryption/decryption operation is completed.

TSF self-testing

The TOE runs self-tests (Health Check) at regular intervals (1 hour) during initial start-up and normal operation to demonstrate the correct operation of its components – Server, Client and Console. Client runs the self-test together, only if it is activated, at regular intervals during initial start-up and normal operation. The objects of the self-test include critical processes that perform the TSF, and the validated encryption modules are the result of the self-test.

The TOE provides the function to verify the integrity on TSF data such as key execution files and configuration, and the TSF itself. The integrity verification is performed when authorized administrator wants or at regular intervals (1 hour) during initial start-up and normal operation. The integrity data of the TOE is registered in DBMS, and is compared with TOE's configuration information distributed to judge if it is consistent with the configuration information.

The objects of integrity verification are key execution files and configuration files.

- Server, Client, Console execution files and library files
- Client configuration file

Testing of external entities

In order to demonstrate the correct operation of mail server and DMS, which are the objects of external entity testing, of Server as a component of the TOE, its operation status is examined at regular intervals (3 minutes) during initial start-up and normal operation. For mail server, the operation status is judged by test mail sending result. For DBMS, a query that returns current time is transmitted to judge the status of the operation based on the query result.

※ Related SFRS

- FPT_ITT.1, FPT_PST.1, FPT_PST.2, FPT_TST.1, FPT_TEE.1

6.7 TOE Access (FTA)

Per user attribute limitation on multiple concurrent sessions

The TOE limits the number of concurrent sessions up to 1 to block simultaneous access to the same account. It also blocks simultaneous access to the same authority. When there is an attempt at simultaneous access to the same account or the same authority, it blocks new connection and maintains the existing connection.

Management of TSF-initiated sessions

The TOE terminates a session if there is no activity during a certain amount of idle time (five minutes by default) after server manager or chief console manager or middle console manager logs in.

TOE session establishment

The TOE controls TOE access by allowing only registered IP (one IP by default) to access the security management interface. Upon the first log-in after the installation of the TOE, connection IPs are established. After the installation, the connection IPs can be added, modified and deleted by establishing the list of IPs that are allowed to log in to security management. When establishing IP, it is not allowed to add an IP address range. Furthermore, IPs such as 0.0.0.0, 192.168.10.*, any, etc. is not allowed to be established.

※ Related SFRS

- FTA_MCS.2, FTA_SSL.5, FTA_TSE.1