MarkAny

Document SAFER Blue 2

Security Target

V 1.10

MarkAny

* 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	2017-11-01	Initial version	DRM Division Development Team	DRM Division Business Manager
1.01	2017-12-20	Updated	DRM Division Development Team	DRM Division Business Manager
1.02	2018-01-05	Updated	DRM Division Development Team	DRM Division Business Manager
1.03	2018-01-19	Updated	DRM Division Development Team	DRM Division Business Manager
1.04	2018-05-25	Updated	DRM Division Development Team	DRM Division Business Manager
1.05	2018-05-30	Updated	DRM Division Development Team	DRM Division Business Manager
1.06	2018-07-16	Updated	DRM Division Development Team	DRM Division Business Manager
1.07	2018-10-29	Updated	DRM Division Development Team	DRM Division Business Manager
1.08	2019-03-13	Updated	DRM Division Development Team	DRM Division Business Manager
109	2019-05-28	Updated	DRM Division Development Team	DRM Division Business Manager
1.10	2019-07-09	Updated	DRM Division Development Team	DRM Division Business Manager

Table of Contents

1. ST Introduction

This document is a MarkAny Document SAFER Blue 2 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 2 Security Target
Version	V1.10
Created by	DRM Division Development Team, MarkAny Inc.
Data Created	2019-07-09
TOE	Document SAFER Blue 2
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 2	
Version	2.1.09	
Components	Document SAFER Blue 2 Server 2.1.03 Document SAFER Blue 2 Agent 2.1.03 Document SAFER Blue 2 Core 2.1.03	Software(CD)
Guidance Documents	Document SAFER Blue 2 Operation Guide V1.03 Document SAFER Blue 2 Preparative Procedure V1.05	PDF(CD)
Developer	MarkAny Inc.	

1.3. TOE overview

'Document SAFER Blue 2' (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 V2.00. The security and implementation conformance of MarkAny MACRYPTO V2.00 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.

The Document SAFER Blue 2 Server, Agent, Core are the indispensable TOE components that perform the security features of the TOE.

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 (DEK)' and 'Key encryption key (KEK') 'are used for the document encryption / decryption function. TOE generates DEK and KEK and Server distributes DEK as Agent and Core module,

in which the encryption key is distributed in a secure way. The Agent or Core module encrypts the body of the protected document with the corresponding encryption key or decrypts the encrypted body. DEK, KEK cryptographic key is generated by symmetric key method, and asymmetric key is used for DEK distribution.

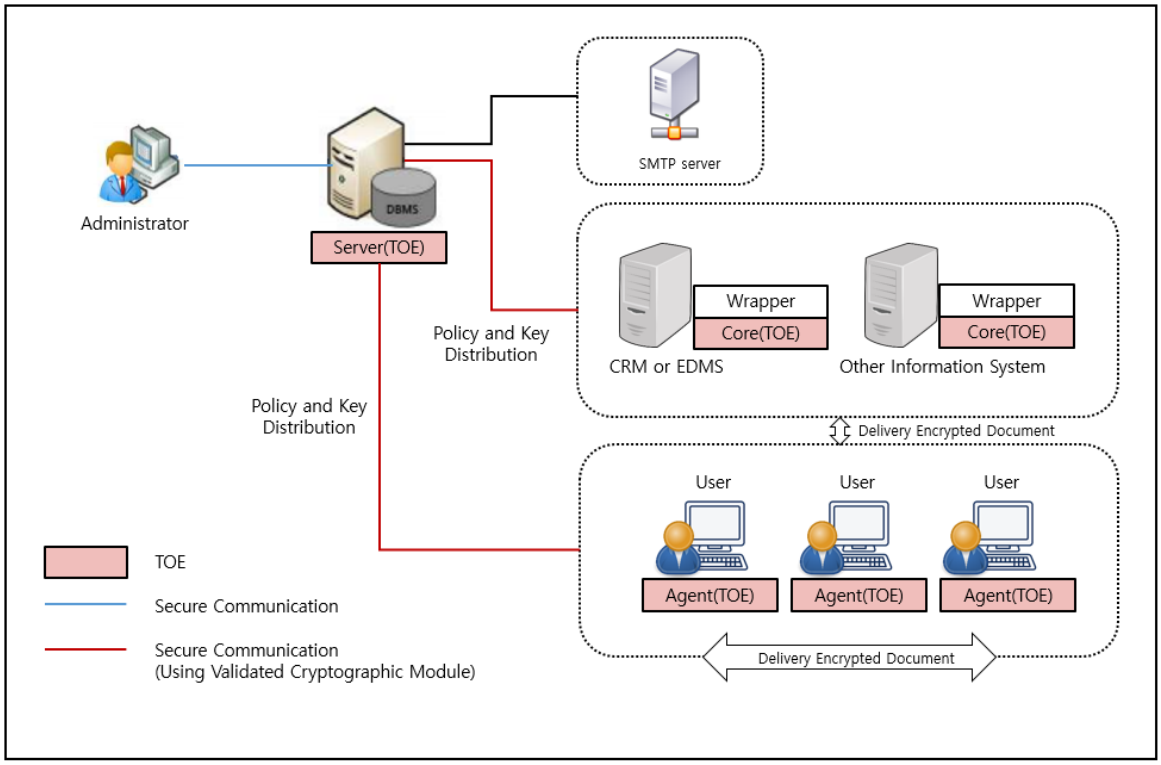
Agent and Core modules destroy the encryption key in the memory by overwriting '0' when the encryption key is no longer used.

The administrator can specify documents that shall be encrypted/decrypted through the Server, and assign the document access right to the document user. Only the authorized document user can encrypt/decrypt the document, as the Server distributes a cryptographic key to the document user according to policy configured.

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 sets the policy for each document user or information system through the Server, which distributes the policy and cryptographic key configured by the administrator to the Agent and Core. 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 V2.00, 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) Xeon(R) 2.45GHz or higher
		RAM	8GB or higher
		HDD	1TB or higher
		NIC	10/100/1000 Ethernet Card 1Port or higher
	OS	Windows Server 2016 Standard (64 bit) CentOS 6.10 (2.6.32-754.el6.x86_64 (64 bit))	
	SW	JDK 1.8.0_77 Tomcat 8.5.24 Oracle 12c(12.2.0.1.0) OpenSSL 1.0.2q	
Agent	HW	CPU	Intel Core 2.50 GHz or higher
		RAM	2GB or higher
		HDD	500GB or higher
		NIC	10/100/1000 Ethernet Card 1Port or higher

Component			Requirement
	OS	Windows 7 Professional (32/64bit) Windows 8.1 Pro (32/64bit) Windows 10 Pro (32/64bit) Windows 10 Enterprise (32/64bit)	
	SW	MS Visual C++ 2008 redistributable 9.0.30729.1 MS Notepad, MS Wordpad, MS Paint Microsoft Office 2013, 2016 Hancom Office 2010 SE, 2014, 2018 Acrobat Reader 11, DC	
Core	HW	CPU	Intel(R) Xeon(R) 2GHz or higher
		RAM	4GB or higher
		HDD	500GB or higher
		NIC	10/100/1000 Ethernet Card 1Port or higher
	OS	CentOS 6.10 (2.6.32-754.el6.x86_64 (64 bit))	
	SW	JDK 1.8.0_77 OpenSSL 1.0.2q	

The external IT entities and software necessary for the operation of the TOE are as in the following, and the following are excluded from the scope of the assessment.

- SMTP server used to send security alerts by email to the administrator
- Environment to operate the Server and Core

  - JDK 1.8.0_77
- Web browsers that support SSL communication

  - Internet Explorer 11
- Web application server used by the Server

  - Tomcat 8.5.24
- DBMS to store audit data of the Server

  - Oracle 12c (12.2.0.1.0)
- Library for TLS communication

  - OpenSSL 1.0.2q

- For installation of the Client, required library must be installed for compatibility.

  - Visual C++ 2008 redistributable 9.0.30729.1

- Application for document user

  - MS Notepad, MS Wordpad, MS Paint

  - MS Office 2013, 2016

  - Hancom Office 2010 SE, 2014, 2018

  - Acrobat Reader 11, DC

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

Component		Requirement
HW	CPU	Intel Core 2.50 GHz or higher
	RAM	2GB or higher
	HDD	500GB or higher
	NIC	10/100/1000 Ethernet Card 1Port or higher
OS	Windows 10 (64bit)	
SW	Internet Explorer 11	

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.

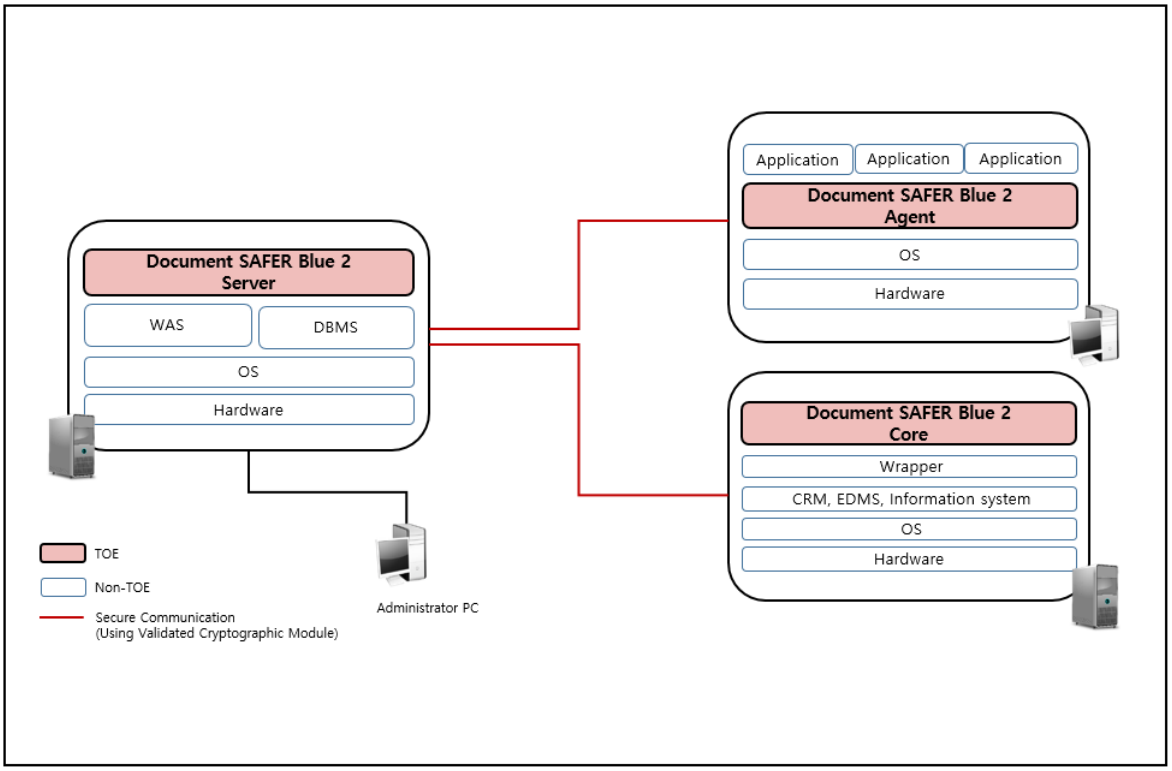
TOE component	Document SAFER Blue 2 Server 2.1.03	Software(CD)

	(Document_SAFER_Blue_2_Server_2.1.03.sh) (Document_SAFER_Blue_2_Server_2.1.03.exe)	
	Document SAFER Blue 2 Agent 2.1.03 (Document_SAFER_Blue_2_Agent_2.1.03.exe)	
	Document SAFER Blue 2 Core 2.1.03 (Document_SAFER_Blue_2_Core_2.1.03.sh)	
TOE Guidance documents	Document SAFER Blue 2 Operation Guide V1.03 (Document SAFER Blue 2 Operation Guide V1.03.pdf) Document SAFER Blue 2 Preparative Procedure V1.05 (Document SAFER Blue 2 Preparative Procedure V1.05.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

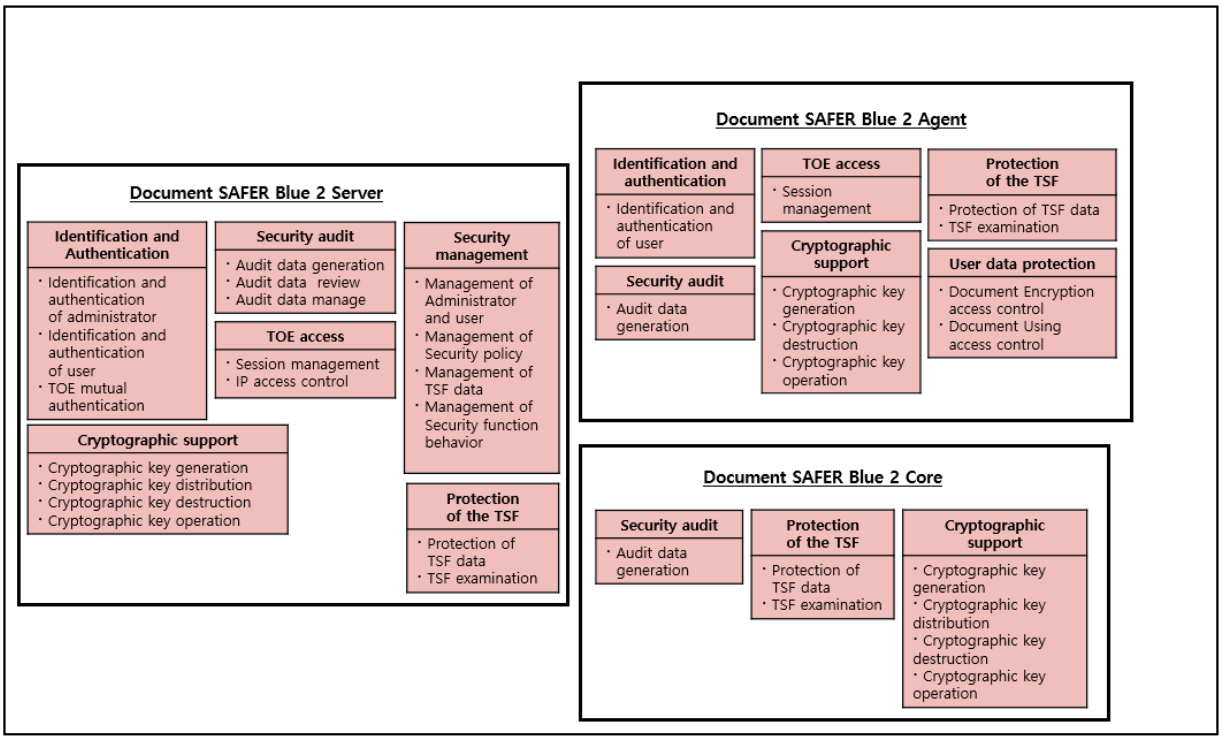
[Figure 2] TOE's physical scope



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



1.4.2.1 Identification and authentication

The TOE provides identification and authentication process based on ID/PW for the administrators and document users.

The Server and Agent, Server and Core go through a mutual authentication process.

Administrators and users must change their passwords during the initial connection.

When an administrator or user enters password to log in, it is masked to prevent disclosure and in case of authentication failure, the reason is not provided

The password must be at least 9 characters (max 15) in length, with at least one alphabetic character, numeric character, and special character.

If the authentication failure exceeds the limit set by the administrator, the login function is disabled for 5 minutes.

Only the authorized administrators can manage the security functions through the web browser.

When the agent is activated for document user identification and authentication, the user is authenticated through the login function. Only when the authentication is successful, the document can be viewed and stored according to the access right.

1.4.2.2 Security management

Server provides functions such as TOE security function management, security attribute management and TSF data management to the authorized administrator.

1.4.2.3 Security audit

The server generates and stores audit data in the DBMS (Oracle), including the data, time, type, and the result of the event when the event occurs.

Provides the ability to query and selectively review audit data to the authorized administrator.

If any potential security violation such as integrity violation, and audit data exceeds the defined threshold of Table-Space capacity is detected, the TOE sends an alert E-mail to the authorized administrator and overwrite old data

The Agent generates all audit data of the user's document usage and sends the operation, user information, and results to the Server

1.4.2.4 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.

1.4.2.5 Protection of the TSF

The TOE communicates securely to protect transmission data between components and secures confidentiality and integrity. The TOE also protects the TSF data from unauthorized exposure and modification by using encrypted and independent protocols using a validated cryptographic module.

1.4.2.6 Cryptographic support

The TOE performs cryptographic operation and cryptographic key management such as generation, distribution and destruction through MarkAny MACRYPTO V2.00.
HASH_DRBG is used to generate document encryption key.
The TOE performs operation in the ARIA-CTR mode for encryption/decryption of document and TSF data.

1.4.2.7 User data protection

The TOE protects user data.
The TOE creates a secured document by encrypting a plain document and protects the secured document by controlling access to the secured document according to the policy set by the administrator.

The policy is set differently depending on the user ID, group, job title, group head, document owner. Permissions to access the secured documents are view, edit, print, screen capture, change permission, decrypt, time period to view, revoke, etc. and depending on the permissions granted, access to the secured document is controlled.

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 *underlined and italicized.*

Refinement

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

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(August 18, 2017)
	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 V1.0'.

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	For communication between the web browser of the administrator PC and the web server which is the operation environment of the management server, TLS 1.2 shall be used to guarantee the confidentiality and integrity of the transmitted data.

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 TOE Internal mutual authentication	1

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].

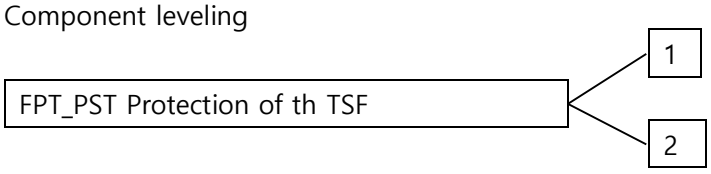
4.4. FPT, Protection of the TSF

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

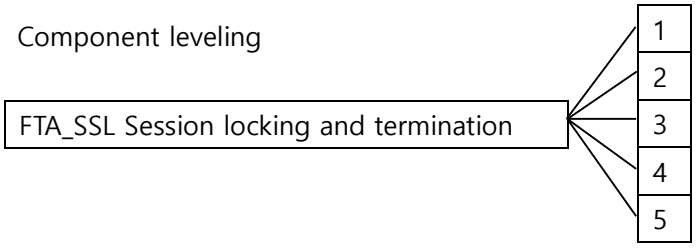
Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_PST.2.1	The TSF shall [selection: detect, prevent] the unauthorized deletion for [assignment: TSF data].
FPT_PST.2.2	The TSF shall [selection: detect, prevent] the unauthorized termination for [assignment: TSF data].

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.



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

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE. The following table defines all the subjects, objects, operations, security attributes used in the security functional requirements.

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, Period, Exchange, Owner	View Edit Print Encrypt Decrypt Screen capture Copy & Paste Insert & Extract

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
FDP_ACF.1(2)	Successful request of operation execution regarding the Object identification object handled by SFP	Object identification
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.

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 [[integrity failure of server/agent/core, audit store threshold Exceeded] 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 [searching] 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 provide the ability to apply [Send E-mail to 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 size [Cryptographic key size in [Table 5-2]] that meet the following [List of standards in [Table 5-2]].

[Table 5-2] Cryptographic key generation algorithm

Category	Cryptographic key generation algorithm	cryptographic key size	List of standards
Document Encryption	**HASH_DRBG**	**256bit**	**TTAK.KO-12.0190**

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 a specified cryptographic key size [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	**HASH_DRBG**	**128bit**	**TTAK.KO-12.0190**
Transfer data Encryption	**HASH_DRBG**	**128bit**	**TTAK.KO-12.0190**

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 distribute cryptographic keys in accordance with the specified cryptographic distribution method [Cryptographic key distribution method of [Table 5-4] Cryptographic key distribution] that meets the following [List of standards of [Table 5-4] Cryptographic key distribution].

[Table 5-4] Cryptographic key distribution algorithm

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

5.1.2.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components.

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data 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 [overwrite security parameters to '0'] that meets the following: [No other components].

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 the cryptographic operation list [Cryptographic operation list in [Table 5-5]] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in Table 5-5] and a specified cryptographic key size [Cryptographic key size in [Table 5-5]] that meet the following [List of standards in [Table 5-5]].

[표 5-5] Cryptographic operation Algorithm

Cryptographic operation Algorithm	cryptographic key size	List of standards	Cryptographic operation list
ARIA-CBC	**256bit**	**KS X 1213-2**	**Encryption/decryption of documents**

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 the cryptographic operation list [Cryptographic operation list in [Table 5-6]] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in [Table 5-6]] and a specified cryptographic key size [Cryptographic key size in [Table 5-6]] that meet the following [List of standards in [Table 5-6]].

[Table 5-6] Cryptographic operation Algorithm

Cryptographic operation Algorithm	cryptographic key size	List of standards	Cryptographic operation list

ARIA-CBC	**128bit**	**KS X 1213-2**	**Encryption/decryption of TSF data**
ARIA-CBC	**128bit**	**KS X 1213-2**	**Encryption/decryption for communication**
SHA-512	**512bit**	**ISO/IEC 10118-2**	**Self-Test**
SHA-512	**512bit**	**ISO/IEC 10118-2**	**Encryption of password**
RSAES-OAEP	**3072bit**	**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**	**TTAK.KO-12.0190**
HASH_DRBG	**128bit**	**TTAK.KO-12.0190**

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 [list of subjects, objects, and operations among subjects and objects covered by SFP].

[

- Subject list

  Authorized user

- Object list

  Secured document

- Operation list

  I. View

  II. Edit

  III. Save

  IV. Copy & Paste

  V. Encrypt

  VI. Decrypt

]

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 [list of subjects, objects, and operations among subjects and objects covered by SFP].

[

- Subject list

  Authorized user

- Object list

  Secured document

- Operation list

  I. Print, Print count

  II. Screen capture

  III. Takeout

  IV. Period

V. View count

VI. Exchange

]

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, Group ID, Grade ID ● Security attribute of Object System information, Document ID, Document type, Period, View Count]
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

I. Print, Print count

II. Screen Capture

III. Takeout

IV. Period

V. View count

VI. Exchange

]

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 unsuccessful authentication attempts of [3] 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 Internal mutual authentication

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication between [Server-Client 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. [Action list I. Mutual authentication and key exchange for data encryption / decryption between TOEs II. Self-Test]
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 Identification

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.

[

T Action list

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

II. Self-Test

]

5.1.5. Security management (FMT)

5.1.5.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MOF.1.1	The TSF shall restrict the ability to *conduct administrative actions of* [the following] List of functions in [Table 5-8]] to [the authorized administrator].

[Table 5-8] List of management functions

Menu	Category	Management behavior
General management	System	Add, Modify, Delete
	Administrator/User/Group	Add, Modify
	Audit Data(Default, Login, Admin behavior, Start, Send E-mail, Cryptographic key generation, Approval)	Search
	Self-Test	Perform
	Approve Management	Approve
	Cryptographic key generation	Perform
Document Security management	Company policy, ACL policy	Add, Modify, Delete
	Review audit data	Search
	Statistics of audit data	Search
Print Security management	Company policy	Modify
	Review audit data	Search
	Statistics of audit data	Search
Personal Information Security management	Company policy	Modify
	Review audit data	Search
	Statistics of audit data	Search

5.1.5.2 FMT_MSA.1 Management of security attributes

Hierarchical to No other components.

Dependencies [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

MT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [access control SFP] to restrict the ability to [*change default, query, modify, delete, [none]*] the security attributes of [the following Security attribute list] to [the authorized administrator].

[

Security attribute list

I. Allowed IP

II. Document security policy: target application, automatic encryption, count control, virtual printer, exchange policy, whether to save and edit, block copy, screen capture prevention, takeout control, uninstall agent

III. Print security policy: print control, watermark, file print, mask personal information, allowed printer

IV. Personal information security policy: real-time inspection, compressed file inspection, detection processing method, inspection pattern

]

5.1.5.3 FMT_MSA.3 Static attribute initialization

Hierarchical to	No other components.
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce 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 administrator] 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 Data management

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MTD.1.1	The TSF shall restrict the ability to *manage* the [the following TSF data list in [Table 5-9]] to [the authorized administrator].

[표 5-8] TSF data list

Category		Management behavior
Audit data	Administrator login log	Query
	Management log	
	User login log	
	Service start log	
	Send E-mail log	
	Security Document log	
	출력물보안 로그	
	개인정보보안 로그	
Cryptographic key data Authentication data	Cryptographic key	Query, Modify
	Company ID	
	ID and password hash	Query Add, Modify, Delete
	Self-Test	
Group and User	User	Query Add, Modify
	Group	
Document security policy	-	Query, Modify
Print security policy	-	Query, Modify
Personal information security policy	-	Query, Modify

5.1.5.5 FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

1. [none]

2. [none]

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

1. [none]

2. [none]

FMT_PWD.1.3 The TSF shall provide the capability to *change the password when an authorized*

administrator first accesses it.

5.1.5.6 FMT_SMF.1 Specification of management functions

Hierarchical to No other components.

Dependencies No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions.

[

- TSF function management: items specified in FMT_MOF.1
- TSF security attributes management: items specified in FMT_MSA.1
- TSF data management: items specified in FMT_MTD.1.1

]

5.1.5.7 FMT_SMR.1 Security roles

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification

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

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

5.1.6. Protection of the TSF (FPT)

5.1.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to No other components.

Dependencies No dependencies.

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

5.1.6.2 FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PST.1.1 The TSF shall protect [cryptographic data, password of administrator and

document user, password for device cryptographic key file and TOE setting value] stored in containers controlled by the TSF from unauthorized *disclosure, modification.*

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

Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_PST.2.1	TSF shall *prevent* the unauthorized deletion for [execution file of Agent, registry value].
FPT_PST.2.2	TSF shall *prevent* the unauthorized termination for [process of Agent].

5.1.6.4 FPT_TST.1 TSF self-testing

Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self-tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of [TSF].
FPT_TST.1.2	The TSF shall provide a function that verifies integrity of [TSF data] to the *authorized administrator.*
FPT_TST.1.3	The TSF shall provide a function that verifies integrity of [TSF] to the *authorized administrator.*

5.1.7. TOE access (FTA)

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

Hierarchical to	FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies	FIA_UID.1 Timing of identification
FTA_MCS.2.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [The maximum number of concurrent sessions for administrator management access session restricted to one,

prohibition of same user both concurrent connections of management access session and local access session].

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

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

Hierarchical to No other components.

Dependencies No dependencies.

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

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	AGD_OPE.1	Operational user guidance

documents	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]

No.	Security functional requirements	Dependency	Reference No.
		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 FCS_CKM.1]	[- or - or 9]
		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

No.	Security functional requirements	Dependency	Reference No.
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
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 2 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:

- Audit data generation
- Audit data lookup/search
- Audit data protection

6.1.1.1 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 into logs for administrator management functions, logs for administrator and document user logins, logs for document usage, logs for output, logs for personal information checks, and logs for systems.

The TOE records the log when a security violation occurs and sends a warning e-mail to the administrator.

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.
Print log	Logs for printing on encrypted documents
Personal information inspection log	Logs for personal information inspection of documents

Types of audit records	Description
System log	Logs for starting and stopping the server, self-validating, sending e-mail, etc.
Login Log	Logs for identification and authentication of administrators and users
Approval management log	Logs for registration and authorization of Agent and Core
Key generation	Log for encryption key generation

Related SFRs
FAU,GEN.1

6.1.1.2 Look up/search audit data

The TOE provides a function to inquire the stored audit data to the authorized administrator.
User ID, user name, department name, IP, file name, program, operation and event type, etc. by the AND operator.

Related SFRs
FAU_SAR.1, FAU_SAR.3

6.1.1.3 Protect audit data

The TOE protects the audit data by sending a warning e-mail to the administrator when the audit data exceeds 70% of the designated DB Table Space capacity and overwriting the oldest audit record when the threshold value is exceeded.

Related SFRs
FAU_ARP.1, FAU_SAA.1, FAU_STG.3, FAU_STG.4

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 Cryptographic key generation

The TOE generates 256-bit and 128-bit symmetric keys by using the MarkAny Verification Cryptographic Module (MACRYPTO V2.00) 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	**HASH_DRBG**	**256bit**	**TTAK.KO-12.0190**
TSF data Encryption	**HASH_DRBG**	**128bit**	**TTAK.KO-12.0190**
Transfer data Encryption	**HASH_DRBG**	**128bit**	**TTAK.KO-12.0190**

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-OAEP**	**3072bit**	**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 operation of document encryption, TSF data, transfer data, password encryption, and module self-test using the following cryptographic algorithms, and after the operation is completed, the security parameters are overwritten to '0' to destroyed.

Category	Cryptographic key	Cryptographic operation	Cryptographic key and parameter destruction
Document Encryption	ARIA-CBC	256bit	overwrite security parameters to '0'
Encryption of transmitted data	ARIA-CBC	128bit	overwrite security parameters to '0'

Category	Cryptographic key	Cryptographic operation	Cryptographic key and parameter destruction
Encryption of TSF data	ARIA-CBC	128bit	overwrite security parameters to '0'
Encryption of password	SHA-512	512bit	-
Self-Test	SHA-512	512bit	-
Mutual authentication, Key exchange	RSAES-OAEP	3072bit	overwrite security parameters to '0'

관련 SFR
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**	**TTAK.KO-12.0190**
HASH_DRBG	**128bit**	**TTAK.KO-12.0190**

관련 SFR
FCS_RBG.1

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

Category	Sub category	Description
Validated cryptographic module	Name	MACRYPTO V2.00
	Validation number	CM-147-2023.12
	Developer	MarkAny Inc.
	Date verified	2023-12-05

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

The authorized administrator can set permissions (view, edit, save, block copy, encryption / decryption) and related policies, and according to the set security policies, document encryption or decryption activities by document users are controlled. Controls access to all operations of the authorized user and the protected document (printing, print count, screen capture, document export, period of use, number of browsing, document exchange)

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

6.1.3.2 Document Usage access control

The authorized administrator controls the access of the security document through the subject security attributes (user ID, user group ID, grade ID) and security attributes of the object (system information, document ID, document type, period of use, number of view).

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

6.1.4 Identification and authentication

Identification and authentication performs the following functions.

- Identification and authentication of administrator
- Identification and authentication of user

6.1.4.1 Administrator identification and authentication

It is mandatory to create a new administrator upon the installation of the TOE, and using the ID and password inputted, administrator authentication data is generated. The generated data is encrypted (SHA-256) and stored in the DBMS.

There is no executable action until the identification and authentication of the administrator are complete.

The password inputted during the access attempt is masked with "●" to prevent disclosure on the screen. In the case of authentication failure, only the error message "Please check your login information and try again" will be displayed.

If the administrator's authentication attempt fails 3 times, the authentication is disabled for 5 minutes.

Related SFRs
FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FMT_PWD.1

6.1.4.2 User identification and authentication

The ID of the document user and the password (SHA-512) encrypted are transmitted to the server, and the user is identified and authenticated.
The identification and information of the document user further includes a timestamp to prevent reuse of data.
The password inputted during the access attempt is masked with "●" to prevent disclosure on the screen. In the case of authentication failure, only the error message "Please check your login information and try again" will be displayed.
If the user's authentication attempt fails 3 times, the authentication is disabled for 5 minutes.

Related SFRs
FIA_AFL.1, FIA_IMA.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1

6.1.5 Security management

Security management performs the following functions.

- Common management
- Document security policy management
- Print security policy management
- Personal information security policy management
- Log management

6.1.5.1 Common management

The TOE provides an IP setting function accessible for server security and self-test function.
In addition, users can be created with administrator and document user rights, and functions of creating, modifying, and deleting groups are provided.

6.1.5.2 Management of permission settings of secured documents

The TOE provides the function to set policies such as document exchange, print, save and edit, block copying, etc. based on the document security access control policy

6.1.5.3 Print security policy management

TOE provides print security policy management function, such as whether to allow printing of security documents, and whether to print watermarks when printing.

6.1.5.4 Personal information security policy management

TOE provides personal information security policy management functions such as application of real-time personal information inspection to document and specification of document to be inspected, folder designation.

6.1.5.5 Log management

The TOE consists of the server / service startup, login, administrator management activity, send mail log, installation history of document security, usage history, print history of policy change log and print security, policy change and personal information Security detection contents history, policy change history, and so on.

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

6.1.6 Protection of the TSF

Protection of the TSF performs the following functions.

- Protection of the TSF
- Self-testing

6.1.6.1 Protection of the TSF data

For the safe cryptographic communication among the TOE components, the transmitted TSF data is protected using the confidentiality (ARIA-CBC, 128bit) and integrity (SHA-512, 512bit) algorithms of the validated cryptographic module.(MACRYPTO V2.00)

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

6.1.6.2 TSF self-test

The TOE provides integrity verification using SHA-512 algorithm at startup and periodically. If integrity failure are found, send an alert E-mail to the authorized administrator

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

6.1.7 TOE access

The TOE access performs the following functions

- Session management

6.1.7.1 Session management

The TOE provides accessable IP registration function and permits the server access only to IPs allowed when the administrator logs in. In addition, the maximum number of concurrent sessions is limited to 1 for a management connection session.
After the administrator's inactivity period (5 minutes), the administrator's interactive session ends.

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 v1.0 for the country, IT Security Certification Center, 2017.8.18**