Common Criteria Certification

Document SAFER Blue 3

Security Target

V 1.02

MarkAny Inc.

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

Revision history

Version	Date revised	Details	Created by	Reviewed by
1.00	2023-09-08	Initial version	ES Business Unit PIO 1Team	ES Business Manager
1.01	2023-12-15	Add features and interfaces	ES Business Unit PIO 1Team	ES Business Manager
1.02	2024-1-15	Add features and modify changes	ES Business Unit PIO 1Team	ES Business Manager

Table of Contents

1. ST Introduction

This document is a MarkAny Document SAFER Blue 3 Security Target that targets the Common Criteria EAL1+ level.

1.1. ST reference

This ST is identified as follows.

Item	Specification
Title	Document SAFER Blue 3 Security Target
Version	V1.02
Created by	ES Business Unit PIO 1Team, MarkAny Inc.
Data Created	2024-1-15
TOE	Document SAFER Blue 3
Evaluation Assurance Level	**EAL1+(ATE_FUN.1)**
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation

1.2. TOE reference

TOE is identified as follows.

Item	Specification	
TOE	Document SAFER Blue 3	
Version	3.0.02	
Components	Document SAFER Blue 3 Server 3.0.02 Document SAFER Blue 3 Agent 3.0.02 Document SAFER Blue 3 Core 3.0.02	Software(CD)
Guidance Documents	Document SAFER Blue 3 Operation Guide V1.02 Document SAFER Blue 3 Preparative Procedure V1.02	PDF(CD)
Developer	ES Business Unit PIO 1Team, MarkAny Inc.	

1.3. TOE overview

‘Document SAFER Blue 3' (hereinafter referred to as “TOE”) is used to protect important documents managed by the organization. The TOE encrypts electronic documents to protect the 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 can encrypt or decrypt documents to be protected by specifying individual documents, document types(PDF, HWP, MS-Office, etc.), etc., and the TOE encrypt the entire contents of the documents.

The primary security features provided by the TOE include the encryption/decryption of the document to be protected and cryptographic key management. For this encryption function, the TOE uses a validated cryptographic module, MarkAny MACRYPTO V3.00. The security and implementation conformance of MarkAny MACRYPTO V3.00 are validated by the Korea Cryptographic Module Validation Program (KCMVP)

1.3.1. TOE Type

The TOE is ‘Document Encryption’ that prevents information leakage by encrypting/decrypting important documents within the organization and is provided as software. The TOE supports both of “user device encryption” type and “information system encryption” type

In the ‘user terminal encryption’ method, Document SAFER BLUE 3 Server (hereinafter referred to as Server) and Document SAFER BLUE 3 Agent (hereinafter referred to as Agent) are essential TOE components.
In the ‘information system encryption’ method, Server, Agent, and Document SAFER BLUE 3 Core (hereinafter referred to as Core) are essential TOE components.

1.3.2. TOE usage and major security features

The TOE performs document encryption/decryption according to the policy set by the administrator in order to protect the important documents managed within the organization, it includes the cryptographic key management function. Besides, the TOE also provides other functions, such as the security audit function that records major events at the time of starting up the security or management function as the audit data for management, identification and authentication function (e.g., administrator and document user identity verification, authentication failure processing, and mutual authentication among TOE components), security management function for security function, role definition, and configuration, the function of protecting the data stored in the repository controlled by the TSF, TSF protection function like the TSF’s self-test, and the TOE access function to manage the interacting session of the authorized administrator.

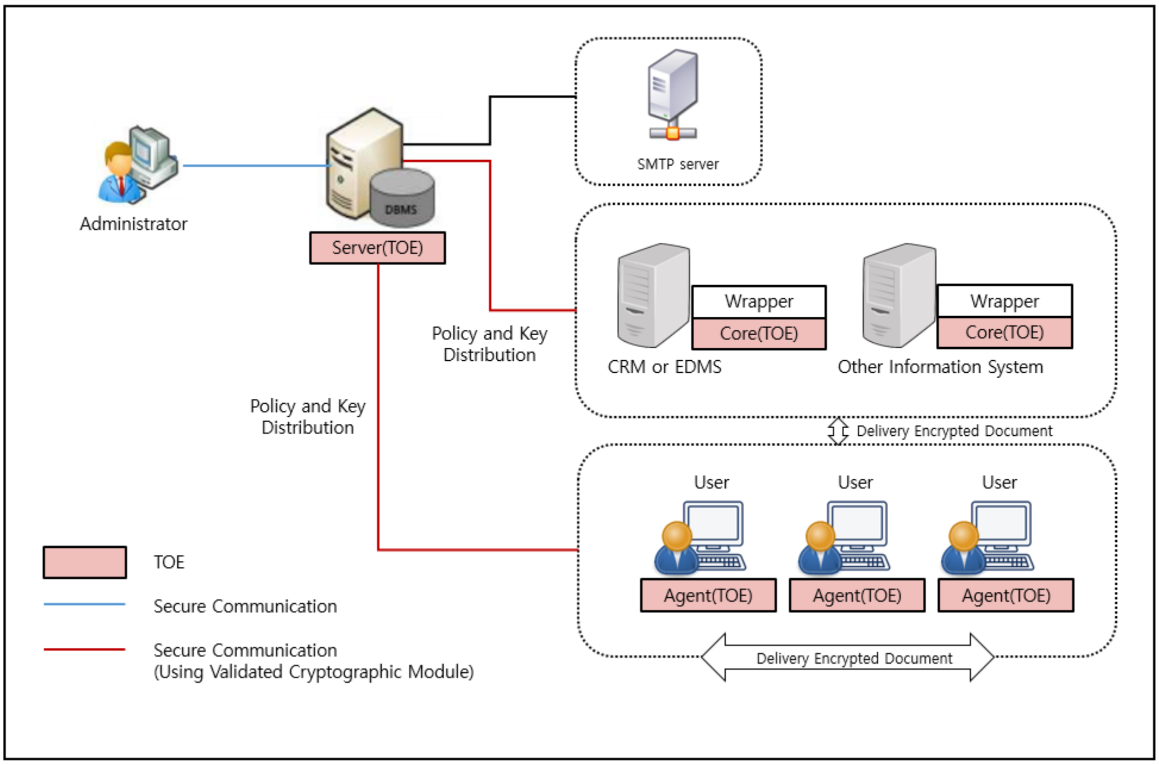
'Data encryption key (hereinafter 'DEK')' and 'Key encryption key (hereinafter 'KEK')' are used for document encryption and decryption functions. The Server creates DEK and KEK and distributes them to Agent and Core modules, and at this time, the encryption key is distributed in a secure manner. The Agent or Core module encrypts or decrypts the document encryption key stored in the header of the document to be protected with the DEK for document encryption key encryption. KEK is used as a symmetric key, and DEK is used as a symmetric key and asymmetric key depending on the purpose.

If the encryption key is no longer used, the TOE destroys the encryption key in memory by overwriting it with '0' three times. Administrators can designate documents subject to encryption and decryption through the server and grant access rights to documents to document users. The server distributes encryption keys to document users according to the set policy, so only authorized document users can encrypt and decrypt documents.

1.3.3. Non-TOE and TOE operational environment

[Figure 1] shows the operational environment where the TOE is operated. The TOE is composed of the Server, Agent, and Core and should be installed and operated inside the internal network of the protected organization.

[Figure 1]TOE operational environment



The TOE is composed of the Server which manages the security policy and cryptographic key, the Agent that performs Document encryption/decryption installed in the user PC, and the Core that performs Document encryption installed in the information system in the form of API module. A wrapper is used for compatibility between the Core and various information systems, but it is excluded from the scope of the TOE.

The administrator uses the server to set policies for document users or information systems, and distributes encryption keys to the Agent and Core according to the policy and document exchange policy configured by the administrator.
The Agent performs Document encryption/decryption using the validated cryptographic module according to the distributed policy. Upon the request from the information system, the Core performs Document encryption/decryption using the validated cryptographic module according to the distributed policy.

The validated cryptographic module, MarkAny MACRYPTO V3.00, is used for the cryptographic operation of the major security features of the TOE and used for the communication between the TOE components.
TLS 1.2 is used when the administrator accesses the Server using the web browser.

As other external entities necessary for the operation of the TOE, there are email server to send alerts by email to the authorized administrator.

The requirements for hardware, software and operating system to install the TOE are as in the following.

Component			Requirement	
Server	HW	CPU	Intel(R) 2.45GHz or higher	
		RAM	8GB or higher	
		HDD	1TB or higher for the installation of TOE	
		NIC	100/1000 Ethernet Card 1Port or higher	
	OS		Windows Server 2022 Standard (64 bit)	Ubuntu 22.04 (5.15.0-53-generic) 64bit
	SW		OpenJDK 1.8.0_392 Apache Tomcat 9.0.85 Oracle 19c(19.3.0.0.0)	OpenJDK 1.8.0_392 Apache Tomcat 9.0.85 Mariadb 11.0.4
Agent	HW	CPU	Intel Core 2.50 GHz or higher	
		RAM	4GB or higher	

Component			Requirement
		HDD	500GB or higher for the installation of TOE
		NIC	100/1000 Ethernet Card 1Port or higher
	OS		Windows 10 pro(64bit) Windows 11 pro(64bit)
Core	HW	CPU	Intel(R) 2GHz or higher
		RAM	8GB or higher
		HDD	500GB or higher for the installation of TOE
		NIC	100/1000 Ethernet Card 1Port or higher
	OS		Ubuntu 22.04 (5.15.0-53-generic) 64bit
	SW		OpenJDK 1.8.0_392

- **3rd party S/W included in the TOE (3rd party distributed as included in the installation file)**
  - **OpenSSL 3.2.0**
  - **Visual C++ 2008 redistributable 9.0.30729.1**

- **Document viewing and creation program for document users**

  - MS Notepad, MS Wordpad, MS Paint

  - MS Office 2021 (WINWORD, EXCEL, POWERPOINT)

  - Hancom Office 2020 (HWP)

  - Acrobat Reader DC

- **The external IT entity SMTP server is used to send security alerts to administrators by email.**

The requirements for the administrator PC for TOE security management are as in the following.

항목	사양

Web browser	Chrome 120.0.6099.217

1.4. TOE description

1.4.1. Physical scope of the TOE

The TOE is composed of the Server, Agent, Core, and guidance documents (Operation Guide, Preparative Procedure).

Server manages policy and security data for document encryption / decryption and provides the function to apply to Agent.

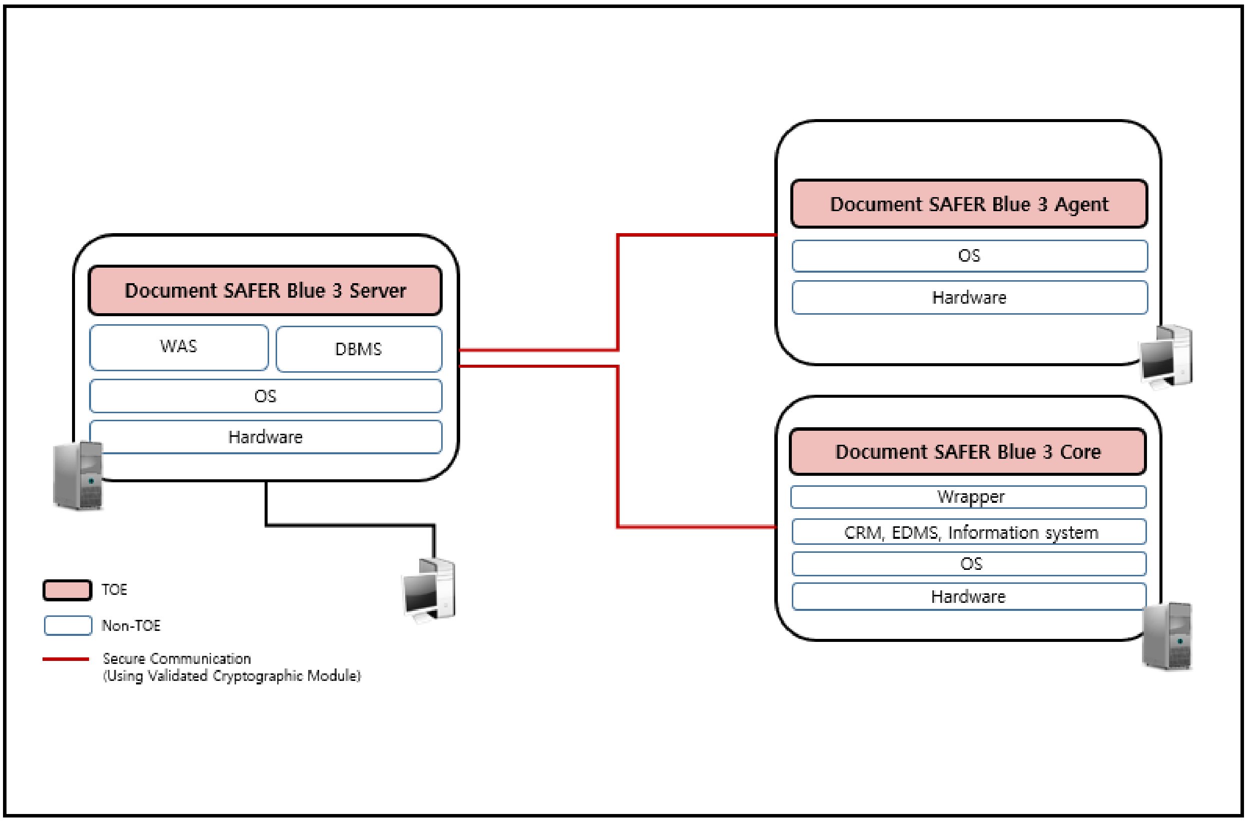
Agent controls the access rights of document according to the policy applied from Server and performs encryption / decryption of security document. Core interacts with information system software and performs the encryption and decryption of security documents according to the policies applied from the server.

TOE component	Document SAFER Blue 3 Server 3.0.02 (Document_SAFER_Blue_3_Server_3.0.02.sh) (Document_SAFER_Blue_3_Server_3.0.02.exe)	Software(CD)
	Document SAFER Blue 3 Agent 3.0.02 (Document_SAFER_Blue_3_Agent_3.0.02.exe)	
	Document SAFER Blue 3 Core 3.0.02 (Document_SAFER_Blue_3_Core_3.0.02.sh)	
TOE Guidance documents	Document SAFER Blue 3 Operation Guide V1.02 (Document SAFER Blue 3 Operation Guide V1.02.pdf) Document SAFER Blue 3 Preparative Procedure V1.02 (Document SAFER Blue 3 Preparative Procedure V1.02.pdf)	PDF(CD)

The hardware and operation system where the TOE is installed, the word processing program that a user uses, the wrapper for compatibility with information systems and external systems and other software necessary to operate the TOE are excluded from the scope of the TOE.

The physical scope of the TOE is as in [Figure 2] below

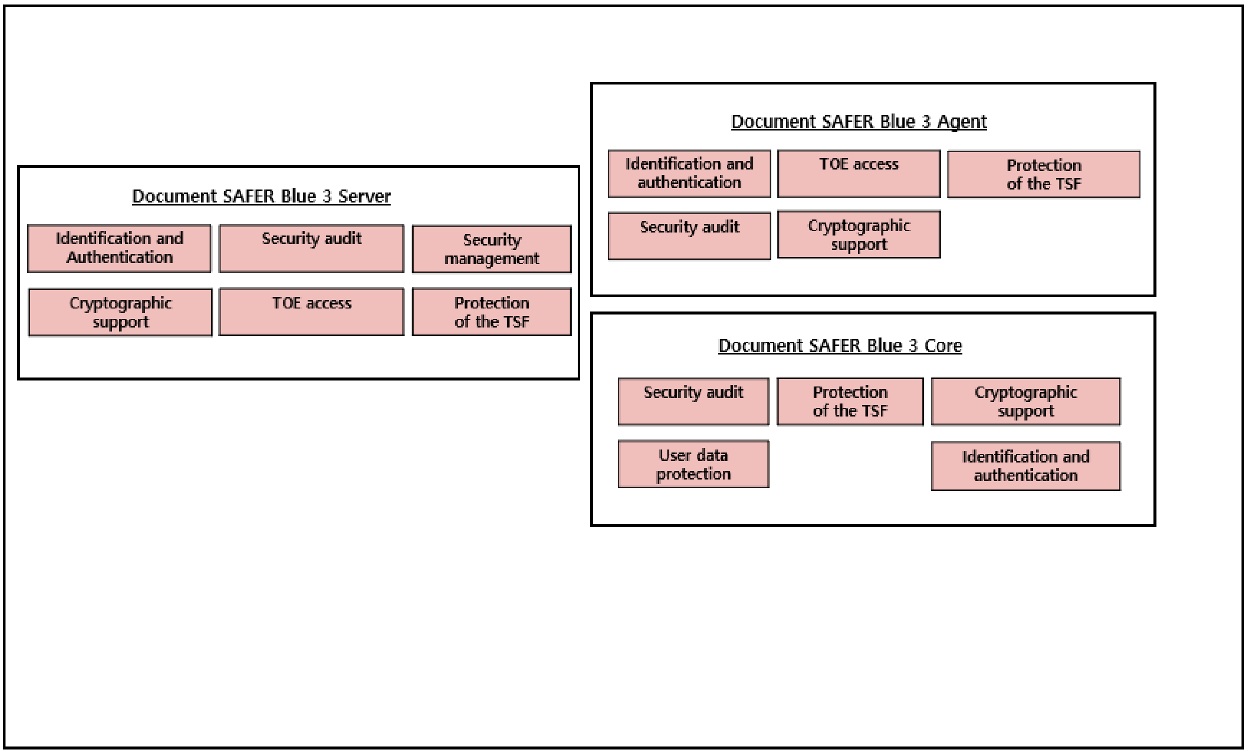
[Figure 2] TOE's physical scope


Document SAFER Blue 3 Server
WAS
DBMS
OS
Hardware
Document SAFER Blue 3 Agent
OS
Hardware
Document SAFER Blue 3 Core
Wrapper
CRM, EDMS, Information system
OS
Hardware
TOE
Non-TOE
Secure Communication
(Using Validated Cryptographic Module)

1.4.2. Logical scope of the TOE

The logical scope of the TOE is as in [Figure 3] below

[Figure 3] TOE's logical scope



[Document SAFER Blue 3 Server]

Identification and authentication

Server provides ID and password-based user identification and authentication to administrators and users. The administrator performs identification and authentication through the administrator web browser. Only authorized administrators who have performed identification and authentication can perform security management functions.

The administrator displays the password by masking it with '*' to prevent it from being exposed when logging in to the administrator page. When administrator identification and authentication fails, the reason for the failure is not provided.

The administrator password consists of a minimum of 9 characters and a maximum of 15 characters in length with a combination rule of at least 3 of English letters/numbers/special characters. If the number of administrator authentication failures exceeds 3, the login function is disabled for 5 minutes.

The server uses a CSRF token to prevent reuse of administrator authentication information.

Server uses timestamps to prevent reuse of user authentication information.

The server performs mutual authentication with other components, Agent and Core, through its own implemented protocol.

Security audit

The server generates audit data related to the initiation/termination of audit and security functions. This data includes events such as the occurrence time of defined audit-targeted events, event types, the identity of the entity triggering the event, task details, and outcomes. The generated audit data is stored in a DBMS (Oracle, MariaDB). Additionally, the server provides functionality for authorized administrators to query the stored audit data based on server time in descending order using AND conditions.

In the event of potential security breaches, such as failed administrator/user authentication audits, document encryption/decryption failures, self-tests, integrity violations, and verification failure of the password module self-test, an alert email is sent to the registered administrator's email address. Additionally, if the Table Space capacity of the DBMS (Oracle, MariaDB) where audit data is stored exceeds the defined threshold (70%), a warning email is sent to the administrator. If the data becomes saturated (90%), old data is overwritten, and a warning email is sent to the administrator.

Security management

The administrator must change the administrator password when first accessing the management screen through a web browser. Only authorized administrators can perform security management through a web browser.

Authorized administrators have only one authority, which is the highest administrator.

The authorized administrator is provided with the following functions.

- Basic management: Provides user and department management, log data management, agent approval, and key management
- Document security: Provides policy management necessary for users to use documents

Cryptographic support

The server generates and distributes cryptographic keys using the MACRYPTO V3.00 validation-required cryptographic module. For all Data Encryption Key (DEK) generation, HASH_DRBG is employed, and key distribution is securely performed using RSAES. The Key Encryption Key (KEK) is securely generated using PBKDF2. Administrator and user passwords are hashed unidirectionally with SHA-512 and stored in the DBMS. After every use, all cryptographic keys undergo three overwrites with zeros.

TOE access

The server terminates the login session after a time interval of inactivity from logging in for secure session management of the authorized administrator. If the administrator's previous session is maintained and reconnected with administrator's authority, the previous connection is terminated and a message is provided so that the ending party can recognize the fact. In addition, Server verifies that the IP address of the administrator PC is the IP address allowed for security management when connecting to Server, and blocks access from IP address other than the allowed IP address.

The allowed address has only one IP address, which is the IP address of the installed server during the initial setup. To access from other locations, one must connect as an administrator from that server and add the IP address.

Protection of the TSF

To protect the confidentiality and integrity of transmitted TSF (Trusted Security Function) data, the server ensures confidentiality and integrity during communication between each component. Encryption is applied to configuration values for stored TSF data protection, ensuring both confidentiality and integrity. The server conducts self-tests and integrity verification during startup and periodically.

[Document SAFER Blue 3 Agent]

Identification and authentication

The agent performs mutual authentication with the server during initial startup and provides user identification and authentication based on user ID and password for users. Users must change their password during their initial login.

To prevent exposure during password entry, the input is displayed as "***" when the user enters the login password. Passwords must consist of a minimum of 9 characters and a maximum of 15 characters, with a combination of at least three of the following: uppercase letters, lowercase letters, numbers, and special characters. If authentication exceeds the limit set by the administrator, the login function is disabled for 5 minutes.

For document user identification and authentication, the agent authenticates users through the login function when it starts, allowing document viewing and saving only upon successful authentication without disclosing the reason for failure.

To prevent the reuse of user authentication information, the agent uses timestamps.

Security audit

The agent generates comprehensive audit logs for all user document activities, including operations, user information, results, etc., and transmits them to the server.

User data protection

The agent encrypts regular documents to create secure documents and protects them by controlling access to the documents according to security policies set by the administrator. Policies vary based on user ID, group, position, document owner, and exchange policies.

To access secure documents, users undergo an authentication process through the login procedure. After successful login, users are controlled based on the permissions set by the administrator for the user or the document itself, including permissions for viewing, editing, printing, and exchanging.

Cryptographic support

The agent performs key generation, deletion, and cryptographic operations through MarkAny MACRYPTO V3.00. After using the main security variables, the memory is overwritten with '0'.

For the protection of documents, cryptographic keys, TSF data, and communication data between components, the agent performs encryption and decryption using the ARIA-CBC mode. During document encryption and decryption operations, the ARIA-CBC mode is applied through the Document Encryption Key (DEK). Similarly, during TSF data encryption and decryption operations, the ARIA-CBC mode is applied through the TSF Data Encryption Key (DEK).

The encryption and decryption of transmitted data involve generating a session key (DEK) during session establishment. The DEK is encrypted with the registered public key during agent authentication and then distributed. Subsequently, using this session key (DEK), the agent protects the transmitted data between the TOE (Target of Evaluation).

Protection of the TSF

The agent securely communicates between components to protect transmitted data, ensuring confidentiality and integrity. Additionally, it safeguards TSF (Trusted Security Function) data from unauthorized exposure and alterations through the use of a validation-required cryptographic module for encryption and independent protocols. The agent also provides periodic self-tests during startup and integrity verification periodically during normal operation.

To prevent unauthorized deletion of configuration values, executable files, etc., the agent implements measures to thwart unauthorized deletions. Furthermore, it offers a termination prevention feature to ensure that the process is not arbitrarily terminated.

[Document SAFER Blue 3 Core]

Identification and authentication

The core performs mutual authentication with the server during the initial startup.

Security audit

The core generates comprehensive audit logs for all document encryption and decryption activities in the integrated system and transmits operations, results, etc., to the server.

User data protection

The core encrypts documents to create secure documents and protects them by controlling access to the documents according to the security policies set by the administrator.

Cryptographic support

The core performs key generation, deletion, and cryptographic operations through MarkAny MACRYPTO V3.00. After using the main security variables, the memory is overwritten with '0'.

For the protection of documents, cryptographic keys, TSF data, and communication data between components, the core performs encryption and decryption using the ARIA-CBC mode. During document encryption and decryption operations, the ARIA-CBC mode is applied through the Document Encryption Key (DEK). Similarly, during TSF data encryption and decryption operations, the ARIA-CBC mode is applied through the TSF Data Encryption Key (DEK).

The encryption and decryption of transmitted data involve generating a session key (DEK) during session establishment. The DEK is encrypted with the registered public key during core authentication and then distributed. Subsequently, using this session key (DEK), the core protects the transmitted data between the TOE (Target of Evaluation).

Protection of the TSF

To secure communication between components and ensure confidentiality and integrity, the core employs secure communication for the protection of transmitted data. Additionally, it uses a validation-required cryptographic module to safeguard TSF (Trusted Security Function) data from unauthorized exposure and alterations through encryption. The core also provides periodic self-tests during startup and periodic integrity verification during regular operation.

1.5. Conventions

This Security Target uses a mixture of English for some abbreviations and clear meanings. The notation, form and writing rules used shall conform to the Common Criteria.

The Common Criteria allows the iteration, allocation, selection, and refinement operations that can be performed in the SFR. Each operation is used in this security target.

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 <u>*underlined and italicized.*</u>

Refinement

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

1.6. Terms and definitions

Terms used in this ST, which are the same as in the Common Criteria, follow those in the Common Criteria.

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

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

Approved mode of operation

The operation mode of the cryptographic module using only the approved cryptographic algorithm

Approved cryptographic algorithm

A cryptographic algorithm selected by Korean 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

Validated Cryptographic Module

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

Attack potential

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

Public Security Parameters, PSP

Security-related public information that could compromise the security of the cryptographic module if it changes

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

Management access

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

Management console

An application that provides the administrator with a graphical interface (GUI), a command-based interface (CLI)

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

Group Based Access Control

One of the random access control methods is an access control method that controls access to objects based on group identifiers

Random bit generator(RBG)

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

Symmetric cryptographic technique

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

Data Encryption Key(DEK)

Key that encrypts the data

Local access

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

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, Computer Aided Design (CAD), etc.)

Iteration

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

Security Target(ST)

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

Security Policy Document

The document to be published with the name of the cryptographic module in the list of verification cryptographic modules, which is a summary of the cryptographic module type, the verification target encryption algorithm provided by the cryptographic module, and the operating environment

Security Token

In order to securely store and archive secret information, a hardware device implemented such that key generation and digital signature generation are processed in the device

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

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

Non-Approved mode of operation
It is a mode that can operate the non-verification target encryption algorithm, and the verification target encryption algorithm can be used

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

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

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

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

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

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

Element
Indivisible statement of a security need

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

Role Based Access Control, RBAC

When a user accesses an object, the access control system controls the access through the relation of the user-role, the access permission-role, and the role according to the characteristics of the organization, rather than the direct relationship between the user and the access permission

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

External Entity

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

Threat Agent

Entity that can adversely act on assets

Authorized Administrator

Authorized user to securely operate and manage the TOE

Authorized Document User

Authorized user to securely operate and manage the TOE

Authentication Data

Information used to verify the claimed identity of a user

Application Programming Interface, API

A set of system libraries existing between the application layer and the platform system, enables the easy development of the application running on the platform

Self-tests

Pre-operational or conditional test executed by the cryptographic module

Assets

Entities that the owner of the TOE presumably places value upon

Refinement

Addition of details to a component

Access Control List, ACL

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

Information System

Systematic system of devices and software related to the collection, processing, storage, search, sending, receiving, and utilization of the information

Organizational Security Policies

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

Dependency

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

Subject

Active entity in the TOE that performs operations on objects

Sensitive Security Parameters, SSP

Core Security Parameters (CSP) and Open Security Parameters (PSP)

Augmentation

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

Component

Smallest selectable set of elements on which requirements may be based

Class

Set of CC families that share a common focus

Key Encryption Key : KEK

Key that encrypts another cryptographic key

TOE, Target of Evaluation

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

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

Family

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

Assignment

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

Shall/must

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

Critical Security Parameters, CSP

Security-related information that can compromise the security of the cryptographic module when exposed or altered (eg, secret / private keys, authentication data such as passwords or personal identification numbers)

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

TSF Data

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

Secure Sockets Layer(SSL)

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

Transport Layer Security(TLS)

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

Wrapper

Interface to connect the TOE with various types of information system

1.7. Security Target Configuration

Chapter 1 introduces the ST and provides the TOE reference, TOE overview, TOE description, composition rules, terminology definition, and configuration information of the ST.

Chapter 2 declares compliance with the CC, PP, and package as a conformance claim and describes the rationale for the declaration of compliance.

Chapter 3 Describes the security objectives for the TOE operational environment.

Chapter 4 Define an extended component that is additionally required according to the 'document encryption' property in the extended component definition.

Chapter 5 Security requirements describe security functional requirements and assurance requirements for satisfying security objectives.

Chapter 6 Summarizes the security functions of the TOE.

Chapter 7 References refer to the data referenced in this ST.

2. Conformance claim

This section describes how this ST complies with the CC, PP, and package.

2.1. CC, PP and package conformance claim

CC		Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 ● 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 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)
Conformant type	Part 2 Security functional components	Extended: FCS_RGB.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2, FTA_SSL.5
	Part 3 Security assurance components	Conformant
	PP	Korean National Protection Profile for Electronic Document Encryption V1.0(December 11, 2019)
	Package	Augmented : EAL1 augmented(ATE_FUN.1)

2.2. Rationale of Conformance claim

This ST claims conformance to security objectives and security requirements by strict adherence to ‘Korean National Protection Profile for Electronic Document Encryption V1.1’.

2.3. How to comply with PPs

This ST conforms to "strict PP Conformant".

3. Security objectives

The followings are the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

3.1. Security objectives for the operational environment

The following table describes the security objectives for the operational environment.

Security objectives for the operational environment

Item	Description
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	The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidance.
OE.RELIABLE_TIME_STAMP	The TOE shall use reliable time information provided by the TOE operating environment.
OE.RELIABLE_STORAGE	The audit repository associated with the TOE shall ensure that it maintains secure and trusted operations.
OE.LOG_BACKUP	The authorized administrator 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 removing all unnecessary services or means and performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
OE.SECURE_DEVELOPMENT	The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the

	requirements of the manual provided with the TOE.
OE.MANAGEMENT_ACCESS	It is necessary to ensure the confidentiality and integrity of the transmitted data between the web browser on the administrator's PC and the operating environment of the management server, which is the web server.

4. Extended components definition

4.1. FCS, Cryptographic support

4.1.1 Random bit generation

Family Behavior

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

Component leveling

FCS_RBG Random bit generation

1

FCS_RBG.1 random bit generation, requires the 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 a cryptographic key using the specified random bit generator that meets the following [assignment: list of standards].

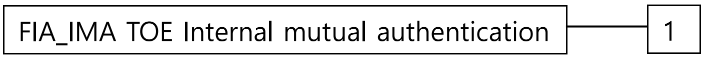
4.2. FIA, Identification & authentication

4.2.1 TOE Internal mutual authentication

Family Behavior

This family defines requirements for providing mutual authentication function 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 meets the following: [assignment: *list of standards*].

4.3. FMT, Security Management

4.3.1 ID and password

Family Behavior

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

Component leveling

FMT_PWD ID and password

1

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*].

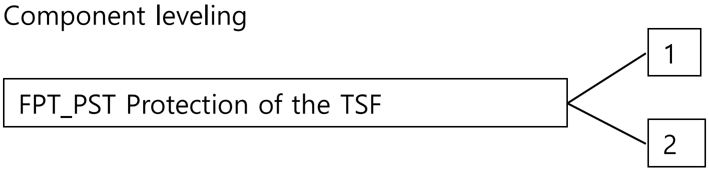
4.4. FPT, Protection of the TSF

4.4.1 Protection of stored TSF data

Family Behavior

This family defines rules to protect the 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 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.2.2 The TSF shall [selection: detect, *prevent*] the unauthorized termination for [assignment: *TSF data*].

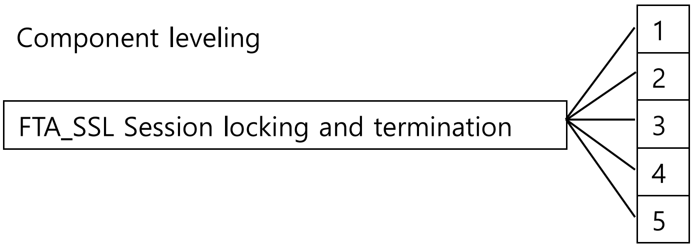
4.5. FTA, TOE Access

4.5.1 Session locking and termination

Family Behavior

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

Component leveling



In CC Part 2, the session locking and termination family consists of four components. In this ST, 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 during which the session locking and termination occurs to each user
b) Specification for the time interval of default user inactivity during which the session locking and termination occurs.

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

This chapter describes the functional and assurance requirements that must be satisfied in the TOE.

This Security Target defines the subjects, objects, operations, security attributes, external entities, and other conditions used in the security requirements as follows.

Definition of subjects, objects, relevant security properties and operations

Subject	Subject security attributes	Object	Object security attribute	Operation
Authorized administrator	Admin ID, Password, IP address	Security management data	-	Query, modify
		Administrator setting data		Query, modify
		User management data		Query, modify
		Group management data		Query, modify
		Security policy data		Query, modify
		Audit data		Query
Authorized document user	User ID, Password	Secured documents	Access, Exchange	View Edit Print Encrypt Decrypt

5.1. Security functional requirements

The security requirements describe the security functional requirements and assurance requirements that the TOE that conforms to the PP must satisfy. The security functional requirements defined in the PP are expressed by selecting the relevant security functional components from CC Part 2 and Chapter 4 extended component definition.

The following is a summary of the security functional requirements components.

Security functional requirements

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation (Document Encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data Encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Document Encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data Encryption)
	FCS_RBG.1(Extended)	Random bit generation
FDP	FDP_ACC.1(1)	Subset access control (Document Encryption access control)
	FDP_ACC.1(2)	Subset access control (Document Usage access control)
	FDP_ACF.1(1)	Security attribute-based access control (Document Encryption access control)
	FDP_ACF.1(2)	Security attribute-based access control (Document Usage access control)
FIA	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE Internal mutual authentication

	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Identification
FMT	FMT_MOF.1	Management of security functions
	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
FPT	FPT_ITT.1	Basic internal TSF data transmission protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_PST.2(Extended)	Availability protection of TSF data
	FPT_TST.1	TSF self-testing
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

5.1.1. Security audit (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to No other components.

Dependencies FAU_SAA.1 Potential violation analysis.

FAU_ARP.1.1 The TSF shall take [sending E-mail to the administrator] upon detection of a potential security violation.

5.1.1.2 FAU_GEN.1 Audit data generation

Hierarchical to No other components.

Dependencies FPT_STM.1 Reliable time stamps.

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

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

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

c) [Refer to the "auditable events" in [Table5-1] 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 or failure) of the event.

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST [Refer to the contents of "additional audit record" in [Table 5-1] Audit events, [none]].

[Table 5-1] Audit events

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(1)	Success and failure of the activity	
FCS_CKM.1(2)	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Document Encryption)	
FCS_CKM.4	Success and failure of the activity (applying to destruction of key related to Document Encryption)	
FCS_COP.1	Success and failure, and the type of cryptographic operation	
FDP_ACF.1(1)	Successful request of operation execution regarding the Object identification object handled by SFP	Object identification information
FDP_ACF.1(2)	Successful request of operation execution regarding the Object identification object handled by SFP	Object identification information
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_IMA.1(Extended)	Success and failure of mutual authentication	
FIA_UAU.1	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the 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	TSF self-testing and the results of the tests	Modified TSF data or module information 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	

5.1.1.3 FAU_SAA.1 Potential violation analysis

Hierarchical to No other components

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 [Server, Agent, Core self-test and integrity failure, audit storage threshold exceeded, audit storage threshold exceeded, administrator/user authentication failure, document encryption/decryption and access control failure, verified password module self-test failure] known to indicate a potential security violation

b) [none]

5.1.1.4 FAU_SAR.1 Audit review

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

5.1.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to	No other components.
Dependencies	FAU_SAR.1 Audit review
FAU_SAR.3.1	The TSF shall provide the ability to apply [Descending search function based on server time] of audit data based on [AND operation].

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

Hierarchical to No other components.

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1	The TSF shall [Notification to the authorized administrator, [None]] If the audit trail exceeds [DB table space capacity 70%].

5.1.1.7 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 E-mail to the authorized administrator] if the audit trail is full.

5.1.2. Cryptographic support(FCS)

5.1.2.1 FCS_CKM.1(1) Cryptographic key generation (Document Encryption)

Hierarchical to	No other components.

Dependencies [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in [Table 5-2]] and a specified cryptographic key sizes [Cryptographic key size in [Table 5-2]] that meet the following: [List of standards in [Table 5-2]].

[표 5-2] Cryptographic key generation algorithm

Category	Cryptographic key generation algorithm	cryptographic key size	List of standards
Document Encryption/ Decryption DEK	HASH_DRBG	256bit	KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2
KEK for Document Encryption/Decryption DEK	HASH_DRBG	128bit	KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2

5.1.2.2 FCS_CKM.1(2) Cryptographic key generation (TSF Data Encryption)

Hierarchical to No other components.

Dependencies [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in [Table 5-3]] and specified cryptographic key sizes [Cryptographic key size in [Table 5-3]] that meet the following: [List of standards in [Table 5-3]].

[Table 5-3] Cryptographic key generation algorithm

Category	Cryptographic key generation algorithm	cryptographic key size	List of standards
TSF data Encryption/Decryption DEK	**HASH_DRBG**	**128bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2**
Transfer data between TOEs Encryption/Decryption DEK	**HASH_DRBG**	**128bit**	**TTAK.KO-12.0190**
KEK for TSF data DEK	**PBKDF2**	**128bit**	**PKCS #5(RFC 8018)**
Cryptographic key distribution DEK	**RSAES**	**3072bit**	**KS X ISO/IEC 18033-2**

5.1.2.3 FCS_CKM.2 Cryptographic key distribution

Hierarchical to No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [[Table 5-4] Cryptographic key distribution] that meets the following: [List of standards of [Table 5-4]].

[표 5-4] Cryptographic key distribution algorithm

Category	Cryptographic key distribution algorithm	cryptographic key size	List of standards
Cryptographic key distribution	**RSAES**	**3072bit**	**KS X ISO/IEC 18033-2**

5.1.2.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components

Hierarchical to No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destruct cryptographic keys in accordance with the specified cryptographic key destruction method [After using the encryption key and key security parameters loaded in memory, change them to '0' three times] that meets the following: [none].

5.1.2.5 FCS_COP.1(1) Cryptographic operation (Document Encryption)

Hierarchical to No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

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

[Table 5-5] Cryptographic operation Algorithm

Cryptographic operation Algorithm	cryptographic key size	List of standards	Cryptographic operation list
ARIA-CBC	256bit	KS X 1213-1 KS X 3254 KS X ISO/IEC 10116	Encryption/decryption of documents
ARIA-CBC	128bit	KS X 1213-1 KS X 3254 KS X ISO/IEC 10116	DEK encryption and decryption for document encryption and decryption

5.1.2.6 FCS_COP.1(2) Cryptographic operation (TSF Data Encryption)

Hierarchical to No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Cryptographic operation list in [Table 5-6]] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in [Table 5-6]] and cryptographic key sizes [Cryptographic key size in [Table 5-6]] that meet the following: [List of standards in [Table 5-6]].

[Table 5-6] Cryptographic operation Algorithm

Cryptographic operation Algorithm	cryptographic key size	List of standards	Cryptographic operation list
ARIA-CBC	128bit	KS X 1213-1 KS X 3254 KS X ISO/IEC 10116	Encryption/decryption of TSF data DEK encryption and decryption for TSF data encryption
ARIA-CBC	128bit	KS X 1213-1 KS X 3254 KS X ISO/IEC 10116	Encryption/decryption for communication
SHA-512	-	KS X ISO/IEC 10118-3:2001	Integrity Check
SHA-512	-	KS X ISO/IEC 10118-3:2001	Encryption of password
PBKDF2	128bit	PKCS #5(RFC 8018)	TSF data DEK encryption and decryption
RSAES	3072bit	KS X ISO/IEC 18033-2	Mutual authentication and key exchange

5.1.2.7 FCS_RBG.1 Random bit generation (Extended)

Hierarchical to No other components.

Dependencies No dependencies

FCS_RBG.1.1 The TSF shall generate random bits using the specified random bit generator that meets the following [[Table 5-7] Random bit generation].

[Table 5-7] Random bit generation algorithm

Random bit generation algorithm	cryptographic key size	List of standards
HASH_DRBG	**256bit**	**KS X ISO/IEC 18031** **TTAK.KO-12.0331-Part1-2**
HASH_DRBG	**128bit**	**KS X ISO/IEC 18031** **TTAK.KO-12.0331-Part1-2**

5.1.3. User data protection (FDP)

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

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 TSF shall enforce the [document encryption access control] on [the list of subjects, objects, and operations among subjects and objects covered by SFP].

[

- Subject list

  Authorized user

- Object list

  Secured document

- Operation list

  I. Decrypt upon viewing

  II. Encryption when editing and saving

]

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

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 TSF shall enforce the [document usage access control] on [the list of subjects, objects, and operations among subjects and objects covered by SFP].

[

- Subject list

  Authorized user

- Object list

  Secured document

- Authorized user

  I. Document exchange (group-based)

  II. Viewing Control

  III. Save and editing controls

  IV. Print Control

]

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

Hierarchical to No other components.

Dependencies FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 TSF shall enforce the [Document Encryption access control] on objects based on [the list of subjects and objects controlled by the following SFP, security attribute appropriate for SFP regarding each subject and object, or group of named security attributes].

[

- Subject list

  Authorized user

- Object list

  Secured document

- Security attribute of Subject

  User ID, User Group

- Security attribute of Object

  Document created by a designated document viewing program

  I. List of designated document viewing programs

     A. MS-OFFICE 2021(WORD, EXCE, POWERPOINT)

     B. HWP 2020

     C. NOTEPAD

     D. MSPAINT

     E. Acrobat Reader DC

     F. Wordpad

- Operation

  I. Decrypt upon viewing

  II. Encryption when editing and saving

]

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 additional rules:

[none]

FDP_ACF.1.4 TSF shall explicitly deny access of the subject to objects based on the following additional rules:

[none]

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

Hierarchical to No other components.

Dependencies FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 TSF shall enforce the [Document usage access control] on objects based on [the list of subjects and objects, operations between subject and object controlled by the following SFP].

[

- Subject list

  Authorized user

- Object list

  Secured document

- Operation list

  User ID, User Group

- Security attribute of Object

  Document created by a designated document viewing program

I. List of designated document viewing programs

A. MS-OFFICE 2021(WORD, EXCEL, POWERPOINT)

B. HWP 2020

C. NOTEPAD

D. MSPAINT

E. Acrobat Reader DC

F. Wordpad

- operation

I. Document exchange (group-based)

II. Viewing Control

III. Save and editing controls

IV. Print Control

]

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 additional rules:

[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)

5.1.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to No other components.

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *[3]* unsuccessful authentication attempts occur related to [authentication of administrator, 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 in 5-minute].

5.1.4.2 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-Agent and Server-Core] in accordance with a specified [internally implemented authentication protocol] that meets the following: [none].

5.1.4.3 FIA_SOS.1 Verification of secrets

Hierarchical to No other components.

Dependencies No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following password permission criteria].

[

permission criteria:

- English letters (case sensitive) : a - z, A - Z

- Numbers : 0 - 9
- special characters : !, @, #, $, %, ^, *, +, =, -

Password must be composed of 3 or more combinations of alphabets / numbers / special characters and be at least 9 characters, but not more than 15 characters.

]

5.1.4.4 FIA_UAU.1 Authentication

Hierarchical to No other components.

Dependencies FIA_UID.1 Identification

FIA_UAU.1.1 The TSF shall allow [the following list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

[

List of actions mediated by the TSF

I. Mutual authentication and key exchange for data encryption / decryption between TOEs

II. Check forgery and alteration status of Agent module

]

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user, except for the actions specified in FIA_UAU.1.1.

5.1.4.5 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [ID/PW based authentication].

5.1.4.6 FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components.

Dependencies FIA_UAU.1 authentication

FIA_UAU.7.1 The TSF shall provide only [the following feedback list] to the user while the authentication is in progress.

[

Feedback list

I. All passwords entered are indicated by "*".

II. If the authentication fails, only the error message "Please check your login information and try again" will be displayed.

]

5.1.4.7 FIA_UID.1 식별

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UID.1.1 The TSF shall allow [the following list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

[

The following is a list of actions mediated by the TSF

I. Mutual authentication and key exchange for TOE communication data encryption/decryption.

II. Verification of the tamper status of the Agent module.

]

5.1.5. Security Management (FMT)

5.1.5.1 FMT_MOF.1 Security Function Management

Hierarchical to No other components.

Dependencies FMT_SMF.1 Management Function Specification

FMT_SMR.1 Security Roles

FMT_MOF.1.1 The TSF shall restrict the ability to *conduct management actions of* the functions [[Table 5-8 Management Function List] to [Authorized Administrators].

[Table 5-8] Management Function List

Menu	Category	Management Action
Basic Management	System	Add, Modify, Delete
	Administrator, User, Department	Add, Modify
	Audit Logs (Basic, Login, Administrator, Startup, Mail Sending, Key Generation, Approval)	Search
	Forgery inspection	Perform
	Agent Approval Management	Approve
	Key Generation	Perform
Document Security	Corporate Policy, ACL Policy	Add, Modify, Delete
	History Inquiry	Search
	Historical Statistics	Search

5.1.5.2 FMT_MSA.1 Security Attribute Management

Hierarchical to No other components.

Dependencies [FDP_ACC.1 Partial Access Control or

FDP_IFC.1 Partial Information Flow Control]

FDP_SMF.1 Management Function Specification

FMT_SMR.1 Security Roles

FMT_MSA.1.1 The TSF shall enforce the [Security Functional Policy Access Control] to restrict the ability to *change_default, query, modify, delete, [none]* the security attributes [The Following Security Attribute List] to [Authorized Administrators].

[

Security Attribute List

I. Server Access Allowed IP

II. Document Security Policy: Target Application, Exchange Policy, Allow Storage and Editing, Allow Agent Deletion

]

5.1.5.3 FMT_MSA.3 Static Attribute Initialization

Hierarchical to No other components.

Dependencies FMT_MSA.1 Security Attribute Management

FMT_SMR.1 Security Roles

FMT_MSA.3.1 The TSF shall enforce the [Access Control SFP] 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 Administrators] to specify alternative initial values to override the default values when an object or information is created..

5.1.5.4 FMT_MTD.1 TSF TSF Data Management

Hierarchical to No other components.

Dependencies FMT_SMF.1 Management Function Specification

FMT_SMR.1 Security Roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** the [TSF data listed in [Table 5-9]] to [the Authorized Administrators].

[Table 5-9] TSF Data List and Management Capabilities

Category		Capability
Audit Data	Administrator Login Log	Query
	Administrator Management Behavior Log	
	User Login Log	
	Server/Service Startup Log	
	Email Sending Log	
	Document Security Log	
Key Data Constituting TOE	Encryption Key	

Category		Capability
	Company ID	Query, Modify
Identification and Authentication Data	ID and Password Hash	Query, Add, Modify, Delete
Group and User Data	User ID	Query, Add, Modify, Delete
	Group Information	
Document Encryption Permission and Policy Data	-	Query, Modify

5.1.5.5 FMT_PWD.1 ID and Password Management (Extended)

Hierarchical to No other components.

Dependencies FMT_SMF.1 Security Management Functions Specification

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 password when the authorized administrator accesses for the first time.*

5.1.5.6 FMT_SMF.1 Security Management Functions Specification

Hierarchical to No other components.

Dependencies No dependencies

FMT_SMF.1.1 The TSF shall be capable to perform the following management functions:

[

Security Management Functions:

- Security Function Management: As specified in FMT_MOF.1

- Security Attribute Management: As specified in FMT_MSA.1
- TSF Data Management: As specified in FMT_MTD.1
- ID and Password Management: As specified in FMT_PWD.1

].

5.1.5.7 FMT_SMR.1 Security Roles

Hierarchical to No other components.

Dependencies FIA_UID.1 Identification

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator].

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

5.1.6. TSF Protection (FPT)

5.1.6.1 FPT_ITT.1 Basic Protection of Internal Transfer of TSF Data

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.

5.1.6.2 FPT_PST.1 Basic Protection (Extended) of Stored TSF Data

Hierarchical to No other components.

Dependencies No dependencies

FPT_PST.1.1 The TSF shall protect [Administrator and user passwords, TOE settings, policies, and core security parameters] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

5.1.6.3 FPT_PST.2 Availability Protection (Extended) of Stored TSF Data

Hierarchical to No other components.

Dependencies No dependencies

FPT_PST.2.1 TSF shall *prevent* the unauthorized deletion of [Agent's configuration values, executable files].

FPT_PST.2.2 TSF shall *prevent* the unauthorized termination of [Agent processes].

5.1.6.4 FPT_TST.1 TSF Self-Test

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 *the TSF*.

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

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

5.1.7. TOE Access (FTA)

5.1.7.1 FTA_MCS.2 Limitation of Concurrent Sessions per User Attribute

Hierarchical to FTA_MCS.1 Basic Limitation of Concurrent Sessions

Dependencies FIA_UID.1 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 number of maximum concurrent sessions as 1 for administrator management access sessions, rules for the number of maximum concurrent sessions {none}].

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

5.1.7.2 FTA_SSL.5 Session Management by the TSF (Extended)

Hierarchical to No other components.

Dependencies No dependencies

FTA_SSL.5.1 The TSF shall *terminate* an interactive session of the **administrator** after a [5-minute period of administrator inactivity].

5.1.7.3 FTA_TSE.1 TOE Session Establishment

Hierarchical to No other components.

Dependencies No dependencies

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

5.2. Security assurance requirements

This section defines the assurance requirements for the TOE. Assurance requirements are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

Security assurance class	Security assurance component	
Security Target	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claim
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedure
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

5.2.1. Security Target Evaluation

5.2.1.1 ASE_INT.1 Security target 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 identify the TOE.

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

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

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

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

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

Evaluator action elements

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

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

5.2.1.2 ASE_CCL.1 Conformance claim

Dependencies ASE_INT.1 Security target 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 to a package of the ST as either package-conformant or package-augmented.

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

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

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

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security

	requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

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

5.2.1.3 ASE_OBJ.1 Security objectives for the operational environment

Dependencies	No dependencies

Developer action elements

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

Content and presentation elements

ASE_OBJ.1.1C	The statement of security objectives shall describe the security objectives for 49 the operational environment.

Evaluator action elements

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

5.2.1.4 ASE_ECD.1 Extended components definition

Dependencies	No dependencies

Developer action elements

ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended

component is related to the existing CC components, families, and classes.

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

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

Evaluator action elements

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

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

5.2.1.5 ASE_REQ.1 Stated security requirements

Dependencies ASE_ECD.1 Extended component 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 security requirements rationale.

Content and presentation elements

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

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

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

ASE_REQ.1.4C All operations shall be performed correctly.

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

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

Evaluator action elements

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

5.2.1.6 ASE_TSS.1 TOE summary specification

Dependencies ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.2. Development

5.2.2.1 ADV_FSP.1 Basic functional specification

Dependencies No dependencies

Developer action elements

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

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

Content and presentation elements

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

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

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of 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

5.2.3.1 AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the useraccessible functions and privileges that shall 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 display, 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.

5.2.3.2 AGD_PRE.1 Preparative procedure

Dependencies No dependencies

Developer action elements

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

Content and presentation 54 elements

AGD_PRE1.1C The preparative procedure shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedure.

AGD_PRE1.2C The preparative procedure 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 procedure to confirm that the TOE can be securely prepared for operation.

5.2.4. Life-cycle support

5.2.4.1 ALC_CMC.1 Labeling of the TOE

Dependencies ALC_CMS.1 TOE configuration management coverage

Developer action elements

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

Content and presentation elements

ALC_CMC.1.1C The TOE shall label for the 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.

5.2.4.2 ALC_CMS.1 TOE CM coverage

Dependencies No dependencies

Developer action elements

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

증거 요구사항

ALC_CMS.1.1C The configuration list shall include the evaluation evidence required by the TOE and 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 meet requirements for content and presentation of evidence.

5.2.5. Tests

5.2.5.1 ATE_FUN.1 Functional testing

Dependencies ATE_COV.1 Evidence of coverage

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plan, expected test results and the 56 actual test results.

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

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

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

Evaluator action elements

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

5.2.5.2 ATE_IND.1 Independent testing: conformance

Dependencies ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedure

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.6. Vulnerability assessment

5.2.6.1 AVA_VAN.1 Vulnerability survey

Dependencies ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedure

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 success potential of basic attack.

5.3. Security requirements rationale

5.3.1. Dependency rationale of security functional requirements

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	OE. RELIABLE_TIME_STAMP
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	OE. RELIABLE_STORAGE
7	FAU_STG.4	FAU_STG.1	OE. RELIABLE_STORAGE
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	[10 or 12]
		FCS_CKM.4	11
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	[10 or 13]
		FCS_CKM.4	11
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[- or - or 8, 9]
		FCS_CKM.4	11
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[- or - or 8, 9]
12	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[- or - or 8]
		FCS_CKM.4	11
13	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or	[- or - or 9]

No.	Security functional requirements	Dependency	Reference No.
		FCS_CKM.1]	
		FCS_CKM.4	11
14	FCS_RBG.1	-	-
15	FDP_ACC.1(1)	FDP_ACF.1(1)	17
16	FDP_ACC.1(2)	FDP_ACF.1(2)	18
17	FDP_ACF.1(1)	FDP_ACC.1	15
		FMT_MSA.3	28
18	FDP_ACF.1(2)	FDP_ACC.1	16
		FMT_MSA.3	28
19	FIA_AFL.1	FIA_UAU.1	22
20	FIA_IMA.1	-	-
21	FIA_SOS.1	-	-
22	FIA_UAU.1	FIA_UID.1	25
23	FIA_UAU.4	-	-
24	FIA_UAU.7	FIA_UAU.1	22
25	FIA_UID.1	-	-
26	FMT_MOF.1	FMT_SMF.1	31
		FMT_SMR.1	32
27	FMT_MSA.1	FDP_ACC.1	15, 16 or -
		FMT_SMF.1	31
		FMT_SMR.1	32
28	FMT_MSA.3	FMT_MSA.1	27
		FMT_SMR.1	32
29	FMT_MTD.1	FMT_SMF.1	31
		FMT_SMR.1	32

No.	Security functional requirements	Dependency	Reference No.
30	FMT_PWD.1	FMT_SMF.1	31
		FMT_SMR.1	32
31	FMT_SMF.1	-	-
32	FMT_SMR.1	FIA_UID.1	25
33	FPT_ITT.1	-	-
34	FPT_PST.1	-	-
35	FPT_PST.2		
36	FPT_TST.1	-	-
37	FTA_MCS.2	FIA_UID.1	25
38	FTA_SSL.5	FIA_UAU.1	22
39	FTA_TSE.1	-	-

Although FAU_GEN.1 has dependency on FPT_STM.1, TOE uses Reliable time stamp provided in TOE operating environment to accurately record security related events. Therefore, Dependency of FAU_GEN.1 is satisfied by OE. RELIABLE_TIME_STAMP in security objective for operating environment instead of FPT_STM.1.

FAU_STG.3 and FAU_STG.4 have dependencies on FAU_STG.1, but the TOE uses the trusted audit repository provided by the TOE operating environment to accurately store the audit data related to the operation of the TOE and to perform unauthorized deletion or change , The dependency of FAU_STG.3 and FAU_STG.4 is satisfied by the security objective OE. RELIABLE_STORAGE for the operating environment instead of FAU_STG.1.

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

6. TOE summary specification

This chapter briefly and explicitly specifies how the security functions of the TOE are implemented and how the functions meet the assurance requirements.

6.1. TOE security functions

This chapter describes the security functions provided by the TOE and how the security functions of Document SAFER Blue 3 satisfy all the security requirements specified in Chapter 5.

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access

6.1.1 Security audit

Security audit performs the following functions:

- Security alerts
- Audit data generation
- Potential violation analysis
- Audit review
- Selective audit review
- Response actions for predicting audit data loss
- Prevention of audit data loss

6.1.1.1 **Security alerts**

The TOE logs security violation incidents and sends warning emails to administrators when the following occur:

- Administrator/user authentication failure audit events
- Document encryption/decryption failures
- Self-test failures
- Integrity failures
- Validation-required cryptographic module self-test failures
- Audit record exceeded and saturated

6.1.1.2 Audit data generation

The audit data generation function generates and stores a log of events occurring in the TOE security function.

Audit data is categorized and stored as logs for administrator management functions, logs for administrator and document user logins, logs for document usage, and logs for system events.

Types of audit records	Description
Administrator log	Logs about changes of security policy , management user/group made by the administrator while executing security management functions.
Document usage log	Logs about users' document usage such as viewing, editing and printing secured documents on users' PC.
System log	Logs for server start and stop, self-verification, email sending, mutual authentication, and validity verification.
Login log	Logs for administrator and user identification and authentication, attempts to reuse authentication data, lockout upon reaching the log authentication failure limit, and denial and lockout for the same session.
Authorization management log	Logs for registration and approval of the Agent and Core.
Key management log	Logs for cryptographic key generation, distribution, exchange, and destruction.
Encryption/decryption log	Logs for encryption and decryption success and failure.

Related SFRs	
FAU,GEN.1	

6.1.1.3 Potential violation analysis

The TOE can apply rules when examining audited events.

6.1.1.4 Audit Review

The TOE provides authorized administrators with the ability to query stored audit data. This includes.

- Basic audit logs
- Login logs
- Administrator logs
- Server/service startup logs
- Email sending logs
- Server/client integrity verification logs
- Agent approval management logs
- Key generation logs
- Agent key logs
- Self-test logs
- Encryption/decryption operation success/failure logs

- Key destruction logs
- Document security audit logs

6.1.1.5 Selective Review

The TOE allows confirmation by searching based on combinations of user ID, username, department name, IP, filename, program, and operation, among others, sorted in descending order by time.

6.1.1.6 Response Actions for Predicting Audit Data Loss

If the TOE predicts that audit data will exceed 70% of the specified DB Table Space capacity, it sends a warning email to the administrator.

6.1.1.7 Prevention of Audit Data Loss

To protect audit data, the TOE overwrites the oldest audit records when the audit data storage is saturated and sends an email notification.

6.1.2 Cryptographic support

The TOE performs the following functions for cryptographic support.

- Cryptographic key generation
- Cryptographic key distribution
- Cryptographic operation and Cryptographic key destruction
- Random bit generation

6.1.2.1 ryptographic key generation

The TOE generates 256-bit and 128-bit symmetric keys and 3072-bit public key pairs by using the MarkAny Verification Cryptographic Module (MACRYPTO V3.00) for document encryption, TSF data protection, and inter-TOE communication data protection.

Category	Cryptographic key generation algorithm	cryptographic key size	List of standards
Document encryption/decryption DEK	**HASH_DRBG**	**256bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2**
KEK for document encryption/decryption DEK	**HASH_DRBG**	**128bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2**
TSF data encryption/decryption	**HASH_DRBG**	**128bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-**

DEK			**Part1-2**
DEK for encryption and decryption of transmitted data between TOEs	**HASH_DRBG**	**128bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2**
KEK for TSF data DEK	**PBKDF2**	**128bit**	**PKCS #5(RFC 8018)**
Key distribution DEK	**RSAES**	**3072bit**	**KS X ISO/IEC 18033-2**

Related SFRs
FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1

6.1.2.2 Cryptographic key distribution

The TOE server performs mutual authentication with the Agent and Core, and securely distributes the generated cryptographic key through the asymmetric cryptographic algorithm.

Category	**Cryptographic key generation algorithm**	**cryptographic key size**	**List of standards**
Key Distribution	**RSAES**	**3072bit**	**KS X ISO/IEC 18033-2**

Related SFRs
FCS_CKM.1(2), FCS_CKM.2, FIA_IMA.1

6.1.2.3 Cryptographic operation and Cryptographic key destruction

The TOE performs cryptographic operations, including document encryption, TSF data encryption, TOE-to-TOE data transmission, password encryption, and module self-test encryption, using the following cryptographic algorithms. After the operations are completed, the TOE initializes security parameters to '0' three times for secure disposal.

Category	**Cryptographic algorithm**	**Cryptographic key size**	**Cryptographic key and parameter destruction**
Document encryption and decryption	ARIA-CBC	256bit	overwrite security parameters to '0' three time
Document encryption and decryption DEK encryption and decryption	ARIA-CBC	128bit	overwrite security parameters to '0' three time
Encryption and decryption of transmitted data between	ARIA-CBC	128bit	overwrite security parameters to '0' three time

Category	Cryptographic algorithm	Cryptographic key size	Cryptographic key and parameter destruction
TOEs			
TSF data encryption and decryption	ARIA-CBC	128bit	overwrite security parameters to '0' three time
Encryption of password	SHA-512	-	-
Self-Test	SHA-512	-	-
KEK for TSF data DEK	ARIA-CBC	128bit	overwrite security parameters to '0' three time
Mutual authentication, Key exchange	RSAES-OAEP	3072bit	overwrite security parameters to '0' three time

Related SFRs
FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2)

6.1.2.4 Random bit generation

The TOE performs random bit generation using the following random number generator.

Random bit generation algorithm	cryptographic key size	List of standards
HASH_DRBG	**256bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2**
HASH_DRBG	**128bit**	**KS X ISO/IEC 18031 TTAK.KO-12.0331-Part1-2**

Related SFR
FCS_RBG.1

The validated cryptographic module used in cryptographic management is as follows.

Category	Sub category	Description
Validated cryptographic module	Name	MACRYPTO V3.00
	Validation number	CM-224-2027.12

Category	Sub category	Description
	Developer	MarkAny Inc.
	Date verified	2027-12-05

6.1.3 User data protection

User data protection performs the following functions.

- Document Encryption access control
- Document Usage access control

6.1.3.1 Document Encryption Access Control

Authorized administrators can set permissions (viewing, saving) and security policies for the encryption/decryption of secure documents. Access to document encryption is controlled based on the configured policies.

Related SFRs
FDP_ACC.1(1), FDP_ACF.1(1)

6.1.3.2 Security Attribute-Based Access Control

Authorized administrators control access to secure documents based on subject security attributes (user ID, user group ID) and object security attributes (document permissions). Additionally, access to all operations (document exchange, viewing, saving and editing, printing) for authorized users and protected documents is controlled.

Related SFRs
FDP_ACC.1(2), FDP_ACF.1(2)

6.1.4 Identification and Authentication

Identification and authentication perform the following functions.

- Administrator identification and authentication
- Handling of administrator identification and authentication failures, and protection of authentication feedback
- Prevention mechanism for administrator reuse
- Document user identification and authentication
- Handling of document user identification and authentication failures, and protection of authentication feedback

- Prevention mechanism for document user reuse
- Password validation
- TOE mutual authentication

6.1.4.1 Identification and Authentication of Administrators

Upon initial installation, the TOE creates an administrator, and during the initial login using the generated administrator ID and password, it is mandatory to change the password. This data is stored in an encrypted (SHA-512) state in the DBMS.

No actions related to administration can be performed until the identification and authentication of the administrator are completed.

In case of three failed authentication attempts by the administrator, an authentication delay of 5 minutes is imposed.

6.1.4.2 Handling of Administrator Identification and Authentication Failures and Authentication Feedback

All passwords entered during administrator identification and authentication are displayed as "*". In case of authentication failure, only the error message "Please retry after checking login information." is output, providing no information about the reason for the failure.

6.1.4.3 Mechanism for Preventing Administrator Reuse

In addition to administrator identification and authentication information, a CSRF token is used to prevent data reuse.

6.1.4.4 Identification and Authentication of Document Users

The ID and encrypted (SHA-512) password of the document user are transmitted to the server for the identification and authentication of the respective user.
In case of three failed authentication attempts by the user, an authentication delay of 5 minutes is imposed. The Agent module's integrity status is checked for user identification.

6.1.4.5 Handling of Document User Identification and Authentication Failures and Authentication Feedback

All passwords entered during document user identification and authentication are displayed as "*". In case of authentication failure, only the error message "Please retry after checking login information." is output, providing no information about the reason for the failure.

6.1.4.6 Mechanism for Preventing Document User Reuse

In addition to document user identification and authentication information, a timestamp is included to prevent data reuse.

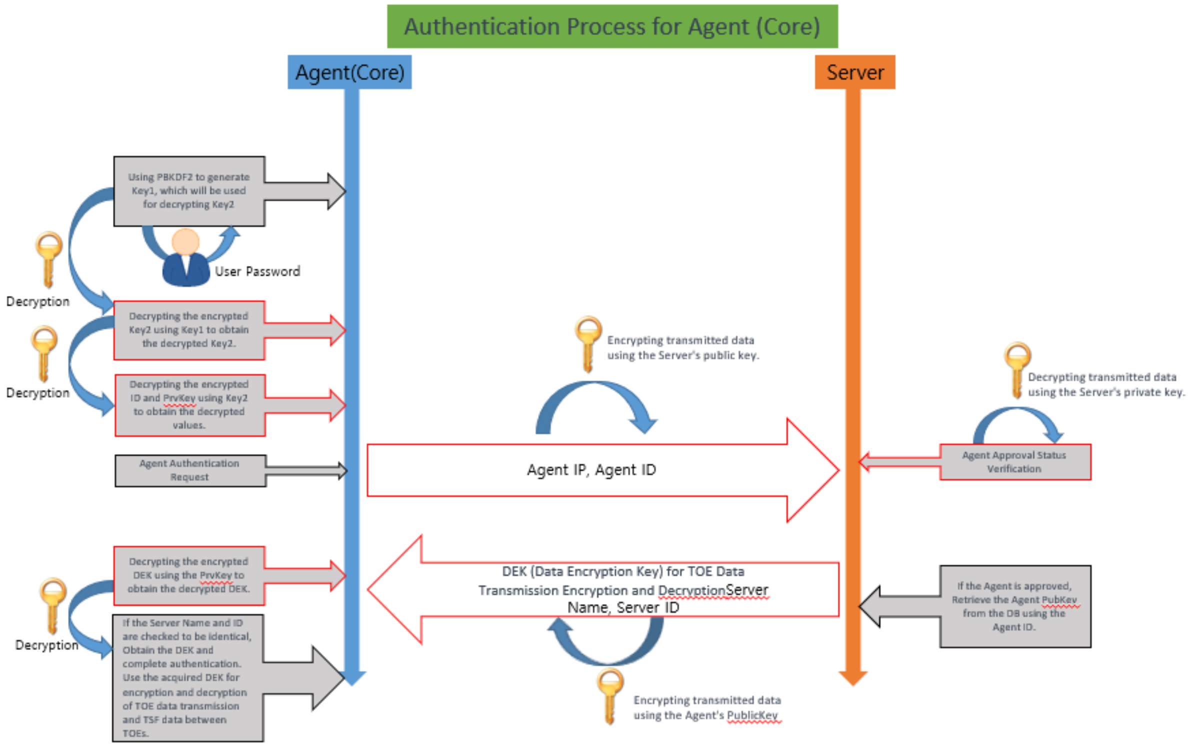
6.1.4.7 Password Validation

When registering administrators and users on the administrator page, passwords must be provided and must satisfy the following criteria:

- Alphabetic characters (case-sensitive): a - z, A - Z
- Numbers: 0 - 9
- Special characters: !, @, #, $, %, ^, *, +, =, -
- Password must consist of a combination of at least three of the following: alphabetic characters, numbers, and special characters.
- Passwords must have a minimum length of 9 characters and a maximum length of 15 characters.

6.1.4.8 Mutual Authentication

The Agent and Core perform mutual authentication with the Server upon initial execution.


Authentication Process for Agent (Core)
Agent(Core)
Server
Using PBKDF2 to generate Key1, which will be used for decrypting Key2
User Password
Decryption
Decrypting the encrypted Key2 using Key1 to obtain the decrypted Key2.
Decryption
Decrypting the encrypted ID and PrvKey using Key2 to obtain the decrypted values.
Agent Authentication Request
Encrypting transmitted data using the Server's public key.
Agent IP, Agent ID
Decrypting transmitted data using the Server's private key.
Agent Approval Status Verification
Decrypting the encrypted DEK using the PrvKey to obtain the decrypted DEK.
Decryption
If the Server Name and ID are checked to be identical, Obtain the DEK and complete authentication. Use the acquired DEK for encryption and decryption of TOE data transmission and TSF data between TOEs.
DEK (Data Encryption Key) for TOE Data Transmission Encryption and DecryptionServer Name, Server ID
If the Agent is approved, Retrieve the Agent PubKey from the DB using the Agent ID.
Encrypting transmitted data using the Agent's PublicKey

1. At runtime, the user inputs a password, and KEK (KEY1) is generated using PBKDF2.
2. Using this KEK, decrypt KEK (KEY2) used to encrypt the Agentkey.
3. Decrypt AgentID and Agent public key using KEY2, then encrypt them using the Server's public key

before transmitting to the SERVER.
4. On the Server side, decrypt the incoming data using the Server's private key and verify the approval status of the Agent.
5. If the AgentID is approved, encrypt the DEK used for TOE data transmission with the public key of that AgentID and transmit it to the Agent.
6. Decrypt the received data using the Agent's private key, compare the values with ServerName and ServerID, and if confirmed, obtain the DEK to complete the authentication.

6.1.5 Security management

Security management performs the following functions.

- Common management
- Document security policy management
- Log management

6.1.5.1 Common management

The TOE provides an IP configuration function for securing the Server. Additionally, it allows the creation of users with administrator and document user permissions, and offers functionality to create, modify, and delete groups.

Administrators can change the passwords of users from the administrator page, while users can change their passwords from the agent. There is only one role for administrators, which is the top-level administrator.

6.1.5.2 Document Security Policy Management

The TOE provides a function to set document security access control policies, such as policies for document exchange, printability, and permissions for storage and editing.

6.1.5.5 Log Management

The TOE offers the capability to view, query, and inspect logs generated as audit data for basic management activities. These logs include server/service startup, login, administrator management actions, mail generation logs, installation history of document security, usage history, policy change logs, and other policy-related changes.

Related SFRs
FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.1.5.6 Administrator Security Attribute List (Initial Values)

- Server Access Allowed IP (192.168.0.1)

- Document Security Policy
- Exchange Policy (Internal Only)
- Storage and Editing Permissions (Based on Encryption Header Attribute)
- Printability (Based on Encryption Header Attribute)
- Agent Deletion Permission (Allowed)

6.1.6 TSF Protection

TSF protection performs the following functions.

- Internal Transfer TSF Data Protection
- Stored TSF Data Protection
- Availability Protection of TSF Data
- TSF Self-Test

6.1.6.1 Internal Transfer TSF Data Protection

TSF data transmitted between TOEs is protected using the encryption algorithm (ARIA-CBC, 128-bit) and integrity check (SHA-512, 512-bit) of the validated cryptographic module (MACRYPTO V3.00).

6.1.6.2 Stored TSF Data Protection

When storing TSF data, TOE encrypts the data for protection using the following methods.

TOE component	TSF data	Protection algorithm
Server	**Password**	**SHA-512, 512bit**
Agent	**Cryptographic key**	**ARIA-CBC, 128bit**
	Policy	**ARIA-CBC, 128bit**
	Group/User information	**ARIA-CBC, 128bit**
	Password	**SHA-512, 512bit**
Core	**Cryptographic key**	**ARIA-CBC, 128bit**
	Password	**ARIA-CBC, 128bit**

The list of TSF data is as follows, and management is restricted to authorized administrators.

Category		Capability
Audit Data	Administrator Login Log	Query
	Administrator Management Action Log	
	User Login Log	
	Server/Service Startup Log	
	Mail Sending Log	

Category		Capability
Critical Data Constituting TOE	Document Security Log	Query, Modification
	Encryption Keys	
	Self-Test	
	Success or Failure of Encryption/Decryption Operations	
	Key Disposal	
	Company ID	
Identification and Authentication Data	ID and Password Hashes	Query, Addition, Modification, Deletion
Group and User Data	User ID	Query, Addition, Modification, Deletion
	Group Information	
Document Encryption Authorization and Policy Data	-	Query, Modification

6.1.6.2 Protection of TSF Data Availability

If there is an attempt to arbitrarily terminate the Agent's executable file, an authorization error is generated to prevent the termination.
During Agent deletion, a permission check is performed to encourage deletion, and in the case of forced deletion of installed modules, an authorization error is generated to prevent the deletion from succeeding.

6.1.6.3 TSF Self-Test

The TOE provides a self-test function during startup and periodically uses the SHA-512 algorithm to verify the integrity and integrity of the core module. If tampering or integrity issues are detected or if the self-test fails, a warning email is sent to the authorized administrator.

- List of integrity-target files

TOE Components	List of integrity-target files
Agent	**MADRMAgent.exe**
	PolicyServerService.exe
	Macrypto32.dll/Macrypto.dll
	macrypto32.dll.sign/macrypto.dll.sign
	Manager.DLL/Manager64.dll
	integrateLayer.dll
	DS_CipherLayer.dll/DS_CipherLayer64.dll

	AcapIconMgr.dll/ AcapIconMgr64.dll
	DSH_PickUp.dll/ DSH_PickUp64.dll
	DSH_PMI.dll/ DSH_PMI64.dll
	DSP_01_2016.dll/ DSP_01_201664.dll
	DSP_02_2016.dll/ DSP_02_201664.dll
	DSP_03_2016.dll/ DSP_03_201664.dll
	AcapProp.exe
	DSP_HOFFICE.dll
	DSP_LOCALPOLICY.dll/ DSP_LOCALPOLICY64.dll
	DSP_MSPaint.dll/ DSP_MSPaint64.dll
	DSP_Notepad.dll/DSP_Notepad64.dll
	DSP_Notepad_1164.dll
	DSP_PDF_ControlMgr.dll/ DSP_PDF_ControlMgr64.dll
	DSP_WordPad.dll/DSP_WordPad64.dll
	MAShlMgr.dll/ MAShlMgr64.dll
	NtProcMonitor64.sys
	uninst.exe
	PrctPcss64.sys
	PpConfig.mpc
	PrctPcssCtl32.dll/ PrctPcssCtl64.dll
	masysid.dll/ masysid_x64.dll
	MALogSender.exe
	MaHWP.exe
	ServerPub.kff
	AgentSalt.kff
	AgentPub.kff
	AgentPrv.kff
	AgentId.kff
	AgentDek.kff
	Cfa.ccf
	Cfc.ccf

	Cfs.ccf
	UserInfo.mds
	Vifkbx.kbx
	Server_info.ini
	Init.ini
Core	libMaACD.1.07.so
	libMaAdmin.1.02.so
	libMaCrypt.1.00.so
	libv6.0.1.13.so
	libMaFile.1.02.so
	libMaIpc.1.00.so
	libMaJSCom.1.06.so
	libMaKcmvp3Wrapper.1.00.so
	libMaLicense.1.03.so
	libMaNet.1.01.so
	libMaNetStream.1.01.so
	libMaOSSLHandler.1.00.so
	libMaSSL.1.00.so
	libMaString.1.09.so
	libMaXmlWrapper.1.08.so
	libv51014.1.02.so
	libcrypto.so.1.0.0
	libssl.so.1.0.0
	libxml2.so.2.9.1
	libmacrypto.so
	.MaDocSaferrc
	.Setting.cfg
	.ma_js.crt
	.ma_svr.aid
	.ma_svr.crt
	.ma_svr.pri

	.ma_svr.rk
	.rk.info
	Proc.cfg
	MA6_PUSH
	MA6_DDS
	MA6_PMS
	MA6_DEC
	MA6_FILECHK

- List of Self-Test Targets

TOE Components	Process List
Server	WEB_SERVER
	WEB_SERVER encryption module
	SERVICE_INTEGRATION
	SERVICE_INTEGRATION encryption module
	SERVICE_LOG
	SERVICE_LOG encryption module
	SERVICE ReturnKey
	SERVICE ReturnKey encryption module
Agent	MADRMAgent.exe
	PolicyServerService.exe
	DSH_Service64.exe
	DSH_Loader.exe/DSH_Loader64.exe
	AcapProp.exe
	MALogSender.exe
Core	MA6_DDS
	MA6_DEC
	MA6_PUSH
	MA6_FILECHK
	MA6_PMS

Related SFRs
FPT_ITT.1, FPT_PST.1, FPT_PST.2, FPT_TST.1

6.1.7 TOE Access

TOE access performs the following functions.

- Session Management

6.1.7.1 Session Management

TOE provides an accessible IP registration function and allows server access only for the permitted IPs when an administrator logs in. In addition, the maximum number of concurrent sessions for administrative connections is limited to 1. The administrator's session is terminated after a period of inactivity (5 minutes).

Related SFRs
FTA_MCS.2, FTA_SSL.5, FTA_TSE.1

7. References

- **Information security system evaluation and certification guidelines [MSID 2017-7, 2017.8.24]**
- **Common Criteria for Information Technology Security Evaluation [CC/CEM V3.1 R5]**
- **Document Encryption Protection Profile v1.1 for the country, IT Security Certification Center, 2019.12.11**