ShadowCube V7.0 Security Target

ShadowCube

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

Table of Contents

1. ST Introduction

This document is the Security Target (ST) of ShadowCube V7.0 by Duruan Co., Ltd. that intends to achieve the goal of EAL1+ level under the Common Criteria.

1.1 ST Reference

This ST is identified as follows:

- Title: ShadowCube V7.0 Security Target
- ST Version: V1.9
- Author: Duruan Co., Ltd.
- Date: February 4, 2021
- Evaluation Criteria: Common Criteria for Information Technology Security Evaluation
- Common Criteria Version: v3.1 r5
- Evaluation Assurance Level: EAL1+(ATE_FUN.1)
- Keywords: Document, Encryption
- File Name: ShadowCube V7.0 Security Target V1.9.pdf

1.2 TOE Reference

The Target of Evaluation (TOE) that complies with this ST is identified as follows:

- Developer: Duruan Co., Ltd.
- TOE Identification/Version

- TOE Identifier: ShadowCube V7.0
- TOE Version: 7.0.7
    - TOE Component
- Policy Center: 7.0.7.1409
- Client: 7.0.7.1409
    - Publication Date: February 3, 2021

1.3 TOE Overview

This section describes the usage of the TOE and its major security features. It also identifies the TOE type and any major hardware and software additionally required for the operation of the TOE, and explains the physical scope and the logical scope of the TOE.

1.3.1 Document encryption overview

The TOE is an “Electronic Document Encryption (hereinafter referred to as the “TOE”) product” used to protect important documents managed by an organization.

The primary security features provided by the TOE includes the encryption/decryption of the document to be protected and cryptographic key management, and the encryption/decryption of the critical security parameters (CSP) used by the TOE and cryptographic key management. The cryptographic function herein must use the approved cryptographic algorithm of the validated cryptographic module (MagicCrypto V2.2.0).

Validated cryptographic module

- Cryptographic Module Name: MagicCrypto V2.2.0
- Validation Number: CM-162-2025.3
- Developer: Dream Security Co., Ltd.
- Validation Date: March 3, 2020
- Expiration Date: March 3, 2025

Cryptographic algorithm

- Cryptographic algorithm for documents: ARIA_CTR 128 bits
- Cryptographic algorithm for CSP: ARIA_CBC 256 bits, RSA 2048 bits

The TOE encrypts/decrypts documents in accordance with the document group-based access control policy established by an authorized administrator. In addition, it encrypts TSF data in order to protect TSF data when they are transmitted between separate parts of the TOE and when TSF data are stored. The TOE prevents the unauthorized deletion and termination of TSF data, runs self tests on TSF, and provides the capability to verify the integrity of the TSF and TSF data.

The TOE allows and blocks access by an administrator and a document user, provides a mechanism for password verification, and inactivates the identification and authentication if the login attempts have been denied for a defined number of times configured by the authorized administrator (default value: 3 times). It performs mutual authentication between communication partners by using ECDH algorithm of the validated cryptographic module.

The TOE generates audit records when an auditable event occurs, and sends an email to the authorized administrator in case of a potential security violation to inform him/her of the event.

The authorized administrator of the TOE can use the security management function of the TOE through the web-based security management interface (HTTPS) in the operational environment of the TOE. The authorized administrator of the TOE can establish access control policies; check the process status and set the interval of monitoring; and view audit data.

The TOE can be accessed only from an IP address that has been registered in advance, and restricts the number of the authorized administrator sessions to one. When the specified time interval of inactivity is met, it terminates the administrator session.

1.3.2 TOE operational environment and non-TOE

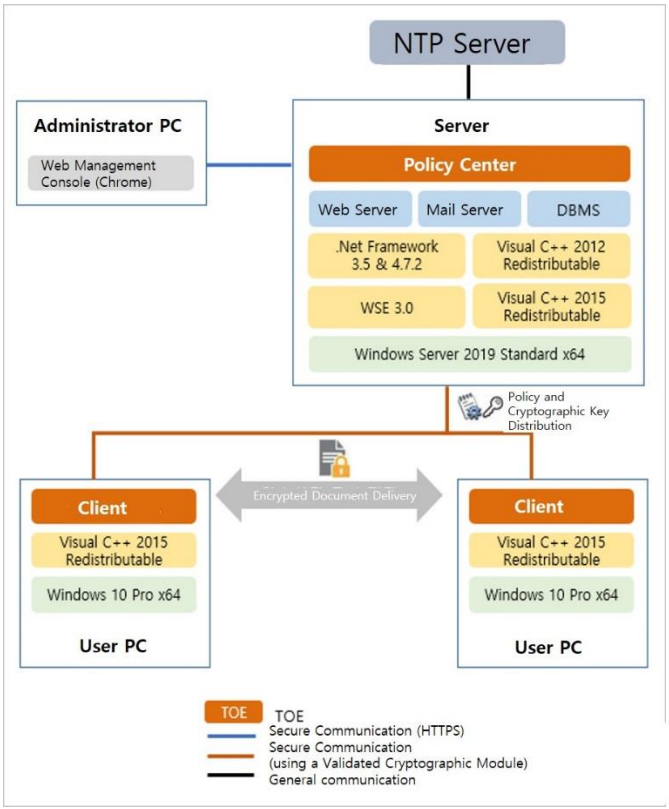
The TOE defined herein is "Electronic Document Encryption" that prevents an information leakage by encrypting/decrypting important documents within the organization. The operational environment provided by the TOE and non-TOE entities additionally used for the operation are as follows:

Operational environment of the "user device encryption" type

The TOE consists of the Policy Center that is installed in the server system and manages security policies, and the client that is installed in the user system and performs the encryption/decryption of the document.

The authorized administrator establishes the document group-based access control policy for each document user through the Policy Center, and the Policy Center distributes the policy and cryptographic key configured by the authorized administrator.

The client installed in the user system performs reading, encryption (writing) and decryption of the document to be protected, using the validated cryptographic module according to the distributed policy. The encrypted/decrypted document is stored as a file in the user device.



[Figure 1] Operation of user device encryption type

3rd party products used in the TOE

OpenSSL 1.1.1i

3rd party module included in the TOE and used in the web management access communication between the administrator and the policy center.

MagicCrypto V2.2.0

3rd party module included in the TOE. It is a validated cryptographic module used for the encryption/decryption of the document to be protected and cryptographic key management, and the encryption/decryption of CSP and cryptographic key management.

IIS (Internet Information Services) 10.0

3rd party module not included in the TOE. IIS 10.0, which is a service provided in Windows Server 2019 Standard and plays a role as a web server, is used for the operation of the security management by the administrator through HTTPS.

SMTP Virtual Server 10.0

3rd party module not included in the TOE. SMTP Virtual Server 10.0, which is a service provided in Windows Server 2019 Standard, plays a role as a mail server and is used to send an alarm email.

PostgreSQL 12.5

3rd party module not included in the TOE. It plays a role as DBMS and is used for safe storage of audit data and configuration data generated in the TOE.

Microsoft Visual C++ 2012 Redistributable (x86, x64) - 11.0.61030

3rd party module not included in the TOE. It is Visual C++ runtime library used to run an application program developed with Visual C++. It is used for the compatibility with a lower version of the Policy Center.

Microsoft Visual C++ 2015 Redistributable (x86, x64) - 14.0.24215

3rd party module not included in the TOE. It is Visual C++ runtime library used to run an application program developed with Visual C++.

Microsoft .NET Framework 3.5

3rd party module not include in the TOE. It is a library that supports the .NET execution environment necessary for the operation of Web Services Enhancements (WSE) 3.0.

Microsoft .NET Framework 4.7.2

3rd party module not included in the TOE. It is a library that supports the .NET execution environment necessary for the operation of the service of the TOE (Policy Center) developed with ASP. NET.

Web Services Enhancements (WSE) 3.0

3rd party module not included in the TOE. It is a library that supports the .NET execution environment used to support web service communication between the TOE (Policy Center) developed with ASP .NET and the client.

Non-TOE

Administrator System

An administrator system where a web browser program (Chrome 88.0) can run is required in order to use the security management function of the TOE.

User System

A user system where Microsoft Office, Hancom Office, AutoCAD, etc. can run is require in order to perform the document encryption/decryption.

System requirements

[Table 1] Policy Center

Classification	Specification
OS	Microsoft Windows Server 2019 Standard (64bit)
DBMS	PostgreSQL 12.5
S/W	IIS (Internet Information Services) 10.0 SMTP Virtual Server 10.0 Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030 Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030 Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24215 Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215 Microsoft .NET Framework 3.5 Microsoft .NET Framework 4.7.2 WSE 3.0 Chrome 88.0
H/W	CPU: Intel i7 Quad Core 2.0GHz or higher Memory: 8GB or higher HDD: 600MB or higher required for installing the TOE 1 or more network interfaces: 100/1000 Mbps or higher

[Table 2] Client

Classification	Specification
OS	Microsoft Windows 10 Pro (64bit)
S/W	Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24215 Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215 MS Notepad, MS WordPad, MS Paint Microsoft Office 2007, 2010, 2013, 2016, 2019 Hancom Office 2010, 2014(VP), NEO, 2018, 2020 Acrobat Reader 11, DC Autodesk AutoCAD 2019, 2020, 2021
H/W	CPU: Intel i3 Dual Core 1.0GHz or higher Memory: 4GB or higher HDD: 180 MB or higher required for installing the TOE 1 or more network interfaces: 100/1000 Mbps or higher

[Table 3] Administrator (HTTPS Communication)

Classification	Specification
S/W	Chrome 88.0

External IT entity

NTP Server

It is used when synchronizing time information to provide a trusted time stamp in the TOE.

Document Encryption Support

The Client, which is a TOE component, supports the encryption for the following application programs and document types:

Application Program	Program Version	Document Type (Extension)
Notepad	Default version provided on Windows 10 Pro x64, the operational environment of the client	txt
MSpaint		bmp, gif, jpg, png, tif
Wordpad		rtf
MS Office Word	2007, 2010, 2013, 2016, 2019	doc, docx
MS Office Excel	2007, 2010, 2013, 2016, 2019	xls, xlsx
MS Office Powerpoint	2007, 2010, 2013, 2016, 2019	ppt, pptx
Hancom Office Word	2010, 2014(VP), NEO, 2018, 2020	hwp, hwpx
Hancom Office Cell	2010, 2014(VP), NEO, 2018, 2020	nxl, cell
Hancom Office Show	2010, 2014(VP), NEO, 2018, 2020	show
Acrobat Reader DC	11, DC	pdf

Autodesk AutoCAD	2019, 2020, 2021	dwg, dxf

1.3.3 TOE description

The TOE encrypts electronic documents to protect the important documents managed by the organization according to the policy set by the administrator, and decrypts a document according to a document user's request and right.

1.3.3.1 Physical scope of the TOE

The TOE components are divided into the Policy Center that manages the security policy, and the client that encrypts/decrypts electronic documents.

The physical scope of the TOE consists of the software exclusive for the TOE and guidance documentation. The software exclusive for the TOE is provided in the form of an EXE file, and guidance documentation in the form of a PDF file, which are distributed as a CD.

[Table 4] Physical scope of the TOE

Composition	Element	Distribution Format
Software exclusive for the TOE	Policy Center installation file: server_7.0.7.1409.exe	CD 1EA
	Client installation file: scsetup_7.0.7.1409.exe	
Guidance	Administrator Operational Guidance: ShadowCube V7.0 Administrator Operational Guidance V1.4.pdf	
	User Guidance: ShadowCube V7.0 User Guidance V1.4.pdf	
	Preparative Procedure: ShadowCube V7.0 Preparative Procedure V1.5.pdf	

3rd party products included in the TOE

3rd party products are used in performing the function of the encryption/decryption, and distributed, being included in the installation files of the TOE components - the Policy Center and the client.

Policy Center

- Validated Cryptographic Module: MagicCrypto V2.2.0
- Encryption Support Library: OpenSSL 1.1.1i

Client

- Validated Cryptographic Module: MagicCrypto V2.2.0

0 Logical scope of the TOE

The logical scope of the TOE is as follows:

Policy Center

- Security audit
- Cryptographic support

- Electronic document encryption
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access

Client

- Security audit
- Cryptographic support
- Electronic document encryption
- Identification and authentication
- Protection of the TSF

Logical Scope / TOE			
Policy Center	Security Audit	• Security alarms • Audit data generation • Potential violation analysis • Audit review	• Selectable audit review • Action in case of possible audit data loss • Prevention of audit data loss
	Cryptographic Support	• Cryptographic key generation, distribution and destruction • Cryptographic operation	• Random bit generation (extended)
	Electronic Document Encryption	• Subset access control (document group based access control) • Security attribute based access control (document group based access control)	
	Identification and Authentication	• Authentication failure handling • TOE internal mutual authentication • Verification of secrets • Authentication	• Single-use authentication mechanism • Protected authentication feedback • Identification
	Security Management	• Management of security functions behaviour • Management of security attributes • Static attribute initialization • Management of TSF data	• Management of ID and password (extended) • Specification of management functions • Security roles
	Protection of the TSF	• Basic internal TSF data transfer protection • TSF testing	
	TOE Access	• Per user attribute limitation on multiple concurrent sessions • Management of TSF-initiated sessions (extended)	• TOE session establishment
Client	Security Audit	• Security alarms	• Audit data generation
	Cryptographic Support	• Cryptographic key generation, distribution and destruction • Cryptographic operation	• Random bit generation (extended)
	Electronic Document Encryption	• Subset access control (document group based access control) • Security attribute based access control (document group based access control)	
	Identification and Authentication	• Authentication failure handling • TOE internal mutual authentication • Verification of secrets • Authentication	• Single-use authentication mechanism • Protected authentication feedback • Identification
	Protection of the TSF	• Basic internal TSF data transfer protection • Basic protection of stored TSF data (extended)	• Availability protection of TSF data (extended) • TSF testing

[Figure 2] Logical scope of the TOE

Security Audit

The TOE generates audit data on the performance of any security function, and then, if a potential security violation occurs, sends an alarm email to the authorized administrator and records the event as audit data.

The TOE generates audit data for each TOE component as follows:

Policy Center

- Start-up/shutdown of the audit functions
- Success/failure of identification and authentication of the administrator

- Details of changes in product settings
- Details of the performance of the security functions

Client

- Start-up/shutdown of the audit functions
- Operation performed on an object
- Success/failure of identification and authentication of a document user
- Results of TSF self tests and results of integrity verification

Audit data includes the date and time of the event, type of the event, subject identity and the details of major event and outcome (success/failure) in detail.

The authorized administrator can review all audit data generated by the TOE through the GUI interface. The audit records are generated in a manner suitable for the authorized administrator to interpret the information, and the selective audit review based on logical relationships such as AND and OR, etc. is available.

In case of possible audit data loss, the TOE generates audit data and sends an email to the authorized administrator. It provides the function to overwrite the oldest stored audit records if the audit trail is full and send an email to the authorized administrator in case of the audit data loss.

Cryptographic Support

The TOE uses MagicCrypto V2.2.0, the validated cryptographic module developed by Dream Security, in order to apply the encryption/decryption algorithms to the TSF data according to the security policy, through which it provides assurance on the confidentiality, integrity and authentication.

Encryption/decryption algorithms used in cryptographic key generation and cryptographic key distribution, and cryptographic key sizes are specified below. If a cryptographic key and CSP being loaded on the memory are no longer used, they are zeroized and destructed

Client: Electronic document encryption

- ARIA_CTR 128 bits

Client: Verification of the signature of a document file's author and the client log originator

- RSA-PSS (SHA-256)

Policy Center, Client: Encryption of TSF data and communication data

- ARIA_CBC 256 bits
- RSA 2048 bits

Policy Center, Client: HASH generation

- SHA-256

Policy Center, Client: Cryptographic key distribution

- RSAES (SHA-256)

Policy Center, Client: Mutual authentication key agreement between TOE components

- ECDH (SHA-256)

Policy Center, Client: KEK generation

- PBKDF2 (SHA-256)

Policy Center, Client: Random bit generation

- HASH_DRBG (SHA-256)

Electronic Document Encryption

On the Policy Center, which is a TOE component, the authorized administrator can define the document group-based access control policy required for a document user to encrypt/decrypt a document to be protected. The client, which is a TOE component, provides the function of reading, encrypting (writing) and decrypting a document to be protected, according to the document group-based access control policy defined by the authorized administrator.

Identification and Authentication

The TOE identifies and authenticates the identity of the administrator or a document user through a GUI interface, and limits access if an authentication attempt fails. In case of identification and authentication failures, the TOE does not provide the feedback for the cause of failure (e.g., ID error, password error, etc.). Authentication data of the administrator or a document user are processed so as not to be reused. When the number of unsuccessful authentication attempts defined by the administrator has been met, the authentication is inactivated for five minutes in the case of the administrator, and inactivated until the system is rebooted in the case of a document user.

The TOE performs mutual authentication by using ECDH algorithm provided by the validated cryptographic module when communicating between the Policy Center and the client.

The administrator or a document user password must be at least 9 digits up to 16 digits in length and is required to contain a combination of uppercase/lowercase alphabetic characters, numeric characters and special characters.

The TOE identifies and authenticates the administrator on the basis of the administrator ID and an email authentication code, and identifies and authenticates a document user on the basis of a document user certificate. In addition, the password shall not be shown to the administrator and the user while the authentication is in progress.

Security Management

The TOE provides the function that enables the authorized administrator to set and manage security functions, security policies, security roles, etc.

Protection of the TSF

The TOE protects TSF data from disclosure and modification by encrypting the TSF data with the validated cryptographic module when it is transmitted between separate parts of the TOE. In addition, it protects TSF data stored in containers controlled by the TOE from unauthorized disclosure and modification by encrypting the TSF data with the validated cryptographic module.

The Policy Center, a TOE component, runs a suite of self tests and integrity verification during initial start-up, periodically during normal operation and at the request of the authorized administrator. The client, a TOE component, runs a suite of self tests on major processes in the TOE and verifies the integrity of the TSF data and TSF during initial start-up and periodically during normal operation.

The TOE prevents the unauthorized deletion for the environment configuration files and executable files of the client, which is a TOE component, and prevents the unauthorized termination for the executable files.

The Policy Center and the client, which are TOE components, provide the function to view the version information.

TOE Access

The TOE performs the function to terminate a session of the authorized administrator who has logged in through a GUI interface in case of the session timeout. It also provides the function that enables the authorized administrator to terminate a session for him/herself.

The TOE restricts the number of administrator sessions to one. If one device makes administrator's management access and another device performs a login process, a new access session is allowed and the previous access session is blocked.

Only IP addressed registered in advance can make access to the Policy Center. The authorized administrator can establish the number of connection IPs that can be registered. As many connection IP addresses as set by the authorized administrator can be registered

1.4 Conventions

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

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

Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection

This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized.*

Refinement

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

Security Target (ST) Author

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

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

1.5 Terms and Definitions

Terms in this ST, which are the same as in the CC, follows those in the CC and are not additionally stated herein.

Private Key

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

Object

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

Approved mode of operation

Operation mode of a cryptographic module using an approved cryptographic algorithm

Approved cryptographic algorithm

Cryptographic algorithm selected by the cryptographic module verification institution, considering the safety, the reliability, the interoperability and other factors in relation to block cipher, hash function, message authentication code, random bit generator, key setting, public key cryptography and digital signature cryptographic algorithm

Validated Cryptographic Module

Cryptographic module validated and approved by the cryptographic module verification institution, and to which a validation number was assigned

Public Key

Cryptographic key used together with an asymmetric cryptographic algorithm and is uniquely combined with a single entity (the subject that uses the public key). It can be disclosed.

Public Key(asymmetric) cryptographic algorithm

Cryptographic algorithm that uses a pair of a public key and a private key

Management console

Application program that provides GUI, CLI, etc. to the administrator and provides system management and configuration

Random bit generator (RBG)

Device or algorithm that outputs statistically independent and unbiased binary digits. The RBG used for cryptographic application generally generates 0 and 1 bit strings, and the sequence can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic types. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a "seed key," and the non-deterministic type RBG generates the output dependent on unpredictable physical sources.

Symmetric cryptographic technique

Cryptographic technique that uses the same secret key on both encryption and decryption mode. It is also called secret key cryptographic technique.

License

It means a variety of setting information such as access permission, operational environment configuration and policies necessary to use ShadowCube. It includes user information, document group certificate and use permission, license expiration, license expiration date, application program information and client setting information. License is assigned by the Policy Center. It is automatically renewed to the latest license if there is any change in the policy or setting information or according to the specified interval of license update.

Document group

It means items used to grant, to a ShadowCube user or department, permissions such as read, encryption (write) and decryption of a document to be protected. If a user who belongs to the document group generates a document, the document group information is immediately included in the document upon the generation and affects permissions of the document group.

Document Group Based Access Control

As the one of the discretionary access control, performing the access control for the entity based on group identity

Word processing program

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

Iteration

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

Target of security

It refers to an application program of a document to be protected that is encrypted/decrypted by ShadowCube.

Security Target (ST)

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

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Decryption

Restoration of the ciphertext into the original plaintext by using a decryption key

Secret Key

Cryptographic key used together with a secret key cryptographic algorithm and uniquely combined with one or multiple entities. It must not be disclosed.

User license

User license allows a user to make basic settings such as shell settings and client setting information, which is necessary to control document-related activities and operate ShadowCube.

Selection

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

System unique information

Unique information distinct from other information systems

Korea Cryptographic Module Validation Program (KCMVP)

Scheme to validate the security and implementation conformance of cryptographic modules used for the protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions

Encrypted file

Encrypted file

Encryption

The act of converting the plaintext into the ciphertext using the encryption key

Role Based Access Control (RBAC)

An access control that restricts access not by the direct relationship (e.g., user-access permission) but by the role defendant on the properties of the organization (e.g., user-role, access permission-role), when the user accesses an object

Operation (on a component of the CC)

Modification or repetition of a component. Allowed operation on components are assignment, iteration, refinement and selection.

Operation (on an object)

Specific type of action performed by a subject on an object

Authorized administrator

Authorized user to securely operate and manage the TOE

Authorized document user

The TOE user who may, in accordance with the SFRs, perform an operation

Authentication data

Information used to verify the claimed identity of a user

Regular file

A file that has not been encrypted or a file encrypted and then decrypted

Application Programming Interface (API)

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

Self-tests

Pre-operational or conditional test executed by the cryptographic module

Policy Center

Management server of ShadowCube that manages the security polices and cryptographic keys

Dependency

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

Subject

Active entity in the TOE that performs operations on objects

Client

ShadowCube agent program installed on the document user system

File conversion

Function to convert a file subject to the security into a regular file, a secure file and an executable secure file, respectively. File conversion is allowed only for a user granted the decryption permission and export permission of the document group.

Target of Evaluation (TOE)

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

Evaluation Assurance Level (EAL)

Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Family

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

Hard disk serial number

Unique number of individual hard disk assigned during the manufacturing process

TOE Security Functionality (TSF)

Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the security functional requirements (SFRs)

TSF Data

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

1.6 Security Target Contents

Chapter 1 ST Introduction describes ST reference and TOE overview.

Chapter 2 Conformance Claim describes the conformance with the Common Criteria, protection profile and package, and presents the conformance rationale and protection profile conformance statement

Chapter 3 Security Objectives defines the security objectives for the operational environment supported from

the operational environment in order to provide TOE security functionality more accurately.

Chapter 4 Extended Components Definition defines the extended components additionally needed according to the features of "Electronic Document Encryption."

Chapter 5 Security Requirements describes the security functional requirements and security assurance requirements.

Chapter 6 TOE Summary Specification explains the security functionality of the TOE that satisfies the security functional requirements.

1.7 Annex

The following document is annexed to this ST.

- Security policy document of the validated cryptographic module: MagicCrypto V2.2.0_Security Policy.pdf

2. Conformance Claim

This chapter describes how this ST confirms with the CC.

2.1 CC Conformance Claim

This ST and the TOE conforms to the Common Criteria as follows:

Classification	Conformance
Common Criteria	Common Criteria for Information Technology Security Evaluation V3.1 R5 * Common Criteria Part 1: Introduction and General Model, V3.1r5 (CCMB-2017-04-001, 2017. 4) * Common Criteria Part 2: Security Functional Components, V3.1r5 (CCMB-2017-04-002, 2017. 4) * Common Criteria Part 3: Security Assurance Components, V3.1r5 (CCMB-2017-04-003, 2017. 4)
Part 2 Security Functional Requirements	Extended: FCS_RBG.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2, FTA_SSL.5
Part 3 Security Assurance Requirements	Conformance
Package	Augmented: EAL1+ (ATE_FUN.1)

2.2 PP Conformance Claim

This ST conforms to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017).

Title	National Protection Profile for Electronic Document Encryption
Version	1.1
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Author	National Security Research Institute, Telecommunications Technology Association, Korea System Assurance
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Notification No. 2013-51 of the Ministry of Science, ICT and Future Planning, August 8, 2013)
CC Version	CC V3.1 r5
Certificate No.	KECS-PP-0821a-2017
Keywords	Document, Encryption
PP Conformance Type	Strict PP conformance

2.3 Package Conformance Claim

This ST claims conformance to assurance requirement package EAL1, and additionally defines some assurance requirements.

* Assurance package: EAL1 +(ATE_FUN.1)

2.4 Conformance Claim Rationale

Since this ST adopts the TOE type, security objectives of the operational environment, security requirements and assurance requirements in the same way as the Protection Profile, it "strictly conforms to the PP" as required in the National Protection Profile for Electronic Document Encryption V1.1.

2.4.1 Rationale in the TOE type

ST	PP	Rationale
Electronic Document Encryption Product	Adopts the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)

2.4.2 Rationale in security objectives for the operational environment

ST	PP	Rationale
OE.PHYSICAL_CONTROL	Adopts the National Protection Profile for electronic Document Encryption V1.1 (KECS-PP-0821a-2017)	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)
OE. TRUSTED_ADMIN		
OE.LOG_BACKUP		
OE. OPERATION_SYSTEM_REINFORCEMENT		
OE.SECURE_DBMS	Added	Augmented to security objectives for the operational environment since the TSF stores audit data on the operation of the TOE using a storage managed by DBMS according to OE.SECURE_DBMS in the National PP for Electronic Document Encryption, and protects audit data against unauthorized deletion or modification to support the stability
OE. TRUSTED_PATH		Augmented to security objectives for the relevant operational environment according to application notes of 'FTP_TRP.1' as the security management function is provided by the communication between a web browser on the administrator PC and the web server, an operational environment of the Policy Center.

OE.TIME_STAMP		Augmented to security objectives for the operational environment as the TSF is provided with the reliable time stamp function from the operational environment such as the reliable time synchronization of the external IT entity (e.g., reliable NTP server) according to OE.TIMESTAMP in the National PP for Electronic Document Encryption.

0 Rationale in security requirements

ST		PP	Rationale
Security Audit (FAU)	FAU_ARP.1	FAU_ARP.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)
	FAU_GEN.1	FAU_GEN.1	
	FAU_SAA.1	FAU_SAA.1	
	FAU_SAR.1	FAU_SAR.1	
	FAU_SAR.3	FAU_SAR.3	
	FAU_STG.3	FAU_STG.3	
	FAU_STG.4	FAU_STG.4	
Cryptographic Support (FCS)	FCS_CKM.1(1)	FCS_CKM.1(1)	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)
	FCS_CKM.1(2)	FCS_CKM.1(2)	
	FCS_CKM.2	FCS_CKM.2	
	FCS_CKM.4	FCS_CKM.4	
	FCS_COP.1(1)	FCS_COP.1(1)	
	FCS_COP.1(2)	FCS_COP.1(2)	
	FCS_RBG.1(Extended)	FCS_RBG.1(Extended)	
User Data Protection (FDP)	FDP_ACC.1	FDP_ACC.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)
	FDP_ACF.1	FDP_ACF.1	
Identification and Authentication (FIA)	FIA_AFL.1	FIA_AFL.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)
	FIA_IMA.1(Extended)	FIA_IMA.1(Extended)	
	FIA_SOS.1	FIA_SOS.1	
	FIA_UAU.1	FIA_UAU.1	
	FIA_UAU.4	FIA_UAU.4	
	FIA_UAU.7	FIA_UAU.7	
	FIA_UID.1	FIA_UID.1	
Security Management (FMT)	FMT_MOF.1	FMT_MOF.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS- PP-0821a-2017)
	FMT_MSA.1	FMT_MSA.1	
	FMT_MSA.3	FMT_MSA.3	
	FMT_MTD.1	FMT_MTD.1	

ST		PP	Rationale
	FMT_PWD.1(Extended)	FMT_PWD.1(Extended)	
	FMT_SMF.1	FMT_SMF.1	
	FMT_SMR.1	FMT_SMR.1	
Protection of the TSF (FPT)	FPT_ITT.1	FPT_ITT.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
	FPT_PST.1(Extended)	FPT_PST.1(Extended)	
	FPT_PST.2(Extended)	FPT_PST.2(Extended)	
	FPT_TST.1	FPT_TST.1	
TOE Access (FTA)	FTA_MCS.2	FTA_MCS.2	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
	FTA_SSL.5(Extended)	FTA_SSL.5(Extended)	
	FTA_TSE.1	FTA_TSE.1	

2.4.4 Rationale in security assurance requirements

Security Assurance Class	Assurance Component	PP	Rationale
Security Target Evaluation	ASE_INT.1	ASE_INT.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
	ASE_CCL.1	ASE_CCL.1	
	ASE_OBJ.1	ASE_OBJ.1	
	ASE_ECD.1	ASE_ECD.1	
	ASE_REQ.1	ASE_REQ.1	
	ASE_TSS.1	ASE_TSS.1	
Development	ADV_FSP.1	ADV_FSP.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
Guidance Documents	AGD_OPE.1	AGD_OPE.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
	AGD_PRE.1	AGD_PRE.1	
Life-cycle Support	ALC_CMC.1	ALC_CMC.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
	ALC_CMS.1	ALC_CMS.1	
Tests	ATE_FUN.1	ATE_FUN.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)
	ATE_IND.1	ATE_IND.1	
Vulnerability Assessment	AVA_VAN.1	AVA_VAN.1	Equivalent to the National Protection Profile for Electronic Document Encryption V1.1 (KECS-PP-0821a-2017)

0 PP Conformance Statement

This ST strictly conforms to the National Protection Profile for Electronic Document Encryption. In addition, this ST can perform evaluation as “low-assurance ST” only.

3. Security Objectives

The following security objectives for the operational environment are those handled by technical and procedural methods supported from the operational environment so that the TOE can provide security functionality more accurately.

0 Security Objectives for the Operational Environment

Policy Center

OE.PHYSICAL_CONTROL

The place where the Policy Center is installed and operated shall be equipped with access control and protection facilities so that it is accessible only by the authorized administrator.

OE.TRUSTED_ADMIN

The authorized administrator shall not have malicious intentions, shall be properly trained for the management functions of the Policy Center, and shall accurately fulfill the duties in accordance with the administrator guidance.

OE.LOG_BACKUP

The authorized administrator shall check the spare space in the audit data repository on a periodic basis in preparation for audit record loss and carry out audit data backup (external log server, separate storage device, etc.) to prevent audit data loss.

OE.OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator shall ensure the reliability and the security of the operating system by taking reinforcement measures to address the latest vulnerability of the operating system on which the Policy Center is installed and operated.

OE.SECURE_DBMS

The authorized administrator shall make sure that the audit data on the operation of the TOE are stored in the DBMS used by the TOE and the audit data are protected against unauthorized deletion or modification, thereby ensuring the stability.

OE.TRUSTED_PATH

The authorized administrator shall be provided with the security management function for secure communication between a web browser on the administrator PC and a web server, the operating environment of the Policy Center.

OE.TIME_STAMP

The TOE shall accurately record security-relevant events by using reliable time stamps provided by the OS of the Policy Center.

Client

OE.TRUSTED_ADMIN

The authorized administrator shall not have malicious intentions, shall be properly trained for the management functions of the client, and shall accurately fulfill the duties in accordance with the administrator guidance.

OE.OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator shall ensure the reliability and the security of the operating system by taking reinforcement measures to address the latest vulnerability of the operating system on which the client is installed and operated.

4. Extended Components Definition

4.1 Cryptographic Support (FCS)

4.1.1 Random bit generation

Family Behaviour

This family (FCS_RBG, Random Bit Generation) defines requirements for the capability that generates random numbers required for TOE cryptographic operation.

Component Levelling

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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

FCS_RBG.1 Random bit generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG.1.1

The TSF shall generate random bits, required to generate a cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

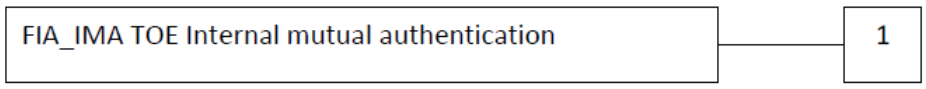
4.2 Identification & Authentication (FIA)

4.2.1 TOE internal mutual authentication

Family Behaviour

This family (FIA_IMA, TOE Internal Mutual Authentication) defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.

Component Levelling



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

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of mutual authentication

FIA_IMA.1 TOE internal mutual authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_IMA.1.1

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

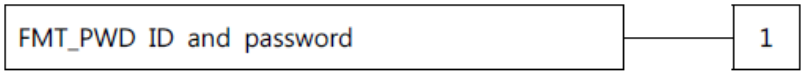
0 Security Management (FMT)

4.3.1 ID and password

Family Behaviour

This family (FMT_PWD, ID and password) 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 Levelling



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

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:

a) Management of ID and password configuration rules

Audit: FMT_PWD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password

FMT_PWD.1 Management of ID and password

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_PWD.1.1

The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: password combination rules and/or length]

2. [assignment: other management such as management of special characters unusable for password, etc.]

FMT_PWD.1.2

The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified* roles].

1. [assignment: *ID combination rules and/or length*]

2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3

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

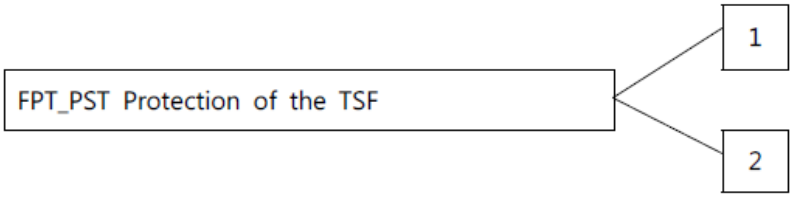
4.4 Protection of the TSF (FPT)

4.4.1 Protection of stored TSF data

Family Behaviour

This family (FPT_PST, Protection of Stored TSF data) defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component Levelling



FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.

FPT_PST.2 Availability protection of TSF data requires the TSF to ensure the defined level of availability for the TSF data.

Management: FPT_PST.1, FPT_PST.2

There are no management activities foreseen.

Audit: FPT_PST.1, FPT_PST.2

There are no auditable events foreseen.

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*].

FPT_PST.2 Availability protection of TSF data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.2.1

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

FPT_PST.2.2

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

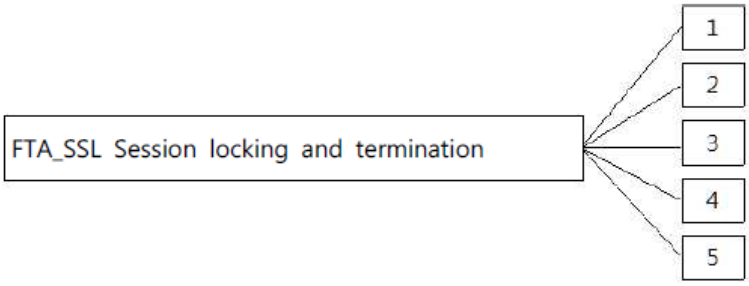
4.5 TOE Access (FTA)

4.5.1 Session locking and termination

Family Behaviour

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

Component Levelling



In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending on additional component as follows.

※ The relevant description for four components contained in CC Part 2 is omitted.

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

Management: FTA_SSL.5

The following actions can be considered for the management functions in FMT:

a) Specification of the time period of user inactivity that results in session locking or termination for

each user

b) Specification of the default user inactivity period that results in session locking or termination

Audit: FTA_SSL.5

It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive sessions

FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 authentication or No dependencies]

FTA_SSL.5.1

TSF shall [selection: • *lock the session and/or re-authenticate the user before unlocking the session,* • *terminate*] an interactive session after a [assignment: *time period of user inactivity*].

5. Security Requirements

This chapter specifies security functional requirements and assurance requirements that must be satisfied by the TOE.

[Table 5] Definition of subjects, objects, relevant security attributes and operations

Subject (user)		Object (information)		Operation	Relevant SFR
List	**Security attributes**	**List**	**Security attributes**		
Document user	• Document user ID • Password	• Document to be protected	• Document group ID • Document name • Document type • Document path	• Allowed to read a document if granted with read and encryption (write) permission, and encrypt and save a document • Decrypt a document if granted with decryption permission	• FDP_ACC.1 • FDP_ACF.1
Authorized administrator	• Administrator ID • Password • Authentication code	• Identification and authentication data	-	• Identification and authentication • Modify, delete	• FMT_MTD.1
		• Audit data	-	• Query	• FMT_MTD.1
		• Access IP setting	-	• Query, modify, delete, add	• FMT_MTD.1
		• Time of session timeout • Number of unsuccessful login attempts allowed • Minimum length of password	-	• Specification of limits • Modify	• FMT_MTD.1
		• TSF data	-	• Integrity verification	• FPT_MOF.1
		• Security attributes	-	• Query, delete, add default values	• FMT_MSA.1

		• Security function	-	• Determine a behaviour, inactivate, modify a behaviour	• FMT_MOF.1

※ The TOE provides only one type of an authorized administrator, that is, a web administrator designated in the process of TOE installation.

5.1 Security Functional Requirements

The TOE satisfies the security functional requirements as specified in the following table:

[Table 6] Security functional requirements

Security functional class	Security functional component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (Electronic Document Encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF Data Encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Electronic Document Encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF Data Encryption)
	FCS_RGB.1(Extended)	Random bit generation
Electronic Document Encryption (FDP)	FDP_ACC.1	Subset access control (Document Group Based-Access Control)
	FDP_ACF.1	Security attribute-based access control (Document Group Based-Access Control)
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback

Security functional class	Security functional component	
Identification and Authentication (FIA)	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_PST.2(Extended)	Availability protection of stored TSF data
	FPT_TST.1	TSF testing
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions (Policy Center)
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

5.1.1 Security audit (FAU)

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1

The TSF shall take [assignment: list of actions] upon detection of a potential security violation.

• Send an email to the authorized administrator upon detection of a potential security violation.

Policy Center	Client
• If a threshold for the unsuccessful authentication attempts has been reached • If self test or integrity verification fails • If self test of the validated cryptographic module fails • If the audit storage limit is expected to be exceeded • If the audit storage limit is exceeded	• If a threshold for the unsuccessful authentication attempts has been reached • If self test or integrity verification fails • If self test of the validated cryptographic module fails • In violation of control rules

• Inactivate the authentication if authentication attempts fail for the defined number of times.

Policy Center	Client
Inactivate the identification and authentication for five minutes	Reboot the PC and disable the identification and authentication for five minutes

• Reboot the system if the self test of the validated cryptographic module fails in the client.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

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

1. Start-up and shutdown of the audit functions;
2. All auditable events for the *not specified level* of audit; and
3. [Refer to the "auditable events" in [Table 7] Auditable events, [none]]

FAU_GEN.1.2

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

1. Date and time of the event, type of event, subject identity (if applicable), details of the event and the outcome (success or failure) of the event
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Refer to the content of "additional audit record" in [Table 7] Auditable events, [none]]

[Table 7] Auditable events

TOE component	Functional component	Auditable event	Additional audit record
Policy Center	FAU_ARP.1	Actions taken due to potential security violations	
	FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
	FAU_STG.3	Actions taken due to exceeding of a threshold	
	FAU_STG.4	Actions taken due to the audit storage failure	
	FCS_CKM.1(2)	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.4	Success and failure of the activity	
	FCS_COP.1	Success and failure, and the type of cryptographic operation	
	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken	

TOE component	Functional component	Auditable event	Additional audit record
Policy Center	FIA_IMA.1(Extended)	Success and failure of mutual authentication	
	FIA_UAU.1	All results of administrator authentication	
	FIA_UAU.4	Attempts to reuse email authentication code	
	FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
	FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
	FMT_MSA.1	All modifications to the security attributes	Modified security attribute value
	FMT_MSA.3	Modifications to the basic settings of allowance or restriction rules, All modifications to the initial values of security attributes	Modified security attribute value
	FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data value
	FMT_PWD.1(Extended)	Modification to the password combination rules	
	FMT_SMF.1	Use of the management functions	
	FPT_TST.1	* The results of TSF self tests and the results of integrity verification * The results of failure of self tests of the validated cryptographic module and the results of integrity verification	Executable file whose integrity has been violated
	FTA_MCS.2	Termination of existing access based on the limitation of multiple concurrent sessions	
	FTA_SSL.5(Extended)	Termination of management access sessions after a period of inactivity of the authorized administrator	
	FTA_TSE.1	Denial of management access session establishment of the administrator based on access IP	
Client	FCS_CKM.1(2)	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.4	Success and failure of the activity	
	FCS_COP.1	Success and failure, and the type of cryptographic operation	

TOE component	Functional component	Auditable event	Additional audit record
Client	FDP_ACF.1	Execution of an operation on an object	Identity information of an object
	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken	
	FMT_IMA.1(Extended)	Success and failure of mutual authentication	
	FIA_UAU.1	All results of the authentication of a document user	
	FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
	FPT_TST.1	* The results of TSF self tests and the results of integrity verification * The results of failure of self tests of the validated cryptographic module and the results of integrity verification	Executable file whose integrity has been violated

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1

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

FAU_SAA.1.2

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

1. Accumulation or combination of [authentication failure audit event among auditable events in FIA_UAU.1, integrity violation audit event and failure of self tests of the validated cryptographic module among auditable events in FPT_TST.1, audit event where a threshold on the audit trail ex exceeded in FAU_STG.3, audit event where the audit trail is full in FAU_STG.4, violation of control rules in FDP_ACF.1]

2. [None]

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

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

FAU_SAR.1.2

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [search or ordering method of sorting in ascending/descending order] of audit data based on [[Table 8] Audit data type and selection of audit data type].

[Table 8] Audit data type and selection of audit data type

Audit data type	Audit record	Logical relationship	Ordering method
User audit	Classification, date and time of task, IP, MAC, department code, department name, employee number, user name, job title, module, message, recording date	All combination of audit records (AND)	Search
		Combination of classification records (OR)	Search
		Based on one item selected in the audit records	Sort
Administrator audit	Classification, menu, date and time of task, IP, department code, department name, employee number, administrator, job title, task details	All combination of audit records (AND)	Search
		Combination of classification records (OR)	Search
		Combination of menu records (OR)	Search
		Based on one item selected in the audit records	Sort
System audit	Date and time of task, IP, task details	Date and time of task	Search
		Based on one item selected in the audit records	Sort
Document log	Document group, target of security, date and time of task, department code, department name, employee number, user name, job title, total, create, read	All combination of audit records (AND)	Search
		Combination of document group records (OR)	Search
		Combination of records of target of security (OR)	Search
		Based on one item selected among department code, department name, employee number, user name, job title, total, create and read	Sort
Document detail log	Date and time of task, license, classification, IP, MAC, department code, department, employee number, user, job title, program name, version, storage device, file name, full path, document group	All combination of audit records (AND)	Search
		Combination of license records (OR)	Search
		Combination of classification records (OR)	Search
		Based on one item selected in the audit records	Sort

Audit data type	Audit record	Logical relationship	Ordering method
Decryption log	Document group, date and time of task, department code, department name, employee number, user name, job title, decryption count	All combination of audit records (AND)	Search
		Based on one item selected among department code, department name, employee number, user name, job title and decryption count	Sort
Decryption detail log	Time and date of task, license, classification, IP, MAC, department code, department, employee number, user, job title, file name, size	All combination of audit records (AND)	Search
		Combination of license records (OR)	Search
		Combination of classification records (OR)	Search
		Based on one item selected in the audit records	Sort
Integrity verification history	Date and time of task, computer name, IP, MAC, hard disk, client version, message	All combination of audit records (AND)	Search
		Based on one item selected in the audit records	Sort
Login history based on period	Date and time of task, login, logout, IP, MAC, host name, hard disk serial, department code, department name, employee number, user name, job title, login method, date and time of recording	All combination of audit records (AND)	Search
		Combination of login method records (OR)	Search
		Based on one item selected among login, logout, IP, MAC, host name, hard disk serial, department code, department name, employee number, user name, job title, login method and date and time of recording	Sort
Last login based on user	Department code, department, employee number, user, job title, date and time of last login	All combination of audit records (AND)	Search
		Based on one item selected in the audit records	Sort

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1

The TSF shall [notification to the authorized administrator, [none]] if the audit trail exceeds [-10% of the storage defined by the authorized administrator as follows].

- Default value: 70% of the audit storage (configurable range: 50%-90% of the audit storage)

※ The value defined by the authorized administrator is the full capacity of the audit trail. The audit trail storage begins to be predicted to be full when the audit trail reaches the volume "10% lower than its full capacity."
※ The authorized administrator is notified via email.

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1

The TSF shall *overwrite the oldest stored audit record in each log stored in each table* and [record audit logs, send an email to the authorized administrator] if the audit trail is full.

5.1.2 Cryptographic support (FCS)

The TOE uses approved cryptographic algorithms of the validated cryptographic module (MagicCrypto V2.2.0) as follows:

[Table 9] Approved cryptographic algorithm of the validated cryptographic module

List of standards	Encryption method	Cryptographic algorithm	Key size	Use
KS X 1213-1	Block cipher	ARIA_CTR	128	User data encryption • Client: file encryption when a document to be protected is saved

		ARIA_CBC	256	TSF data encryption
				• Policy Center
				  • DEK
				  • DB password
				  • Document group key
				• Client
				  • Private key of the user certificate
				  • License file
				  • Configuration file

		ARIA_CBC (SHA256)	256	Protection of data transmitted between TOE components (Policy Center – client)
ISO/IEC 11770-3	Key setting	ECDH (SHA-256)	256	Mutual authentication key agreement between TOE components (Policy Center – Client)
TTAS.KO-12.0334	Key deviation	PBKDF2 (SHA-256)	256	DEK encryption

ISO/IEC 18031	Random bit generator	HASH_DRBG (SHA-256)	256	• TSF data and document encryption
				  • Policy Center: DB password, license
				  • Client: document
				• Generation of 16-digit authentication code
				  • Policy Center: when the web administrator logs in
				  • Client: when issuing a document user certificate

List of standards	Encryption method	Cryptographic algorithm	Key size	Use
ISO/IEC 18033-2	Public key cryptography	RSAES (SHA-256)	2048	The Policy Center distributes DEK to the client.

ISO/IEC 14888-2	Electronic signature	RSA-PSS (SHA-256)	2048	Client: Verify the signatures of the document author and audit log originator

ISO/IEC 10118-3	Hash function	SHA-256	256	• Policy Center
				  • Store the web administrator's password in the DB (SALT added)
				  • Hash the KEK generated with CPU ID + web server start time + random bits
				  • Store HASH of files subject to integrity verification
				• Client
				  • Hash the KEK generated with email + reverse (email) + random bits

※ Random bits used in generating the KEK are generated with HASH_DRBG (SHA-256) which is a random bit generator of the validated cryptographic module.

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

Hierarchical: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FCS_RBG.1(Extended) Random bit generation

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified [cryptographic key algorithm] and specified [key sizes] that meet the following [list of standards].

Type	Cryptographic algorithm	Key size	List of standards
DEK	HASH_DRBG (SHA-256)	256 bits	ISO/IEC 18031

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

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FCS_RBG.1(Extended) Random bit generation

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified [cryptographic key algorithm] and specified [key sizes] that meet the following [list of standards].

Type	Cryptographic algorithm	Key size	List of standards	Use
KEK	PBKDF2 (SHA-256)	256 bits	TTAS.KO-12.0334	Generation of the first KEK by deriving the key with the password entered upon login
KEK	SHA-256	256 bits	ISO/IEC 10118-3	Generation of the KEK to be used in memory

				loading
DEK	HASH_DRBG (SHA-256)	256 bits	ISO/IEC 18031	Random bit generation
Session key	ECDH (SHA-256)	256 bits	ISO/IEC 11770-3	Session key agreement during mutual authentication
Session key pair	ECDH (SHA-256)	256 bits	ISO/IEC 11770-3	Generation of a key pair for session key agreement

※ Random bits used in generating the KEK are generated with HASH_DRBG (SHA-256) which is a random bit generator of the validated cryptographic module.

※ KEK generated with SHA-256 HASH consists of the following information:

* Policy Center: CPUID + web server start time + random bits

* Client: Email address + reverse (email address) + random bits

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

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

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified distribution method [ECDH (SHA-256), RSAES (SHA-256)] that meet the following [list of standards].

Classification	Cryptographic algorithm	List of standards	Distribution method
Session key	ECDH (SHA-256)	ISO/IEC 11770-3	Session key agreement through the generated key pair
DEK	RSAES (SHA-256)	ISO/IEC 18033-2	Distribution of the DEK used in electronic document encryption/decryption through the pubic key method

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1(1) Cryptographic key generation (electronic document encryption), FCS_CKM.1(2) Cryptographic key generation (TSF data encryption)]

FCS_CKM.4.1

The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization of DEK, KEK and critical security parameters] that meets the following [none].

Type	Key	Cryptographic algorithm	Timing of destruction
Electronic document encryption	DEK	HASH_DRBG (SHA-256)	•Client: when terminating an application program (document program)
TSF data encryption	KEK	PBKDF2 (SHA-256)	•Policy Center: when terminating IIS or the system •Client: when a user logs out or when terminating the system
		SHA-256	
	DEK	HASH_DRBG (SHA-256)	
	Session key	ECDH (SHA-256)	• Policy Center: when terminating IIS or the system • Client: when terminating the system
	Session key pair		

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], FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [electronic document encryption/decryption] in accordance with a specified cryptographic algorithm [ARIA_CTR] and cryptographic key sizes [128 bits] that meet the following [list of standards].

Cryptographic algorithm	Key size	List of standards	List of cryptographic operations
ARIA_CTR	128 bits	KS X 1213-1	Electronic document encryption/decryption

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

Hierarchical to: No other components.

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

key destruction

FCS_COP.1.1

The TSF shall perform [list of cryptographic operations] in accordance with a specified cryptographic algorithm [ARIA_CBC, RSAES (SHA-256), ECDH (SHA-256)] and a specified cryptographic key size [256 bits, 2048 bits] that meet the following [list of standards].

Cryptographic algorithm	Cryptographic key size	List of standards	List of cryptographic operations
ARIA_CBC	256 bits	KS X 1213-1	• Transmission between the Policy Center and the client • Encryption/decryption of TOE security policy data • Policy Center • DB password encryption • DEK and KEK encryption • Client • Encryption/decryption of security header of an encrypted document • Encryption/decryption of text and structure that stores security attributes of an encrypted document • Encryption/decryption of private key of a document user's certificate • Encryption/decryption of authentication data when issuing a document user's certificate • Encryption/decryption of a document user's certificate • Encryption/decryption of a document user's license • DEK and KEK encryption

RSAES (SHA-256)	2048 bits	ISO/IEC 18033-2	• Policy Center • Verification of log signature transmitted from the client • Client • Document user certificate signature / verification of signature • Document user license signature / verification of signature • Log signature/verification of signature • Encryption/decryption of cryptographic key of document user license • Encryption/decryption of cryptographic key of security header of an encrypted document
ECDH (SHA-256)	256 bits	ISO/IEC 11770-3	Session key agreement in mutual authentication

FCS_RBG.1(Extended) Random bit generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RGB.1.1

The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following [list of standards].

Classification	Cryptographic algorithm	Key Size	List of standards
Random bit generator	HASH_DRBG (SHA-256)	256 bits	ISO/IEC 18031

5.1.3 Electronic document encryption (FDP)

FDP_ACC.1 Subset access control (document group-based access control)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1

The TSF shall enforce the [document group-based access control] on [document users to read, encrypt(write) and decrypt a protected document].

1. Subject: Document users who encrypt/decrypt the information through the TOE

2. Object: Document to be protected

3. Operation: Read, encrypt (write), decrypt

※ Document group-based access control means that use permissions such as read, encrypt (write), decrypt, etc. are assigned to document users according to their document groups, and document encryption/ decryption is performed according to the established policy.
※ Read means an act of opening a protected document file. Encrypt (Write) means an act of editing a document to be protected and encrypting the document when saving it. Decrypt means an act of decrypting an encrypted document into plaintexts.

FDP_ACF.1 Security attribute-based access control (document group-based access control)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

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

Subject

• Document user who encrypts/decrypts the information through the TOE

Security attributes of the subject

• Document user ID

• Document group ID

Object

• Document to be protected

Security attributes of the object

• Document group ID
• Document name
• Document type
• Document path

FDP_ACF.1.2

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

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

b) *None*

]

FDP_ACF.1.3

The TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [none]

FDP_ACF.1.4

The TSF shall explicit4ly deny access of the subject to objects based on the following additional rules: [none]

※ Document group-based access control means that use permissions such as read, encrypt (write), decrypt, etc. are assigned to document users according to their document groups, and document encryption/

decryption is performed according to the established policy.

5.1.4 Identification and authentication (FIA)

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 *administrator configurable positive integer within [1~5]* unsuccessful authentication attempts occur related to [the following list of authentication events].

- Administrator authentication through GUI of the Policy Center
- Document user authentication through GUI of the client

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall perform [the following list of actions].

Authentication event	Action
Administrator authentication through GUI of the Policy Center	• Inactivate the authentication for five minutes (no configurable range) • Send an email to the authorized administrator after audit log is recorded
Document user authentication through GUI of the client	• Inactivate the authentication until the rebooting of the document user's PC is completed • Send an email to the authorized administrator after audit log is recorded

※ The number of unsuccessful authentication attempts configurable by the authorized administrator is 1~5, and the default value is 3.

FIA_IMA.1(Extended) TOE internal mutual authentication

Hierarchical to: No other components

Dependencies: No dependencies.

FIA_IMA.1.1

The TSF shall perform mutual authentication between [TOE components in [Table 10] Cryptographic algorithm provided by the validated cryptographic module] in accordance with a specified [cryptographic algorithm in [Table 10] Cryptographic algorithm provided by the validated cryptographic module] that meets the following [standard in [Table 10] Cryptographic algorithm provided by the validated cryptographic module].

[Table 10] Cryptographic algorithm provided by the validated cryptographic module

TOE component	Cryptographic algorithm	Standard
Policy Center	ECDH (SHA-256)	ISO/IEC 11770-3

Client		

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [the following defined quality metric].

• Combination of three types of characters: Uppercase/lowercase alphabetic characters, numeric characters and special characters (!, @, #, $, %, ^, *, -, _, +, =)
• At least 9 digits up to 16 digits

FIA_UAU.1 Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

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

Administrator authentication
• Request to enter an email authentication code
• Request for the identification and authentication procedure (login screen)

Document user authentication
• Certificate issuance
  • Request for document user certificate
  • Request to enter an email authentication code
  • Generation of a document user certificate
  • Request for the identification and authentication procedure (login screen)
• After the certificate is issued
  • Selection of the document user certificate
  • Request for the identification and authentication procedure (login screen)

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.

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 [the following identified authentication mechanism(s)].

Authentication target	Authentication mechanism
Administrator authentication	Email authentication code
Document user certificate issuance	Email authentication code

※ Email authentication code is One-time Password (OTP) that cannot be reused after the authentication.
※ Document user authentication is processed with a certificate that is encrypted with the validated cryptographic algorithm ARIA_CBC (256 bits) and stored on the document user's system. Since the password cannot be checked, it ensures the uniqueness of the session in the client environment.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Authentication

FIA_UAU.7.1

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

Policy Center

- Administrator ID
- Masked password
- Email authentication code
- Authentication failure feedback (message)
  - Authentication failure

Client

- Document user certificate
- Masked password
- Authentication failure feedback (message)
  - Authentication failure

※ Application notes: In case of failed identification and authentication, feedback on a reason for the failure (e.g. ID error, password error) shall not be provided.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1

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

- Administrator authentication: Request for the identification and authentication procedure (login screen)
- Document user authentication: Request to select a document user certificate

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.

5.1.5 Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

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

FMT_MOF.1.1

The TSF shall restrict the ability to ***conduct management actions of the functions*** [in [Table 11] Security functions and management ability].

[Table 11] Security functions and management ability

Administrator type	Classification	Security function	Ability			
			Determine a behaviour	Disable	Enable	Modify a behaviour
Authorized administrator	Object setting	Department management	O	-	-	O
		User management	O	-	-	O
	Policy setting	Document group policy	O	-	-	O
		Policy for target of security	O	-	-	O
		Basic license policy	-	-	-	O
		Multi-license policy	-	-	-	O
	Authentication management	Certificate issuance status	O	-	-	O
		License issuance status	O	-	-	O
	Log statistics	User audit	O	-	-	-
		Administrator audit	O	-	-	-
		System audit	O	-	-	-
		Document log	O	-	-	-
		Decryption log	O	-	-	-
		Integrity verification history	O	-	-	-

		Login history	O	-	-	-
	Environment configuration	Environment configuration	-	-	-	O
		Disk usage check	-	-	-	O
		Policy Center self test and integrity verification	-		O	O

※ 'O' indicates the management function is provided, and '-' indicates there is no management ability provided.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall restrict the ability to ***conduct management actions of the functions*** [in [Table 12] Security attribute and access control SFP].

[Table 12] Security attribute and access control SFP

Access control SFP	Security attribute	Ability			
		Query	Modify	Delete	Add
Document group-based access control	Document user ID	O	-	O	O
	Document group ID	O	-	O	O
	Target of security	O	-	O	O

※ 'O' indicates the management function is provided, and '-' indicates there is no management ability provided.

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 [document group-based access control policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

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

FMT_MTD.1 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*** the [[Table 13] TSF data and management ability] to [the authorized administrator].

[Table 13] TSF data and management ability

Authorized role	TSF data	Ability			
		Query	Modify	Delete	Add
Authorized administrator	Document user certificate	O	-	O	-
	Audit data	O	-	-	-
	Access IP setting	O	O	O	O
	Time of session timeout	O	O	-	-
	Allowed number of unsuccessful login attempts	O	O	-	-
	Minimum digits of password	O	O	-	-
Document user	Document user certificate	O	O	O	O
	License	O	O	-	-
	Environment configuration	O	O	-	-

※ 'O' indicates the management function is provided, and '-' indicates there is no management ability provided.

※ The ability of the authorized administrator to manage the deletion of a document user certificate means the revocation of the certificate.

※ The ability of a document user to manage the deletion of a certificate means the deletion of the certificate that has been issued or the revocation of the certificate.

※ The modification of a license means the update of the license.

※ The modification of the environment configuration means the function of language setting.

FMT_PWD.1(Extended) Management of ID and password

Hierarchical to: No other components.

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

FMT_PWD.1.1

The TSF shall restrict the ability to manage the password of [the following password combination rules and length] to [the authorized administrator].

1. [Password combination rules and length]
   - Combination of three types of characters: Uppercase/lowercase alphabetic characters, numeric characters and special characters (!, @, #, $, %, ^, *, -, _, +, =)

- At least 9 digits up to 16 digits

2. [None]

FMT_PWD1.2

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

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

FMT_PWD.1.3

The TSF shall provide the capability for *setting ID and password when installing*.

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: [the following list of management functions to be provided by the TSF].

- List of security functions specified in FMT_MOF.1
- List of management of TSF data specified in FMT_MTD.1
- List of security attributes specified in FMT_MSA.1
- Security attribute initialization specified in FMT_MSA.3
- FMT_PWD.1(Extended) Management of ID and password

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Identification

FMT_SMR.1.1

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

FMT_SMR.1.2

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

※ Only one type of the administrator is provided to manage the TOE product, which is a web administrator designated in the process of the product installation. The authorized administrator accesses through the web interface (HTTPS) and manages the function of security management.

5.1.6 Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1

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

Classification	Encryption object	Encryption method	Cryptographic algorithm	Data Storage	List of standards
Transmission between the Policy Center and the client	Security policy data	Block cipher	ARIA_CBC (SHA256)	Packet	KS X 1213-1

FPT_PST.1(Extended) Basic protection of the TSF

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1

The TSF shall protect [[Table 14] Stored TSF data] stored in containers controlled by the TSF from unauthorized *disclosure, modification.*

[Table 14] Stored TSF data

TOE component	DBMS	File system
Policy Center	Administrator password	N/A
	Document user certificate	
	License	
	Environment configuration	
	Audit data	
Client	N/A	Document user certificate
		Document user private key
		TOE environment configuration file
		Audit data

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.2.1

The TSF shall *prevent* the unauthorized deletion for [the following TSF data].

Executable files of the client

- sccm.exe
- scconv.exe
- scmain.exe
- scboots64.exe
- scboot64.exe
- scboot.exe
- scsysinfo.exe
- scsysinfo64.exe

FPT_PST.2.2

The TSF shall *prevent* the unauthorized termination for [the following TSF data].

Executable files of the client

- scmain.exe
- scboots64.exe
- scboot64.exe
- scboot.exe

FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1

The TSF shall run a suite of self tests during *initial start-up, periodically during normal operation* to demonstrate the correct operation of [*the following parts of TSF*].

TOE components	TSF	Role
Policy Center	ShadowCubeSelfTest.exe	Process related to the operation of security functions
Client	scmain.exe	Process for user GUI support
	scboots64.exe	Process related to the operation of user security functions

FPT_TST.1.2

The TSF shall provide the **authorized administrator** with the capability to verify the integrity of [*the following parts of TSF Data*].

TOE component	TSF	Role
Policy Center	config.ini	Configuration file used in the web service in the process of initializing the Policy Center
	db.config	Configuration file used in the web service to connect DBMS
	log4net.xml	Configuration file used in the web service in logging setting
	web.config	Web service configuration file

FPT_TST.1.3

The TSF shall provide the **authorized administrator** with the capability to verify the integrity of [*the following parts of TSF*].

TOE component	TSF	Role
Policy Center	admin.dll	Management of security attributes
	scbase.dll	Management of security attributes related to license
	scpclib.dll	Management of security attributes related to database
	scpcws.dll	Management of security attributes related to client

	ssDeulmeori.dll	Process for the management of identification and authentication
	ssJikimi.dll	Process for the use of the validated cryptographic module
	ssNeobi.dll	Utility process for the support of management console
	ssNeonadeuli.dll	Process for encryption/decryption processing
	ssServerHelper.dll	Process for the management of cryptographic functions
	MagicCryptoV22.dll	Validated cryptographic module
Client	scboot.exe, scboot64.exe, scboots64.exe	Process related to the operation of security functions
	sccm.exe	Certificate management console
	scconv.exe	File encryption/decryption management console
	scmain.exe	Management console to support user GUI
	scsysinfo.exe, scsysinfo64.exe	Process related to the operation of security functions
	scewvsc.dll, scewvsc64.dll, scewvsd.dll, scewvsd64.dll, scewvsp.dll, scewvsp64.dll, scewwss.dll, scewwss64.dll	Process for access control rules
	scshell.dll, scshell64.dll	Process to connect Windows File Explorer
	scwinui.dll, scwinui64.dll	Process for the support of identification and authentication

TOE component	TSF	Role
Client	ssDeulmeori.dll	Process for the management of identification and authentication
	ssJikimi.dll	Process for the use of the validated cryptographic module
	ssMigratorHelp.dll	Process for the support of ShadowCube version compatibility
	ssNeobi.dll	Utility process for the support of management console
	ssNeonadeuli.dll	Process for encryption/decryption processing
	ssServerHelper.dll	Process for the management of cryptographic functions
	MagicCryptoV22.dll MagicCrypto32V22.dll	Validated cryptographic module

5.1.7 TOE Access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

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

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1

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

FTA_MCS.2.2

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

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication or no dependencies.

FTA_SSL.5.1

The TSH shall *terminate* an interactive session of the **authorized administrator** after [a time interval of the **authorized administrator** inactivity as follows].

- Default value: 10 minutes (configurable range: 1 to 10 minutes)

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1

The TSF shall be able to deny the **authorized administrator's management access session** establishment based on [connection IP, *none*].

※ Two connection IPs are provided by default, and the number of IPs configurable by the authorized administrator is two to five.

5.2 Security Assurance Requirements

Assurance requirements of this ST are comprised of assurance components in CC Part 3, and the evaluation assurance level is EAL1+. [Table 15] below summarizes assurance components.

[Table 15] Assurance requirements

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

5.2.1 Security Target evaluation

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements

ASE_INT.1.1D

The developer shall provide a 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 summarise the usage and major security features of the TOE.

ASE_INT.1.5C

The TOE overview shall identify the TOE type.

ASE_INT.1.6C

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

ASE_INT.1.7C

The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C

The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

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

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

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction, ASE_ECD.1 Extended components definition, ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D

The developer shall provide a conformance claim.

ASE_CCL.1.2D

The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C

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

ASE_CCL.1.2C

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

ASE_CCL.1.3C

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

ASE_CCL.1.4C

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

ASE_CCL.1.5C

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

ASE_CCL.1.6C

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

ASE_CCL.1.7C

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

ASE_CCL.1.8C

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

ASE_CCL.1.9C

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

ASE_CCL.1.10C

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

Evaluator action elements

ASE_CCL1.1E
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies

Developer action elements

ASE_OBJ.1.1D

The developer shall provide a statement of security objectives.

Content and presentation elements

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

Evaluator action elements

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies

Developer action elements

ASE_ECD.1.1D

The developer shall provide a statement of security requirements.

ASE_ECD.1.2D

The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C

The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C

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

ASE_ECD.1.3C

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

ASE_ECD.1.4C

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

ASE_ECD.1.5C

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

Evaluator action elements

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

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

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.1.1D

The developer shall provide a statement of security requirements.

ASE_REQ.1.2D

The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C

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

ASE_REQ.1.2C

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

ASE_REQ.1.3C

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

ASE_REQ.1.4C

All operations shall be performed correctly.

ASE_REQ.1.5C

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

ASE_REQ.1.6C

The statement of security requirements shall be internally consistent.

Evaluator action elements

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

ASE_TSS.1 TOE summary specification

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

Developer action elements

ASE_TSS.1.1D

The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C

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

Evaluator action elements

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

ASE_TSS.1.2E

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

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies

Developer action elements

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

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

Content and presentation elements

ADV_FSP.1.1C

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

ADV_FSP.1.2C

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

ADV_FSP.1.3C

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

ADV_FSP.1.4C

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

Evaluator action elements

ADV_FSP.1.1E

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

ADV_FSP.1.2E

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

5.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D

The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C

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

AGD_OPE.1.2C

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

AGD_OPE.1.3C

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

AGD_OPE.1.4C

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

AGD_OPE.1.5C

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

AGD_OPE.1.6C

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

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E

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

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies

Developer action elements

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C

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

AGD_PRE.1.2C

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

Evaluator action elements

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

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

5.2.4 Life-cycle support

ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C

The TOE shall be labelled with its unique reference.

Evaluator action elements

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

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies

Developer action elements

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

Content and presentation elements

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

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

Evaluator action elements

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

5.2.5 Tests

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements

ATE_FUN.1.1D

The developer shall test the TSF and document the results.

ATE_FUN.1.2D

The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C

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

ATE_FUN.1.2C

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

ATE_FUN.1.3C

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

ATE_FUN.1.4C

The actual test results shall be consistent with the expected test results.

Evaluator action elements

ATE_FUN.1.1E

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

ATE_IND.1 Independent testing: conformance

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

Developer action elements

ATE_IND.1.1D

The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.1.1C

The TOE shall be suitable for testing.

Evaluator action elements

ATE_IND.1.1E

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

ATE_IND.1.2E

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

5.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

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

Developer action elements

AVA_VAN.1.1.D

The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.1.1C

The TOE shall be suitable for testing.

Evaluator action elements

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

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

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

5.2.7 Security requirements rationale

Dependency of the security functional requirements

The following table shows dependency of security functional requirements.

No.	Functional component	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4

6	FAU_STG.3	FAU_STG.1	Rationale (2)
7	FAU_STG.4	FAU_STG.1	Rationale (2)
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	10, 12
		FCS_CKM.4	11
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	10, 13
		FCS_CKM.4	11
10	FCS_CKM.2	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1]	8, 9
		FCS_CKM.4	11
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
12	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	11
13	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9
		FCS_CKM.4	11
14	FCS_RBG.1(Extended)	-	-
15	FDP_ACC.1	FDP_ACF.1	16
16	FDP_ACF.1	FDP_ACC.1	15
		FMT_MSA.3	26
17	FIA_AFL.1	FIA_UAU.1	20
18	FIA_IMA.1(Extended)	-	-
19	FIA_SOS.1	-	-
20	FIA_UAU.1	FIA_UID.1	23
21	FIA_UAU.4	-	-
22	FIA_UAU.7	FIA_UAU.1	20
23	FIA_UID.1	-	-
24	FMT_MOF.1	FMT_SMF.1	29
		FMT_SMR.1	30
25	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	15
		FMT_SMF.1	29
		FMT_SMR.1	30

No.	Functional component	Dependency	Reference No.
26	FMT_MSA.3	FMT_MSA.1	25
		FMT_SMR.1	30
27	FMT_MTD.1	FMT_SMF.1	29
		FMT_SMR.1	30
28	FMT_PWD.1(Extended)	FMT_SMF.1	29
		FMT_SMR.1	30
29	FMT_SMF.1	-	-
30	FMT_SMR.1	FIA_UID.1	23
31	FPT_ITT.1	-	-
32	FPT_PST.1(Extended)	-	-
33	FPT_PST.2(Extended)	-	-
34	FPT_TST.1	-	-
35	FTA_MCS.2	FIA_UID.1	23
36	FTA_SSL.5(Extended)	FIA_UAU.1	20
37	FTA_TSE.1	-	-

※ Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1. However, reliable time stamp provided by OE.Time Stamp, the security objective for the operational environment of this ST, is used, thereby satisfying the dependency.
※ Rationale (2): FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1. However, it is protected from unauthorized deletion or modification in accordance with OE.SECURE_DBMS, the security objective for the operational environment of this ST, thereby satisfying the dependency.

Dependency of the security assurance requirements

The dependency of each assurance package provided in Common Criteria for Information Technology Security Evaluation is already satisfied. Thus, the rationale is omitted herein.

The augmented SAR ATE_FUN.1 has a dependency on ATE_COV.1. ATE_FUN.1has been augmented to ensure that the developer performs tests on test items correctly and documents them in the documentation. However, ATE_COV.1 is not included in this ST since it is deemed not necessarily required to include ATE_COV.1 that presents the consistency between test items and TSFI.

6. TOE Summary Specification

This chapter specifies the security functionality of the TOE that satisfies the SFRs.

6.1 Security Audit

The TOE sends an alarm email to the administrator upon detection of a potential security violation and generates audit data which can be reviewed by the authorized administrator. It also provides the function to protect the audit data.

Security alarms

If an event deemed as a potential security violation occurs, the TOE generates audit data on the even and send an alarm email to the authorized administrator.

- If authentication fails
- In violation of control rules
- If self test fails or the integrity is violated
- If self test of the validated cryptographic module fails
- If the defined audit storage limit is reached
- If the audit storage is full

Audit data management

The TOE generates audit records if an auditable event occurs, and records the time and date of audit logs by synchronizing reliable time information. Audit logs are stored in an audit trail storage managed by the DBMS, and protected from unauthorized deletion or modification. It provides audit records in a manner suitable for the authorized administrator to interpret the information by providing him/her with the function to read all audit data. The TOE provides the authorized administrator with the ability to search audit records in ascending and descending orders, and to review audit records by applying logical relationships such as AND and OR, based on selectable audit data type including type, date and time, department name, user name and message. If the audit trail storage is predicted to reach (10% lower than the full capacity) the defined threshold (default value: 70%, configurable range: 50-90%), the TOE generates audit data and sends an alarm email to the authorized administrator. If the audit trail exceeds the defined threshold, it overwrites the oldest stored audit record, and sends an alarm email to the authorized administrator.

TOE component	Functional component	Auditable event	Additional audit record
Policy Center	FAU_ARP.1	Actions taken due to potential security violations	-
	FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	-
	FAU_STG.3	Actions taken due to exceeding of a threshold	-
	FAU_STG.4	Actions taken due to the audit storage failure	-
	FCS_CKM.1(2)	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	

	FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.4	Success and failure of the activity	
	FCS_COP.1	Success and failure, and the type of cryptographic operation	
	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken	-
	FIA_IMA.1(Extended)	Success and failure of mutual authentication	-
	FIA_UAU.1	All results of administrator authentication	-

TOE component	Functional component	Auditable event	Additional audit record
Policy Center	FIA_UAU.4	Attempts to reuse email authentication code	
	FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
	FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
	FMT_MSA.1	All modifications to the security attributes	Modified security attribute value
	FMT_MSA.3	Modifications to the basic settings of allowance or restriction rules, All modifications to the initial values of security attributes	Modified security attribute value
	FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data value
	FMT_PWD.1(Extended)	Modification to the password combination rules	
	FMT_SMF.1	Use of the management functions	
	FPT_TST.1	* The results of TSF self tests and the results of integrity verification * The results of failure of self tests of the validated cryptographic module and the results of integrity verification	Executable file whose integrity has been violated
	FTA_MCS.2	Termination of existing access based on the limitation of multiple concurrent sessions	
	FTA_SSL.5(Extended)	Termination of management access sessions after a period of inactivity of the authorized administrator	
	FTA_TSE.1	Denial of management access session establishment of the administrator based on access IP	
Client	FCS_CKM.1(2)	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
	FCS_CKM.4	Success and failure of the activity	
	FCS_COP.1	Success and failure, and the type of cryptographic operation	
	FDP_ACF.1	Execution of an operation on an object	Identity information of an object
	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken	
	FIA_IMA.1(Extended)	Success and failure of mutual authentication	
	FIA_UAU.1	All results of the authentication of a document user	

	FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
	FPT_TST.1	* The results of TSF self tests and the results of integrity verification * The results of failure of self tests of the validated cryptographic module and the results of integrity verification	Executable file whose integrity has been violated

Protected audit trail storage

If the audit trail storage is predicted to reach (10% lower than the full capacity) the defined threshold, the TOE generates audit data and sends an alarm email to the authorized administrator. If the audit trail exceeds the defined threshold, it overwrites the oldest stored audit record, and sends an alarm email to the authorized administrator. The defined thresholds are as follows:

- Minimum: 50(%)
- Maximum: 90(%)
- Default: 70(%)

Relevant SFR: FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.3, FAU_STG.4

6.2 Cryptographic Support

The TOE performs electronic document encryption and TSF data encryption by using the validated cryptographic module whose security and implementation conformance has been confirmed by the Korea Cryptographic Module Validation Program (KCMVP). The TOE supports the cryptographic functions of cryptographic key generation, cryptographic key distribution, cryptographic key destruction and random bit generation as detailed below:

Validated cryptographic module

- Cryptographic module name: MagicCrypto V2.2.0
- Validation number: CM-162-2025.3
- Developer: Dream Security Co., Ltd.
- Validation date: March 3, 2020
- Expiration date: March 3, 2025

Approved cryptographic algorithm of the validated cryptographic module

List of standards	Encryption method	Cryptographic algorithm	Key size	Use
KS X 1213-1	Block cipher	ARIA_CTR	128	User data encryption • Client: file encryption when a document to be protected is saved

		ARIA_CBC	256	TSF data encryption
				• Policy Center
				  • DEK
				  • DB password
				  • Document group key
				• Client

				• Private key of the user certificate • License file • Configuration file
		ARIA_CBC (SHA256)	256	Protection of data transmitted between TOE components (Policy Center - client)
ISO/IEC 11770-3	Key setting	ECDH (SHA-256)	256	Mutual authentication key agreement between TOE components (Policy Center - Client)
TTAS.KO-12.0334	Key deviation	PBKDF2 (SHA-256)	256	DEK generation
ISO/IEC 18031	Random bit generator	HASH_DRBG (SHA-256)	256	• TSF data and document encryption • Policy Center: DB password, license • Client: Document • Generation of 16-digit authentication code • Policy Center: When the web administrator logs in • Client: When issuing a document user certificate
ISO/IEC 18033-2	Public key cryptography	RSAES (SHA-256)	2048	The Policy Center distributes DEK to the client
ISO/IEC 14888-2	Electronic signature	RSA-PSS (SHA-256)	2048	Client: Verify the signatures of the document author and audit log originator
ISO/IEC 10118-3	Hash function	SHA-256	256	• Policy Center • Store the web administrator's password in the DB (SALT added) • Hash the KEK generated with CPU ID + web server start time + random bits • Store HASH of files subject to integrity verification • Client • Hash the KEK generated with email + reverse (email) + random bits

Cryptographic key generation

The TOE applies the following methods to generate a cryptographic key used in electronic document encryption and TSF data encryption in order to comply with the standards as follows:

[Table 16] Electronic document Encryption

List of standards	Cryptographic algorithm	Key size	List of standards
DEK	HASH_DRBG (SHA-256)	256 bits	ISO/IEC 18031

[Table 17] TSF Data Encryption

List of standards	Cryptographic algorithm	Key size	List of standards	Use
KEK	PBKDF2 (SHA-256)	256 bits	TTAS.KO-12.0334	Key derivation with the password entered during login
	SHA-256	256 bits	ISO/IEC 10118-3	Encryption of KEK during memory loading
DEK	HASH_DRBG (SHA-256)	256 bits	ISO/IEC 18031	Random bit generation
Session key	ECDH (SHA-256)	256 bits	ISO/IEC 11770-3	Session key agreement during mutual authentication
Session key pair	ECDH (SHA-256)	256 bits	ISO/IEC 11770-3	Generation of a key pair for session key agreement

Cryptographic key distribution

The TOE distributes a cryptographic key by using RSAES (SHA-256) of the validated cryptographic module.

Classification	Cryptographic algorithm	List of standards	Distribution method
Session key	ECDH (SHA-256)	ISO/IEC 11770-3	Session key agreement through the generated key pair
DEK	RSAES (SHA-256)	ISO/IEC 18033-2	Distribution of the DEK used in electronic document encryption/decryption through the public key method

Cryptographic key destruction

The TOE destructs a generated cryptographic key that has been generated if a user logs out from the client or the management server shuts the system down. The TOE initializes and zeroizes all cryptographic key-related data, cryptographic keys and critical security parameters by calling a memory destruction function provided by the KCMVP, which, then, are returned to the system resource.

Classification	Key	Cryptographic algorithm	Timing of destruction	Destruction method
Electronic document encryption	DEK	HASH_DRBG (SHA-256)	• Client: when terminating an application program (document program)	1. Call a memory destruction function of the validated cryptographic module 2. Initialize the cryptographic key and CSPs with '0' 3. Return it to the system resource
TSF data encryption	KEK	PBKDF2 (SHA-256)	• Policy Center: when terminating IIS or the system	
	DEK	HASH_DRBG (SHA-256)	• Client: when a user logs out or when terminating the system	
	Session key	ECDH (SHA-256)	• Policy Center: when terminating IIS or the system	
	Session key pair		• Client: when terminating the system	

Cryptographic key operation

The TOE uses the following methods in order to process electronic document encryption and TSF data operation in accordance with the standards.

[Table 18] Electronic document Encryption

Cryptographic algorithm	Key size	List of standards	List of cryptographic operations
ARIA_CTR	128 bits	KS X 1213-1	Encryption/decryption of an electronic document

[Table 19] TSF Data Encryption

Cryptographic algorithm	Key size	List of standards	Cryptographic operation
ARIA_CBC	256 bits	KS X 1213-1	• Transmission between the Policy Center and the client • Encryption/decryption of the TOE security policy data • Policy Center • Encryption of DB password • DEK and KEK encryption • Client • Encryption/decryption of security header of an encrypted document • Encryption/decryption of text and structure that stores security attributes of an encrypted document • Encryption/decryption of private key of a document user's certificate • Encryption/decryption of authentication data when issuing a document user's certificate • Encryption/decryption of a document user's certificate • Encryption/decryption of a document user's license • DEK and KEK encryption
RSAES (SHA-256)	2048 bits	ISO/IEC 18033-2	• Policy Center • Verification of log signature transmitted from the client • Client • Document user certificate signature / verification of signature • Document user license signature / verification of signature •Encryption/decryption of cryptographic key of document user license •Encryption/decryption of cryptographic key of security header of an encrypted document • Log signature to be transmitted to the Policy Center
ECDH (SHA-256)	256 bits	ISO/IEC 11770-3	Session key agreement through a key pair

Random bit generation

The TOE generates random bits by using HASH_DRBG (SHA256), a random bit generator of the

validated cryptographic module.

Relevant SFR: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_RBG.1

6.3 Electronic Document Encryption

The TOE allows a document user to perform the encryption/decryption of an electronic document to be protected in accordance with the document group-based access control rule established by the authorized administrator.

Subset access control

The TOE performs the function of document group-based access control that restricts reading, encryption (writing) and decryption of an electronic document to be protected when a document user accesses such document, based on the following security attributes established by the authorized administrator.

- Document group ID
- Document user ID
- Target of security

Document group-based access control

If a document user makes an attempt to read, encrypt (write) or decrypt a document to be protected, the TOE checks the user's permission to access the document, based on security attributes such as the document group ID and the document user ID. Then, if the policy established by the administrator allows, the TOE allows the user to read, encrypt (write) or decrypt the document. Otherwise, it performs the function of restriction.

Subject (user)		Object (information)		Operation
List	Security attributes	List	Security attributes	
Document user	• Document user ID • Password	• Document to be protected	• Document group ID • Document name • Document type • Document path	• Allowed to read a document if granted with read and encryption (write) permission, and encrypt and save a document • Decrypt a document if granted with decryption permission

Relevant SFR: FDP_ACC.1, FDP_ACF.1

6.4 Identification and Authentication

The TOE provides the function of identification and authentication for the administrator and document users, and performs TOE internal mutual authentication.

Identification and authentication of the administrator

The TOE shall allow the following actions before the administrator is authenticated, and allow the authentication of the administrator through "Request for the identification and authentication procedure

(login screen)" before the administrator is identified.

- Request to enter an email authentication code
- Request for the identification and authentication procedure (login screen)

The TOE allows and blocks access by the administrator through the identification and authentication process of the administrator, and inactivates the identification and authentication if the login attempts have been denied for a defined number of times configured by the authorized administrator (default value: 3 times, the configurable number of unsuccessful authentication attempts: 1-5 times).

The TSF requires the administrator to be successfully authenticated before allowing any other TSF- mediated actions on behalf of the administrator. A verification mechanism is provided to ensure that a password satisfies the password combination rules to combine three types of uppercase/lowercase alphabetic characters, numeric characters and special characters (!, @, #, $, %, ^, *, -, _, +, =) in 9 to 16 digits. During the login by the administrator, a one-time authentication code, which is generated by the random bit generator of the validated cryptographic module and is received to the email address, is used in order to prevent the reuse of the authentication information. While the authentication is in progress, only the administrator ID and the masked administrator password are displayed and a reason for authentication failure (e.g., ID error and password error) is not provided.

User identification and authentication

The TOE shall allow the following actions before a document user is authenticated, and allow the authentication of the document user by selecting the document user certificate before the user is identified.

- Certificate issuance
  - Request for document user certificate
  - Request to enter an email authentication code
  - Generation of a document user certificate
  - Request for the identification and authentication procedure (login screen)
- After the certificate is issued
  - Selection of the document user certificate
  - Request for the identification and authentication procedure (login screen)

The TOE allows and blocks access by a document user though the identification and authentication process of the document user, and reboots the document user's PC and inactivates the identification and authentication for 5 minutes if the login attempts have been denied for a defined number of times configured by the authorized administrator (default value: 3 times, the configurable number of unsuccessful authentication attempts: 1-5 times).

The TSF requires the document user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the document user. A verification mechanism is provided to ensure that a password satisfies the password combination rules to combine three types of uppercase/lowercase alphabetic characters, numeric characters and special characters (!, @, #, $, %, ^, *, -, _, +, =) in 9 to 16 digits. When the document user's certificate is generated, a one-time authentication code, which is generated by the random bit generator of the validated cryptographic module and is received to the email address, is used in order to prevent the reuse of the authentication information. While the authentication is in progress, only the document user's certificate and the masked password of the document user are displayed and a reason for authentication failure (e.g., ID error and password error) is not provided.

TOE internal mutual authentication

The TOE performs mutual authentication between the Policy Center and the client before performing encrypted communication between TOE components through the key agreement process of ECDH algorithm in HTTP communication. TOE internal mutual authentication is carried out at the time when

the rebooting of the Policy Center system and the client system is completed, respectively.

Relevant SFR: FIA_AFL.1, FIA_IMA.1(Extended), FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1

6.5 Security Management

The TOE provides the security management function for the authorized administrator and document users to set and manage TOE security functions, TSF data, etc.

Management function of the authorized administrator

There is only one type of the administrator role provided, and the ability to manage security functions is restricted to the authorized administrator.

Classification	Security function	Ability			
		Determine a behaviour	Disable	Enable	Modify a behaviour
Object setting	Department management	O	-	-	O
	User management	O	-	-	O
Policy setting	Document group policy	O	-	-	O
	Policy for target of security	O	-	-	O
	Basic license policy	-	-	-	O
	Multi-license policy	-	-	-	O
Authentication management	Certificate issuance status	O	-	-	O
	License Issuance status	O	-	-	O
Log statistics	User audit	O	-	-	-
	Administrator audit	O	-	-	-
	System audit	O	-	-	-
	Document log	O	-	-	-
	Decryption log	O	-	-	-
	Integrity verification history	O	-	-	-
	Login history	O	-	-	-
Environment configuration	Environment configuration	-	-	-	O
	Disk usage check	-	-	-	O
	Policy Center self test and integrity verification	-		O	O

The authorized administrator can query, delete and add security attributes such as document user ID, document group ID and target of security in order to establish the document group-based access control rule as follows. When a document user is assigned to a document group, read/write(encryption) permission is granted by default. The authorized administrator is provided with the function to set read/write(encryption) and decryption permission of a document group for document users.

Access control SFP	Security attribute	Ability			
		Query	Modify	Delete	Add
Document group-based access control	Document user ID	O	-	O	O
	Document group ID	O	-	O	O
	Target of security	O	-	O	O

The authorized administrator can query, modify, delete and add the following TSF data.

TSF data	Ability			
	Query	Modify	Delete	Add
Document user certificate	O	-	O	-
Audit data	O	-	-	-
Access IP setting	O	O	O	O
Time of session timeout	O	O	-	-
Allowed number of unsuccessful login attempts	O	O	-	-
Minimum digits of password	O	O	-	-

Administrator ID and password can be set in installing the TOE. The authorized administrator can change the length of password that complies with the password combination rule to combine three types of characters, which are uppercase/lowercase alphabetic characters, numeric characters and special characters (!, @, #, $, %, ^, *, -, _, +, =), as follows:

- Minimum: 9 digits
- Maximum: 16 digits
- Default: 9 digits

Management function of a document user

A document user can query, modify, delete and add the following TSF data.

TSF data	Ability			
	Query	Modify	Delete	Add
Document user certificate	O	O	O	O
License	O	O	-	-
Environment configuration	O	O	-	-

A document user can query/modify/delete/add a document user certificate, license and environment configuration information according to a type of TSF data. The user can modify the length (at least 9 digits up to 16 digits) of password comprised of a combination of three types of characters:

uppercase/lowercase alphabetical characters, numeric characters and special characters (!, @, #, $, %, ^, *, -, _, +, =).

Relevant SFR: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1(Extended), FMT_SMF.1, FMT_SMR.1

6.6 Protection of the TSF

The TOE protects the TSF and runs a suite of self tests and integrity verification.

Protection of TSF data

The TOE protects TSF data when it is transmitted between separate parts of the TOE, or stored in containers controlled by the TSF.

[Table 20] Protection of transmitted data

Classification	Target of encryption	Encryption method	Algorithm	Data storage	List of standards
Transmission between the Policy Center and the client	Security policy data	Block cipher	ARIA_CBC (SHA-256)	Packet	KS X 1213-1

[Table 21] List of security policies and account information encryption

Classification	Target of encryption	Encryption method	Algorithm	Data storage	List of standards
Policy Center	Administrator password	HASH	SHA-256+ SALT	DBMS	ISO/IEC 10118-3
				File	
Client	Document user certificate	Block cipher	ARIA_CBC (SHA256)	File	KS X 1213-1
	Document user private key				
	TOE environment configuration file				
	Audit data	Electronic signature	RSA-PSS (SHA-256)	File	ISO/IEC 14888-2

[Table 22] Protection of TSF data

Target of encryption	Encryption method	Algorithm	Data storage	List of standards
KEK	Block cipher	ARIA_CBC (SHA-256)	Memory	KS X 1213-1
DEK	Block cipher	ARIA_CBC (SHA256)	Memory, file	KS X 1213-1
Transmitted data	Block cipher	ARIA_CBC (SHA256)	Packet	KS X 1213-1

[Table 23] Key encryption key

Classification	Algorithm	List of standards	Use
KEK	PBKDF2 (SHA256)	TTAS.KO-12.0334	Key derivation with the password entered during login

Availability protection of TSF data

The client, which is a TOE component, restricts an attempt to delete an executable file to be protected by monitoring the kernel drive, thereby preventing the executable file from being deleted. When a process is terminated, the client immediately detects and restore it by restarting the process or rebooting the system.

Files prevented from deletion	Files prevented from termination	Mechanism to prevent termination
• sccm.exe • scconv.exe • scmain.exe • scboots64.exe • scboot64.exe • scboot.exe • scsysinfo.exe • scsysinfo64.exe	• scmain.exe • scboots64.exe • scboot64.exe • scboot.exe	• Process rerun: scmain.exe, scboots64.exe • Restoration by rebooting the system: scboot64.exe, scboot.exe

TSF testing

The Policy Center runs a suite of self test during initial start-up and periodically (24-hour interval by default), and the client during initial start-up and periodically (10-minute interval after start-up). The Policy Center verifies the integrity of the TSF and TSF data during initial start-up and at an interval defined by the administrator. The client verifies the integrity of the TSF at the 60-minute interval after initial start-up. In case of booting on safe mode, the integrity verification is performed only during initial start-up as the system is rebooted. If the self test fails, an alarm email is sent to the authorized administrator.

TOE component	Item	Timing	Content (role)
Policy Center	ShadowCubeSelfTest.exe	• During initial start-up •Periodically (at the	Process related to the operation of security functions

		60-minute interval)	
Client	scmain.exe	• During initial start-up • Periodically (at the 60-minute interval)	Process for GUI for user security management
	scboots64.exe		Process related to the operation of user security functions

The integrity verification is performed by checking the items subject to integrity verification with hash values processed with SHA256. The Policy Center verifies the integrity of the TSF and TSF data during initial start-up and at an interval defined by the administrator. The client verifies the integrity of the TSF data during initial start-up and at the 60-minute interval. In case of booting on safe mode, the integrity verification is performed only during initial start-up as the system is automatically rebooted. If the integrity verification fails, an alarm email is sent to the authorized administrator.

TOE component	**Item**	**Timing**	**Content (role)**
Policy Center	config.ini	•During initial start-up •According to the interval set by the authorized administrator •Min:1 (hour) •Max: 24 (hours) •Default: 24 (hours) •At the request of the authorized administrator during the operation	Configuration file used in the web service in the process of initializing the Policy Center
	db.config		Configuration file used in the web service to connect DBMS
	log4net.xml		Configuration file used in the web service in logging setting
	web.config		Web service configuration file
	admin.dll		Management of security attributes
	scbase.dll		Management of security attributes related to license
	scpclib.dll		Management of security attributes related to databases
	scpcws.dll		Management of security attributes related to client
	ssDeulmeori.dll		Process for the management of identification and authentication
	ssJikimi.dll		Process for the use of the validated cryptographic module
	ssNeobi.dll		Utility process for the support of management console
	ssNeonadeuli.dll		Process for encryption/decryption processing
	ssServerHelper.dll		Process for the management of cryptographic functions
	MagicCryptoV22.dll		Validated cryptographic module
Client	scboot.exe, scboot64.exe, scboots64.exe	•During initial start-up • Periodically (at the 60-minute interval)	Process related to the operation of security functions
	sccm.exe		Certificate management console
	scconv.exe		File encryption/decryption management console

	scmain.exe		Management console to support user GUI
	scsysinfo.exe, scsysinfo64.exe		Process related to the operation of security functions

TOE component	Item	Timing	Content (role)
Client	scewvsc.dll, scewvsc64.dll, scewvsd.dll, scewvsd64.dll, scewvsp.dll, scewvsp64.dll, scewwss.dll, scewwss64.dll	•During initial start-up • Periodically (at the 60-minute interval)	Process for document group-based access control rules
	scshell.dll, scshell64.dll		Process to connect Windows File Explorer
	scwinui.dll, scwinui64.dll		Process for the support of identification and authentication
	ssDeulmeori.dll		Process for the management of identification and authentication
	ssJikimi.dll		Process for the use of the validated cryptographic module
	ssMigratorHelp.dll		Process for the support of ShadowCube version compatibility
	ssNeobi.dll		Utility process for the support of management console
	ssNeonadeuli.dll		Process for encryption/decryption processing
	ssServerHelper.dll		Process for the management of cryptographic functions
	MagicCryptoV22.dll MagicCrypto32V22.dll		Validated cryptographic module

Relevant SFR: FPT_ITT.1, FPT_PST.1(Extended), FPT_PST.2(Extended), FPT_TST.1

6.7 TOE Access

The Policy Center, a TOE component, performs the function to terminate a session in order to control the administrator's TOE access.

Session management

As the TOE restricts the number of concurrent sessions that belong to the same user to one in case of successful login with the authorized administrator's account, [actions] are taken in case of concurrent connections. In addition, the TOE terminates the administrator's session after a specified time interval of user inactivity defined by the authorized administrator (default value: 10 minutes). The time of user inactivity can be set from at least 1 minute up to 10 minutes. In the TOE, only the authorized administrator can access the Policy Center from an IP addresses that has been registered in advance. In the initial installation, the number of the IP addresses is restricted to two.

Once the administrator logs in, the TOE terminates a session after a specified time interval of inactivity defined by the authorized administrator. The restriction of administrator's session time is as follows:

- Minimum: 1 (minute)
- Maximum: 10 (minutes)
- Default: 10 (minutes)

The TOE ensures that access to the Policy Center can be made only from the management console with IP address that has been registered in advance. The number of IP addresses that can be registered in advance is restricted as follows:

- Minimum: 2 (IPs)
- Maximum: 5 (IPs)
- Default: 2 (IPs), 1 in addition to the localhost

Relevant SFR: FTA_MCS.2, FTA_SSL.5(Extended), FTA_TSE.1