DocuRay x v3.5

Security Target

v1.6

BlueMoonSoft
The World's Best Security and Automation Software Provider

< Change history >

Version	Date	Contents	Author
v1.0	2024-03-29	Initial registration	Hee Woo Han
v1.1	2024-11-21	Modify observations	Hee Woo Han
v1.2	2024-12-23	Reflect modifications	Hee Woo Han
V1.3	2024-12-27	Reflect CC2022 modifications	Hee Woo Han
V1.4	2025-01-14	Reflect modifications	Hee Woo Han
v1.5	2025-01-31	Validated cryptographic module modifications	Hee Woo Han
v1.6	2025-02-25	Reflect modifications	Hee Woo Han

Table of Contents

1 Security Target Introduction

1.1 Security Target Reference

Security Target Reference [Table 1-1]

Category	Contents
Title	DocuRay x v3.5_Security Target
Security Target	v1.6
Author	BlueMoonSoft Inc.
Creation Date	Jan. 31, 2025
Evaluation Criteria	Common Criteria for Information Security Systems (Ministry of Science, ICT and Future Planning Notification No. 2013-51))
Common Criteria Version	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, 2022.11 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, 2024.07
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keywords	Document, Encryption

1.2 TOE Reference

[Table 1-1] TOE Identification Information

Category		Contents
TOE		DocuRay x v3.5
TOE Details		3.5.5.0
Components	Server	DocuRay x Server 3.5.5.0 (DocuRay_x_Server_Launcher_3.5.5.0.exe)
	Agent	DocuRay x Agent 3.5.5.0 (DocuRay_x_Agent_Setup_3.5.5.0.exe)
Guidance Documents		DocuRay x v3.5 Operational Guidance v1.3 (DocuRay x v3.5 Operational Guidance v1.3.pdf)
		DocuRay x v3.5 Installation Guidance v1.4 (DocuRay x v3.5 Installation Guidance v1.4.pdf)
Developer		BlueMoonSoft Inc.
Release Date		Jan. 31, 2025

1.3 TOE Overview

1.3.1 Document Encryption Overview

DocuRay x v3.5 ("TOE") is used to protect important documents managed by an organization. The TOE performs document encryption according to the policy set by the administrator to protect important documents managed in the organization, and decrypts documents according to the request and permission of the document users.

The TOE encrypts/decrypts the entire contents of the protected documents by specifying the document type (e.g., PDF document, MS Office document, Hangul document, etc.).

The primary security function provided by the TOE is encryption/decryption key management of protected documents. The TOE uses the approved cryptographic algorithm of the validated cryptographic module (MagicCrypto V2.3.0), which has been verified for safety and implementation suitability through the Korea Cryptographic Module Validation Program (KCMVP), for the encryption/decryption of documents, encryption/decryption of critical security parameters used by the TOE and cryptographic key management.

1.3.2 TOE Type

The TOE, as defined in this Security Target, is 'document encryption' that prevents information leakage by performing encryption/decryption on important documents within an organization, and the TOE components are provided in the form of software. The TOE supports 'user terminal encryption' method.

The essential TOE components that perform the security function defined in this Security Target are DocuRay x Server 3.5.5.0 (hereinafter referred to as "DocuRay x Server") and DocuRay x Agent 3.5.5.0 (hereinafter referred to as "DocuRay x Agent").

1.3.3 TOE Objectives and Major Security Features

The TOE performs encryption/decryption of documents according to the policy set by the administrator to protect important documents managed in the organization, and includes the cryptographic key management function. In addition, the TOE provides security audit function to record and manage major events as audit data during the operation of the security function and management function, identification and authentication function (administrator and document user identity verification, handling authentication failure, mutual authentication between TOE components), security management function for function/role definition/configuration, function to protect data stored in storage controlled by the TSF, Protection of the TSF function such as TSF-testing, and TOE access function for access session management of the authorized administrator.

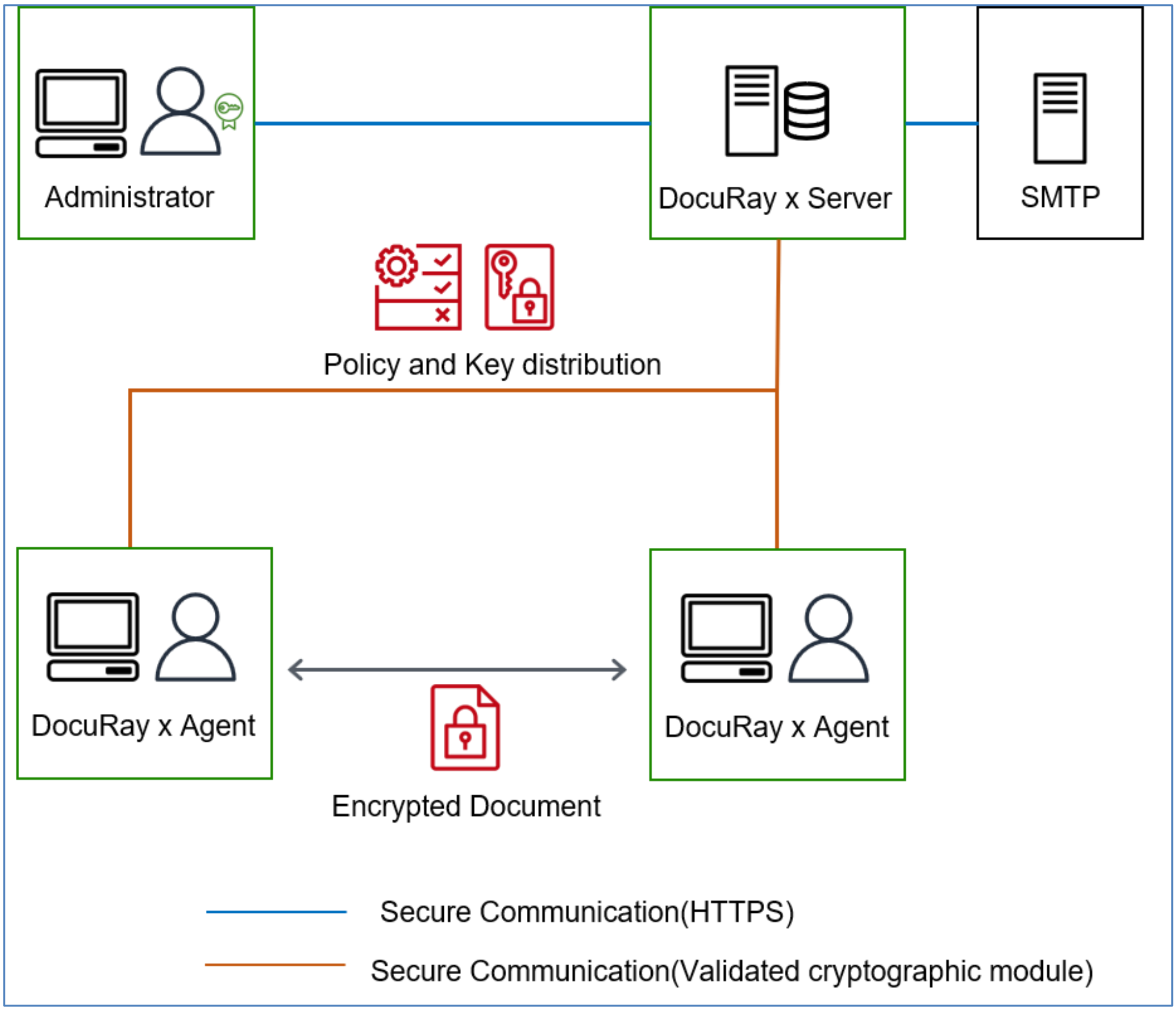
‘Document data cryptographic key’ (hereinafter referred to as ‘Document DEK’) and 'Header Data Cryptographic key' (hereinafter referred to as 'Document Header DEK') are used. There are two types of document header DEK depending on the policy. The body of the protected document is encrypted with the document DEK according to the policy set by the administrator, and the generated document DEK is stored in the header of the secure document. The header is encrypted and stored as document header DEK.

DocuRay x Server generates document header DEK and distributes it to DocuRay x Agent, which distributes the cryptographic key in a secure encrypted communication. DocuRay x Agent generates the Document DEK and uses the generated Document DEK to encrypt the body of the protected document or decrypt the encrypted body. DocuRay x Agent uses the distributed document header DEK to encrypt and store the header. TOE provides a function to destroy the cryptographic key when it is no longer used.

The Administrator can specify documents for decryption through the management server and grant document users access permission to these documents. The management server distributes the cryptographic key to document users according to the set policy, so only authorized document users can decrypt documents.

1.3.4 Non-TOE and TOE Operational Environment

The TOE has 'user terminal encryption’ as its operational environment. [Figure 1] shows the operational environment of the TOE. The TOE consists of DocuRay x Server and DocuRay x Agent, which must be installed and operated on the internal network of the protected organization.


Administrator
DocuRay x Server
SMTP
Policy and Key distribution
DocuRay x Agent
DocuRay x Agent
Encrypted Document
Secure Communication(HTTPS)
Secure Communication(Validated cryptographic module)

[Figure 1] TOE Operational environment

The TOE consists of DocuRay x Server, which manages the security policy and cryptographic key, and DocuRay x Agent, which is installed on the user's PC and performs document encryption/decryption.

The administrator sets the policy for each document user through DocuRay x Server, and DocuRay x Server distributes the policy and cryptographic key set by the administrator to the agents. The agent installed on the user's device performs encryption/decryption of documents using the validated cryptographic module (MagicCrypto V2.3.0) according to the distributed policy, and the documents are saved as a file on the user's device.

The function to encrypt/decrypt documents when they are delivered outside of an organization where the agent is not installed is not within the scope of the TOE.

Cryptographic operations for the encryption/decryption-related security function use the validated cryptographic module (MagicCrypto V2.3.0). Communication between the TOE components and the administrator (e.g., when accessing DocuRay x Server to set the policy using a web browser) use TLS 1.3 encryption.

The external entity used to operate the TOE uses an SMTP server for email notifications to the authorized administrator.

All hardware, software, and firmware required for the TOE installation are non-TOE and are identified below

- DocuRay x Server

DocuRay x Server requires hardware, operating system, WAS to operate the administrator UI, DBMS to store audit records, and the minimum requirements are listed below.

[Table 1-3] DocuRay x Server Minimum Requirements

Category		Minimum Requirements
Hardware	CPU	Intel Xeon 3.1 GHz or faster
	RAM	8 GB or more
	HDD	500 GB or more of space required for TOE installation
	NIC	10/100/1000 Mbps Ethernet
Operating System		Microsoft Windows Server 2019 Standard 64bit
Required software	WAS	Apache Tomcat 9.0.98
	DBMS	MariaDB 10.11.10
	JAVA	JDK 1.8.0.422 (Azul Zulu)

- DocuRay x Agent

The DocuRay x Agent installed on the user's PC is responsible for encryption/decryption, and the following minimum specifications are listed below.

[Table 1-2] Agent Minimum Requirements

Category		Minimum Requirements
Hardware	CPU	Intel i7 4th Gen 2.2 GHz or faster
	RAM	12 GB or more
	HDD	300 GB or more space required for TOE installation
	NIC	10/100/1000 Mbps Ethernet
Operating System		Microsoft Windows 11 Pro 64bit

- Authorized administrator PC

The authorized administrator can access the administrator UI to perform security management and view audit records. TOE's connection to DocuRay x Server uses TLS 1.3 encrypted communication.

The recommended specifications for the authorized administrator PC are listed below

[Table 1-3] Minimum Requirements for Authorized Administrator PC

Category	Minimum Requirements
Web browser for security management	Microsoft EDGE - Version: 129.0.2792.52 or later

- Document Editors

The list of software necessary for the TOE operation is shown in the following.

[Table 1-6] Supported Document Editors

Encryption Target	Software
MSOFFICE	MS Office 2019
HWP	Hancom Office 2018
ADOBE READER	Adobe Acrobat Reader
TEXTEDIT	MS Notepad
AUTO CAD	Auto Cad 2024
AUTO INVENTOR	Auto Inventor 2024

- SMTP Server

The TOE provides the function to send notifications to the authorized administrator when policy violationes occur. Notifications are sent via an SMTP server supported by the registered administrator's email account.

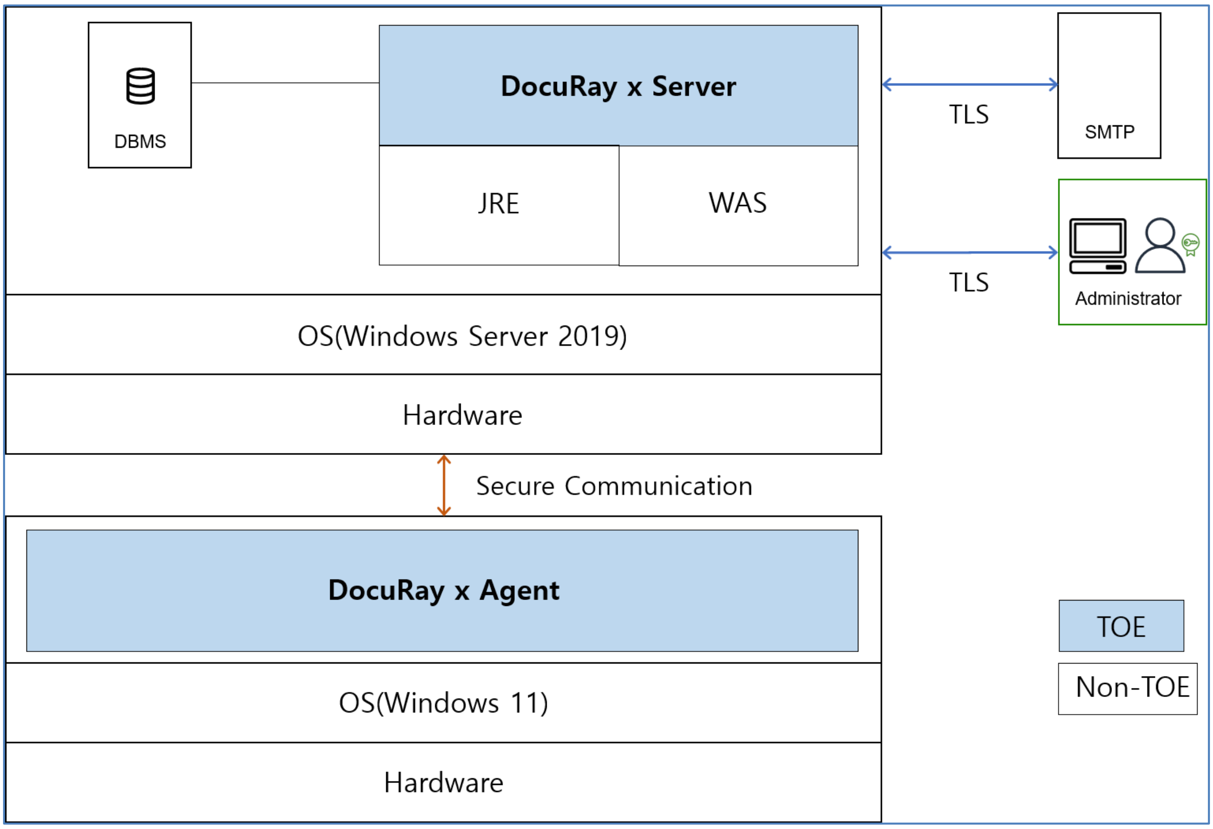
1.4 TOE Description

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

1.4.1 Physical Scope of the TOE

The TOE is DocuRay x v3.5, which is a software consists of DocuRay x Agent, a security function processing part and DocuRay x Server, the security management part. DocuRay x Agent is installed on the user's PC and performs the security function such as data protection by encrypting important documents according to the policy, and DocuRay x Server is installed on an internal independent server to perform the security management function such as DocuRay x Agent control, policy settings and administrator page. The administrator can access the administrator page through WAS to perform the function such as policy settings and security auditing. Communication between DocuRay x Server and DocuRay x Agent and access to the administrator page are done through TLS communication. The hardware and OS on which the TOE is installed are not included in the

physical scope of the TOE, and the WAS, JRE, and DBMS, which are included on the CD for DocuRay x Server operation and must be installed first by the administrator when installing DocuRay x Server, are non-TOE.
The physical extent of the TOE is shown in the following [Figure 1-2].



[Figure -11] Physical scope of the TOE

The TOE is provided as a setup package on a CD and includes an operational guidance, installation guidance, and license certificate, which are distributed to the customer as electronic documents (PDF) to enable effective operation of the TOE.
The provided components include DocuRay_x_Server_Launcher_3.5.5.0.exe, DocuRay_x_Agent_Setup_3.5.5.0.exe, DocuRay x v3.5 Installation Guidance v1.4.pdf, DocuRay x v3.5 Operations Guidance v1.3.pdf
The provided physical scope of the TOE in the Setup package is identified in the Table 1-7 below.

[Table1 -7] Physical Scope of the TOE

Category	Name	Form	Deployment Types
TOE Name	DocuRay x v3.5	-.	-.
Version Details	3.5.5.0	-.	-.

Setup Package	Server	DocuRay x Server 3.5.5.0 (DocuRay_x_Server_Launcher_3.5.5.0.exe)	Software	CD
	Agent	DocuRay x Agent 3.5.5.0 (DocuRay_x_Agent_Setup_3.5.5.0.exe)	Software	
Electronic Documentation	User Guide	DocuRay x v3.5 Operational Guidance v1.3 (DocuRay x v3.5 Operations Guidance v1.3.pdf)	PDF	
	Preparation	DocuRay x v3.5 Installation Guidance v1.4 (DocuRay x v3.5 Installation Guidance v1.4.pdf)		

The 3rd party software included in the TOE is identified as shown in the [Table 1-8].

- Validated Cryptographic Module

The TOE uses the validated cryptographic module to perform document encryption of security requirements and encryption of TOE configuration files, and its library information is described below.

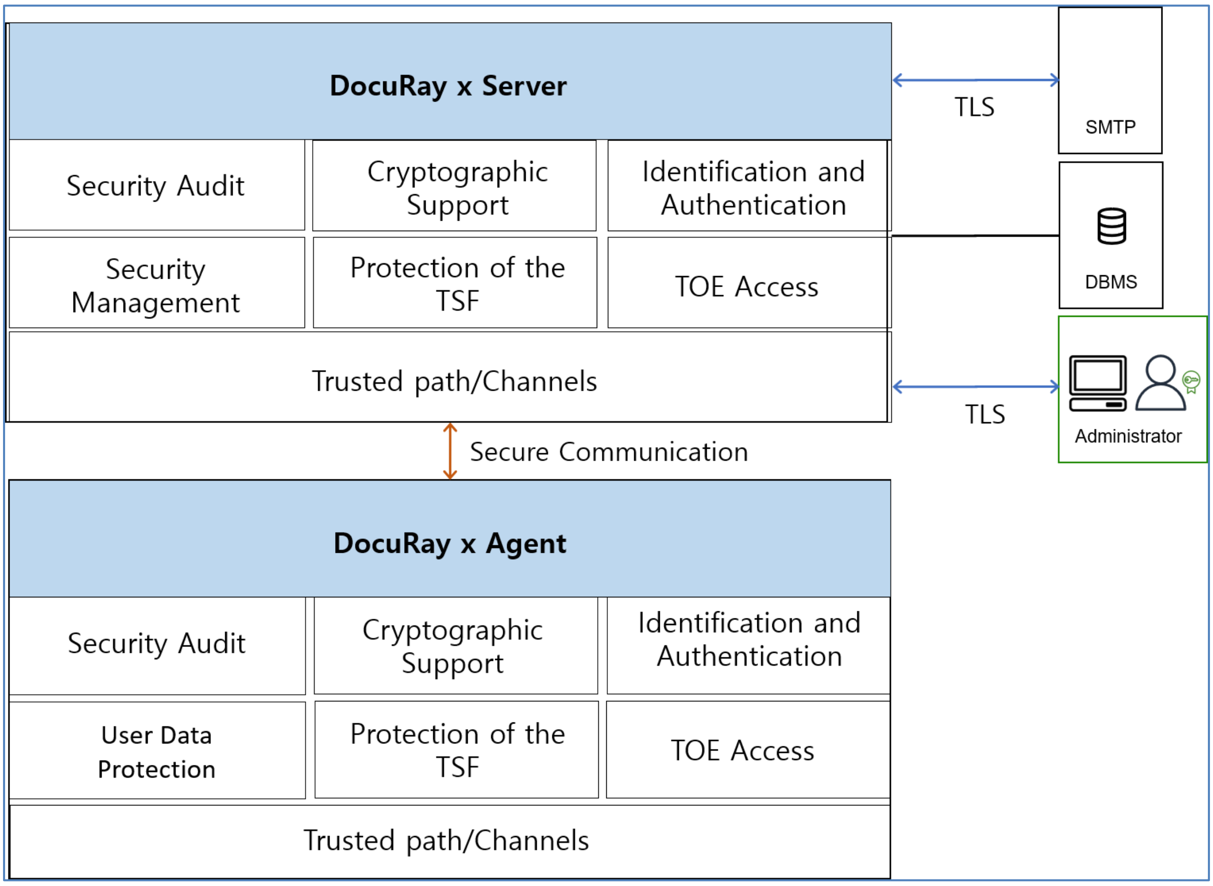
- Cryptographic Name: MagicCrypto V2.3.0
- Validation Number: CM-263-2030.1
- Developer: DreamSecurity Inc.
- Validation Date: 2025-01-24
- Expiration Date: 2030-01-24

[Table1 - 8] 3rd Party Information in the TOE

Category	Name	Contents
DocuRay x Server	OpenSSL 3.4.0	Module for secure communication
	MagicCrypto V2.3.0	Validated Cryptographic Module
DocuRay x Agent	OpenSSL 3.4.0	Module for secure communication
	MagicCrypto V2.3.0	Validated Cryptographic Module

1.4.2 Logical Scope of the TOE

The logical scope of the TOE is described below.



[Figure -12] Logical Scope of the TOE

1.4.2.1 Security Audit

The TOE stores the audit function's start/stop history and the events related to the security functions as audit records in the DBMS. Among the audit records, document usage history is selectively generated based on encryption/decryption/viewing activities. The audit data includes detailed information such as the date and time of the event, the type of the event, the identity of the subject involved, the operation history, and the result. Time synchronization is performed between servers and agents to ensure accurate time information for key events. The authorized administrator can view the generated audit history and search using various criteria, such as event type, date, or user. Stored audit records in audit trails do not include any user interface or functionality that allows deletion or modification, even for the authorized administrator.

When a potential security violation is detected, such as an integrity violation, failed testing, or audit threshold exceeded (>90% of total disk capacity), the TOE notifies the authorized administrator via email of the potential violation.

The TOE responds to storage failures by sending an email notification to the administrator when audit data growth exceeds saturation (>95% of total disk capacity) and by sequentially overwriting older audit records.

1.4.2.2 Cryptographic Support

The TOE uses MagicCrypto V2.3.0 to perform cryptographic operations and cryptographic key management such as generation, distribution, and destruction. HASH_DRBG (SHA-256) is used to generate DEK (data cryptographic key), and RSAES (SHA-256) algorithm is used to generate private and public key pairs. Also, HASH_DRBG (SHA-256) algorithm is used to generate Salt and IV. A KEK (Key Encryption Key) is generated from the runtime password and derived using the PBKDF2 (HMAC-SHA-256) algorithm. The ARIA_CBC mode and RSAES (SHA-256) are used to distribute the cryptographic key between components.

The TOE performs operations through ARIA_CTR mode when encrypting/decrypting the document body, and ARIA_CBC mode is used to encrypt the document header, communication , and cryptographic key. During the communication process, the cryptographic key and authentication information are encrypted with RSAES (SHA-256), and an electronic signature is generated with RSA-PSS (SHA-256) algorithm. The verification code of inter-module communication (IPC), module integrity verification value, and original document validation value recorded in the document header are generated using SHA-512. Passwords of the authorized administrator and document users are stored using HMAC (SHA-256), and settings such as DBMS password are stored using ARIA_CBC mode. When destroying the cryptographic key and authentication information, the memory is overwritten with '0' or '1' at least 3 times.

1.4.2.3 User Data Protection

The TOE protects user documents.

1) The TOE creates protected documents by encrypting plain text documents according to the policy set by the authorized administrator, and protects them by controlling access to the protected documents. It blocks the clipboard for protected documents and prevents document leakage. Policies are set differently depending on user identifiers, file permissions, and target document types. Access to decrypt documents is controlled according to decryption permissions.
2) Protected documents are encrypted with cryptographic support and can only be accessed by authorized document users. Even if the protected document is leaked externally, unauthorized document users cannot access its contents.

DocuRay x Agent encrypts and stores documents on the user’s PC.

DocuRay x Agent supports the following main document types

[Table1 - 9] Supported Document Type

Encryption Target	Category	Operations			
		Write	View	Manual encryption	Manual decryption
MSOFFICE	Process	winword.exe, excel.exe, powerpnt.exe		-.	
	Document type	MSOffice document header	Secure document header	MSOffice document header, PDF document header	Secure document header
HWP	Process	hwp.exe		-.	
	Document type	Hangul document header	Security document header	Hangul document header	Security document header
ADOBE READER	Process	acrobat.exe		-.	
	Document type	PDF document headers	Secure document header	PDF document header	Secure document header
TEXTEDIT	Process	notepad.exe		-.	
	Document types	All Files	Secure document header	TXT document header	Secure document header
AUTO CAD	Process	acad.exe		-.	
	Document type	Auto Cad document Header	Secure document headers	Auto Cad document header	Secure document header
AUTO INVENTOR	Process	inventor.exe		-.	
	Document type	Auto Inventor document Header	Secure document header	Auto Inventor document header	Secure document header

1.4.2.4 Identification and Authentication

The TOE provides an identification and authentication process based on IDs and passwords for the administrator and document users. Only authorized administrator can access the administrator page through a web browser to manage security features. When a document user logs in to DocuRay x

Agent, the identification and authentication process is performed through mutual authentication between DocuRay x Server and DocuRay x Agent.

When the administrator and document users enter their passwords into DocuRay x Server or DocuRay x Agent, they are masked with '●' to prevent exposure, and if authentication fails, no specific reason for the failure is provided. A password must be at least nine characters long and include at least one uppercase letter, and lowercase letter, one number, and one special character. Additionally, the following rules must be followed: the password cannot be the same as your user ID, the same letter or number cannot be repeated more than 3 times consecutively, more than four consecutive letters or numbers on the keyboard cannot be used, and the last password cannot be reused. If an admin or document user fails to authenticate more than five times, their account will be locked for five minutes.

The credentials of the administrator or document users are timestamped to prevent reuse. A timestamp is sent along with the credentials and saved when authentication is successful. When logging in, the timestamp is used to authenticate the user, and if the timestamp is smaller than the timestamp stored in the DB, authentication fails, and if it is larger, the authentication process proceeds. When the authentication process is completed, the timestamp is saved.

After successful authentication, you can use the security features provided by TOE.

1.4.2.5 Security Management

Only the authorized administrator can perform security management through the admin page. Upon initial access, the administrator must change the default password. The authorized administrator can configure security attributes, such as the types of documents to be encrypted, and execute the security functions, including deleting modules and performing server integrity verification, through the policy menu. SMTP account information and connection IP management can be set for security features. The authorized administrator can add, delete, or change the password of document users in oranization chart management menu. Only one administrator account is provided.

1.4.2.6 Protection of the TSF

The TOE communicates securely to protect transmitted data between components, ensuring confidentiality and integrity.

The TOE prevents unauthorized exposure and tampering of TSF data through encryption, hashing, and digital signatures.

DocuRay x Agent's TSF data is stored in the installation directory and is monitored to prevent unauthorized access and termination. The TOE performs the testing and integrity verification at startup, periodically, and on administrator request to ensure normal operation. If an integrity verification fails, the TOE performs an automated recovery.

1.4.2.7 TOE Access

In order to ensure secure session management for an authorized administrator, the TOE terminates login sessions after a period of inactivity on the admin page. For secure session management for document users, The TOE also overwrites the display so that the current content is unreadable after a period of inactivity.

The authorized administrator can only sign in from the device specified as the accessible IP. If you try to sign in with the same account, the existing connection is terminated and the sign-in succeeds.

Duplicate document user logins for the agent are blocked using an additional attribute, while the existing connection is maintained.

1.4.2.8 Trusted path/Channel

The TOE provides a trusted channel to protect data from unauthorized changes or exposure when interfacing with a mail server to send mail to the authorized administrator in the event of a potential violation.

1.5 Terms and Definitions

The terms used in this Security Target that are identical to those in the Common criteria follow the Common criteria definitions

Private Key

A Cryptographic key used in conjunction with an asymmetric cryptographic algorithm, uniquely associated with a single entity (the subject using the private key), and must not be made public

Object

A passive entity within the TOE that is the target the subject’s operation and either contains or receives information

Approved mode of operation

The mode of operation of a cryptographic module that exclusively uses the approved cryptographic algorithm

Approved cryptographic algorithm

A cryptographic algorithm selected by the cryptographic module validation institution, considering factors such as stability, reliability, and interoperability, for block ciphers, hash functions, message verification codes, random number generators, key settings, public key ciphers, and electronic signature cryptographic algorithms

Validated Cryptographic Module

A cryptomodule that has been validated and approved by the cryptographic module validation institution, with a validation number assigned

Attack potential

The level of effort required for an attack on the TOE, as determined by factors such as the attacker's expertise, resources, and motivation

Public Security Parameters (PSP)

Security-related public information that, if changed, could compromise the security of the cryptographic module

Public Key

A cryptographic key used in conjunction with an asymmetric cryptographic algorithm, uniquely associated with a single entity (the subject using the public key), and can be made public

Public Key (asymmetric) cryptographic algorithm

A Cryptographic algorithm that uses a pair of public and private keys

Management access

The action of an administrator attempting to access the TOE for management using HTTPS, SSH, TLS, or IPSec

Manangement console

An application that provides graphical interface (GUI), or command-line interface (CLI) to the administrator for system management and configuration

Recommend/be recommended

The terms "recommended" or "be recommended" presented in the application notes refer to requirements that are not mandatory for the TOE, but are suggested to apply for ensuring the secure operation

Group Based Access Control

An access control method that controls access to objects based on the group's identifier, as one of discretionary access methods

Random bit generator (RBG)

A device or algorithm that generates a statistically independent and unbiased binary sequence

Random bit generators used for cryptographic applications typically produce sequences of bits (0s and 1s), which can be combined into random blocks. Random bit generators are categorized into deterministic and non-deterministic types. Deterministic random bit generators use an initial value known as a seed key to generate the bit sequence, while non-deterministic random bit generators generate outputs that depend on unpredictable physical sources

Symmetric cryptographic technique
A cryptographic technique that uses the identical secret key for both encryption and decryption, also known as a secret key cryptographic technique

Local access
A configured connection between the administrator and the TOE through a console port

Data Cryptographic key (DEK)
A key used to encrypt data

Management access
The action of administrator attempting to directly access the device through its console port for TOE management

Word processing program
A program used to create, modify, manipulate, and print documents on a computer, such as Hangul, MS Word, Acrobat, and CAD (Computer Aided Design) for processing important documents.

Iteration
The use of the identical component to express two or more different requirements

Security Target (ST)
A security requirement specification that is implementation-dependent for the specific TOE

Security Policy Document
A document published with the module’s name in the list of validated cryptographic modules, which summarizes the cryptographic module’s type, the approved cryptographic algorithm provided by the cryptographic module and the operational environment

Security Token
A hardware device that is implemented so that key generation and electronic signature generation

are processed internally in order to securely store and preserve secret information

Protection Profile (PP)

A security requirements specification that is Implementation-independent for TOE types

Decryption

The process of restoring ciphertext to its original plaintext using the decryption key

Non-Approved mode of operation

A mode that allows the operation of the non-approved cryptographic algorithm, while also enabling the use of the approved cryptographic algorithm

Secret Key

A cryptographic key used in conjunction with a secret key cryptographic algorithm, uniquely associated with one or more entities, and must not be made public

User

"External entities" are referenced, but within the TOE, the users are the authorized administrator and authorized document users

Selection

Specifying one or more items from the list described in the component.

Manual recovery

Recovery through user execution or user intervention via an update server

Identity

A unique representation that identifies an authorized user, which could be the user's real name, a nickname, or a pseudonym.

Encryption

The process of converting plaintext into ciphertext using an cryptographic key

Korea Cryptographic Module Validation Program (KCMVP)

A system to validate the security and implementation suitability of cryptographic modules used to protect important information that is not classified as secret, transmitted over national or public institution communication networks

Agent Type1

Antivirus products, software-based secure USB products, host data leakage prevention products, etc.

- The endpoint on which the agent is located is typically a PC with a Windows® operating system accessible by employees within the organization, if the agent is compromised, the data on the user's host can be corrupted and leaked, therefore, this product type must be applied the strict security requirements in terms of confidentiality, integrity, and availability

Agent Type2

Network access control products, and patch management systems, etc.

- The endpoint on which the agent is located is typically a PC with a Windows® operating system accessible by employees within the organization, if the agent is compromised, while the likelihood of data corruption or leakage on the user's host, there can be issues in the normal usage of resources provided by the organization, therefore, this product must be applied the security requirements in terms of confidentiality and integrity

Agent Type3

Database access control products, operating system (server) access control products, and integrated security management products, etc.

- The endpoint on which the agent is located, is only accessible by the authorized employees within the organization, therefore, the risk of threats is relatively low

Endpoint

A point at where TOE components, such as the agent, the client, are installed and operated without further subordinate interconnected entities

Element

The smallest indivisible unit of security requirements

Role

A predefined set of rules that defines the allowed interactions between the user and the TOE

Role Based Access Control (RBAC)

An access control method that controls access by mediating the relationship between the user and access permissions through roles, based on the organization's characteristics, rather than directly linking the user and permissions.

(Operation (on a component of the CC)

Modifying or iterating over a component. The allowed operations on a component include assignment, iteration, refinement, and selection.

(Operation (on a subject)

A specific action performed by the subject on the object

External Entity

An entity (person or IT) outside the TOE that interacts with the TOE

Threat Agent

An unauthorized external entity that poses a threat to assets by causing illegal access, modification, or deletion

Authorized Administrator

An authorized user who operates and manages the TOE securely

Authorized Document User

A user who can execute functions according to the SFR (Security Functional Requirements)

Authentication Data

Information used to authenticate the identity of a user

Application Programming Interface (API)

A set of software libraries that exist between the application layer and the platform system layer, making It easier to develop applications running on the platform

Automated Recovery

A recovery action that does not involve user intervention

Assets

An entity to which the owner of the TOE assigns value

Refinement

Addition of details to a component

Access Control Lists (ACLs)

A list that records the subjects authorized to access an object and the types of access these subjects are permitted to perform

Information System

An organized system of devices and software related to the collection, processing, storage, retrieval, transmission, reception, and utilization of information

Organizational Security Policy
A set of security rules, procedures, practices, and guidelines that are currently assigned or are anticipated to be assigned on an operational environment by a real or virtual organization.

Dependency
A relationship between components, where if the requirements based on the dependent component are included in the protection profile, security objectives specification, or package, the requirements based on the dependent component must also be included in the protection profile, security target, or package.

Subject
An active entity within the TOE that performs operations on an object

Sensitive Security Parameters (SSP)
Core Security Parameters (CSP) and Public Security Parameters (PSP)

Augmentation
Addition of one or more requirements to a package

Component
The smallest unit of selection that can be used to form the basis of requirements as a set of elements.

Client Type
Virtual private network products, wireless LAN authentication products, etc.
- A client is an entity installed on a user's host that requests communication with the server on behalf the user.

Class
A collection of common criteria families with the identical security objectives

Key Cryptographic key (KEK)
A key used to encrypt other cryptographic keys

Target of Evaluation (TOE)
A set of software, firmware, and/or hardware accompanied by the relevant documentation

Evaluation Assurance Level (EAL)

An assurance package consisting of three assurance requirements with predefined assurance levels in the Common criteria

Family

A collection of components that have similar objectives but different emphases or levels of rigor

Assignment

Specifically specifying the parameters identified within a component or requirement (of the Common criteria).

Shall/Must

The terms “shall” or “must” presented in the application notes refer to requirements that must be mandatorily applied to the TOE.

Can/could

The terms "can" or "could" presented in the application notes refer to requirements that can be applied to the TOE at the discretion of the security target author.

Critical Security Parameters (CSP)

Security-related information that, if exposed or modified, could compromise the security of the cryptographic module (e.g., secret/private keys, authentication data such as passwords or personal identification numbers)

TOE Security Functionality (TSF)

A set of all hardware, software, and firmware of the TOE that contribute to the appropriate performance of SFR (Security Functional Requirements)

TSF Data

Data created by the TOE for the TOE that can influence its operation

Secure Sockets Layer (SSL)

A security protocol proposed by Netscape to provide security such as confidentiality and integrity in computer networks.

Transport Layer Security (TLS)

An encryption and authentication communication protocol between server and client based on SSL, specified in RFC 2246

Wrapper

An Interface for interconnecting the TOE with various types of information systems

1.6 Conventions

This Security Target uses some abbreviations and mixes English for clarity. The notation, format and authoring rules used follow the Common criteria.

The Common criteria operations such as iteration, assignment, selection, and refinement that can be performed in the Security Functional Requirements. Each operation is used in this Security Target.

Iteration

It is used when an operation is applied in various ways to iterate a component multiple times. The result of the iteration operation is indicated by the repetition number in parentheses after the component identifier, i.e. (iteration number).

Assignment

It is used to assign a specific value to an unspecified parameter (for example, the length of a password). The result of the assignment operation is indicated in square brackets, i.e. [assign value].

Select

It is used to select one or more of the options provided in the Common criteria for Information Security Systems when describing requirements. The result of the selection operation is displayed in *underlined italicized*.

Refinement

It is used to further restrict the requirements by adding details to the requirements. The result of the refinement operation is displayed in **bold text**.

Security Target Author

It is used to indicate that the final determination of the attribute is made by the security target author. The Security Target Author operation is represented as { Determined by the Security Target Author } in curly braces. In addition, operations of the Security Functional Requirements that are not fully performed in the Security Target must be fully performed by the Security Target Author.

This Security Target clarifies the meaning of the requirements, provides information about options of implementation, and defines the criteria for "conformance/non-conformance" through the “Application Notes.” The Application Notes are provided with the requirements when necessary.

2 Conformance

2.1 Conformance Claim

2.1.1 CC Conformance Claim

The Security Target, the Common Criteria and Protection Profile that the TOE complies with, the assurance requirements package, and the security requirements are as shown in [Table 2-1] below.

[Tables 2-1] Criteria Complied by the Security Target and TOE

CC		Common Criteria for Information Security Systems Version CC:2022 Revision 1 - Common Criteria for Information Security Systems Part 1: Introduction and General Model, Version CC:2022 R1 (CCMB-2022-11-001, 2022.11) - Common Criteria for Information Security System Part 2: Security Functional Component, Version CC:2022 R1 (CCMB-2022-11-002, 2022.11) - Common Criteria for Information Security Systems Part 3: Security Assurance Component, Version CC:2022 R1 (CCMB-2022-11-003, 2022.11) - Common criteria for Information Security Systems Part 4: Framework for Evaluation Methods and Activities Specification, Version CC:2022 R1 (CCMB-2022-11-004, 2022.11) - Common Criteria for Information Security System Part 5: Predefined Security Requirements Package, Version CC:2022 R1 (CCMB-2022-11-005, 2022.11) - Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, (CCMB-2024-07-002, 2024.07)
Protection Profile		Korean National Protection Profile for Electronic Document Encryption V3.0
Conformance Claim	Part 2 Security Functional Components	Extended: FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2
	Part 3 Security Assurance Components	Conformant

	Package	Augmented: EAL1 augmented (ATE_FUN.1)

2.1.2 Conformance Type

This Security Target "strictly complies with the protection profile.

2.1.3 PP Synthesis Conformance Claim

This Security Target does not synthesize any other Protection Profiles.

2.1.4 PP Conformance Claim

This Security Target has strictly complied with the ‘Korean National Protection Profile for Electronic Document Encryption V3.0’, ensuring that the security objectives and security requirements for the operational environment are fully identical.

2.1.5 Package Conformance Claim

The assurance requirements package that this Security Target complies with is EAL1, which defines some additional assurance requirements.

- Augmented Package: EAL1 Augmented (ATE_FUN.1)

2.1.6 Conformance Claim Rationale

Since this Security Target is identical to the TOE type, security objectives, and security requirements of the Protection Profile, the conformance declaration for the ‘Korean National Protection Profile for Electronic Document Encryption V3.0’ is ‘Strict Protection Profile Conformance’.

The security target rationale according to the Selection of the ‘Korean National Protection Profile for Electronic Document Encryption V3.0'

Item	Security objectives	Rationale
Security Objectives for Operational Environment	OE. Timestamp	An additional security objective for the operational environment has been included by using a trusted timestamp provided by the TOE operational environment to accurately record security-related events
	OE. DBMS	An additional security objective for the operational environment has been included by protecting the audit data repository through the DBMS provided by the TOE operational environment
	OE. Trusted path	An additional security objective for the operational environment has been included by performing administrative access through the web

		server provided by the TOE operational environment

2.2 Conformance Methodology

2.2.1 References to Evaluation Methods/Activities

The 'EAL1+' package complied with in this Security Target requires the use of the evaluation methods and activities defined in <6.2. Assurance Requirements>.

The 'Korean National Protection Profile for Electronic Document Encryption V3.0' complied with in this Security Target requires the use of the evaluation methods and activities defined in the <Korean National Protection Profile for Electronic Document Encryption V3.0 Supplementary Document>.

3 Security Problem Definition

The security problem definition defines the threats, organizational security policy, and assumptions that intended to address the TOE and its operational environment.

3.1 Assets

The primary assets protected by the TOE are as follows:

- Important documents managed by an organization
- TOE and Important data about the TOE operations (e.g., TSF data)

3.2 Threats

Threat actors are generally unauthorized IT entities and users who attempt to protect important documents managed by an organization internally and illegally leak them externally or pose the TOE and internal assets in an abnormal manner. Threat actors possess a basic level of expertise, resources, and motivation and may give rise to a variety of threats such as follows:

T. Stealing Cryptographic key
A threat actor can steal the cryptographic key during the cryptographic key distribution process by intercepting communication data.

T. Unauthorized Information Leakage
A threat actor can leak internal information to the outside world through an external path.

T. Disabling Agent
A threat actor can delete or forcefully terminate the agent to disable the security functions of the product.

T. Bypassing Access Control
A threat actor can bypass access control by changing the security attributes of important documents managed by your organization.

T. Record Failure
A threat actor can exhaust storage capacity to prevent security-related events from being recorded.

T. Bypassing Administrator
A threat actor can pose as an authorized administrator to gain access to a management server.

T. Bypassing Document User

A threat actor can pose as an authorized document user to leak or modify protected documents.

T. Server Spoofing

A threat actor can pose an administrative server to distribute malware or gain decryption permissions.

T. Continuous Authentication Attempt

A threat actor can repeatedly attempt authentication to gain authorized user permissions.

T. Credential Inference

A threat actor can infer credentials from authentication failure messages to gain authorized user permissions.

T. Accessing Idle Session

A threat actor can access the TOE through administrator or document user sessions that have not been used for a period of time.

T. Transmitted Data Leakage and Corruption

A threat actor can leak, modify, or delete data in transit between components of the product in an unauthorized manner.

T. Stored Data Corruption

A threat actor can leak, modify, or delete operationally critical data stored inside the product in an unauthorized manner.

T. Weak password

A threat actor can pose an authorized administrator by obtaining poorly managed passwords such as default or low-level passwords to access to the TOE.

3.3 Organizational security policies

P. Audit

In order to track accountability for security-related actions, security-related events must be recorded and maintained, and the recorded data must be reviewed. In addition, the available space on the disk for storing audit data must be regularly monitored to prevent audit data from being lost and must be protected it to prevent unauthorized modifications and deletions to stored audit

P. Secure Operation

The administrator must securely configure the TOE to comply with the organizational security policy and provide management tools to ensure the TOE is operated accurately according to the TOE operational Guidance.

P. Password Strength

An organization must apply encryption to the storage and transmission of important data, such as user passwords, and use secure cryptographic algorithms.

3.4 Assumptions

A. Physical Security

The TOE is located in a physically secure environment that is accessible to authorized users.

A. Secure Maintenance

When your internal network environment changes, such as network configuration changes, hosts being added or removed, services being added or removed, the environment and security policy are immediately reflected in the TOE operational policy to maintain the identical level of security as before.

A. Authorized Administrator

An authorized administrator of the TOE is well-intentioned, properly trained in the TOE administrative functions, and fulfill his/her duties accurately according to all administrative guidelines.

A. Authorized Document User

A document user, controlled by the TOE agent, is guaranteed to be identified and authenticated users of the protected assets.

A. Log backup

An authorized administrator of the TOE must periodically monitor the free space of the audit data storage in case of audit data loss and perform audit record backup (external log server, separate storage device, etc.) to prevent the audit records from being exhausted.

A. Operating System Reinforcement

An authorized administrator of the TOE must reinforce against operating system vulnerabilities and prevent the interference between TOEs and other applications.

A. DBMS

The DBMS must be installed on the same operating system as the TOE, receiving identification and authentication functions from the DBMS to protect against deletions or modifications by unauthorized users.

A. Trusted path

The TOE must use an encrypted communication channel and encrypts transmission data when an authorized user access through an external IT entity such as a web browser.

A. Timestamp

Trusted time must be provided for the time referenced by the TOE.

4 Security Objectives

The following security objectives for the operational environment are security objectives that must be addressed by the technical and procedural means supported in the operational environment to ensure that the TOE accurately provides the security functionality.

4.1 Security Objectives for the Operational Environment

OE. Physical Control

The place where the management server among the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.

OE. Trusted Administrator

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 the administrator guidance.

OE. Log Backup

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

OE. Operation System Reinforcement

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

OE. DBMS

If audit records are stored in a DBMS installed on the identical operating system as the TOE, the identification and authentication functions of the DBMS must be used to protect against deletions or modifications by unauthorized users.

OE. Trusted path

The TOE must use an encrypted communication channel and encrypts transmission data when an authorized user access through an external IT entity such as a web browser.

OE. Timestamp

The TOE must accurately record security-related events using reliable timestamps from the TOE's operational environment.

4.2 Security Objectives Rationale

The security objectives rationale demonstrates that the stated security objectives are appropriate, sufficient to address the security problems, not excessive, and strictly necessary

The security objectives rationale demonstrates that

- Each threat, organizational security policy, and assumption is addressed by at least one security objective.
- Each security objective addresses at least one threat, organizational security policy, and assumption.
- Because assumptions are always set for the TOE operational environment, the TOE security objectives are not tracked as assumptions.

4.2.1 Rationale of Security Objectives for the Operational Environment

Security objectives Define Security problems	OE. Physical Control	OE. Trusted Admin	OE. Log Backup	OE. Operational System Reinforcement	OE. DBMS	OE. Trusted Path	OE. Time Stamp
P.Audit			X		X		
P.Secure Operation		X					
P.Password Strength		X			X		
A.Physical Security	X						
A.Authorized Administrator		X					
A.Log Backup			X				
A.Operating System Rinforcement				X			
A.DBMS					X		
A.Trusted path						X	
A.Timestamp							X

P.Audit

P. Auditing is performed by OE.Timestamps.

OE.Timestamps store audit records using trusted time information provided by the operating system.

P.Secure operation

P.Secure operation is performed by OE.Trusted administrator.

The trusted administrator performs all security management of the TOE and ensures that the administrator operates the TOE according to the organizational security policy and operational guidance.

A.Physical Control

A.Physical Control is supported by OE.Physical control.

OE. Physical control places the TOE in a location equipped with protective facilities and controls access to ensure that only authorized users can access it.

A.Log backup

A.Log backup is performed by OE.LogBackup.

OE.LogBackup performs regular audit trail backups to ensure that audit trails are not exhausted by periodically scanning the audit data store for audit trail loss.

A.Operation System Reinforcement

A.Operation System Reinforcement is supported by OE.Operating System Enforcement.

OE.Operation System Reinforcement ensures that the TOE's authorized administrator reinforce against the latest vulnerabilities of the operating system on which TOE is installed and operates, to ensure the reliability and safety of the operating system.

A.DBMS

A.DBMS is performed by OE.DBMS.

OE.DBMS stores audit records in a DBMS installed on the identical operating system as the TOE, the identifications and authentication functions of the DBMS must be used to protect against deletions or modifications by unauthorized users.

A.Trusted path

A.Trusted path is performed by OE.Trusted path.

OE.Trusted path must use an encrypted communication channel and encrypts transmission data during the management access through a web browser.

A.Timestamp

A.Timestamp is performed by OE.Timestamp.

OE.Timestamp provides time information to the TOE using trusted time information provided by the operating system.

5 Extended Components Definition

This chapter describes the components of the Security Target that are extended upon in Part 2 or 3 of the Common Criteria.

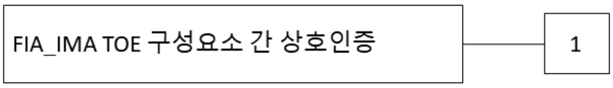
5.1 Identification & Authentication (FIA)

5.1.1 TOE Internal Mutual Authentication

Family Behavior

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

Component Leveling



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

Management: FIA_IMA.1

There are no management activities foreseen

Audit: FIA_IMA.1

When the FAU_GEN security audit data generation family is included in a protection profile/security Target, it is recommended that the following actions be audit recorded

a) Minimal: Success and failure of mutual authentication

5.1.1.1 FIA_IMA.1 TOE Internal Mutual Authentication

Hierarchical to	No other components
Dependencies	No dependencies

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

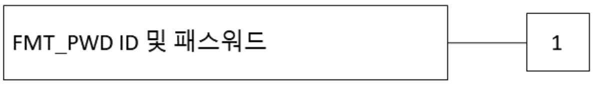
5.2 Security Management (FMT)

5.2.1 ID and password

Family Behavior

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

Component Leveling



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

Management: FMT_PWD.1

The following management function can be considered for FMT

a) Management of ID and password 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

5.2.1.1 FMT_PWD.1 ID and Password Management

Hierarchical to No other components

Dependencies FMT_SMF.1 Specification Management Function
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].

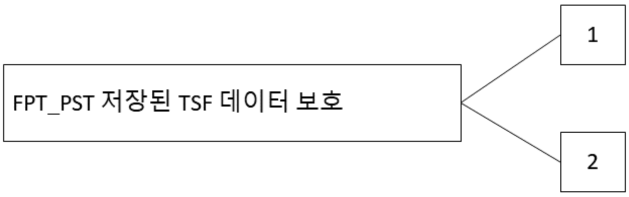
5.3 Protection of the TSF (FPT)

5.3.1 Protection of Stored TSF Data

Family Behavior

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

Component Leveling



FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored incontainers controlled by the TSF
FPT_PST.2 Availability protection of Stored 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 audit events foreseen

5.3.1.1 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].

5.3.1.2 FPT_PST.2 Availability Protection of Stored 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].

6 Security requirements

This section describes the functional and assurance requirements that must be satisfied by the TOE.

This Security Target uses the evaluation methods/evaluation activities defined in <6.2.1 Security Target Evaluation>, and there are no additional evaluation methods and evaluation activities.

All subjects, objects, operations, security attributes, etc. used in the security requirements of this Security Target are defined as follows [Table 6-1].

[Table 6-1] Definition of subjects, objects and their associated security attributes and operations

Subjects (user)	Subject (user) Security Attributes	Objects (Information)	Object (Information) Security Attributes	Operations
Authorized administrator	ID, Password, IP	Audit Data	-	Read, Backup
		TSF Data	-	Change defaults, Query, Modification, Delete, Create, Backup
		Security Attributes	-	Change defaults, Query, Modification, Delete, Create
Authorized user (Document User)	ID, Department, Document permissions	Electronic document	Document program, Document type	View, Save, Manual encryption, Manual decryption
		Process	Process name	Clipboard

6.1 Security Functional Requirements

The security functional requirements defined in this Security Target are expressed by selecting relevant security functional components from CC Part 2 to satisfy the security objectives identified in Chapter 4. The following Table 6-2 summarizes the security functional components used in this Security Target.

[Table 6-2] Security Functional Requirements

Security Function	Security Functional Components

Class		
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.	Action in case of Possible Audit Data Loss
	FAU_STG.5	Prevention of Audit Data Loss
FCS	FCS_CKM.1(1)	Cryptographic Key Generation (Electronic document encryption)
	FCS_CKM.1(2)	Cryptographic Key Generation (TSF data encryption - TOE Server)
	FCS_CKM.1(3)	Cryptographic Key Generation (TSF data encryption - TOE Agent)
	FCS_CKM.1(4)	Cryptographic Key Generation (TSF data encryption - Communication)
	FCS_CKM.2	Cryptographic key Distribution
	FCS_CKM.6	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic operation (Electronic document encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF Data - TOE Server)
	FCS_COP.1(3)	Cryptographic operation (TSF Data - TOE Agent)
	FCS_COP.1(4)	Cryptographic operations (TSF Data - Communication)
	FCS_RBG.1	Random Bit Generation (RBG)
	FCS_RBG.3	Random Bit Generation (Internal seeding - single source)
FDP	FDP_ACC.1(1)	Subset Access Control (Electronic document encryption access control)
	FDP_ACC.1(2)	Subset Access Control (Electronic document usage access control)
	FDP_ACF.1(1)	Subset Control Based on Security Attributes (Electronic document encryption access control)
	FDP_ACF.1(2)	Subset Control Based on Security Attributes (Electronic document usage access control)
FIA	FIA_AFL.1	Authentication Failures Handling
	FIA_IMA.1 (Extended)	TOE Internal mutual authentication

	FIA_SOS.1	Verification of Secrets
	FIA_UAU.1	Authentication
	FIA_UAU.2	Timing of Authentication
	FIA_UAU.4	Single-use Authentication mechanisms
	FIA_UAU.7	Protected Authentication feedback
	FIA_UID.1	Identification
	FIA_UID.2	Timing of Identification
FMT	FMT_MOF.1	Management of Security Functions behavior
	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	Management Functional Specification
	FMT_SMR.1	Security Roles
FPT	FPT_FLS.1	Secure State Maintenance in case of failure
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_PST.1 (Extended)	Basic Protection of Stored TSF Data
	FPT_PST.2 (Extended)	Availability Protection of Stored TSF Data
	FPT_RCV.2	Automated Recovery
	FPT_TST.1	TSF Testing
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.1	TSF – Initiated Session Locking
	FTA_SSL.3	TSF – Initiated Termination
	FTA_TSE.1(1)	TOE Session Establishment
	FTA_TSE.1(2)	TOE Session Establishment
FTP	FTP_ITC.1	Inter-TSF Trusted Channel

6.1.1 Security Audit (FAU)

6.1.1.1 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 [assignment: list of actions] upon detection of a potential security violation.

[Table 6-3] Potential Security Violation Response Actions

Security Component	Timing	Potential Security Violation	Response Actions
FAU_STG.4	Audit trail storage exceeded 90%	Anticipated audit data loss event	- Notify the administrator via their registered email about the potential violation analysis event
FAU_STG.5	Audit trail storage exceeded 95%	Prevented audit data loss event	- Notify the administrator via their registered email about the potential violation analysis event - Overwrite the oldest audit record.
FPT_TST.1	Operation/Cycle	TOE Server testing, integrity violation audit event, and testing failure event for a validated cryptographic module	- Notify the administrator via their registered email about the potential violation analysis event
	Operation/Cycle	TOE Agent testing failure event, testing failure event for validated a cryptographic module	- After the next run is completed, notify the administrator via their registered email about the potential violation analysis event. - Stopping the program from running
	Operation/Cycle	TOE Agent integrity violation audit event	- After a successful automated recovery, notify the administrator via their registered email about the potential violation analysis event. - If the automated recovery fails, notify the administrator via their registered email about the potential violation analysis event after the next run is completed.

6.1.1.2 FAU_GEN.1 Audit Data Generation

Hierarchical to None

Dependencies FPT_STM.1 Reliable time stamps

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

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

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

c) [assignment: other specifically defined audit events]

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

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

b) For each audit event type, based on the audit event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

[Table 6-4] Audit Events and Additional Audit Log Contents

Security Functional Components	Audit events	Additional Audit Information
FAU_STG.5	Response actions and results (success, failure) when audit saving fails	-.
FCS_CKM.1	Cryptographic key generation failure	-.
FCS_COP.1	Cryptographic operation failure (per cryptographic function, such as document encryption failure, encrypted communication failure, file encryption failure, etc.)	-.
FDP_ACF.1	Successful request to perform operations on objects covered by the document encryption and decryption access control SFP	Identifying information about the object
FIA_AFL.1	Response actions and results (success, failure) when user authentication attempt threshold is reached	-.
FIA_UAU.1	User login success or failure	-.
FIA_UAU.4	Authentication failure due to detection of attempts to reuse of credentials	-.
FMT_MOF.1	All changes of the ["List of Security Functions" in Table 6-25, "Security Functions"] as specified in FMT_MOF.1.1	Changed security attribute data
FMT_MTD.1	User registration, deletion, change, and authorization history (admin history)	-.
	All changes of the password	-.
	TOE agent startup and registration status changes	-.
	All changes related to '[Table 6-27] TSF Data List' as	Changed TSF data

	specified in FMT_MTD.1.1	
FMT_PWD.1	All changes of the default account (ID), password	-.
FPT_TST.1	TOE server testing and results (success, failure)	Failed security features
	Integrity verification on TOE components and results (success, failure)	Components whose integrity verification failed, the number of files checked, and a list of failures.
FTA_MCS.2	Denial of new sessions based on the limit on the number of concurrent sessions	-.
	Response actions when detecting duplicate logins from the same account	
	Blocking duplicate access and results (success, failure)	
FTA_SSl.1	User's session locking and the result (success, failure)	-.
FTA_SSL.3	User's session termination and the result (success, failure)	-.
FTA_TSE.1	Blocking IP access to management terminals	-.
Other	User logout success or failure	-.
	Start and shutdown the TOE audit function	-.

6.1.1.3 FAU_SAA.1 Potential Violation Analysis

Hierarchical 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 known [FPT_TST.1 audit events of integrity violationes and failed testing of validated cryptographic module and failed testing, FAU_STG.4 audit incremental storage usage anticipated to exceed 90%, FAU_STG.5 audit incremental storage saturation]

b) [None]

6.1.1.4 FAU_SAR.1 Audit Review

Hierarchical No other components

Dependencies FAU_GEN.1 Audit Data Generation

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

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

6.1.1.5 FAU_SAR.3 Selectable Audit Review

Hierarchical to No other components

Dependencies FAU_SAR.1 Audit Review

FAU_SAR.3.1 The TSF must provide the ability to apply ["Methods of selection and/or ordering" in [Table 6-5]] to audit data based on ["Criteria with Logical Relations" in [Table 6-5]]**.**

[Table 6-5] Criteria based on audit data type

Audit data Type	Criteria with Logical Relations	Methods of selection and/or ordering
Document Encryption History	- Department / User && - Document name - Document path && - Encryption date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (timestamp)
Document Decryption History	- Department / User && - Document name - Document path && - Encryption date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (timestamp)

Document Viewing History	- Department / User && - Document name - Document path && - Encryption date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (timestamp)
User Sign in History	- Department / User && - Status: Multiple selections (All, Login, Logout) && - Result: Multiple selections (All, Success, Failure) && - Details (Login): Multiple selections (All, Successful Login, Password mismatch, Login attempt with nonexistent account, Login attempt while locked, Reuse of credentials, Agent-User information mismatch|| - Details (Logout): Multiple selections (All, Logout) || - Access date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (access date)
User Account Lockout History	- Department / User && - Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (timestamp)
PC Installation/Deletion History	- Department / User && - Status: Multiple selections (All, Install, Delete) - Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, set period) &&	Inquiry, Sort (timestamp)
Admin History	- Category: Multiple selections (All, Admin, Organizational chart, PC management, Policy, Other) && - Sub-Category : Multiple Selections (Change policy, Batch policy change, Create policy, Modify policy (Set policy), Modify policy (Policy management), Delete policy, Add sub-department, Change department name, Move department, Delete department, Add user, Modify user, Move user to another department, Delete user, Delete agent, Add access allowed IP, Delete access allowed IP, Set smtp account information, Set admin email notification, Change default password, Change ID and password, Login success, Login failure, Duplicate	Inquiry

	Login attempt, Logout, Logout due to duplicate login, Logout due to session expiration, ID block, Account lock, Account unlock) &&	
Integrity Verification History	- Department / User && - Category: Multiple selections (All, Server, Agent) && - Result: Multiple selections (All, Success, Failure, Recovery) && - Success Failure Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort by (date)
Testing History	- Department / User && - Category: Multiple selections (All, Server, Agent) && - Result: Multiple selections (All, Success, Failure, Recovery) && - Target && - Success Failure Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort by (date)
Audit Function Start/Shutdown History	- Department / User && - Category: Multi-Select (Policy, Server, Agent) - Start/Shutdown separation: Single selection (All, Start, End) && - Access date (Today, Yesterday, Last week, Last week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort by (date)
Audit Threshold Exceeded Response History	- Deletion date (Today, Yesterday, Last week, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (entire column)
Email Sending History	- Category: Multiple selections (Server integrity failure notification, Agent integrity failure notification, Server testing failure notification, Agent testing failure	Inquiry, Sorting (date sent, content,

	notification, Threshold exceeded notification, Admin login lock notification, User login lock notification) &&	recipient)
Failure in Cryptographic key Generation History	- Departments / Users && - Category: Multiple selections (All, Server, Agent) && - Failure date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort by (date)
Failure in Password Operations History	- Departments / Users && - Category: Multiple selections (All, Server, Agent) && - Failure date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort by (date)
(*Legend: The && symbol above means "and" and the || symbol means "or" condition)		

6.1.1.6 FAU_STG.4 Action in case of Possible Audit Data Loss

Hierarchical to No other components

Dependencies FAU_STG.2 Protected of Audit Trail Storage

FAU_STG.4.1 The TSF shall [send an alert email to authorized administrators] when the audit data store exceeds [disk usage (90%) where TOE Server is installed].

6.1.1.7 FAU_STG.5 Prevention of Audit Data Loss

Hierarchical to FAU_STG.4 Action in case of Possible Audit Data Loss

Dependencies FAU_STG.2 Protected of Audit Trail Storage

FAU_STG.5.1 The TSF shall *overwrite the oldest audit record* and [send a warning mail to authorized administrators] if the audit data store is saturated.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1(1) Cryptographic key Generation (document encryption)

Hierarchical to None

Dependencies [FCS_CKM.2 Cryptographic Key Distribution or
FCS_CKM.5 Cryptographic key Derivation or
FCS_COP.1 Cryptographic Operations]

[FCS_RBG.1 Random Bit Generation or
FCS_RNG.1 Random Bit Generation]]
FCS_CKM.6 Cryptographic key Destruction

FCS_CKM.1.1 The TSF shall generate **data cryptographic keys (DEK)** in accordance with **a** specified cryptographic key generation algorithm ["Cryptographic key generation algorithm" in [Table 6-6]] and specified cryptographic key sizes ["Cryptographic key sizes" in [[Table 6-6]] that meet the following ["List of standards" in [Table 6-6]].

[Table 6-6] Criteria Based on Audit Data Type

Cryptographic key	Cryptographic key generation algorithm	Cryptographic key sizes	List of standards
Document header DEK	HASH_DRBG (SHA-256)	256 bit	ISO/IEC 18031
Documentation DEK			

6.1.2.2 FCS_CKM.1(2) Cryptographic key Generation (TSF Data Encryption - TOE Server)

Hierarchical to No other components

Dependencies [FCS_CKM.2 Cryptographic Key Distribution or
FCS_CKM.5 Cryptographic key Derivation or
FCS_COP.1 Cryptographic Operations]
[FCS_RBG.1 Random Bit Generation or
FCS_RNG.1 Random Bit Generation]]
FCS_CKM.6 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 6-7]] and specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-7]] that meet the following ["List of standard" in [Table 6-7]].

[Table 6-7] TSF Data Encryption - TOE Server

Cryptographic key	Cryptographic key generation algorithm	Cryptographic key sizes	List of standards
Server KEK	PBKDF2(HMAC-SHA-256)	256 bit	TTAK.EN-12.0334
Server DEK	HASH_DRBG (SHA-256)	256 bit	ISO/IEC 18031
Server Asymmetric Key	RSAES (SHA-256)	2048 bit	ISO/IEC 18033-2

6.1.2.3 FCS_CKM.1(3) Cryptographic key Generation (TSF Data Encryption - TOE Agent)

Hierarchical to No other components

Dependencies [FCS_CKM.2 Cryptographic Key Distribution or
FCS_CKM.5 Cryptographic key Derivation or
FCS_COP.1 Cryptographic Operation]
[FCS_RBG.1 Random Bit Generation or
FCS_RNG.1 Random Bit Generation]]
FCS_CKM.6 Cryptographic key Destruction

FCS_CKM.1.1 A TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ["Cryptographic key generation algorithm" in [Table 6-8]] and the specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-8]] that meet the following ["Standard list" in [Table 6-8]].

[Table 6-8] TSF Data Encryption - TOE Agent

Cryptographic key	Cryptographic key generation algorithm	Cryptographic key length	List of standards
Agent KEK	PBKDF2(HMAC-SHA-256)	256 bit	TTAK.EN-12.0334
Agent DEK	HASH_DRBG (SHA-256)	256 bit	ISO/IEC 18031
Agent Asymmetric Key	RSAES (SHA-256)	2048 bit	ISO/IEC 18033-2

a

6.1.2.4 FCS_CKM.1(4) Cryptographic Key Generation (TSF Data Encryption - Communication)

Hierarchical to No other components

Dependencies [FCS_CKM.2 Cryptographic Key Distribution or
FCS_CKM.5 Cryptographic key Derivation or
FCS_COP.1 Cryptographic Operation]
[FCS_RBG.1 Random Bit Generation or
FCS_RNG.1 Random Bit Generation]
FCS_CKM.6 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 6-9]] and specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-9]] that meet the following ["List of standards" in [Table 6-9]].

[Table 6-9] TSF Data Encryption - Communication

Cryptographic key	Cryptographic key generation algorithm	Cryptographic key sizes	List of standards
Agent Communication DEK	HASH_DRBG (SHA-256)	256 bit	ISO/IEC 18031

6.1.2.5 FCS_CKM.2 Cryptographic Key Distribution

Hierarchical to None

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 or
FCS_CKM.5 Cryptographic key Derivation]
FCS_CKM.3 Cryptographic key Access

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [self cryptographic key distribution method] that meet the following [none].

6.1.2.6 FCS_CKM.6 Cryptographic key Destruction

Hierarchical to None

Dependencies [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
Generate FCS_CKM.1 cryptographic key or
FCS_CKM.5 Cryptographic key Derivation]

FCS_CKM.6.1 The TSF must destroy ["Target" in [Table 6-10]] *when it is no longer needed*.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and key material specified in FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method ["Cryptographic key destruction method" in [Table 6-10]] that meet the following [none].

[Table 6-10] Cryptographic key destruction

Category	Target	Timing	Cryptographic key destruction method
Server	Server DEK	- Immediately after use	- Overwrite with 0 or 1 more

	Server Asymmetric Key	- Upon TOE shutdown	than 3 times
	Agent Communication DEK		
	Document header DEK		
	Server KEK		
	Critical security parameters		
Agent	Agent DEK		
	Agent Asymmetric Key		
	Agent Communication DEK		
	Documentation DEK		
	Agent KEK		
	Critical security parameters		
	Document headerDEK	- Immediately after use - Upon TOE shutdown - Upon TOE logout	

6.1.2.7 FCS_COP.1(1) Cryptographic Operation (Electronic 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 or
FCS_CKM.5 Cryptographic Key Derivation]
FCS_CKM.6 Cryptographic Key Destruction

FCS_COP.1.1 The TSF shall perform ["list of cryptographic operations" in [Table 6-11]] in accordance with a specified encryption algorithm ["cryptographic algorithm" in [Table 6-11]] and specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-11]] that meet the following ["List of standards" [in Table 6-11]]

[Table 6-11] List of Cryptographic Operations

List of operations	cryptographic algorithm	Cryptographic key sizes	List of standards
Document Security Header Encryption/Decryption	ARIA_CBC	256 bit	KS X 1213-1
Document Encryption/Decryption	ARIA_CTR		

6.1.2.8 FCS_COP.1(2) Cryptographic Operation (TSF Data - TOE Server)

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 or
FCS_CKM.5 Cryptographic Key Derivation]
FCS_CKM.6 Cryptographic Key Destruction

FCS_COP.1.1 The TSF shall perform ["list of cryptographic operations" in [Table 6-12]] in accordance with a specified encryption algorithm ["cryptographic algorithm" in [Table 6-12]] and specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-12]] that meet the following ["List of standards" [in Table 6-12]]

[Table 6-12] List of Cryptographic Operations

List of operations	cryptographic algorithm	Cryptographic key sizes	List of standards
Server DEK Encryption and Decryption	ARIA_CBC	256 bit	KS X 1213-1
Server private key Encryption and Decryption			
DBMS password Encryption and Decryption			
Component integrity verification	SHA-512	-.	ISO/IEC 10118-3
Admin and document user password Encryption	HMAC (SHA-256)	256 bit	ISO/IEC 9797-2

6.1.2.9 FCS_COP.1(3) Cryptographic Operation (TSF Data - TOE Agent)

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 or

FCS_CKM.5 Cryptographic Key Derivation]
FCS_CKM.6 Cryptographic Key Destruction

FCS_COP.1.1 The TSF shall perform ["list of cryptographic operations" in [Table 6-13]] in accordance with a specified encryption algorithm ["cryptographic algorithm" in [Table 6-13]] and specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-13]] that meet the following ["List of standards" [in Table 6-13]]

[Table 6-13] List of password operations

List of operations	cryptographic algorithm	Cryptographic key sizes	List of standards
AgentDEK encryption and decryption	ARIA_CBC	256 bit	KS X 1213-1
Agent private key encryption and decryption			
Agent Communication DEK Encryption			
Audit data encryption and decryption			
Component integrity verification	SHA-512	-.	ISO/IEC 10118-3

6.1.2.10 FCS_COP.1(4) Cryptographic Operation (TSF Data - Communication)

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 or
FCS_CKM.5 Cryptographic Key Derivation]
FCS_CKM.6 Cryptographic Key Destruction

FCS_COP.1.1 The TSF shall perform ["List of cryptographic operations" in [Table 6-14]] in accordance with a specified encryption algorithm ["Cryptographic algorithm" in [Table 6-14]] and specified cryptographic key sizes ["Cryptographic key sizes" in [Table 6-14]] that meet the following ["List of standards" [in Table 6-14]]

[Table 6-14] List of password operations

List of operations	cryptographic algorithm	Cryptographic key sizes	List of standards
Transmitted data Encryption and Decryption	ARIA_CBC	256 bit	KS X 1213-1
	RSAES (SHA-256)	2048 bit	ISO/IEC 18033-2
Electronic signatures generation	RSA-PSS (SHA-256)	2048 bit	ISO/IEC 14888-2

and validation			
Transmitted data integrity	SHA-512	-.	ISO/IEC 10118-3

6.1.2.11 FCS_RBG.1 Random Bit Generation (RBG)

Hierarchical to No other components

Dependencies [FCS_RBG.2 Random Bit Generation (External Seeding) or
FCS_RBG.3 Random Bit Generation (Internal Seeding - Single Source)]
FPT_FLS.1 Secure State Maintenance in case of failure
FPT_TST.1 TSF Testing)

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services after initialization using the ["Random Bit Generation (RBG) algorithm" in [Table 6-15]] according to the ["List of standards" in [Table 6-15]].

FCS_RBG.1.2 The TSF shall use the *TSF entropy source [CryptGenRandom]* for initialization and seeding.

FCS_RBG.1.3 The TSF shall update the DRBG state by *reseeding* using the *TSF entropy source [CryptGenRandom]* according to the ["List of standards" [Table 6-15]] under the following circumstance
o The following circumstance is:
- Under the condition of failure in [Noise Source Health Test]

[Table 6-15] Random Bit Generation (RBG)

List of Operations	Random Bit Generation (RBG) Algorithm	Random number sizes	List of standards
Cryptographic key generation	HASH_DRBG (SHA-256)	256 bit	ISO/IEC 18031

6.1.2.12 FCS_RBG.3 Random bit generation (internal seeding - single source)

Hierarchical to No other components

Dependencies FCS_RBG.1 Random Bit Generation (RBG)

FCS_RBG.3.1 The TSF shall be able to seed DRBG using a *TSF software-based entropy source* [CryptGenRandom] with the minimum-entropy of at least [128] bits.

6.1.3 User Data Protection (FDP)

6.1.3.1 FDP_ACC.1(1) Subset Access Control (Electronic 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 ["Access control policy" in [Table 6-16]] for the ["List of subjects", "List of objects", and "List of operations" among subjects and objects covered by SFP in [Table 6-17]].

[Table 6-16] Subset Access Control

List of subjects	List of objects	List of operations	Access control policy
Document user	Security documentation, Process	View/Save/ Manual Encryption/Manual Decryption	Document Encryption/Decryption Policy

6.1.3.2 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 ["Access control policy" in [Table 6-17]] for the ["List of subjects", "List of objects", and "List of operations" among subjects and objects covered by SFP in [Table 6-17]].

[Table 6-17] Subset Access Control

List of subjects	List of objects	List of operations	Access control policy
Document user	Process	Clipboard Copy & paste	Document Encryption/Decryption Policy

6.1.3.3 FDP_ACF.1(1) Security attribute based access control (Electronic 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 The TSF shall enforce the ["Access control policy" in [Table 6-18]] on objects based on ["List of subjects" and "List of objects" controlled by the follow SFP, appropriate "Security attribute of subjects" and "Security attribute of subjects" SFP, or group of named security attributes in [Table 6-18]].

[Table 6-18] Security Attribute Based Access Control

Access control policy	List of subjects	Security attribute of subjects	List of objects	Security attributes of Objects
Document Encryption/Decryption Policy	Document users	User ID	Security documentation, Process	Document access permissions, Document user ID, Document type, Process name

FDP_ACF.1.2 TSF shall enforce the following rules to determine whether the operations between the controlled subject and objects are allowed: [

a) The operation is allowed to be performed only if the security attribute of the subject included in the access control security attribute of the object, and the operation matches the operation security attribute of the object.

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 authorize access of the subject to objects based on the following additional rules: [none].

6.1.3.4 FDP_ACF.1(2) Security Attribute Based Access Control (Electronic 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 The TSF shall enforce the ["Access control policy" in [Table 6-19]] on objects based on ["List of subjects" and "List of objects" controlled by the follow SFP, appropriate "Security attribute of subjects" and "Security attribute of subjects" SFP, or group of named security attributes in [Table 6-19]].

[Table 6-19] Security Attribute Based Access Control

Access control policy	List of subjects	List of objects	Security attributes of Objects
Document Encryption/Decryption Policy	Document users	Process	Process name

FDP_ACF.1.2 TSF shall enforce the following rules to determine whether the operations between the controlled subject and objects are allowed: [

a) The operation is allowed to be performed only if the security attribute of the subject included in the access control security attribute of the object, and the operation matches the operation security attribute of the object.

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 authorize access of the subject to objects based on the following additional rules: [none].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication failure Handling

Hierarchical to No other components

Dependencies FIA_UAU.1 Authentication

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [user/administrator account authentication failure].

FIA_AFL.1.2 When the number of unsuccessful authentication attempts *reaches* the defined number, the TSF shall perform the ['Authentication Failure Response Actions' in Table 6-20].

[Table 6-20] Authentication Failure Response Actions

Authentication failure response action
- Time required to reactivate authentication: 5 minutes - If authentication fails consecutively for the configured number of attempts, lock the user account and send an email to the administrator

6.1.4.2 FIA_IMA.1 TOE Internal Mutual Authentication (extended)

Hierarchical to No other components

Dependencies No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication between [TOE Server and TOE Agent] by [self-implemented authentication protocol] that meet [none].

6.1.4.3 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 meets [Table 6-21]

[Table 6-21] Password combination rules

Password combination rules
- Ensure a length of at least 9 characters - Include at least one of each: a number, an uppercase letter, a lowercase letter, and a special character - Prohibit using the same password as the user account (ID) - Prohibit repeating the same letter or number more than three times consecutively - Prohibit entering more than four consecutive characters or numbers in keyboard order - Prohibit reusing the previously used password

6.1.4.4 FIA_UAU.1 Authentication

Hierarchical to No other components

Dependencies FIA_UID.1 Identification

FIA_UAU.1.1 The TSF shall allow ['List of TSF mediated actions' in [Table 6-22]] on behalf of the user to be performed before the user is authenticated.

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.

[Table 6-22] List of TSF mediated actions

User	List of TSF mediated actions
Document user	- Enter operating password, view information

6.1.4.5 FIA_UAU.2 Timing of Authentication

Hierarchical to FIA_UAU.1 Authentication

Dependencies FIA_UID.1 Identification

FIA_UAU.2.1 The TSF shall successfully authenticate the **Authorized** Administrator, on behalf of the **Authorized** Administrator, before allowing any actions mediated by the TSF

6.1.4.6 FIA_UAU.4 Single-use Authentication Mechanisms

Hierarchical to No other components

Dependencies No dependencies

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

6.1.4.7 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 ["List of authentication feedback" in [Table 6-23]] to the user while the authentication is in progress

[Table 6-23] List of Authentication feedback

Authentication feedback
- When entering a password, display "●" instead of the entered characters - No feedback is provided on the reason for failure in case of identification and authentication

failure

6.1.4.8 FIA_UID.1 Identification

Hierarchical to No other components

Dependencies No dependencies

FIA_UID.1.1 The TSF shall allow [“List of TSF mediated actions" in [Table 6-24]] on behalf of the user to be performed before the user is identified.

[Table 6-24] List of TSF-mediated actions

User	List of actions that TSF mediates
Document users	- Enter operating password, view information

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

6.1.4.9 FIA_UID.2 Identifies the user before every action

Hierarchical to FIA_UID.1 Identification

Dependencies No dependencies

FIA_UID.2.1 The TSF must successfully identify each **Authorized Administrator,** on behalf of **the Authorized Administrator**, before allowing any actions mediated by the TSF.

6.1.5 Security Management (FMT)

6.1.5.1 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 management actions*** of ["List of Security Functions" in [Table 6-25]] to [the authorized administrator]**.**

[Table 6-25] Security Functions

List of Security Functions	Action Decision	Stop	Initiate	Action Change
User registration, deletion, modification	○	-.	-.	○
Management terminal IP registration, deletion, and modification	○	-.	-.	○
Agent inquiry – status, version, applied security policy	○	-.	-.	○
Agent security policy management – policy configuration, policy transmission	○	-.	-.	○
Configuration of recipient email and SMTP connection information for email sending	○	-.	-.	○
Security function self-test of the management server upon administrator request	○	-.	-.	○
Integrity verification of the management server upon administrator request	○	-.	-.	○
TOE version information inquiry	○	-.	-.	○
Document user session lock time setting	○	-.	-.	○
Document user session lock execution/release (authentication)	○	-.	-.	○
Audit history inquiry	○	-.	-.	○

6.1.5.2 FMT_MSA.1 Management of security attributes

Hierarchical to No other components

Dependencies [FDP_ACC.1 Partial Access Control or
FDP_IFC.1 Partial Information Flow Control]
FMT_SMF.1 Management Function Specification
FMT_SMR.1 Security Roles

FMT_MSA.1.1 The TSF must shall the [*Document Encryption/Decryption Policy*] to restrict the ability to *change_default, query, modify, delete, or other operations* the ["Security Attributes" in Security Attribute Management [Table 6-26]] to [the authorized administrator].

[Table 6-26] Security Attribute Management

Policy	Security Attributes	Default values Change	Query	Change	Delete	Create
Documentat	Policy configuration (User ID)	○	-.	-.	○	○

ion Encryption/ Decryption Policy	Document access permissions (private, public)	-.	○	○	-.	-.
	File decryption permissions	-.	○	○	-.	-.
	Specify encryption targets (process, document type)	-.	○	○	-.	-.

6.1.5.3 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 [*Document Encryption/Decryption Policy*] to provide *limited* default values for security attributes used to enforce the SFP.

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

6.1.5.4 FMT_MTD.1 Management of TSF Data

Hierarchical to No other components

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FMT_MTD.1.1 The TSF shall restrict the ability to manage ["List of TSF Data " in [Table 6-27]] to [the authorized administrator].

[Table 6-27] TSF Data List

TSF Data	Query	Change	Delete	Create
Document user and department management	○	○	○	○
Document user and admin passwords	-.	○	-.	-.
Management terminal IP address	○	○	○	○
Agent inquiry	○	-.	-.	-.
Agent security policy management	○	○	○	○
TOE and TOE component identification	○	-.	-.	-.
Audit history	○	-.	-.	-.
Configuration of recipient email and SMTP connection information for email transmission	○	○	○	○

6.1.5.5 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 [change administrator ID and password, add users, modify users] to [the authorized administrator].

1. [None].
2. [None].

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [change administrator ID and password, add users, modify users] to [the authorized administrator] as follows

1. [None].
2. [None].

FMT_PWD.1.3 The TSF must provide the ability for *changing the password on initial access* to *the authorized administrator*.

6.1.5.6 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: ["List of management functions to be provided by the TSF" in [Table 6-28]]

[Table 6-28] List of Management Functions Provided by the TSF

Management features	List of management functions to be provided by the TSF
Security Functional Management	Items specified by FMT_MOF.1
Security Attribute Management	Items specified by FMT_MSA.1 and FMT_MSA.3
TSF Data Management	Items specified in FMT_MTD.1
ID and Password Management	Items specified in FMT_MTD.1

6.1.5.7 FMT_SMR.1 Security Roles

Hierarchical to None

Dependencies FIA_UID.1 Identification

FMT_SMR.1.1 The TSF must maintain the [Security Roles in [Table 6-29]]**.**

[Table 6-29] Security Roles

Role distinctions	Security Roles
Authorized administrator	- As an authorized administrator via the TOE Admin page, you can modify and manage the document encryption and decryption policy for departments or members of the organization - As an authorized administrator via the TOE Admin page, it has privileges to manage the organization chart and members, view administrator logs, configure access IP settings, and manage the agent
Document user	- A document user can change the default password for its account - A document user can enable and disable session locking

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

6.1.6 Protection of the TSF

6.1.6.1 FPT_FLS.1 Secure State Maintenance in Case of failure

Hierarchical to No other components

Dependencies No dependencies

FPT_FLS.1.1 The TSF shall maintain a secure state in the event of the following types of failures: [Failure in noise health test of random bit generator].

6.1.6.2 FPT_ITT.1 Basic Protection of Internally Transmitted TSF Data

Hierarchical to No other components

Dependencies No dependencies

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

6.1.6.3 FPT_PST.1 Basic protection of TSF data (extended)

Hierarchical to No other components

Dependencies No dependencies

FPT_PST.1.1 The TSF shall protect ["TSF Data" in Table 6-30] stored in containers controlled by the TSF from unauthorized *disclosure, modification*

[Table 6-30] Protected TSF Data

TOE Components	Safeguards	TSF data
Server	Encryption	- Data cryptographic key - DBMS connection information
	Encryption, Access control (DBMS)	- The password that TOE uses to identify and authenticate users - Cryptographic key (symmetric keys, private keys)
	Access control (DBMS)	- TOE settings (security policy, preference parameters) - Audit trail
Agent	Encryption, Access control	- Cryptographic key (symmetric keys, private keys) - TOE Configuration - Audit data

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

Hierarchical to No other components

Dependencies No dependencies

FPT_PST.2.1 The TSF shall prevent unauthorized deletion of [TOE Agent's settings, executable files, etc.].

FPT_PST.2.2 The TSF shall prevent unauthorized termination **abort** for [TOE Agent's process, service].

6.1.6.5 FPT_RCV.2 Automated Recovery

Hierarchical to FPT_RCV.1 Manual Recovery

Dependencies AGD_OPE.1 Operational User Guidance

FPT_RCV.2.1 When automated recovery from [None] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2 The TSF shall use automated procedures for [Information Tampering with the TOE Document Encryption Agent] to ensure that the TOE is returned to a secure state.

6.1.6.6 FPT_TST.1 TSF Testing

Hierarchical to No other components

Dependencies No dependencies

FPT_TST.1.1 The TSF shall run the following testing [Validated cryptographic module testing, TOE Key Process Test] *at startup and periodically during regular operation* to demonstrate the proper operation of *the TSF.*

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*TOE configuration values (policy, preferences*)].

FPT_TST.1.3 The TSF shall provide authorized users with the ability to verify the integrity of the [*TOE itself (Eecutable file, FIlter driver)*].

6.1.7 TOE Access

6.1.7.1 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 Identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions belonging to the same user according to the rules [Limiting the maximum number of concurrent sessions for 1 user who have the same privilege and the same user; {Rules on the maximum number of concurrent sessions for the same user that prohibit concurrent connections of management access and local access sessions}].

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

6.1.7.2 FTA_SSL.1 TSF-Initiated Session Locking (document user)

Hierarchical to No other components
Dependencies FIA_UAU.1 Authorization

FTA_SSL.1.1 The TSF shall lock the interactive document user sessions after [time interval of user inactivity (default 5 minutes, set from 5 minutes to 24 hours)] by:

a) Clearing or overwriting display devices, making the current contents unreadable
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require [*user re-authentication before unlocking the session*] *before unlocking session*.

6.1.7.3 FTA_SSL.3 TSF-Initiated Termination (administrator)

Hierarchical to No other components
Dependencies FMT_SMR.1 Security Roles

FTA_SSL.3.1 The TSF shall terminate interactive administrator sessions after [10 minutes of inactivity].

6.1.7.4 FTA_TSE.1(1) TOE Session Establishment

Hierarchical No other components
Dependencies No dependencies

FTA_TSE.1.1 The TSF shall be able to deny **management access session** establishment based on [access IP, *[whether the management access session is enabled for the same account*].

6.1.7.5 FTA_TSE.1(2) TOE Session Establishment

Hierarchical to No other components

Dependencies No dependencies

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**User PC IP address, User PC MAC address**].

6.1.8 Trusted path/Channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to No other components

Dependencies No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*Trusted IT Product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*email notification*].

6.2 Assurance requirements

The assurance requirements of this Security Target are composed of assurance components from Part 3 of the CC and have an evaluation assurance level of EAL1+. [Table 6-31 Assurance Requirements summarizes the assurance components].

[Table 6-31] Assurance Requirements

Assurance Classes	Assurance Components	
Security Target Evaluation	ASE_INT.1	Security Target Introduction
	ASE_CCL.1	Conformance Claim
	ASE_SPD.1	Definition of Security problems
	ASE_OBJ.1	Security objectives for operational environment
	ASE_ECD.1	Extended Components Definition
	ASE_REQ.1	Direct Evidence Security Requirements
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Documentation	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Scope
Tests	ATE_FUN.1	Functional Testing
	ATE_IND.1	Independent Testing: Functional Verification
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

6.2.1 Security Target Evaluation

ASE_INT.1 **Introduction to the Security Target**

Dependencies No dependencies

Developer action elements

ASE_INT1.1D The developer shall provide an ST introduction.

Content and presentation elements

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

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

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

ASE_INT.1.4C The TOE overview shall 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 the non-TOE equivalent required by the TOE.

ASE_INT.1.7C For multi-assurance ST, the TOE overview shall describe the TSF configuration with respect to in the sub-TSF defined in the PP-synthesis to which the ST declares conformance.

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

ASE_INT.1.9C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

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

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

ASE_CCL.1 Conformance Claims

Dependencies ASE_INT.1 ST Introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated Security Requirements

Developer action elements

ASE_CCL.1.1D The developer must provide a conformance claim

ASE_CCL.1.2D The developer must 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 321) as either CC Part 3 conformant or CC Part 3 extended.

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

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

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

ASE_CCL.1.7C The conformance claim shall describe the conformance of the ST to the PP as PP-conformant.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the TOE type of the ST is consistent with the TOE type of the PP-synthesis or PP, which conformance is being claimed by the ST.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of the ST's security problem definition is consistent with the description of the security problem definition in the PP-synthesis22), PP, and function packages, which conformance is being claimed by the ST.

ASE_CCL.1.10C The conformance claim rationale must demonstrate that the statement of the security objectives of the ST is consistent with the statement of the security objectives of the PP-synthesis23), PP, and function packages, which conformance is being claimed by the ST.

ASE_CCL.1.11C The conformance claim rationale shall demonstrate that the statement of the security requirements of the ST is consistent with the statement of the security requirements of the PP-synthesis24) or PP, which conformance is being claimed by the ST.

ASE_CCL.1.12C The conformance claim for PP(s) or PP-synthesis shall be exact conformance, strict conformance, or demonstrable conformance, or a list of conformance types.

ASE_CCL.1.13C If the conformance claim identifies a set of evaluation methods and evaluation activities derived from a CEM work unit that shall be used for the TOE evaluation, this set shall include all those contained in the package, PP, or PP-module of a PP-synthesis that the ST declares conformance with, and no others are allowed.

Evaluator action elements

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

ASE_SPD.1 Security Problem Definition

Dependencies No dependencies

Developer action elements

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of threat sources, assets, and malicious action.

ASE_SPD.1.3C The security problem definition shall describe the OSP.

ASE_SPD.1.4C The security problem definition shall state assumptions about the TOE operational environment.

Evaluator action elements

ASE_SPD.1.1E The evaluator must verify that the information provided satisfies all evidence requirements.

ASE_OBJ.1 Security Objectives for the Operational Environment

Dependencies ASE_SPD.1

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of the security objectives for the operational environment.

ASE_OBJ.1.2D The developer shall provide a security objectives rationale for the operational environment.

Content and presentation elements

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

ASE_OBJ.1.2C The security objectives rationale shall trace each security objective for the operational environment to the threats addressed by the security objective, the OSP performed by the security objective, and the assumptions supported by the security objective.

ASE_OBJ.1.3C The security objectives rationale shall demonstrate that the security objective for the production environment supports all assumptions.

Evaluator action elements

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

ASE_ECD.1 Extended Components Definition

Dependencies No dependencies

Developer action elements

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

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

Content and presentation elements

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

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

ASE_ECD.1.3C The extended component definition shall describe how each extension component is related to 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 component shall consist of measurable and objective elements to demonstrate conformance with each element.

Evaluator action elements

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

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

ASE_REQ.1 Stated Security Requirements

Dependencies ASE_ECD.1 Extended Component Definition
ASE_OBJ.1 Security Objectives for the Operational Environment

Developer action elements

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

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

Content and presentation elements

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

ASE_REQ.1.2C For a single-assurance ST, the Security Requirement statement shall define a global set of a SAR that apply to the entire TOE. The set of SAR shall be consistent with the PP or PP-synthesis to which the ST declares conformance.

ASE_REQ.1.3C For multi-assurance ST, the security requirements Statement must define a global set of the SAR that apply to the entire TOE and a set of SAR that apply to the sub-TSF. The set of SAR must be consistent with the multi-assurance PP-synthesis to which the ST declares conformance.

ASE_REQ.1.4C 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.1.5C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.6C All operations shall be performed correctly.

ASE_REQ.1.7C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.8C The security requirements rationale must trace each SFR to the threats addressed by the SFR and the OSPs performed by the SFR.

The security requirements rationale should demonstrate that the SFR addresses all threats to the TOE (along with security objectives for the operational environment).

ASE_REQ.1.9C The security requirements rationale shall demonstrate that the SFR performs all OSP for the TOE (with security objectives for the operational environment).

ASE_REQ.1.10C The security requirements rationale shall explain why the SAR was selected.

ASE_REQ.1.11C The statement of security requirements shall be internally consistent.

ASE_REQ.1.12C If an ST defines a set of SAR that extends the SAR set of PP or PP-synthesis to which it claims conformance, the security requirements rationale shall include a security requirements rationale that justifies the consistency of the extension and provides the rationale for the treatment of the evaluation methods and evaluation activities identified in the conformance methods affected by the extension of the SAR set.

Evaluator action elements

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

ASE_TSS.1 TOE Summary Specification

Dependencies ASE_INT.1 ST Introduction
ASE_REQ.1 Stated Security Requirements
ADV_FSP.1 Basic Functional Specification

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

6.2.2 Development

ADV_FSP.1	**Basic Functional Specification**
Dependencies	No dependencies

Developer action elements

ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit 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.

6.2.3 Guidance Documents

AGD_OPE.1	**Operational User Guidance**
Dependencies	ADV_FSP.1 Basic Functional Specification

Developer action elements

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

Content and presentation elements

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

accessible functions and privileges that 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 describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

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

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

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

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

Evaluator action elements

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

AGD_PRE.1 Preparative Procedures

Dependencies No other components

Developer action elements

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

Content and presentation elements

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

AGD_PRE1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

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

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

6.2.4 Life-cycle Support

ALC_CMC.1 Labeling of the TOE

Dependencies ALC_CMS.1 TOE CM Coverage

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

ALC_CMS.1 TOE CM Coverage

Dependencies No dependencies

Developer action elements

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

Content and presentation elements

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

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

Evaluator action elements

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

6.2.5 Tests

ATE_FUN.1 **Functional Testing**

Dependencies ATE_COV.1 Evidence coverage

Content and presentation 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.

Evaluator action elements

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

ATE_FUN.1.2C The test plans shall identify the 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 requirements

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

ATE_IND.1 **Independent Testing - Functionality Verification**

Dependencies ADV_FSP.1 Basic Functional Specification
AGD_OPE.1 User Operational Guidance
AGD_PRE.1 Preparative Procedures

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

6.2.6 Vulnerability Evaluation

AVA_VAN.1 Vulnerability Survey

Dependencies ADV_FSP.1 Basic Functional Specification
AGD_OPE.1 User Operations 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 Basic attack potential.

6.3 Security Requirements Rationale

6.3.1 Rationale of Security Functional Requirements

The Rationale of Security Functional Requirements demonstrates the following

- Each SFR is addressed by a threat or OSP to at least one TOE.

[Table 6-32] shows the correspondence between SFR and threats or OSP.

[Table 6-32] Security Functional Requirements and Threat and/or OSP Response

Threats and/or OSPs SFR	Threats														OSP		
	T.SEK	T.UIL	T.DA	T.BAC	T.RF	T.BA	T.BDU	T.SS	T.CAA	T.CI	T.AIS	T.TDLC	T.SDC	T.WP	P.A	P.SO	P.PS
FAU_ARP.1																X	
FAU_GEN.1															X		
FAU_SAA.1															X		
FAU_SAR.1															X		
FAU_SAR.3															X		
FAU_STG.4					X										X		
FAU_STG.5					X										X		
FCS_CKM.1(1)		X															
FCS_CKM.1(2)		X															
FCS_CKM.1(3)		X															
FCS_CKM.1(4)												X					
FCS_CKM.2	X																
FCS_CKM.6	X																
FCS_COP.1(1)		X															X
FCS_COP.1(2)		X															X
FCS_COP.1(3)		X															X
FCS_COP.1(4)												X					X
FCS_RBG.1		X															
FCS_RBG.3		X															
FDP_ACC.1(1)				X													
FDP_ACC.1(2)				X													
FDP_ACF.1(1)				X													
FDP_ACF.1(2)				X													
FIA_AFL.1									X								

FIA_IMA.1 (Extended)								X									
FIA_SOS.1														X			
FIA_UAU.1							X										
FIA_UAU.2						X											
FIA_UAU.4						X	X										
FIA_UAU.7										X							
FIA_UID.1							X										
FIA_UID.2						X											
FMT_MOF.1																X	
FMT_MSA.1																X	
FMT_MSA.3																X	
FMT_MTD.1																X	
FMT_PWD.1 (extended)														X			
FMT_SMF.1																X	
FMT_SMR.1																X	
FPT_FLS.1		X															
FPT_ITT.1												X					
FPT_PST.1 (Extended)													X				
FPT_PST.2 (Extended)			X														
FPT_RCV.2			X														
FPT_TST.1													X			X	
FTA_MCS.2						X	X										
FTA_SSL.1							X										
FTA_SSL.3						X											
FTA_TSE.1(1)						X											
FTA_TSE.1(2)							X										
FTP_ITC.1												X					

T. SEK: T. Stealing Cryptographic key
T. UIL: T. Unauthorized Information Leakage
T. DA: T. Disabling Agent
T. BAC: T. Bypassing Access Control
T. RF: Record Failure
T. BA: T. Bypassing Administrator
T. BDU: T. Bypassing Document User

T. SS: T. Server Spoofing
T. CAA: T. Continuous Authentication Attempts
T. CI: T. Credential Inference
T. AIS: T. Accessing Idle Session
T. TDLC: T. Transmitted Data Leakage and Corruption
T. SDC: T. Stored Data Corruption
T. WP: T. Weak Password
P. A: P. Audit
P. SO: P. Secure Operation
P. PS: P. Password Strength

FAU_ARP.1 Security Alarms

FAU_ARP.1 Security alarms correspond to P.Secure Operation.

This component supports P.Secure Operation by providing security alarms when potential security violationes detected.

FAU_GEN.1 Audit Data Generation

FAU_GEN.1 Audit Data Generation corresponds to P.Audit.

This component supports P.Audit by providing the ability to generate audit data for all security-related events for the date of the event, the type of event, the identity of the subject, and the result of the event.

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1 Potential Violation Analysis corresponds to P.Audit.

This component supports P.Audit by providing the function to analyze security violationes by examining audit events.

FAU_SAR.1 Audit Review

FAU_SAR.1 Audit Review corresponds to the P.Audit.

This component supports P.Audit by providing the function for the authorized administrator to review all audit data.

FAU_SAR.3 Selectable Audit Review

FAU_SAR.3 Selectable Audit Review corresponds to P.Audit.

This component supports P.Audit by providing the function to search and sort the required audit data according to the criteria you set.

FAU_STG.4 Action in case of Possible Audit Data Loss

FAU_SAR.4 Action in case of Possible Audit Data Loss is anticipated correspond to P.Audit.

This component supports P.Audit by providing notifications when audit attestations are anticipated to be lost.

FAU_STG.5 Prevention of Audit Data Loss

FAU_SAR.5 Prevention of Audit Data Loss corresponds to P.Audit.

This component supports P.Audit by providing the function to delete existing data and store new audit data when the audit store is saturated.

FCS_CKM.1(1) Cryptographic key Generation (document encryption)

FCS_CKM.1(1) Cryptographic key Generation (document encryption) corresponds to T.Unauthorized Information Leakage.

This component provides the function to securely generate the cryptographic key for document encryption, eliminating T.Unauthorized Information Leakage.

FCS_CKM.1(2) Cryptographic key Generation (TSF Data Encryption - TOE Server)

FCS_CKM.1(2) Cryptographic key Generation (TSF data encryption - TOE Server) corresponds T.Stored Data Corruption.

This component provides the function to securely generate the cryptographic key for TSF data (TOE-Server) encryption, thereby reducing T.Stored Data Corruption.

FCS_CKM.1(3) Cryptographic key Generation (TSF Data Encryption - TOE Agent)

FCS_CKM.1(3) Cryptographic key Generation (TSF data encryption - TOE Agent) correspnds to T.Stored data corruption.

This component provides the function to securely generate the cryptographic key for TSF data (TOE-Agent) encryption, thereby reducing T.Stored Data Corruption.

FCS_CKM.1(4) Cryptographic key Generation (TSF Data Encryption - Communication)

FCS_CKM.1(4) Cryptographic key Generation TSF data encryption - communication) corresponds to T.Transmistted data leakage and corruption.

This component provides the function to securely generate the cryptographic key for TSF data (communication) encryption, thereby reducing the T.Transmitted Data Leakage and Corruption.

FCD_CKM.2 Cryptographic key Distribution

FCS_CKM.2 Cryptographic key Distribution corresponds to T.Stealing Cryptographic key.

This component eliminates T.Stealing Cryptographic Key by providing the ability to securely distribute the cryptographic key.

FCS_CKM.6 Cryptographic key Destruction

FCS_CKM.6 Cryptographic key Destruction correspond to T.Stealing Cryptographic key.

This component reduces T.Unauthorized information leakage, T.Transmitted Data Leakage and Corruption, and T.Storede data corruption by providing a function to safely destroy used the cryptographic key.

FCS_COP.1(1) Cryptographic Operation (Document Encryption)

FCS_COP.1(1) Cryptographic operation (document encryption) correspond to T.Unauthorized Information Leakage and P.Password Strength.

This component provides the function to encrypt documents, eliminating T.Unauthorized Information Leakage and supporting P.Password Strength.

FCS_COP.1(2) Cryptographic Operation (TSF Data - TOE Server)

FCS_COP.1(2) cryptographic operation (TSF data - TOE Server) correspond to T.Stored Data Corruption and P.Password Strength.

This component provides the function to encrypt TSF data (server data), which reduces T.data corruption at rest and supports P.Password Strength.

FCS_COP.1(3) Cryptographic Operation (TSF Data - TOE Agent)

FCS_COP.1(3) Cryptographic operation (TSF data - TOE Agent) correspond to T.Stored Data Corruption and P. Password Strength.

This component provides the function to encrypt TSF data (agent data), which reduces T.Stored Data Corruption and supports P-cipher strength.

FCS_COP.1(4) Cryptographic Operation (TSF Data - Communication)

FCS_COP.1(4) Cryptographic operation (TSF data - communication) correspond to T.Transmission Data Leakage and Corruption, and P. Password Strength.

This component provides the function to encrypt TSF data (communication data) to reduce transmission data leakage and corruption and support password strength.

FCS_RBG.1 Random Bit Generation (RBG)

FCS_RBG.1 Random Bit Generation (RBG) corresponds to T.Unauthorized Information Leakage.

This component eliminates T.Unauthorized Information Leakage by providing the function to securely generate random numbers used to generate the cryptographic key.

FCS_RBG.3 Random Bit Generation (Internal Seeding - Single Source)

FCS_RBG.3 Random Bit Generation (Internal Seeding - Single Source) is T.Unauthorized Information Leakage.

This component eliminates T.Unauthorized Information Leakage by providing the function to securely generate random numbers used to generate the cryptographic key.

FDP_ACC.1(1) Subset Access Control (document encryption access control)

FDP_ACC.1(1) Subset access control (document encryption access control) corresponds to T.Bypassing Access Control.

This component performs encryption on documents, eliminating T.Bypassing Access Control.

FDP_ACC.1(2) Subset Access Control (document usage access control)

FDP_ACC.1(2) Subset access control (document usage access control) corresponds to T.Bypassing Access Control.

This component eliminates T.Bypassing Access Control by controlling the clipboard while the document is in use.

FDP_ACF.1(1) Security attribute based access control (Document Encryption Access Control)

FDP_ACF.1(1) Security attribute based access control (document encryption access control) is countered by T.Bypassing Access Control.

This component performs encryption on documents, eliminating T.Bypassing Access Control.

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

FDP_ACF.1(2) Security attribute based access control (document usage access control) corresponds to T.Bypassing Access Control.

This component eliminates T.Bypassing Access Control by controlling the clipboard while the document is in use.

FIA_AFL.1 Authentication Failure Handing

FIA_AFL.1 Authentication Failure Handling corresponds to T.Continuous Authentication Attempts.

This component eliminates T.Continuous Authentication Attempts by notifying users of failed login attempts and blocking login attempts.

FIA_IMA.1 (Extended) TOE Internal mutual authentication

FIA_IMA.1 (Extended) TOE Internal mutual authentication corresponds to T.Server Spoofing.

This component provides mutual authentication between user agent servers to eliminate T.Server Spoofing.

FIA_SOS.1 Verification of secrets

FIA_SOS.1 Verification of secrets corresponds to the T.Weak Password.

This component reduces T.Weak password passwords by enforcing rules for user passwords.

FIA_UAU.1 Authentication

The FIA_UAU.1 Authentication corresponds to the T.Bypassing Document Users.

This component provides user identification and authentication, eliminating the T.Bypassing

Document Users.

FIA_UAU.2 Timing of Authentication

FIA_UAU.2 Timing of Authentication correspond to the T.Bypassing Administrator.

This component provides administrator identification and authentication, thus eliminating the T.Bypassing Administrator.

FIA_UAU.4 Single-use Authentication Mechanisms

FIA_UAU.4 Anti-reuse Authentication Mechanisms correspond to the T.Bypassing Administrator and T.Bypassing Document Users

This component provides a timestamp on user credentials to remove T.Bypassing Administrator and T.Bypaasing document user references.

FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7 Protected Authentication Feedback corresponds to T.Credential Inference.

This component controls information about user authentication feedback to reduce T.Credential Inference.

FIA_UID.1 Identification

FIA_UID.1 Identification corresponds to the T.Bypassing Document Users.

This component provides user identification and authentication, eliminating the T.Bypassing Document Users.

FIA_UID.2 Timing of Identification

FIA_UID.2 Timing of identification corresponds to the T.Bypassing Administrator.

This component provides administrator identification and authentication, thus eliminating the T.Bypassing Administrator.

FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1 Security function management corresponds to the P.Secure operation.

This component supports secure operation by providing the authorized administrator with the function to manage TOE security functions.

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1 Management of Security Attribute corresponds to the P.Secure Operation.

This component supports secure operations by providing the authorized administrator with the function to manage TSF data.

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3 Static Attribute Initialization corresponds to the P.Secure Operation.

This component supports secure operations by providing the authorized administrator with the function to manage TSF data.

FMT_MTD.1 Management of TSF Data

FMT_MTD.1 TSF Data Management corresponds to the P.Secure Operation.

This component supports secure operations by providing the authorized administrator with the function to manage TSF data.

FMT_PWD.1 (extended) Management of ID and Password

FMT_PWD.1 (Extended) Management of ID and Password corresponds to theT.Weak Passwords.

This component reduces the T.Weak Passwords by providing the authorized administrator with the function to manage administrator and document user passwords.

FMT_SMF.1 Management Function Specification

FMT_SMF.1 Management Function Specification corresponds to the P.Secure operations.

This component supports P.Secure operations by requiring the authorized administrator to provide administrative functions.

FMT_SMR.1 Security Roles

The FMT_SMR.1 Security Roles correspond to the P.Secure Operation.

This component supports P.Secure Operation by requiring security management to be performed in connection with authorized role through identification and authentication.

FPT_FLS.1 Secure State Maintenance in Case of failure

FPT_FLS.1 Secure State Maintenance in Case of Failure corresponds to the T.Unauthorized Information Leakage.

This component eliminates unauthorized information leakage by providing the function to securely generate random numbers used to generate the cryptographic key.

FPT_ITT.1 Basic Protection of Internally Transmitted TSF Data

FPT_ITT.1 Basic protection of internally transmitted TSF data corresponds to leakage and corruption.

This component protects the data in the agent/server transport data from exposure and modification to eliminate the T.Transmitted Data Leakage and Corruption.

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

FPT_PST.1 (Extended) The basic protection of stored TSF data correspond to the T.Stored Data Corruption.

This component reduces the T.Stored Data Corruption by providing protection against exposure and modification of stored data.

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

FPT_PST.2 (extended) Availability protection of Stored TSF data corresponds to the T.Disabling Agent. This component reduces the T.Disabling Agent by providing the function to prevent deletion and termination of agents.

FPT_RCV.2 Automated Recovery

FPT_RCV.2 Automated Recovery corresponds to the T.Disabling Agent.
This component reduces the T.Disabling Agent by providing automated recovery of the agent.

FPT_TST.1 TSF Testing

FPT_TST.1 TSF Testing corresponds to the T.Stored Data Corruption and P.Secure Operations.
This component provides testing and integrity verification functions to prove the operation of the TOE, T.Stored Data Corruption and supporting P.Secure Operation.

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions corresponds to T.Bypassing Administrator and T.Bypassing Document Users.
This component reduces the T.Bypassing Administrator and T.Bypassing Document Users traffic by limiting the rules for the maximum number of concurrent sessions.

FTA_SSL.1 TSF – Initiated Session Locking (Document User)

FTA_SSL.1 TSF – Initiated Session Locking corresponds to the T.Bypassing Document Users and T.Accessing idle session.
This component locks the document user's PC after a period of user inactivity, eliminating the T.Bypassing Document Users and T.Accessing idle session.

FTA_SSL.3 TSF – Initiated Termination (Administrator)

FTA_SSL.3 TSF – Initiated Termination corresponds to the T.Administrator access, T.Accessing idle session.
This component terminates the administrator's session after a period of administrator inactivity, removing the T.Bypassing Administrator and T.Accessing idle session.

FTA_TSE.1(1) TOE Session Establishment

The FTA_TSE.1(1) TOE Session Establishment corresponds to the T.Manager session.
This component reduces T.Admin hits by restricting the administrator access IP when setting up an administrator session.

FTA_TSE.1(2) TOE Session Establishment

The FTA_TSE.1(2) TOE Session Establishment corresponds to the T.Bypassing Document Users. This component reduces the T.Bypassing Document Users by using IP and MAC in addition to document user authentication when establishing a document user session.

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1 Inter-TSF Trusted Channel corresponds to the T.Transmitted Data Leakage and Corruption. This component enforces TLS communication when communicating with SMTP servers for email notifications to eliminate the T.Transmitted Data Leakage and Corruption.

6.3.2 Rationale of Assurance Requirements

The assurance level of this Security Target is EAL1+ according to the "Korean National Protection Profile for Electronic Document Encryption V3.0" to which the Security Target conforms.

EAL1 can be applied where some level of trust in correct operation is required, but the threat to security is not significant. EAL1 is useful when independent assurance is required to demonstrate that appropriate measures have been taken to protect personal or similar information.

EAL1 requires only limited ST, i.e., rather than defining the security objectives from the threats, organizational security policy (OSPs), and assumptions based on the security objectives and deriving the security functional requirements (SFRs) from them, EAL1 simply requires that the security functional requirements be clearly stated in the TOE

While EAL1 does not require evidence of testing performed by the developer based on the functional specification, this protection profile adds ATE_FUN.1 to allow the developer to independently test whether the TSF is implemented correctly and document the results, including whether any defects occur.

6.4 Dependency Rationale

6.4.1 Dependency Rationale of Security Functional Requirements

[Table 6-32] Dependency Rationale

Num ber	Feature Components	Dependency	Reference number
1	FAU_ARP.1	FAU_SAA.1	3

2	FAU_GEN.1	FPT_STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.4	FAU_STG.2	Rationale (2)
7	FAU_STG.5	FAU_STG.2	Rationale (2)
8	FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1(1)	12, 14
		FCS_RBG.1	18
		FCS_CKM.6	13
9	FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1(2)	12, 15
		FCS_RBG.1	18
		FCS_CKM.6	13
10	FCS_CKM.1(3)	FCS_CKM.2 or FCS_COP.1(3)	12, 16
		FCS_RBG.1	18
		FCS_CKM.6	13
11	FCS_CKM.1(4)	FCS_CKM.2 or FCS_COP.1(4)	12, 17
		FCS_RBG.1	18
		FCS_CKM.6	13
12	FCS_CKM.2	fcs_ckm.1(1), fcs_ckm.1(2), FCS_CKM.1(3), FCS_CKM.1(4)	8, 9, 10, 11
13	FCS_CKM.6	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4)	8, 9, 10, 11
14	FCS_COP.1(1)	FCS_CKM.1(1)	8
		FCS_CKM.6	13
15	FCS_COP.1(2)	FCS_CKM.1(2)	9
		FCS_CKM.6	13

16	FCS_COP.1(3)	FCS_CKM.1(3)	10
		FCS_CKM.6	13
17	FCS_COP.1(4)	FCS_CKM.1(4)	11
		FCS_CKM.6	13
18	FCS_RBG.1	FCS_RBG.3	19
		FPT_FLS.1	40
		FPT_TST.1	45
19	FCS_RBG.3	FCS_RBG.1	18
20	FDP_ACC.1(1)	FDP_ACF.1(1)	22
21	FDP_ACC.1(2)	FDP_ACF.1(2)	23
22	FDP_ACF.1(1)	FDP_ACC.1(1)	20
		FMT_MSA.3	35
23	FDP_ACF.1(2)	FDP_ACC.1(2)	21
		FMT_MSA.3	35
24	FIA_AFL.1	FIA_UAU.1	27
25	FIA_IMA.1 (Extended)	-.	-.
26	FIA_SOS.1	-.	-.
27	FIA_UAU.1	FIA_UID.1	31
28	FIA_UAU.2	FIA_UID.1	31
29	FIA_UAU.4	-.	-.
30	FIA_UAU.7	FIA_UID.1	31
31	FIA_UID.1	-.	-.
32	FIA_UID.2	-.	
33	FMT_MOF.1	FMT_SMF.1	38
		FMT_SMR.1	39
34	FMT_MSA.1	FDP_ACC.1(1), FDP_ACC.1(2)	20, 21
		FMT_SMF.1	38
		FMT_SMR.1	39
35	FMT_MSA.3	FMT_MSA.1	34
		FMT_SMR.1	39
36	FMT_MTD.1	FMT_SMF.1	38
		FMT_SMR.1	39
37	FMT_PWD.1 (extended)	FMT_SMF.1	38
		FMT_SMR.1	39
38	FMT_SMF.1	-.	-.
39	FMT_SMR.1	FIA_UID.1	31

40	FPT_FLS.1	-.	-.
41	FPT_ITT.1	-.	-.
42	FPT_PST.1 (Extended)	-.	-.
43	FPT_PST.2 (Extended)	-.	-.
44	FPT_RCV.2	AGD_OPE.1	-.
45	FPT_TST.1	-.	-.
46	FTA_MCS.2	FIA_UID.1	31
47	FTA_SSL.1	FIA_UAU.1	27
48	FTA_SSL.3	-.	-.
49	FTA_TSE.1(1)	-.	-.
50	FTA_TSE.1(2)	-.	-.
51	FTP_ITC.1	-.	-.

Rationale (1): FAU_GEN.1 has a dependency relationship with FPT_STM.1, but the dependency relationship is satisfied by OE.timestamp because it is provided with trusted time information provided by the TOE operational environment.

Rationale (2): FAU_STG.3 and FAU_STG.4 have a dependency relationship with FAU_STG.2, but the dependency relationship is satisfied by OE.DBMS because audit data protection is provided by the DBMS provided by the TOE operational environment.

6.4.2 Dependency rationale of Security Assurance Requirements

[Table 6-33] Dependency Rationale

Number	Assurance Components	Dependency	Reference number
1	ASE_INT.1	-.	-.
2	ASE_CCL.1	ASE_INT.1 ASE_ECD.1 ASE_REQ.1	1, 5, 6
3	ASE_SPD.1	-.	-.
4	ASE_OBJ.1	ASE_SPD.1	3
5	ASE_ECD.1	-.	-.
6	ASE_REQ.1	ASE_ECD.1 ASE_SPD.1 ASE_OBJ.1	5, 3, 4
7	ASE_TSS.1	ASE_INT.1 ASE_REQ.1 ADV_FSP.1	1, 6, 8

8	ADV_FSP.1	-.	-.
9	AGD_OPE.1	ADV_FSP.1	8
10	AGD_PRE.1	-.	-.
11	ALC_CMC.1	ALC_CMS.1	12
12	ALC_CMS.1	-.	-.
13	ATE_FUN.1	ATE_COV.1	Rationale (1)
14	ATE_IND.1	ADV_FSP.1 AGD_OPE.1 AGD_PRE.1	8, 9, 10
15	AVA_VAN.1	ADV_FSP.1 AGD_OPE.1 AGD_PRE.1	8, 9, 10

Rationale (1): The added assurance requirement, ATE_FUN.1, includes ATE_COV.1 as a dependency. ATE_FUN.1 was added to verify that the developer accurately performed the test items and recorded them in the test documentation. However, ATE_COV.1, which presents the correspondence between test items and TSFI, was deemed not strictly necessary and, therefore, was not included in this Security Target.

7 TOE Summary Statement

This chapter provides an overview of the security functions required by the TOE.

7.1 Security audits

7.1.1 Audit Data Generation

When the following audit events [Table 7-1] occur, the TOE generates and reviews audit records of those events to track accountability for security-related action. Audit records are generated in DocuRay x Server or DocuRay x Agent and sent to DocuRay x Server, where they are stored in the DBMS.

[Table 7-1] Recorded Contents of Audit Events

Audit events	Audit record history contents
Response actions and results when audit saving fails (success, failure)	Deletion date, Deletion duration, Threshold criteria, Drive name (storage), Total capacity, Free capacity before deletion, Free capacity after deletion
Cryptographic key generation failure	Date, Category (Server/Client), Department, User, PC name, Inspection target (key that failed to generate and failure algorithm)
Cryptographic operation failure (including cryptographic operation types) ** Examples of cryptographic operation types: Refers to units of cryptographic functionality, such as document encryption failure, encrypted communication failure, file encryption failure, etc.	Date, Category (server/client), Department, User, PC, Inspection targets (operation target and failure algorithm)
Successful request to perform operations on objects covered by the document encryption/decryption access control SFP	Document name, Document path, Size, Department, user, PC name, Result, Date, Details (file Processing date, Result, File status, File path, File name, File permissions, File creation date, File department/user, Encrypted department/user, PC name, IP address, windows login ID, process)
Response actions and results (success, failure) when user authentication attempt reaches the threshold	Date, User, Department, PC name, IP address, MAC address, Details
	Send date, Contents, Recipient
User login success-failure	PC name, IP address, MAC address, Designated user department, Designated user, Login user

	department, Login user, Access date, Status, Result, Details
Authentication failure due to detection of attempts to reuse of credentials	PC name, IP address, MAC address, Designated user department, Designated user, Login user department, Login user, Access date, Status, Result, Details
User registration, change and deletion	Date, admin, IP address, Category, Details (department/user, add/modify/delete)
All changes of the password	'Organizational chart - Edit user'
	'Admin - Change ID and Password'
Registration, deletion and change IP address of the management terminals	Date, admin, IP address, Menu (Category information), Function Category
Agent Inquiry - Status	PC name, IP address, MAC address, Designated user department, Designated user, Recent user department, Recent user, Status, Installation date, Last access time, Deletion history
Agent security policy management - Policy settings	Date, admin, IP address, Category, details
TOE security function testing upon administrator request	Date, Category, Result, Inspection targets and failed security function
Integrity verification on the TOE configuration values and TOE itself upon administrator request	Date, Category, Result, Number of items to be validated and failed to be validated
Change of TOE agent registration status	PC name, IP address, MAC address, Department, User, Status, Date and time
Administrator account (ID) and password change	Date, Admin, IP address, Category, details
TOE Server Testing and results (Success, Failure)	Date, Category, Result, Target Items and failed security function
Integrity verification on TOE components and results (success-failure)	Date, Category, Result, Number of items to be validated and failed to be validated
Response actions when duplicate login attempts of the same account are detected	PC name, IP address, MAC address, Designated user department, Designated user, Login user department, Login user, Login user, Access date, Category (login / logout), Details (duplicate login attempts)
	Date, Admin, IP address, Category, Details
Blocking duplicate connection and results (success-failure)	PC name, IP address, MAC address, Designated user department, Designated user, Login user

	department, Login user, Login user, Access date, Logout, Forced logout (duplicate login)
	Date, admin, IP address, Category, Details
User session termination and results (success, failure)	PC name, IP address, MAC address, Designated user department, Designated user, Login user department, Login user, Access date, result
	Date, Admin, IP address, Category, Details
Blocking IP access for management terminals	Date, Admin, IP address, Category, Details
User logout success-failure	PC name, IP address, MAC address, Designated user department, Designated user, Login user department, Login user, Login user, Access date, Category (login / logout), Details, Result

Related SFR: FAU_GEN.1

7.1.2 Potential Violation Analysis and Security Alarms

When an audit event occurs, the TOE performs appropriate response actions if the event is a potential security violation. The rules by which the TOE examines and applies audit events are as follows

TOE sends a warning message to the administrator's registered email if the audit storage usage exceeds 90% and is below 95%, and deletes the oldest audit data if the storage usage exceeds 95% and sends a corresponding action to the administrator's registered email.

If the TOE determines that a component testing, integrity verification, or cryptomodule testing has failed, it sends the result to the administrator's registered email.

Related SFR: FAU_ARP.1, FAU_SAA.1

7.1.3 Protection of Audit Storage

The TOE stores audit data generated by the occurrence of audit events in a DBMS located in the local storage of DocuRay x Server. The TOE provides only an interface to query the stored audit data to prevent unauthorized modification and deletion of audit history by the authorized administrator.

The DBMS where audit data is stored is installed on a partitioned disk drive, and when the capacity of the disk drive where audit data is stored reaches a certain threshold value based on the capacity of the disk drive, appropriate actions are taken to prevent the audit data loss. If the disk usage exceeds 90% and is below 95%, a warning message is sent to the administrator via email, and if it exceeds 95%, the old inspection records are repeatedly deleted by date until it is below 95%, and the administrator can check the contents by sending the action details via email.

Related SFRs: FAU_STG.4, FAU_STG.5

7.1.4 Audit Review

The TOE provides the authorized administrator with the ability to review audit data stored in the DocuRay x Server's audit data storage. This allows the authorized administrator to view audit history information for audit events specified in the Security Functional Requirements (Security Audit, Password Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, and TOE Access).

The TOE provides the stored audit history information to the administrator according to the query interface requested by the authorized administrator. The query interface is provided as a GUI, and the authorized administrator can set search conditions according to the objective of data review to query the history and rearrange the results.

[Table 7-2] Criteria Based on Audit Data Type

Audit data Type	Criteria with logical relationships	Select and/or Ordering methods
Document Encryption History	- Department / User && - Document name - Document path && - Encryption date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Duration period) &&	Inquiry, Sort (timestamp)
Document Decryption History	- Department / User && - Document name - Document path && - Encryption date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months,	Inquiry, Sort (timestamp)

	Last 6 months, Set period) &&	
Documents Viewing History	- Department / User && - Document name - Document path && - Encryption date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (timestamp)
User Sign in History	- Department / User && - Status: Multiple selections (All, Logged In, Logged Out) && - Result: Multiple selections (All, Success, Failure) && - Details (Login): Multiple selections (All, Successful Login, Password mismatch, Login attempt with nonexistent account, Login attempt while locked, Reuse of credentials, Agent-User information mismatch|| - Details (Logout): Multiple selections (All, Logout) || - Access Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (timestamp)
User Account Lockout History	- Department / User && - Date: Single selection (today only, yesterday, last 1 week, last 2 weeks, last 1 month, last 3 months, last 6 months, set period) &&	Inquiry, Sort (timestamp)
PC Installation/Deletion History	- Department / User && - Status: Multiple selections (All, Install, Delete) - Date: Single selection (today, yesterday, last 1 week, last 2 weeks, last 1 month, last 3 months, last 6 months, set time period) &&	Inquiry, Sort (timestamp)

Admin History	- Category: Multiple selection (All, Admin, Organizational Chart, PC Management, Policy, Other) && - Sub-Category : Multiple selection (Change policy, Batch policy change, Create policy, Modify policy (Set policy), Modify policy (Policy management), Delete policy, Add sub-department, Change department name, Move department, Delete department, Add user, Modify user, Move user to another department, Delete user, Delete agent, Add access allowed IP, Delete access allowed IP, Set smtp account information, Set admin email notification, Change default password, Change ID and password, Login success, Login failure, Duplicate Login attempt, Logout, Logout due to duplicate login, Logout due to session expiration, ID block, Account lock, Account unlock) &&	Inquiry
Integrity verification History	- Departments / Users && - Category: Multiple selection (All, Server, Agent) && - Result: Multiple selection (All, Success, Failure, Recovery) && - Success Failure Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (date)
Testing History	- Departments / Users && - Category: Multiple selections (All, Server, Agent) && - Result: Multiple selections (All, Success, Failure, Recovery) && - Target && - Success Failure Date: Single selection (Today only, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (date)
Audit Function Start/Shutdown History	- Departments / Users && - Category: Multiple selections (Policy, Server, Agent) - Start/Shutdown separation: Single selection (All, Start, End) && - Access date (Today, Yesterday, Last week, Last week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (date)
Audit Threshold	- Deletion date (Today, Yesterday, Last week, Last 1	Inquiry,

Exceeded Response History	week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Sort (entire column)
Email Sending History	- Category: Multiple selection (Server integrity failure notification, Agent integrity failure notification, Server testing failure notification, Agent testing failure notification, Threshold exceeded notification, Admin login lock notification, User login lock notification) &&	Inquiry, Sort (date sent, content, recipient)
Failure in Cryptographic key Generation History	- Departments / Users && - Category: Multiple selections (All, Server, Agent) && - Failure Date: Single selection (Today only, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (date)
Failure in Password Operation History	- Departments / Users && - Category: Multiple selections (All, Server, Agent) && - Failure Date: Single selection (Today, Yesterday, Last 1 week, Last 2 weeks, Last 1 month, Last 3 months, Last 6 months, Set period) &&	Inquiry, Sort (date)
(*Legend: The && symbol above means "and" and the || symbol means "or" condition)		

Related SFRs: FAU_SAR.1, FAU_SAR.3, FAU_GEN.1

7.2 Cryptographic Support

The cryptographic security features provided by the TOE use the MagicCrypto V2.3.0 (2025-01-24 Validation date, Validation number CM-263-2030.1) validated cryptographic module, which has been validated for security and implementation suitability through the Korea Cryptographic Module Validation Program (KCMVP).

7.2.1 Cryptographic key Generation

The data cryptographic key (DEK) for document header, server, agent, and agent communication is generated with the HASH_DRBG (SHA-256) algorithm of the ISO/IEC 18031 standard (cryptographic key length 256 bit).
The cryptographic key (KEK) is generated using the PBKDF2 (HMAC-SHA-256) algorithm of the TTAK.KO-12.0334 standard using SALT with the HASH_DRBG (SHA-256) (cryptographic key length 256 bits) algorithm of the ISO/IEC 18031 standard and the user password for induction.

The asymmetric key is generated with the RSAES (SHA-256) algorithm of the ISO/IEC 18033-2 standard (cryptographic key length 2048 bits).

For a standard list of cryptographic keys, types of cryptographic keys, generation algorithms, and key lengths, refer to [Table 7-3] Cryptographic key Generation.

[Table 7-3] Cryptographic key Generation

Cryptographic key	Cryptographic key generation algorithm	Cryptographic key length	Standard list
Document header DEK	HASH_DRBG (SHA-256)	256 bit	ISO/IEC 18031
Documentation DEK			
Server DEK			
Agent DEK			
Agent Communication DEK			
Server KEK	PBKDF2 (HMAC-SHA-256)	256 bit	TTAK.EN-12.0334
Agent KEK			
Server Asymmetric Key	RSAES (SHA-256)	2048 bit	ISO/IEC 18033-2
Agent Asymmetric Key			

Related SFRs: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4)

7.2.2 Cryptographic key Distribution

TOE's cryptographic key distribution is performed through a self-implementing cryptographic key distribution method.

The cryptographic key of the TOE is distributed through the server public key/agent public key/agent communication DEK and self-implemented secure cryptographic communication using RSAES (SHA-256) (cryptographic key length 2048 bit) algorithm of ISO/IEC 18033-2 standard and ARIA_CBC (cryptographic key length 256 bit) algorithm of KS X 1213-1 standard which are exchanged during the agent registration process.

Related SFR: FCS_CKM.2

7.2.3 Cryptographic key Destruction

The TOE encodes and loads the secret key into memory and immediately destroys the used cryptographic key and critical security parameters. The method of destroying the cryptographic key is to overwrite the cryptographic key and critical security parameters with 0 or 1 at least three times. The document header DEK is encoded and loaded into memory, and the other encoded cryptographic key is additionally destroyed when logging out and terminating the TOE.

[Table 7-5] When to destroy a cryptographic key and critical security parameters

Category	Target	When to destroy	Destruction methods
Server	Server DEK	- Immediately after use - Upon TOE shutdown	- Overwrite with 0 or 1 more than 3 times
	Server Asymmetric Key		
	Agent Communication DEK		
	Document header DEK		
	Server KEK		
	Critical Security Parameters		
Agent	Agent DEK		
	Agent Asymmetric Key		
	Agent Communication DEK		
	Documentation DEK		
	Agent KEK		
	Critical Security Parameters		
	Document Header DEK	- Immediately after use - Upon TOE shutdown - Upon TOE logout	

Related SFR: FCS_CKM.6

7.2.4 Cryptographic Operation

The TOE's document encryption and decryption use the block ciphers ARIA_CBC/CTR of the KS X 1213-1 standard (cryptographic key length 256 bits) and the HASH_DRBG (SHA-256) (cryptographic key length 256 bits) algorithm of the ISO/IEC 18031 standard, which are approved algorithms.

The TOE's TSF data decryption uses ARIA_CBC of KS X 1213-1 standard (cryptographic key length 256 bit), HMAC (SHA-256) of ISO/IEC 9797-2 standard (cryptographic key length 256 bit), and SHA-512 algorithm of ISO/IEC 10118-3 standard.

The TOE uses ARIA_CBC (cryptographic key length 256 bits) of KS X 1213-1 standard, RSAES (SHA-256) (cryptographic key length 2048 bits) of ISO/IEC 18033-2 standard, RSA-PSS (SHA-256) (cryptographic key length 2048 bits) of ISO/IEC 14888-2 standard, and SHA-512 algorithm of ISO/IEC 10118-3 standard to encrypt and decrypt transmitted data for secure communication.

[Table 7-6] List of password operations

Operations list	Password algorithms	Cryptographic key length	Standard list
Document Encryption/Decryption	ARIA_CTR	256 bit	KS X 1213-1
Document Security Header Encryption/Decryption	ARIA_CBC		
Server DEK Encryption/Decryption			
Server private key encryption/decryption			
DBMS Administrator Password Encryption/Decryption			
AgentDEK Encryption/Decryption			
Agent private key Encryption/Decryption			
Agent Communication DEK Encryption/Decryption			
Audit Data Encryption/Decryption			
Transmission data Encryption/Decryption			
Transmission data Encryption/Decryption	RSAES (SHA-256)	2048 bit	ISO/IEC 18033-2
Electronic signatures for transmitted data Creation and Validation	RSS-PSS (SHA-256)	2048 bit	ISO/IEC 14888-2
Integrity verification and transit data hashes	SHA-512	-.	ISO/IEC 10118-3
User password one-way encryption	HMAC (SHA-256)	256 bit	ISO/IEC 10118-3

Related SFRs: FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4

7.2.5 Random Bit Generation (RBG)

When generating a cryptographic key, the TOE generates a minimum length of random numbers that satisfies the Random Bit Generation (RBG) quality metric, which is at least 128 bit of security strength.

TOE uses the HASH_DRBG (SHA-256) algorithm of the ISO/IEC 18031 standard for random bit generation (RBG) to generate random numbers used to perform security functional requirements.

TOE uses a TSF software-based entropy source (CryptGenRandom) to ensure that DRBG seeds are at least128 bit.

If the TOE fails the random bit generator noise source health test, it reseeds to remain secure.

Related SFRs: FCS_RBG.1, FCS_RBG.3, FPT_FLS.1

7.3 Protection of User Data

7.3.1 Document Encryption Access Control

TOE protects user data by controlling unauthorized access through document encryption based on the policy set by the administrator, and if the user's security attribute (user ID) does not match the permissions (public/private) of the encrypted protected document, read/save/manual encryption/manual decryption is not allowed.
The encryption/decryption policy can be set by the administrator on the admin page, and the policy are applied to DocuRay x Agent to control the action of the PC. In the encryption/decryption policy, the administrator can specify whether encryption is applied to document types and document programs and select document permissions.

- Public permissions: Anyone in your entire organization can view the document.
- Personal permissions: Only users with the applied policy can view the document.

Related SFR: FDP_ACC.1(1), FDP_ACF.1(1)

7.3.2 Document Access Control

TOE protects user data by controlling unauthorized copy & paste via the clipboard based on policy set by the administrator, and disallows clipboard copy & paste if the process security attributes are not matched.

Related SFR: FDP_ACC.1(2), FDP_ACF.1(2)

7.4 Identification and Authentication

7.4.1 Authentication Failure Handling

The TOE performs identification and authentication functions prior to any action.
If more than five consecutive failed authentication events occur, the TOE disables the user account and sends an email to the administrator. The default value for the time to reactivate the user account is 5 minutes. The number of times and lockout period for authentication failure lockout processing is fixed at 5 times and 5 minutes.

Related SFR: FIA_AFL.1

7.4.2 TOE Internal Mutual Authentication (Extended)

Mutual authentication for communications between the DocuRay x Server and DocuRay x Agent that constitute the TOE is performed through a self-implementing authentication protocol. The mutual authentication method used by the agent and the server is identical. For encrypted communication, the server generates an asymmetric key at installation and provides the server public key during the agent installation. The agent generates an asymmetric key during the agent installation and passes the agent public key to the server during the agent registration to exchange the agent/server public key. All communication data transmitted by the agent is mutually authenticated using RSA-PSS (SHA-256) (cryptographic key length 2048 bit) of ISO/IEC 14888-2 standard and SHA-512 algorithm of ISO/IEC 10118-3 standard.

Related SFR: FIA_IMA.1

7.4.3 Verification secrets

The TOE verifies that the password entered by the user (administrator, document user) satisfies the security criteria [Table 7-7] whenever the user enters a password, both when creating/changing the password and when changing the password provided by default for initial access to TOE components.

[Table 7-7] Password combination rules

Password combination rules
- Ensure a length of at least 9 characters - Include at least one of each: a number, an uppercase letter, a lowercase letter, and a special character - Prohibit using the same password as the user account (ID) - Prohibit repeating the same letter or number more than three times consecutively - Prohibit entering more than four consecutive characters or numbers in keyboard order - Prohibit reusing the previously used password

Related SFR: FIA_SOS.1

7.4.4 Authentication, Single-Use Authentication Mechanisms, Protected Authentication Feedback, User Identification

The TOE provides an identification and authentication process based on ID and password for the administrator and document users. Only the authorized administrator can access the admin page through a web browser to manage security features. The TOE provides a login UI for DocuRay x Server and a login UI an and information view for DocuRay x Agent, depending on the component, before identification and authentication, The TOE requires user authentication to perform security functions and doesn’t provide security functions before authentication.

When the administrator and document users enter their passwords into DocuRay x Server or DocuRay x Agent, they are masked with '●' to prevent exposure, and if authentication fails, no reason is provided for the failure. If an administrator or document user fails to authenticate more than five times, the account is locked for 5 minutes.

The credentials of the administrator or document users are timestamped to prevent reuse. A timestamp is sent along with the credentials and saved when authentication is successful. When logging in, the timestamp is used to authenticate the user, and if it is smaller than the timestamp stored in the DB, authentication fails, and if it is larger, the authentication process proceeds. When the authentication process is completed, the timestamp is saved.
Related SFR: FIA_UAU.1, FIA_UAU.2, FIA_UAU4, FIA_UAU7, FIA_UID.1, FIA_UID.2

7.5 Security Management

7.5.1 Management of Security Functions Behavior

An authorized administrator manages security functions through the admin page.

User registration, change and deletion
You can manage users from the organization chart management menu on the admin page. The administrator can add, modify, and delete departments in the organization chart, and add, modify, and delete users.

Registration, deletion and change IP address of the management terminals
You can manage IP addresses for managed terminals from the Security Policy menu on the admin page. You can register up to two management terminals, but you can only add one per single host, you can't specify an IP range, and you can't register with an address that means the entire network. At least one allowed IP must exist to access the admin page, so you can't delete them entirely.

Agent Inquiry - status, version, applied security policy
You can look up agents from the PC management menu on the admin page. In PC management, you can view an agent user's PC name, IP address, MAC address, department, user, agent version, enforcement policy, status, integrity verification results, and last access time.

Agent security policy management - policy configuration, policy transmission
You can set and apply policy to agents in Login policy settings in the Policy menu on the admin page. You can select a department or user to change the value of the policy in effect and apply it. You can also select each department and user for bulk changes and switch to a different policy. The applied policy is sent and applied to the agent through communication with the agent.

Configuration of recipient email and SMTP connection information for email sending
You can set SMTP account information for email notifications and administrator email notifications to receive in mail settings on the admin page. You can set SMTP account information by entering host, port, email, password, encoding, and security connection in SMTP account information, and you can set multiple emails by separating emails with commas (,) in admin email notification settings.

Integrity verification of the management server upon administrator request
You can perform an integrity verification of the server by an administrator from the Security Policy menu on the admin page. The administrators can request an integrity verification via the ‘Run Manually’ button and view the results via the View History shortcut.

Document user session lock execution/release (authentication)

You can set the policy that apply to agents in the Login Policy Settings menu on the Admin page. In PC security policy, you can set the session lockout time for the agent. The screen lock wait time can be set from 5 minutes to 24 hours. If the screen remains idle for the specified lock wait time, the screen is locked. The locked screen can be unlocked by authenticating the agent user.

Audit history inquiry

You can view logs from the admin page and audit history from the admin menu. The administrators can view the audit history of document encryption history, document decryption history, document viewing history, user login history, user account lock history, PC installation/deletion history, screen lock history, integrity verification history, testing history, audit function start/stop history, audit threshold exceedance response history, email sending history, cryptographic key generation failure history, and cryptographic operation failure history.

Related SFR: FMT_MOF.1

7.5.2 Management of Security Attributes

The TOE provides the authorized administrator with the function to manage the document encryption and decryption policy for secure documents.

You can create a new policy from the Policy management menu on the admin page. The policy name and policy settings determine the policy's distinguishing factors, and the policy distinction and initial policy assignment allow you to import settings from other policies.

You can set the attributes of a security policy from the Login Policy Settings menu on the Admin page. The policy's security attributes, file permissions settings, can be set to private/public, and the file decryption settings can be enabled/disabled. File viewing and saving settings allow you to change the settings for enabling/disabling the types of documents to be encrypted.

Bulk policy changes allow you to change the policy for specific users and departments, change to a different policy to change to the policy of a parent department or the policy of the change you made, and apply it in bulk to users who are using an individual policy, including subdepartments using the same policy.

DocuRay x Agent can control access to protected documents based on the policy set by the authorized administrator.

Related SFR: FMT_MSA.1

7.5.3 Static Attribute Initialization

The TOE provides limited document encryption/decryption policy default values for secure documents and does not provide the function to edit the default values.

Related SFR: FMT_MSA.3

7.5.4 Management of TSF Data

The TOE provides management of TSF data capabilities to the authorized administrator, and the list of TSF data for which management capabilities are available at is shown in [Table 7-8].

[Table 7-8] TSF Data List

TSF data	Query	Change	Delete	Create
Document user and department management	○	○	○	○
Document user and admin passwords	-.	○	-.	-.
Management terminal IP address	○	○	○	○
Agent Inquiry	○	-.	-.	-.
Agent security policy management	○	○	○	○
TOE and TOE component identification	○	-.	-.	-.
Audit history	○	-.	-.	-.
Configuration of recipient email and SMTP connection information for email transmission	○	○	○	○

Related SFR: FMT_MTD.1

7.5.5 Management of ID and Password (Extended)

The TOE provides the function to change passwords for the authorized administrator and document users.
The admin password should be forced to change if it is the default password for the first login, and document users should be forced to change their password if it was changed by the installer and administrator.

Related SFR: FMT_PWD.1

7.5.6 Specification of Management Functions

TOE's security management functions are provided through the admin page.
The security management functions provided by DocuRay x Server to the authorized administrator are: ① User registration, change and deletion; ② Registration, deletion and change IP address of the management terminals; ③ Agent Inquiry - status, version, applied security policy; ④ Agent security policy management - policy configuration, policy transmission; ⑤ Testing of the server's security functions at the request of the administrator; ⑥ Integrity verification of the server's configuration values and the server itself at the request of the administrator; ⑦ TOE version information inquiry; ⑧ Audit history inquiry; ⑨ Incoming email and SMTP connection information settings for sending emails.
The security management features provided by DocuRay x Agent to document users are: (1) individual user authentication when unlocking a session; and (2) TOE identification Inquiry.

Only the authorized administrator can manage the document encryption/decryption policy in TOE's security attributes. Security attribute management consists of (1) creating a policy and applying them to departments or users, (2) changing file permissions, (3) setting file decryption, and (4) setting file viewing and saving.

It does not provide the ability to change the default values for security features provided by TOE.

Managing TSF data in TOE is limited to authorized administrator and document user role.

Related SFR: FMT_SMF.1

7.5.7 Security Roles

The users provided by TOE are the authorized administrator and documentation users.
The authorized administrator performs security functions through the Administrator page. The security functions performed by the administrator include managing the organization chart, managing policies, setting the IP address of the management terminal, performing testing and integrity verification at the request of the administrator, managing agents, and viewing audit records.
Document users change their default password when they first access TOE.

Related SFR: FMT_SMR.1

7.6 Protection of the TSF

7.6.1 Basic protection of internally transmitted TSF data

In order to ensure the confidentiality and integrity of data transmitted between DocuRay x Server and DocuRay x Agent, the TOE uses SSL communication with TLS 1.3 protocol that the encrypted communication is encrypted using the ARIA_CBC (cryptographic key length 256 bit) of KS X 1213-1 standard, RSAES (SHA-256) (cryptographic key length 2048 bit) of ISO/IEC 18033-2 standard, RSA-PSS (SHA-256) (cryptographic key length 2048 bit) of ISO/IEC 14888-2 standard, and SHA-512 of ISO/IEC 10118-3 standard.

Related SFR: FPT_ITT.1

7.6.2 Basic protection of stored TSF data (extended)

The DEK used by TOE for TSF data encryption is encrypted through KEK, and the KEK generated through the PBKDF2 (HMAC-SHA-256) algorithm of the TTAK.KO-12.0334 standard (cryptographic key length 256 bit) is destroyed immediately after use.

The TOE encodes the cryptographic key and user passwords when they are loaded into memory, and immediately destroys plaintext the cryptographic key and user passwords after they are used.

DocuRay x Server protects TSF data with encryption and DBMS support. The cryptographic key that is encrypted and stored in the DBMS and files uses the ARIA_CBC (cryptographic key length 256 bit) algorithm of the KS X 1213-1 standard, and the administrator and document user passwords are encrypted use the HMAC (SHA-256) (cryptographic key length 256 bit) algorithm of the ISO/IEC 9797-2 standard.

DocuRay x Agent stores TSF data only in the file system, not in the registry. The types of TSF data stored in the file system are cryptographic keys/configuration files/audit data, which are protected by encryption and access control. The cryptographic key/configuration file/audit data is encrypted using the ARIA_CBC (cryptographic key length 256 bit) algorithm of the KS X 1213-1 standard.
For document encryption, the HASH_DRBG (SHA-256) algorithm of the ISO/IEC 18031 standard (cryptographic key length 256 bits) is used to generate the cryptographic key, and the block ciphers ARIA_CBC/CTR algorithm of the KS X 1213-1 standard (cryptographic key length 256 bits) is used to encrypt the document header and body.

Related SFR: FPT_PST.1

7.6.3 Availability Protection of Stored TSF Data

DocuRay x Agent protects the installation path with access control to prevent unauthorized deletion and the running agent from being terminated.

Related SFR: FPT_PST.2

7.6.4 Automated Recovery

DocuRay x Agent creates a backup during the installation phase, which is used for automated recovery. A Value (hash) for integrity verification for the TOE document encryption agent file, and it performs testing and integrity verification to trigger automated recovery in case of a verification failure.

Related SFR: FPT_RCV.2

7.6.5 Testing

In order to demonstrate appropriate operation of DocuRay x Server, testing is performed at startup, periodically (24 hours) to check the health of the process, and integrity verification are performed on the product's configuration values and executable files at startup, periodically (24 hours) or upon request by the authorized administrator, during regular operation. The scope of the integrity verification is the web application distribution directory, the server configuration directory, and the testing include the TOE self-validated modules and the key process.

In order to demonstrate appropriate operation of DocuRay x Agent, perform testing and integrity verification of the installation directory, TOE settings and executable files, and filter drivers at startup and periodically (12 hours) during regular operation.

Related SFR: FPT_TST.1

7.7 TOE Access

7.7.1 Per user attribute limitation on multiple concurrent sessions

DocuRay x Server does not allow duplicate access by authorized administrators. If you try to sign in with the same account on a different device after signing in, it notifies you of the duplicate sign-in attempt and requires you to terminate the previous connection. Based on whether the previous connection is terminated, an audit trail of logouts due to duplicate logins and duplicate login attempts is generated.

Related SFR: FTA_MCS.2

7.7.2 TOE Session Establishment (1)

The TOE provides the security function that controls access to the admin page based on the device IP address. Device IP addresses can only be added one by one on a single host basis, IP ranging is not possible, and network-wide address registration is not possible.
When accessing the TOE, it checks the registered device IP address and displays the login screen if the device IP address attempting to access is an authorized address, displays the 'No access permissions' page if it is an unauthorized address, and generates an audit history.

Related SFR: FTA_TSE.1(1)

7.7.3 TOE Session Establishment (2)

DocuRay x Agent authenticates the user during the user authentication with additional attributes such as the user IP address, MAC address, and the user PC ID obtained during the initial authentication (registration).

Related SFR: FTA_TSE.1(2)

7.7.4 TSF-Initiated Session Locking

DocuRay x Agent provides the function to lock a document user's session if it remains idle since the session lock was executed and logged in. The idle time can be set as a PC Security setting in the Security Policy and can be changed in the Policy Settings menu on the Admin page under PC Security, Screen Lock Dash Time settings. The time can be set to 5 - 10 minutes. Locked sessions can be released by user re-authentication.

Related SFR: FTA_SSL.1

7.7.5 TSF-Initiated Termination

DocuRay x Server provides the function for the authorized administrator to automatically log out of the administrator session if the inactivity time exceeds 10 minutes after logging in to the administrator page. The 10 minutes of inactivity is a fixed value.

Related SFR: FTA_SSL.3

7.8 Trusted Path/Channel (FTP)

7.8.1 Inter-TSF Trusted Channel

DocuRay x Server enforces encrypted communication for the communication used for email notifications. The protocol uses for encrypted communication is TLS.

Related SFR: FTP_ITC.1