KT Secure Vault V1.0

Security Target

Version 1.0.023

Institute of Convergence Technology

KT R&D Center, 151, Taebong-ro, Seocho-gu, Seoul, Korea, 137-792

ict@kt.com

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This document is the security target of the KT Secure Vault V1.0 that was written by the KT Institute of Convergence Technology. It was written in conformance to the Common Criteria for Information Technology Security Evaluation for Common Criteria (also referred to as “CC”) certification.

1.1 ST Reference

This document is identified as shown in [Table 1] ST Reference.

Category	Content
Title	KT Secure Vault V1.0 Security Target
Version	V1.0.023
Document Date	2017.06.27
Author	KT Institution of Convergence Technology
Common Criteria	Common Criteria for Information Technology Security Evaluation (CC V3.1 R4)
Evaluation Assurance Level	EAL1
Key Words	Access control, data security, file encryption

[Table 1] ST Reference

1.2 TOE Reference

This TOE reference is identified as shown in [Table 2] TOE Reference.

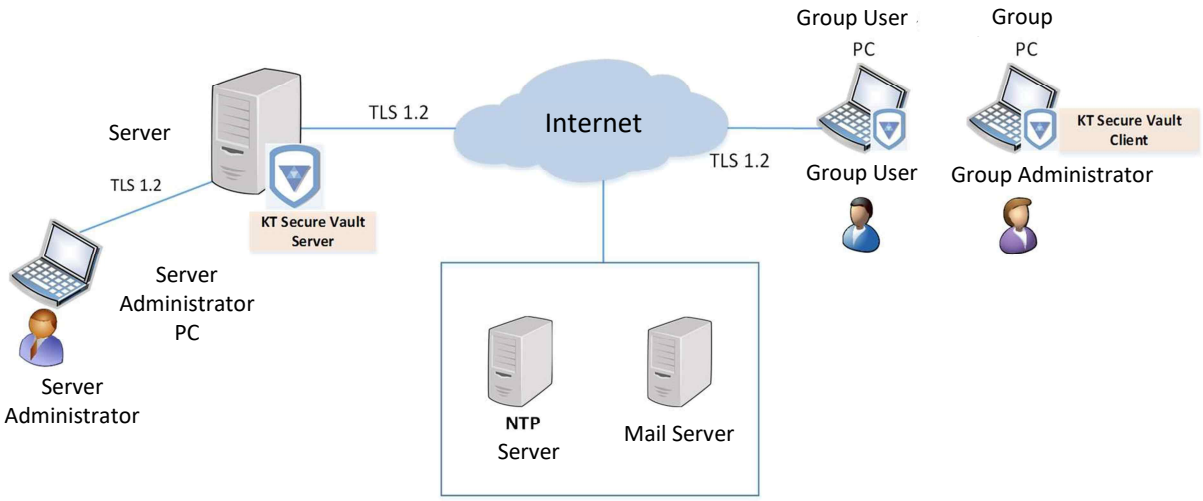
Category	Contents		Notes
TOE Title	KT Secure Vault V1.0		
TOE Version	V1.0.022		
TOE Component	KT Secure Vault Server	KT Secure Vault Server V1.0.B-022.017 (KT_Secure_Vault_Server_V1.0.B- 022.017.tar)	SW Type Distribution (CD)
	KT Secure Vault Client	KT Secure Vault Client V1.0.B-017.019 (KT Secure Vault Client V1.0.B-017.019.exe)	SW Type Distribution (Download from KT Secure Vault Server)
	User Manual	KT Secure Vault V1.0 User Manual V1.0.009 (KT Secure Vault V1.0-USR-V1.0.009.pdf)	Electronic Document (PDF) Distribution
	Preparation Procedure	KT Secure Vault V1.0 Preparation Procedure V1.0.009 (KT Secure Vault V1.0-PRE- V1.0.009.pdf)	Electronic Document (PDF) Distribution
Developer	KT Institution of Convergence Technology		

[Table 2] TOE Reference

1.3 TOE Overview

1.3.1 Purpose of TOE and Major Security Features

KT Secure Vault V1.0 (hereinafter "TOE") is an information security product that offers encryption/decryption and Access Control Functions for securing files stored in the user PC.



[Figure 1] TOE Operating Environment

As with the TOE's operating environment, the KT Secure Vault Client is installed on the group user and group administrator's PCs, and the KT Secure Vault Server is installed in the server. TOE communicates between configuration factors through the IPv4 network to provide security functions.

The server administrator only has access from the allowed IP address by using a web browser from the local network where the KT Secure Vault Server is located. HTTPS protocols are used for communication between the server administrator's PC and the KT Secure Vault Server in order to secure any transmitted data. Moreover, communication must operate in a TLS 1.2 communication operating environment to ensure the confidentiality and integrity of data between TOE components.

Mail servers are used when sending mail to the group administrator or group users, and the NTP server is used to synchronize the time in the KT Secure Vault Server.

Major security features of the TOE

The major security features offered by TOE are as follows.

Security Audit

- Generates records of the authorized administrator's security management performance and user file encryption and decryption as audit data to allow the authorized administrator to query and review the audit data.

Cryptographic Support

- Supports key management and cryptographic operations for using the TOE's encryption function, and encrypts/decrypts authentication data files that will be inspected or secured.

User Data Protection

- Provides the function of controlling access to encrypted files (vault files) based on the group administrator or group user's ID, group information, and permissions level.

Identification and Authentication

- The server administrator provides ID/PW based identification and authentication functions, and the group administrator and group user provide authentication functions through a PIN number.

Security Management

- The server administrator manages all services such as generating groups through security management functions, and the group administrator manages group users through the relevant group's security management functions.

TOE Access

- TOE can terminate an authorized user's session at their request.

TOE safely stores user files and only permits access from authorized users. Its main purposes are as follows.

1) When a file from a user's PC is released to the outside, it ensures that the content of the original file is not exposed regardless of how it was leaked.
2) Grants permissions so that only specially authorized user groups can view files.

1.3.2 TOE Type

TOE is an information security product that offers encryption/decryption and Access Control Functions to secure files saved on a user PC. It is offered in software format. It provides the function of generating encrypted files (vault files) by encrypting random files in accordance with security policies or encrypting certain files saved on the user PC. Encrypted files (vault files) can be decrypted through access by users from a group with access permissions.

1.3.3 Non-TOE Hardware/Software Requirements for TOE Operations

[Table 3] explains the non-TOE hardware and software of the KT Secure Vault Server.

Category	Minimum Requirements
CPU	Intel® Core™ i7, 4Core 2.5Ghz or higher
RAM	2GB or more
NIC	Ethernet 10/100/1000 * 1 port
HDD	2TB or more
OS	CentOS 7.3 (Kernel 3.10.0) 64bit
S/W	Apache-tomcat 8.5.15 httpd 2.4.25 jdk-8u131 PostgreSQL 9.6.3
Library	glibc 2.17 openssl 1.0.2l

[Table 3] Non-TOE Hardware and Software of the KT Secure Vault Server

[Table 4] explains the non-TOE hardware and software of the KT Secure Vault Client.

Category	Minimum Requirements
CPU	Intel® Core2™ duo 2.2 GHz or higher
RAM	1GB or more
NIC	Ethernet 10/100/1000 * 1 port
HDD	500GB or more
OS	Windows 7 Professional (64bit)
S/W	Microsoft Visual C++ 2013 Redistributable (x86) 12.0.30501

[Table 4] Non-TOE Hardware and Software of the KT Secure Vault Client

[Table 5] explains the Non-TOE hardware and software of the administrator PC.

Category	Minimum Requirements
CPU	Intel® Core2™ duo 2.2 GHz or higher
RAM	1GB or more
NIC	Ethernet 10/100/1000 * 1 port
HDD	500GB or more
OS	Windows 7 Professional (64bit)
S/W	FireFox 54.0

[Table 5] Non-TOE Hardware and Software of the Administrator PC

[Table 6] explains the external IT entity.

Category	Content
Mail Server (SMTP)	Server for sending e-mails.
NTP Server	Server for time synchronization.

[Table 6] External IT entity

The following is detailed information on differentiating software and libraries related to non-TOE in the KT Secure Vault.

- Apache-tomcat 8.5.15: A web application server software that supports the TOE's security management functions.
- httpd 2.4.25: A web server software for processing requested received through TOE.
- glibc 2.17: Library that supports the TOE's encryption functions.
- openssl 1.0.2l: Library that supports the protections of data transmitted between TOE.
- jdk 8u131: Runtime platform for operating the KT Secure Vault Server application.
- PostgreSQL 9.6.3: DBMS that supports TSF data storage.
- Microsoft Visual C++ 2013 Redistributable 12.0.30501 (x86): Software for installing and operating the KT Secure Vault Client.
- FireFox 54: KT Secure Vault V1.0 server administrator's operating interface web browser

1.4 TOE Description

1.4.1 Physical Scope of TOE

The physical scope of TOE includes the KT Secure Vault Server that is distributed through a CD and the KT Secure Vault Client that is installed after downloading from the KT Secure Vault Server. It also includes the KT Secure Vault V1.0 Preparation Procedures and the KT Secure Vault V1.0 User Manual that are distributed to end users in the form of a manual so that the TOE can be safely installed and operated. TOE identifiers that are physically distributed are as follows.

KT Secure Vault V1.0

- KT Secure Vault Server V1.0.B-022.017 (CD distribution)

  * KT Secure Vault Client is included in the package.

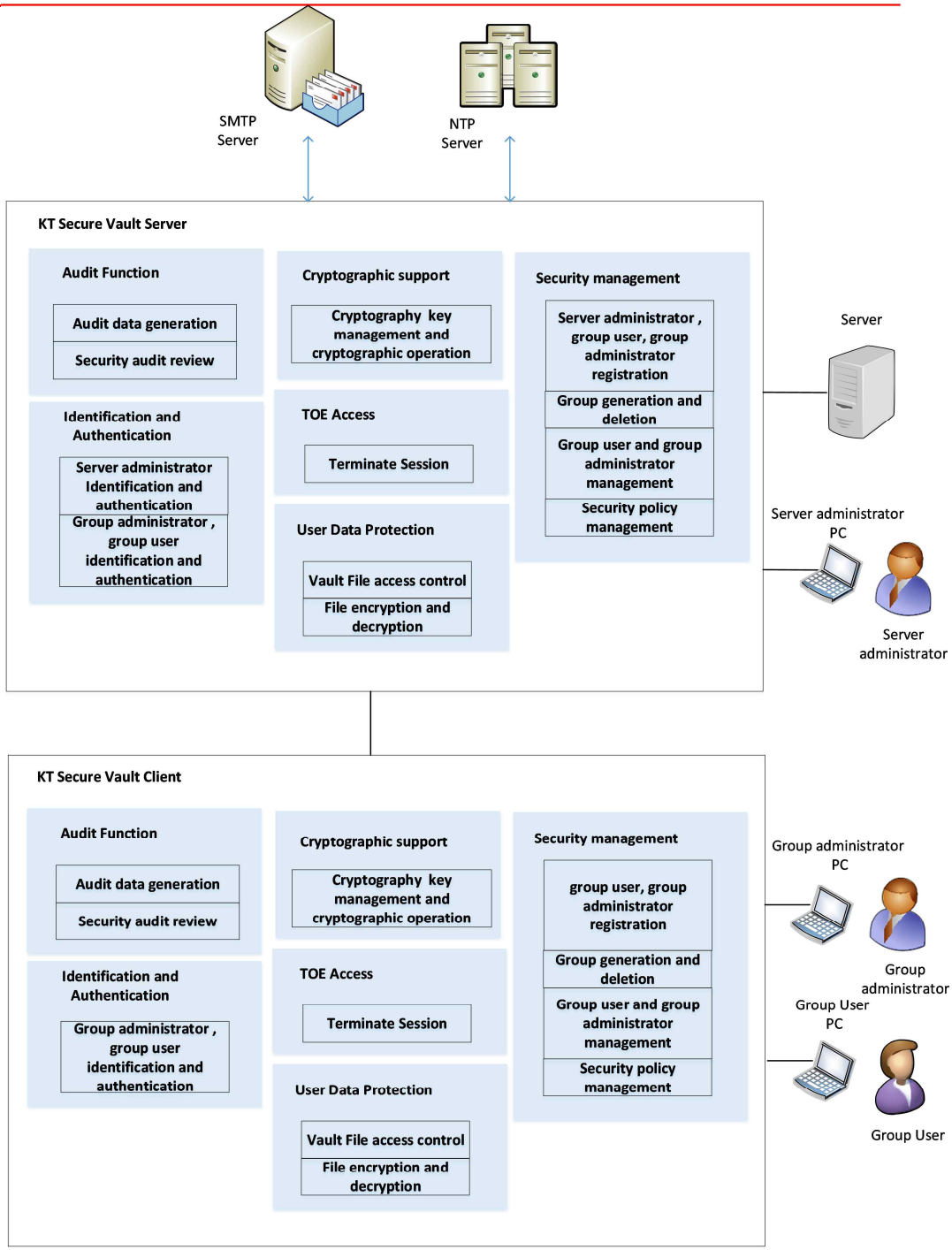
- KT Secure Vault Client V1.0.B-017.019 (download)

Guidance

- KT Secure Vault V1.0 User Manual V1.0.009
- KT Secure Vault V1.0 Preparation Procedures V1.0.009

1.4.2 Logical Scope of TOE

The logical scope of TOE includes Cryptographic Support, identification and authentication, User data protection, security management, audit functions, and TOE access as shown in [Figure 2]. A detailed explanation is as follows.



[Figure 2] Logical Scope of TOE

- **Identification and Authentication:** The server administrator, group administrator, and group user performs identification and authentication functions before preforming security functions in the TOE. The TOE will lock the account upon consecutive authentication failures. Attributes will be granted to the user upon successful authentication. Unnecessary feedback is not provided in the password in order to protect authentication data while authentication is in progress, and password verification is performed for safe authentication procedures. The server administrator's authentication is in ID/PW format, while group administrator and group user authentication involves an encryption key and PIN number for

authentication.

- **Audit Functions:** The TOE Generates audit data and enables the audit data to be reviewed. There are 3 main audit functions.
  1) Group Administrator Audit: Generates audit data regarding security functions performed by the group administrator and stores them in the audit data storage, and enables the server administrator to view the desired audit data through the server management interface.
  2) Server Administrator Audit: Audit data regarding the server administrator's security management performance is generated and stored in the audit data storage, and only the server administrator can view the desired audit data. Relevant to audit data that is generated from the KT Secure Vault Server from the TOE security functions.
  3) Group User Audit: Generates audit data regarding the group user's login records and security functions performed by the group user to encrypt or decrypt files.

- **User Data Protection:** TOE encrypts and decrypts files and performs access control to protect files in user PC
  1) file encryption and decryption: Protects original files by setting permissions levels for files that the group administrator or group user wants to protect or encrypting them in group, Group user can decrypt files by request of decryption or just operation of files. Encryption Target files are distinguished by file extension; default extensions are below.

Category	Encryption target files
Hancom Hangle	hwp
MS Power Point	ppt, pptx
MS Word	doc, docx
MS Excel	xls, xlsx
Acrobat Reader	pdf
AutoCAD	dwg, dwf, dxf

  2) vault file access control: Access is controlled by comparing the attributes of the agent trying to access (view, decrypt, etc.) the encrypted file (Vault file) and the security attributes of the objects included in the encrypted file.

- **Cryptographic Support:** The TOE provides the functions for cryptographic key generation, cryptographic key distribution, cryptographic key destruction, cryptographic operation for the purpose of encryption of authentication data, encrypt/decrypt files. It also generates random bits for safe Cryptographic key generation.

- **TOE Access:** The TOE provides the functions to terminate its own sessions at the request of the user.

- **Security Management:** The TOE provides security management functions to the server administrator and group administrator. The server administrator performs security management by using the web GUI provided in the KT Secure Vault Server. The group administrator logs in through KT Secure Vault Client and performs

security management. The group user, server administrator, and group administrator are managed, groups are generated, group user/group administrator information is revised, and security policies are managed through security management functions.

1.5 Definition of Terms

Of the terms used in this Security Target, the terms that are also used in the Common Criteria will follows the Common Criteria.

- **User** An individual who communicates with the TOE. Refers to all individuals who installs and uses the TOE.
- **External entity** An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE.
- **External IT Object** External IT system that is required to call the TOE's TST.
- **Group** Customer unit that uses the services of the KT Secure Vault V1.0. A gathering of users in a group that shares the same group key.
- **Group Administrator** A group user who uses the administrator functions of the KT Secure Vault Client in the TOE's client area. Adds, views users in the group, views, revises information, deletes, etc. within the group. They manage the group user's permissions and are able to set target files for encryption. The group administrator can use all the functions available to group users, hence all explanations regarding group users are applicable to the group administrator without requiring further descriptions.
- **Group User** A user who uses the KT Secure Vault Client in the TOE's client area.
- **Server Administrator** Adds, views, revises information, and deletes group members and group administrators through the server management UI.
- **Authorized Administrator** A user who was authenticated by the server administrator or group administrator and can perform security management functions.
- **Server Management UI** Server management interface required for the server administrator to perform server management functions.
- **Authentication Key** A unique symmetric key that is generated for each group user, and used to log by sharing with the server.
- **Authentication Code** A random bit from the authentication process that the server transmits to the client.

- **User Registration List** A list of groups (group administrator) or group users that permits registration to the service. It includes fields such as company name, name, e-mail address, etc. Groups can be registered to the list through advanced offline registration, and group users can be registered to the list through a group administrator in the same group.

- **Authentication Text** An alphabet character that is used during the e-mail authentication process that takes place before a group administrator or group user registers for the service. When the group user receives and inputs the authentication text from the e-mail address on the registration list, this confirms their registration on the list and ownership of the registered e-mail address. “Authentication Code” in the group user application program UI refers to this authentication text.

- **Identifier** Refers to the “group user name, team name, permissions level, random bit” values that have the security attributes related to the group user.

- **Encryption Key Seed** A value that is created by encrypting an identifier as a server key.

- **File encryption Key** Key that is used when encrypting/decrypting a key file.

- **Group Key** A unique group key that is generated when the group is registered as a member. It is shared with all users in the group and triggers an encryption key from the encryption key seed that was received from the server.

- **Server Key** A unique group key that is generated when a group becomes registered as a member. The identifier is decrypted to verify the file’s permissions, the encryption key seed is generated according to the permissions, then sent to the client.

- **Pin** When a group user inputs the pin with their ID upon logging in, a unique authentication key is generated to trigger the authentication process. It is often referred to as “PIN Code”.

- **Vault File** The final file type that is created through the TOE from the original file according to an encryption request. Identifiers are included after the original file is encrypted.

- **Designated Encryption Folder** A directory that automatically begins encryption when a group user puts a file inside.

- **Designated Decryption Folder** A special directory where vault files are decrypted back to the original file and saved.

- **Vault File Permissions** The first vault file permissions are the same as the permissions of the vault file encrypt user (group user), and includes file identifiers.

- **Team** A gather of group users with the same team name.

- **Team Encryption** An encryption method that enables decryption only by users with the “same team” attributes.

2 Conformance Claims

2.1 Common Criteria Identification

- Common Criteria of the Information Technology Security Evaluation, Part 1: Introduction and normal model, Version 3.1 Revision 4, 2012.9, CCMB-2012-09-001.
- Common Criteria of the Information Technology Security Evaluation, Part 2: Security function requirements, Version 3.1 Revision 4, 2012.9, CCMB-2012-09-002.
- Common Criteria of the Information Technology Security Evaluation, Part 3: Assurance requirements, Version 3.1 Revision 4, 2012.9, CCMB-2012-09-003.

2.2 Common Criteria Conformance

Common Criteria Part 2 Extended: FCS_RBG.1

Common Criteria Part 3 Conformance

2.3 Protection Profile Conformance

This Security target does not conform to the protection profile.

2.4 Package Conformance

This Security target conforms to the following assurance package.

- EAL1 Conformance

2.5 Conventions

This Security target uses acronyms and English in order to convey accurate meanings. The notations, type, and rules of writing that are used are in accordance with the Common Criteria for Information Technology Security Evaluation (hereafter “Common Criteria”). The Common Criteria permits iteration, assignment, selection, and refinement (revision) operations that may be involved in the security functions requirements, and such operations must be written in accordance with the following rules in the Security target.

- **Iteration** Iteration is used when various operations and other similar components are iterated. Iteration operations result in an iteration number inside parentheses after the component identifier, such as “(Iteration Number)”.
- **Selection** When requirements are written, selection is used upon choosing one or more options that are offered in the Common Criteria for Information Technology Security Evaluation. Selection operations result in *italicized and underlined text*.
- **Refinement** When details are added to requirements, refinement is used to further emphasize the requirements. Refinement operations result in **bolded text**.
- **Assignment** Assignment is used to assign a certain value to an unspecified parameter. Assignment operations result in brackets such as [Assignment_value].

2.6 Conformance Rationale

This ST does not have a protection profile to comply with.

3 Security Objectives

This chapter presents security objectives regarding the operating environment. These security target must be addressed through technical/procedural measures that support the operating environment to enable the TOE to offer precise security functions.

3.1 Security Objectives for the Operational Environment

Label	Content
OE. Physical Security	The TOE must be located in a physically safe environment so that only authorized administrators may have access to it.
OE. Trusted Administrators	The TOE's trusted administrators must have no ill will, must have received proper training regarding TOE management functions, and must accurately perform their duties according to the administrator guidelines.
OE. Safe Management	The TOE must be distributed and installed in a safe manner, and must be configured, managed, and used by authorized administrators through safe methods.
OE. Time Stamp	The TOE must accurately records security related incidents by using reliable time stamps offered by the TOE operating environment.
OE. Operating System Reinforcements	The operating system's reliability and safety must be assured by performing tasks that remove all unnecessary services or means on the operating system and by reinforcing weaknesses in the operating system.
OE. Security Maintenance	When the internal network environment changes due to network configuration changes, host fluctuations, service fluctuations, etc., the changed environment and security policies must immediately be reflected into the TOE operation policies while maintaining the same level of security.
OE. Safe Communication	TLS1.2 must be used in order to ensure the confidentiality and integrity of data that is transmitted regarding communication between TOE configuration factors.
OE. DBMS	The DBMS must be installed and operated so that it is blocked off from all communication aside from connections through the TOE in order to protect the storage where TSF data is stored.

[Table 7] Security Objectives for the Operating Environment

4 Extended Components Definition

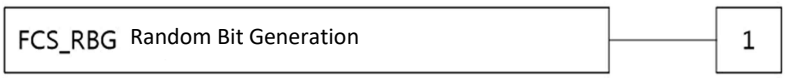
This section explains the extended components from Part 2 or 3 of the Common Criteria in this Security target.

4.1 Cryptographic Support (FCS)

Family Behavior

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

Component levelling



4.1.1 Random Bit Generation (FCS_RBG)

FCS_RBG.1 Random bit generation requires a function that generates random bit values that are required when TSF performs TOE cryptographic operations.

Management: FCS_RBG.1

There are no management activates foreseen.

Audit FCS_RBG.1

There are no auditable events foreseen.

FCS_RBG.1 Random Bit Generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG.1.1 The TSF shall generated the random bits need for Cryptographic key generation by using the specified random bit generator that conforms to the following [Assignment: list of Standard].

5 Security Requirements

This chapter contains the functions and assurance requirements that must be satisfied by the TOE.

The agent, object, operation, security attributes, and external materials that are used in the security requirements in this Security target are defined as follows.

1. Agents, Objects, Related Security attributes, Operations
    - Refer to the [Table 8] below.

Agent (User)		Object (Information)		Operation	Relevant SFR
List	Security attributes	List	Security attributes		
Group User /Group Administrator	Account	Vault File	Vault File Generation Account	View, Change Vault File Permissions Level	FDP_ACC.1 FDP_ACF.1 FCS_COP.1(1)
	Permissions Level		Vault File Permissions Level		FDP_ACC.1 FDP_ACF.1 FCS_COP.1(1)
	Team Name		Vault File Team Name	View	FDP_ACC.1 FDP_ACF.1 FCS_COP.1(1)
Server Administrator /Group Administrator	Account	Audit Record	-	Query	FMT_MTD.1
		TSF Data	-	Change, Generate, Regenerate, Query, Erase	FMT_MTD.1
		Security attributes	-	Delete, Query, Generate	FMT_MSA.1 FMT_MTD.1
		Security Function	-	Permissions Level Range Settings, Set and change target encryption file	FMT_MOF.1

[Table 8] Definition of subjects, Objects, Relevant Security attributes, Operations

2. External entity
    - **Mail Server** E-mail issuance server that issues user authentication text when the mail server is installed
    - **NTP Server** External time synchronization server that synchronizes time in the TOE.

5.1 Security Function Requirements

Security Function Components		
1	FAU_GEN.1	Audit data Generation
2	FAU_GEN.2	User identity association
3	FAU_SAR.1	Audit review
4	FAU_SAR.3	Selectable audit review
5	FCS_CKM.1	Cryptographic key generation
6	FCS_CKM.2	Cryptographic key distribution
7	FCS_CKM.4	Cryptographic key destruction
8	FCS_COP.1(1)	Cryptographic operation (AES)
9	FCS_COP.1(2)	Cryptographic operation (SHA)
10	FCS_RBG.1	Random Bit Generation
11	FDP_ACC. 1	Subset access control
12	FDP_ACF.1	Security attribute based access control
13	FDP_RIP.1	Subset residual information protection
14	FIA_AFL.1(1)	Authentication failure handling (Group user)
15	FIA_AFL.1(2)	Authentication failure handling (Group administrator)
16	FIA_AFL.1(3)	Authentication failure handling (Server administrator)
17	FIA_ATD.1	User attribute definition
18	FIA_SOS.1	Verification of secrets
19	FIA_UAU.2	User authentication before any action
20	FIA_UAU.4	single-use authentication mechanisms
21	FIA_UAU.7	Protected authentication feedback
22	FIA_UID.2	User identification before any action
23	FMT_MOF.1	Management of security functions behavior
24	FMT_MSA.1	Management of security attributes
25	FMT_MTD.1	Management of TSF data
26	FMT_SMF.1	Specification of Management Functions
27	FMT_SMR.1	Security roles
28	FTA_SSL.4	User-initiated termination

[Table 9] Security Function Requirements

5.1.1 Security audit (FAU)

5.1.1.1 Security audit data generation (FAU_GEN)

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 showdown of the audit functions;

b) All auditable event for the *Not specified* level of audit; and

c) [The following audit events in Table 10]

Security Function Components	Audit event type	Additional audit record information
FDP_ACF.1	File encryption	
FDP_ACF.1	File decryption	- Reason for decryption failure
FDP_ACF.1	File permissions change	- Details of change
FIA_UAU.2	Group user login	- Re-authentication that occurs during key reset process - Number of failed logins
FIA_UAU.2	Group administrator login	- Re-authentication that occurs during key reset process - Number of failed logins
FIA_UAU.2	Server administrator login	- Number of failed logins
FMT_MSA.1	Group addition	- Named of added group - Group administrator info
FMT_MSA.1	Group info change	
FMT_MSA.1	Group administrator addition	- Added group administrator account
FMT_MSA.1	Group administrator deletion	- Deleted group administrator account
FMT_MSA.1	Server administrator addition	- Added server administrator account
FMT_MSA.1	Server administrator deletion	- Deleted server administrator account
FMT_MSA.1	Server administrator password change	
FMT_MTD.1	Group user addition	- Added group user account
FMT_MTD.1	Group user deletion	- Deleted group user account
FMT_MTD.1	Group user info change	
FMT_MOF.1	Target encryption file extension change	- Details of extension change

[Table 10] Audit events

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [additional record information specified in Table 10].

FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.2 **Security audit review (FAU_SAR)**

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 [[Table 11] Authorized administrator] with the capability to read [audit target incidents that are applicable to [Table 11]] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Authorized administrator	Audit event type
Group administrator	File encryption
	File decryption
	Vault file permissions change
	General user login
	Group administrator login
Server administrator	Server administrator login
	Group addition
	Group info change
	Group administrator addition
	Group administrator deletion

Server administrator addition
Server administrator deletion
Server administrator password change
Group user addition
Group user deletion
Group user info change
Target encryption file extension change

[Table 11] Authorized Users Who Can Read Audit events

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 ability to apply [following section and/or ordering method] of audit data based on [criteria with the following logical relationship].

[

- criteria with logical relationship: Audit data type in [Table 12] and selection criteria according to audit data type

- Selection and/or ordering method: Descending order based on time of occurrence according to “Selection criteria according to audit data type” in [Table 12]

]

Audit Data Type	Selection criteria According to Audit Data Type	Permitted Ability
Group administrator log	Search Time: (Start Date (Year-Month-Date) ∧ End Date (Year-Month-Date)) ∨ Group Query: Single selection (Group ID)	Search
Server administrator log	Search Time: (Start Date (Year-Month-Date) ∧ End Date (Year-Month-Date)) ∨ Group Query: Single selection (Server Administrator ID)	Search
Group user log	Search Time: (Start Date (Year-Month-Date) ∧ End Date (Year-Month-Date)) ∨ User Query: Single selection (ID)	Search
Fire encryption/decryption log	Search Period: Single selection (Year-Month-Date) ∨ File Generator: Single selection (ID) ∨ File viewer: Single selection (ID) ∨ View Results: Single selection (Success/Fail/All)	Search
(Legend: The ∧ sign means “and” and the∨ sign means “or”)		

[Table 12] Selection criteria according to audit data type

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic key management (FCS_CKM)

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic Key distribution or

FCS _COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [[Table 13] Key generation] and specified cryptographic key sizes [key length is [Table 13] Key generation] that meet the following: [None].

Key Type	Algorithm	Key Length
File encryption key	AES, HASH-DRBG	256bit
Authentication key	HASH-DRBG	128bit
Group key		128bit
Server key		256bit

[Table 13] Key Generation

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [

- Group Key: Use of key distribution methods that conform to the KT key distribution standards

] that meets the following: [None]

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified Cryptographic key destruction method [Table 14 Key Destruction Method] that meets the following [None].

Key Type	Key Storage Location	Destruction Method
File encryption key	Client	Zeroization
Server key	Server	
Group key	Client	
Authentication key	Server	

[Table 14] Key Destruction Method

5.1.2.2 Cryptographic operation (FCS_COP)

FCS_COP.1(1) Cryptographic operation (AES)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) The TSF shall perform [Table 15 Cryptographic operation List]] in accordance with a specified cryptographic algorithm [cryptographic algorithm in Table 15] and cryptographic key sizes [key length in Table 15] that meet the following: [standard list in Table 15].

Standard List	Cryptographic Algorithm	Key Length	Cryptographic Operation	Operation Mode
ISO/IEC 18033-3	AES	128bit	Authentication code verification	Not applicable
		256bit	Encryption key seed generation	Not applicable
		256bit	Identifier generation	CBC mode
		256bit	Data encryption/decryption	CTR mode
		128bit	Authentication key encryption/decryption	CBC mode

[Table 15] Cryptographic Operation

FCS_COP.1(2) Cryptographic operation (SHA)

Hierarchical to: No other components

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2) The TSF shall perform [execute a hash function] in accordance with a specified cryptographic algorithm [SHA-256] and cryptographic key sizes [not applicable] that meet the following: [FIPS PUB 180-3, “Secure Hash Standard”].

5.1.2.3 Random Bit Generation (FCS_RBG)

FCS_RBG.1 Random Bit Generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG.1.1 The TSF shall generate the random bits necessary to generate encryption keys by using the specified random bit generator that conforms to the following [TTAK.KO-12.0190].

5.1.3 User data protection (FDP)

5.1.3.1 Access control policy (FDP_ACC)

FDP_ACC.1 Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Access Control SFP] on [

Subject: Group administrator, group user

Object: Vault File

Operation: Viewing vault files, changing vault file permissions

]

5.1.3.2 Access control functions (FDP_ACF)

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [Access Control SFP] to objects based on the following: [Subject: Group administrator, group user

Subject’s Security attributes: Account, permissions level, team name

Object: Vault File

Object's Security attributes: Vault file permissions level, vault file team name, vault file generation account

]

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

[

- All encrypted vault files can only be opened when the <account> that is trying to view the file and the <vault file generation account> are in the same group.
- Team encrypted vault files can only be opened when the <team name> that is trying to view the file and the <vault file team name> are the same.
- All encrypted vault files can only be opened when the <permissions level> that is trying to view the file is higher than the <vault file permissions level>.
- The permissions level for all encrypted vault files can only be changed when the <permissions level> that is trying to view the file is higher than the <vault file permissions level>.

]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None]

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

5.1.3.3 Residual information protection (FDP_RIP)

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [original files].

5.1.4 Identification and authentication (FIA)

5.1.4.1 Authentication failures (FIA_AFL)

FIA_AFL.1(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 [group user login attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts **of the group user** has been *met*, the TSF shall [prevent the user's authentication until the PIN is re-registered after the authentication key is reset through the authorized group administrator]

FIA_AFL.1(2) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Authentication

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [group administrator login attempts]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts **of the group administrator** has been *met*, the TSF shall [prevent the group administrator's authentication until the group administrator re-registers their authentication key].

FIA_AFL.1(3) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Authentication

FIA_AFL.1.1 The TSF shall detect when [*5]* unsuccessful authentication attempts occur related to [server administrator login attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts **of the server administrator** has been *met*, the TSF shall [prevent the server administrator's authentication].

5.1.4.2 User attribute definition (FIA_ATD)

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

User	Security attributes
Group User	• User Account • Permissions Level • Team Name

Group Administrator	• User Account • Permissions Level • Team Name
Server Administrator	• User Account

[Table 16] User attribute definition

].

5.1.4.3 Specification of secrets (FIA_SOS)

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [[Table 17] Confidential Information Acceptance Criteria].

Confidential Information	Acceptance Criteria
Server administrator password	12 characters or more Numbers, letters, and at least 1 special character
Group administrator and group user PIN	Number between 0000-9999

[Table 17] Confidential Information Acceptance Criteria

5.1.4.4 User authentication (FIA_UAU)

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 [group user and group administrator authentication mechanisms through a signature that uses authentication codes].

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 [change the password or PIN entered by the group user into "*" and print this on the screen] to the user while the authentication is in progress.

5.1.4.5 User identification (FIA_UID)

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)

5.1.5.1 Management of functions in TSF(FMT_MOF)

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of, modify the behavior of* the functions [Table 18 Management-Function List] to [Authorized administrators].

Authorized Administrator	Function
Server Administrator	Set permissions level range
Group Administrator	Set and change target encryption file

[Table 18] Management-Function List

5.1.5.2 Management of security attributes (FMT_MSA)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [access control SFP to restrict the ability to [*operate*] the security attributes [Table 19 Security attributes list] to [authorized administrators].

Security attributes list	Operation	Administrator
Group user account	*Delete, Query, [Generate]*	Group administrator
Group administrator account	*Delete, Query, [Generate]*	Server administrator
Group administrator account	*Delete, Query, [Generate]*	Group administrator
Server administrator account	*Delete, Query, [Generate]*	Server administrator
Permissions level, Team name	*Query, [Generate]*	Group administrator

[Table 19] Security attributes list

5.1.5.3 Management of TSF data (FMT_MTD)

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [*operate Management of TSF data in Table 20*] the [TSF data list of Management of TSF data in Table 20] to [permitted roles for Management of TSF data in Table 20].

TSF Data List	Operation	authorized roles
Group Administrator Log [Table 11 Authorized users who can read audit Incidents]	*Query*	Server administrator
File encryption/decryption history [Table 11 authorized users who can read audit Incidents]	*Query*	Group administrator
Server administrator log [Table 11 authorized users who can read audit Incidents]	*Query*	Server administrator
Group user log [Table 11 authorized users who can read audit Incidents]	*Query*	Group administrator
Group user account, Group administrator account	*Erase, Query, [Generate]*	Server administrator, Group administrator
Permission level, Team name	*Query, [Generate]*	Server administrator, Group administrator
Target encryption file type	*Change, Query, Erase, [Generate]*	Group administrator
Group registration info: Group ID, Group name, Company address, Main Phone No., Max permissions level, etc.	*Change, Erase, Query*	Server administrator
No. of registered groups	*Query*	Server administrator
Group key	*[Regenerate]*	Group administrator
Server key	*Erase (upon withdrawing), Query, [Generate]*	Server administrator
Designated encryption (decryption) folder path	*Change*	Group user

User PIN, Group administrator PIN	*Change, [Generate]*	Group user
Server administrator ID,	*Query, [Generate]*	Server administrator
Password	*Change, [Generate]*	Server administrator

[Table 20] Management of TSF data

5.1.5.4 **Specification of Management Functions (FMT_SMF)**

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: [

1) List of security functions specified in FMT_MOF.1

2) List of security attributes specified in FMT_MSA.1

3) List of Management of TSF data specified in FMT_MTD.1

]

5.1.5.5 **Security management roles (FMT_SMR)**

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [group user, group administrator, and server administrator roles].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.6 TOE Access (FTA)

5.1.6.1 **Session Locking and termination (FTA_SSL)**

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

5.2 Assurance Requirements

The assurance requirements in this Security target are composed of the assurance components in

Part 3 of the Common Criteria. The evaluation assurance level is EAL1. Table 21 Assurance Requirements below summarizes the assurance components of EAL1.

Assurance Class	Assurance Component
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ADV: Development	ADV_FSP.1 Basic function specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

[Table 21] 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 OE 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 identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

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

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to

which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

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

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

ASE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for

content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

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

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

ASE_REQ.1.4C All operations shall be performed correctly.

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

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

Evaluator action elements:

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

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

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

5.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

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

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

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

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

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

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

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements

for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

5.2.4 Life-cycle Support

ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

5.2.5 Tests

ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

5.2.6 Vulnerability Assessment

AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

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

5.3 Dependency Rationale

5.3.1 Dependency Rationale of Security Functional Requirements

No.	Security Function Requirement	Dependency	Reference No.
1	FAU_GEN.1	FPT_STM.1	OE. Time stamp
2	FAU_GEN.2	FAU_GEN.1	1
		FIA_UID.1	-
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.3	FAU_SAR.1	3
5	FCS_CKM.1	FCS_COP.1 or FCS CKM.2	8, 6
		FCS_CKM.4	7
6	FCS_CKM.2	FCS_CKM.1	5
		FCS_CKM.4	7
7	FCS_CKM.4	FCS_CKM.1	5
8	FCS_COP.1	FCS_CKM.1	5
		FCS_CKM.4	7
9	FCS_RBG.1	-	-
10	FDP_ACC.1	FDP_ACF.1	11
11	FDP_ACF.1	FDP_ACC.1	10
		FMT_MSA.3	-
12	FDP_RIP.1	-	-
13	FIA_AFL.1	FIA_UAU.1	-
14	FIA_ATD.1	-	-
15	FIA_SOS.1	-	-
16	FIA_UAU.2	FIA_UID.1	-
17	FIA_UAU.4	-	-
18	FIA_UAU.7	FIA_UAU.1	-
19	FIA_UID.2	-	-
20	FMT_MOF.1	FMT_SMF.1	23
		FMT_SMR.1	24

21	FMT_MSA.1	FDP_ACC.1	10
		FMT_SMF.1	23
		FMT_SMR.1	24
22	FMT_MTD.1	FMT_SMF.1	23
		FMT_SMR.1	24
23	FMT_SMF.1	-	-
24	FMT_SMR.1	FIA_UID.1	-
25	FTA_SSL.4	-	-

[Table 22] Dependency Rationale of Security Functional Requirements.

- FDP_ACF.1 has a Dependencies with FMT_MSA.3. However, security attributes such as permissions level, team name, and user registration list that is the basis for enforcing access control SFP are provided by the TSF by assignment/substantiation/generation. Hence, there is to need for parameters to take default values.

- FAU_GEN.1 has a Dependencies with FPT_STM.1. However, the TOE accurately records security related incidents by using reliable time stamps provided from the TOE operating environment. Hence, the Dependencies of FAU-GEN.1 is satisfied trough the security target OE. Time Stamp regarding the operating environment in place of FPT_STM.1.

- FAU_GEN.2 has a Dependencies with FIA_UID.1, and this is satisfied through FIA_UID.2, which has a hierarchical relationship with FIA_UID.1.

- FIA_UAU.2 has a Dependencies with FIA_UID.1, and this is satisfied through FIA_UID.2, which has a hierarchical relationship with FIA_UID.1.

- FIA_AFL.1 has a Dependencies with FIA_UAU.1, and this is satisfied through FIA_UAU.2, which has a hierarchical relationship with FIA_UAU.1.

- FIA_UAU.7 has a Dependencies with FIA_UAU.1, and this is satisfied through FIA_UAU.2, which has a hierarchical relationship with FIA_UAU.1.

- FMT_SMR.1 has a Dependencies with FIA_UID.1, and this is satisfied through FIA_UID.2, which has a hierarchical relationship with FIA_UID.1.

5.3.2 Dependency Rationale of Security Assurance Requirements

Not applicable

6 TOE Summary

6.1 Security Audit

6.1.1 Audit data generation

Audit data is generated when security related functions are performed through the server administrator, such as company member additions, deletions, information changes, group administrator additions, deletions, information changers, server administrator additions, deletions, information changes. Audit data is also generated when security related functions are performed through the group administrator, such as group user additions, deletions, or policy changes.

Moreover, audit data such as the beginning and end of audit functions or user login history are generated, and audit data is also generated when a group user encrypts/decrypts a file or an authorized group administrator uses the group user policy management tool. Audit data is generated by including the users identify and incident time (and the file concerned) so that the users identify and the target audit incident can be connected.

6.1.2 Audit review

The authorized group administrator and server administrator can search through audit data that was generated through performing security functions. A selective query on security audit data can be performed through AND/OR operations for group ID, search period, pass/fail, and through AND/OR operations.

※ Related SFR: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3

6.2 Cryptographic Support

6.2.1 Cryptographic Key Management and Cryptographic Operations

The AES, HASH-DRBG, and SHA-256 encryption algorithms are supported in order to perform the encryption functions provided in the TOE. The encryption keys used in the AES algorithm include server keys, server encryption keys, authentication keys, and group keys. When the server administrator generates a group, the group's 256bit server is generated and stored on the server. The server is generated through HASH-DRBG. When the group administrator or group user runs the KT Secure Vault Client for the first time, an authentication key (128bit) is generated and a PIN to be safely stored is inputted. The hash value of the SHA-256 is generated through the PIN, and this hash value is used to encode the authentication key.

When file encryption is requested, the requester's identification information and file encryption key (256bit) that is triggered from random bits are generated and used for file encryption/decryption

In order to ensure that group keys are shared only between users in the same group, the administrator must perform an encryption through the authentication key of the group user that will receive the group key before it is send, then the group user that receives the encrypted group key can decrypt it using their authentication key.

The CBC mode using AES-128 is used for group key encryption.

If the server key, group key, authentication key, or file encryption key are no longer needed, they will be deleted through overwriting with 0 and discarded.

※ *Related SFR: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_RBG.1*

6.3 User Data Protection

6.3.1 File encryption and decryption

The file encryption/decryption uses AES-256 algorithm and a vault file is generated when the file encryption is successful. The target file that provides the file encryption function is divided by file extension. The default value is as follow. It also provides the ability for the group administrator to additionally register any extensions.

Category	Encryptiopn target files
Hancom Hangle	hwp
MS Power Point	ppt, pptx
MS Word	doc, docx
MS Excel	xls, xlsx
Acrobat Reader	Pdf
AutoCAD	dwg, dwf, dxf

The KT Secure Vault Client regularly scans the designated encryption folder to identify and encrypt files that are not vault files. When the encryption is completed, it is decrypted and compared with the original file to check if the encryption was successful and to verify that the file is the same. The original file will then be deleted. Encrypted files (vault files) have the capital letter “V” at the end of the original file’s extension. The icon will have the product mark on the original file icon.

Decryption of an encrypted file (vault file) is possible when a decryption group user runs a vault file or requests a decryption. The TOE will automatically delete the decrypted original file when the vault file finishes running.

6.3.2 Vault File Access Control

Decrypting and changing permissions on an encrypted file (vault file) can be performed when conditions are satisfied after comparing the security attributes of the encrypted file (vault file) against the security policies.

- If the file was not generated through team encryption: The permissions level of the generator of the encrypted file that was extracted from the identifier through the KT Secure Vault Server is the same or lower than the permissions level of the decryption requester.

- If the file was generated through team encryption: The team same of the generator of the encrypted file that was generated from the identifier through the KT Secure Vault Server is the same as the decryption requester.

※ *Related SFR*: *FDP_ACC.1, FDP_ACF.1, FDP_RIP.1, FMT_MSA.1*

6.4 Identification and Authentication

6.4.1 Server Administrator Identification and Authentication

The server administrator can log in by entering their server administrator ID and password that were registered in advance. If the server administrator enters the wrong password 5 or more times, their ID will be locked and they will be unable to log in. During the authentication process, the text entered by the server administrator will be changed into "*" and printed on the screen. The server administrator's password must have at least 12 characters in a combination of numbers, special characters, and alphabet characters, and will only be generated when at least 1 is included.

6.4.2 Group Administrator, Group User Identification and Authentication

The group user and group administrator can log in by entering a 4-digit PIN that was registered in advance. If the wrong PIN is entered 5 or more times, the account will be automatically locked. No functions are available without logging into the TOE. During the authentication process, the text entered by the group user will be changed into "*" and printed on the screen. The group administrator and group user's PIN is generated using a number from 0000-9999.
A method that verifies randomly generated bits is used to prevent the reuse of authentication data.

※ *Related SFR: FIA_UID.2, FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_UAU.4, FIA_AFL.1(1), FIA_AFL.1(2), FIA_AFL.1(3), FIA_SOS.1*

6.5 Security Management

6.5.1 Group User/Server Administrator/Group Administrator Registration

- Server administrator registration: The server administrator must be registered in order to use the TOE for the first time. When the server is installed for the first time and the server management UI is accessed through the server administrator's PC web browser, the server administrator's account will be registered automatically.

- Group administrator registration: The server administrator registers the group administrator's account upon generating a group. When the group is registered, the

permissions level range of the group user is also designated. Levels range from 1,2,3,4,5,6,7 (1 to 7 with a minimum of 3).

- Group user registration: The group administrator can register group user accounts from the menu. When the account is registered, the server IP and KT Secure Vault Client installation URL will be sent via e-mail.

6.5.2 Group Generation and Deletion

The KT Secure Vault Server administrator can store the registered group's information and group administrator information (e-mail address, etc.) in the group user registration list after their own account is authenticated.

When the server administrator deletes the group, all information on group users stored on the server will be deleted. The group's unique server key that is stored in the server will also be deleted, and encrypted files will not longer be able to be opened.

6.5.3 Group User, Group Administrator Management

The group administrator can add and delete other group administrators and group users. Information (e-mail address, permissions level, team name, etc.) on the group user/group administrator to be added is inputted and stored in the group user registration list, and the group administrator/group user registers a PIN to be used upon logging in.

When registration is complete, the group user and group administrator will be given security attributes include an ID (e-mail address), PIN, group user registration list (company name, e-mail address), individual permissions level, and team name.

6.5.4 Security Policy Management

The group administrator can set the extension of the document to be encrypted, and allow only files with certain extension to be encrypted by group members. They can also set the permissions level range that is allowed in a group. These policies are applied when a group member logs in.

※ Related SFR: FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.6 TOE Access

6.6.1 Session Termination

Server Administrator: The serve administrator's session that interacts with the TOE can be terminated through the server administrator GUI's "logout" interface.

Group Administrator, Group User: The group administrator and group user can terminate a session that is interacting with the TOE's configuration factors through the "logout" interface.

※ Related SFR: FTA_SSL.4

7 Acronyms

Of the acronyms used in this Security target, those are the identical to the acronyms in the Common Criteria will be in accordance with the Common Criteria.

- **NTP** Network Time Protocol
- **DBMS** DataBase Management System
- **PIN** Personal Identification Number