ShadowCube V8.0 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 V8.0 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 V8.0 Security Target
- ST Version: V1.5
- Author: Duruan Co., Ltd.
- Date: July 28, 2026
- Evaluation Criteria: Common Criteria for Information Technology Security Evaluation
- Common Criteria Version: CC:2022 R1
- Evaluation Assurance Level: EAL1+ (ATE_FUN.1)
- Keywords: Document, Encryption
- File Name: ShadowCube V8.0 Security Target V1.5.docx

1.2 TOE Reference

The TOE conforming to this Security Target is identified as follows:

- Developer: Duruan Co., Ltd.
- TOE Name / Version
  - TOE Identifier: ShadowCube V8.0
  - TOE Detailed Version: 8.0.0
- TOE components
  - Category

    - ShadowCube Server

    - ShadowCube Client
  - Version: 8.0.0
  - Rev: 4517
- Guidance Documents
  - Administrator Operational Guidance: ShadowCube V8.0 Administrator Operational Guidance V1.2.pdf
  - User Guidance: ShadowCube V8.0 User Guidance V1.2.pdf
  - Preparative Procedure: ShadowCube V8.0 Preparative Procedure V1.3.pdf
- Release Date: June 29, 2026

1.3 TOE Overview

This section describes the purpose and key security characteristics of the TOE. It also identifies the TOE type and the main hardware and software additionally required for TOE operation, and explains the physical scope and logical scope of the TOE. The TOE is identified as ShadowCube V8.0 and consists of ShadowCube Server, which creates, manages, and distributes the organization's security policies, and ShadowCube Client, which performs document encryption and decryption. The TOE consists of executable files and guidance documents in PDF format and is distributed on CD.

1.3.1 Document Encryption Overview

The TOE is an "Electronic Document Encryption" product used to protect important documents managed by an organization.

The primary security features provided by the TOE include encryption/decryption of protected documents and cryptographic key management, as well as encryption/decryption of the Critical Security Parameters (CSPs) used by the TOE and cryptographic key management. The cryptographic functions used for these operations use the approved cryptographic algorithms of the validated cryptographic module (MagicCrypto V2.3.0).

Validated Cryptographic Module

- Cryptographic Module Name: MagicCrypto V2.3.0
- Validation Number: CM-263-2030.1
- Developer: Dream Security Co., Ltd.
- Validation Date: January 24, 2025
- Expiration Date: January 24, 2030

Cryptographic Algorithms

- Cryptographic Algorithm for Documents: ARIA_CTR 128 bits
- Cryptographic algorithm for CSP: ARIA_CBC 256 bits, RSAES 2048 bits, SHA-256

Critical Security Parameters

- ShadowCube Server: Administrator login password, database password, document group key
- ShadowCube Client: User certificate private key, user certificate information

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 permits or blocks access by administrators and document users through identification and authentication, provides a password verification mechanism, and disables identification and authentication if login attempts fail more than the number of times configured by the authorized administrator (default: 3). It performs mutual authentication between communication peers using the ECDH algorithm of the validated cryptographic module.

The TOE generates audit records when an auditable event occurs and sends alarm emails to authorized administrators in the event of a potential security violation.

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 IP addresses registered in advance, and restricts the number of authorized administrator sessions to one. When the specified time interval of inactivity is reached, it terminates the administrator session.

1.3.2 TOE Type and Scope

The TOE defined in this ST is ShadowCube V8.0, a software-based document encryption product that prevents information leakage by encrypting/decrypting important documents within an organization.

The essential TOE components that perform the security functions defined in this ST are ShadowCube Server and ShadowCube Client, which implement the user terminal encryption type.

ShadowCube Server is management server software that performs functions such as establishing encryption policies, managing user permissions, and providing audit functions.

ShadowCube Client is agent software installed on user terminals that encrypts documents when they are created and decrypts documents for authorized users.

The TOE components that perform the document encryption/decryption function, which is a major security function of ShadowCube V8.0, include the validated cryptographic module MagicCrypto V2.3.0 and provide secure encryption/decryption operations and cryptographic key management functions.

The security management function of ShadowCube V8.0 is implemented by applying the secure transmission protocol (HTTPS) to both communication between the web browser on the administrator PC and the web server, which is the operational environment of ShadowCube Server, and communication between ShadowCube Client and ShadowCube Server.

Software that provides the TOE's main document encryption/decryption function by interoperating with the encryption/decryption functions of commercial 3rd party products (such as MS Office 2024, Hancom Office 2024, and Notepad) is excluded from the scope of evaluation.

1.3.3 TOE Purpose and Major Security Features

ShadowCube V8.0 performs document encryption/decryption on documents in accordance with policies configured by administrators to protect important documents managed by an organization, and includes cryptographic key management functions.

In addition, ShadowCube V8.0 provides a security audit function that records and manages major events as audit data when security functions and management functions operate; identification and authentication functions such as administrator identity verification, authentication failure handling, and mutual authentication between TOE components; security management functions for defining security functions and roles and configuring environment settings; functions to protect data stored in repositories controlled by the TSF; Protection of the TSF functions such as TSF self-tests; and TOE access functions for managing authorized administrator access sessions.

The procedures for document encryption/decryption and cryptographic key management are as follows.

The document encryption/decryption function uses a Data Encryption Key (hereinafter "DEK") and a Key Encryption Key (hereinafter "KEK").

When encrypting a protected document, ShadowCube Client generates the DEK and encrypts the body of the document with the DEK according to the policy configured by the administrator.

The DEK is encrypted with the KEK and stored in the header of the protected document.

ShadowCube Server generates the KEK and securely distributes it to ShadowCube Client through a mutually authenticated communication channel.

ShadowCube Client uses the DEK to encrypt and decrypt the body of the protected document, and uses the KEK to encrypt or decrypt the DEK.

The DEK is used as a symmetric key and the KEK is used as an asymmetric key. The KEK is issued as a key shared within a group.

ShadowCube Server and ShadowCube Client provide a cryptographic key destruction function when cryptographic keys are no longer used.

Administrators can designate, through ShadowCube Server, the applications whose documents are subject to encryption/decryption as security targets, and can grant document users read/write and decryption permissions for documents.

Because ShadowCube Server distributes cryptographic keys to document users according to configured policies, only authorized document users can encrypt/decrypt documents.

1.3.4 TOE Operational Environment and Non-TOE

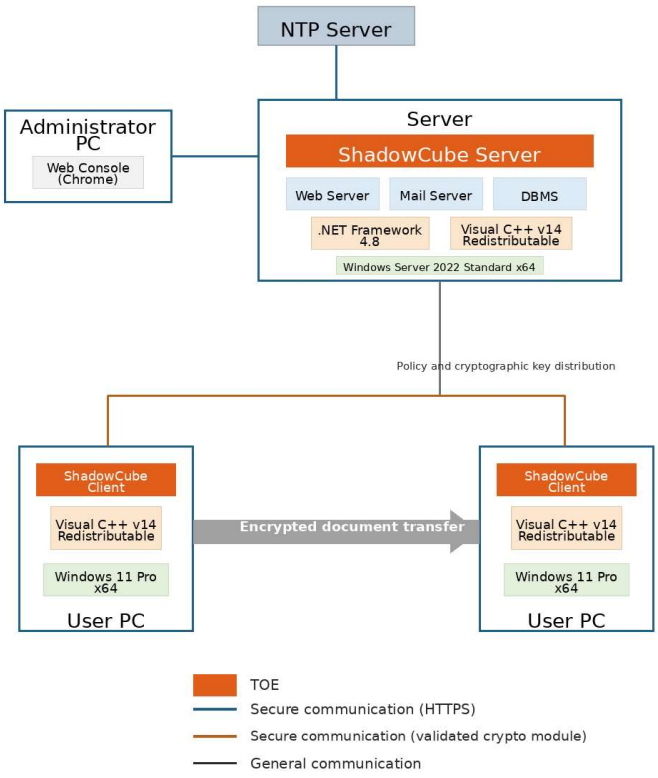
The TOE defined herein is "document encryption" that prevents information leakage by encrypting/decrypting important documents within the organization. The operational environment provided by the TOE and non-TOE entities additionally used for operation are as follows:

Operational Environment for the "User Terminal Encryption" Method

The TOE consists of the ShadowCube Server, which is installed on the server system to manage security policies, and the ShadowCube Client, which is installed on user systems to perform document encryption/decryption.

Authorized administrators configure document group-based access control policies for each document user through the ShadowCube Server, and the ShadowCube Server distributes the policies and cryptographic keys set by the authorized administrators to the ShadowCube Client.

The ShadowCube 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] User Terminal Encryption Operation Method

Third-party Software Used in the TOE

OpenSSL 3.5.4

A third-party module included in the TOE that is used for web management communication between the administrator and the ShadowCube Server.

MagicCrypto V2.3.0

A validated cryptographic module included in the TOE; it is used for the encryption/decryption of protected documents, cryptographic key management, and the encryption/decryption of critical security parameters.

IIS (Internet Information Services) 10.0

This third party module, which is not included in the TOE, functions as a web server on Windows Server 2022 Standard and is used by administrators for security management operations via HTTPS.

MailEnable 10.54

A third-party module not included in the TOE that serves as a mail server and is used to send alarm emails.

PostgreSQL 18.4

A third-party module not included in the TOE that serves as a DBMS and is used for the secure storage of audit data and configuration data generated by the TOE.

Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719

This third party module, which is not included in the TOE, is the Visual C++ Runtime library used when running application programs developed with Visual C++.

Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719

This third party module, which is not included in the TOE, is the Visual C++ Runtime library used when running application programs developed with Visual C++.

Microsoft .NET Framework 4.8

This third party module, which is not included in the TOE, is the .NET runtime environment support library required for operating the TOE (ShadowCube Server) service developed with ASP.NET.

Non-TOE

Administrator System

To use the TOE's security management function, an administrator system capable of running a web browser (Chrome 149.0) is required.

User System

A user system capable of running Microsoft Office, Hancom Office, AutoCAD, and similar applications is required to perform document encryption/decryption.

System Requirements

[Table 1] ShadowCube Server

Category	Specifications
OS	Microsoft Windows Server 2022 Standard (64-bit)
DBMS	PostgreSQL 18.4
Software	IIS (Internet Information Services) 10.0 Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719 Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719 Microsoft .NET Framework 4.8 Chrome 149.0
Hardware	CPU: Intel i7 Quad Core 2.0 GHz or higher Memory: 8 GB or more HDD: At least 600 MB of free space required for TOE installation At least one network interface: 100/1000 Mbps or higher

[Table 2] ShadowCube Client

Category	Specifications
OS	Microsoft Windows 11 Pro (64-bit)
Software	Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719 Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719 MS Office 2024 Hancom Office 2024 Adobe Acrobat Reader DC Autodesk AutoCAD 2026
Hardware	CPU: Intel i3 Dual Core 1.0 GHz or higher Memory: 4 GB or more HDD: At least 180 MB of space required for TOE installation At least one network interface: 100/1000 Mbps or higher

[Table 3] Administrator (HTTPS Communication)

Category	Specifications
Software	Chrome 149.0

External IT Entity

NTP Server

Used for time synchronization to provide trusted timestamps in the TOE.

Document Encryption Support

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

[Table 4] Application Programs

application program	Application Program Version	Document Types (File Extensions)
Notepad	The version included by default in Windows 11 Pro x64, the operational environment for ShadowCube Client	txt
Paint (MS Paint)		bmp, gif, jpg, png, tif
WordPad		rtf
MS Office Word	2024	doc, docx
MS Office Excel	2024	xls, xlsx
MS Office PowerPoint	2024	ppt, pptx
Hancom Office Hangul	2024	hwp, hwpx
Hancom Office HanCell	2024	nxl, cell
Hancom Office HanShow	2024	Show
Acrobat Reader DC	DC	pdf
Autodesk AutoCAD	2026	dwg, dxf

1.3.5 TOE Description

The TOE encrypts 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.

1.3.5.1 Physical Scope of the TOE

The TOE components consist of the ShadowCube Server, which manages security policies, and the ShadowCube Client, which performs document encryption/decryption.

The physical scope of the TOE consists of the TOE components and the documentation; the TOE components are provided as .exe files, and the documentation is provided as PDF files, all distributed on a CD.

[Table 5] Physical Scope of the TOE

Composition	Subitem	Distribution Format
TOE	ShadowCube V8.0	-
TOE component	ShadowCube Server 8.0.0.4517 (server_8.0.0.4517.exe)	Executable (CD 1)
	ShadowCube Client 8.0.0.4517 (scsetup_8.0.0.4517.exe)	
Guidance	Administrator Operational Guidance: ShadowCube V8.0 Administrator Operational Guidance V1.2.pdf	Electronic Files (CD 1)
	User Guidance: ShadowCube V8.0 User Guidance V1.2.pdf	
	Preparative Procedure: ShadowCube V8.0 Preparative Procedure V1.3.pdf	

Validated cryptographic modules and third-party

These are used to perform encryption/decryption functions and are distributed as part of the installation files for the ShadowCube Server and ShadowCube Client, which are TOE components.

ShadowCube Server

- Validated Cryptographic Module: MagicCrypto V2.3.0
- Cryptographic Support Library: OpenSSL 3.5.4

ShadowCube Client

- Validated Cryptographic Module: MagicCrypto V2.3.0

1.3.5.2 Logical Scope of the TOE

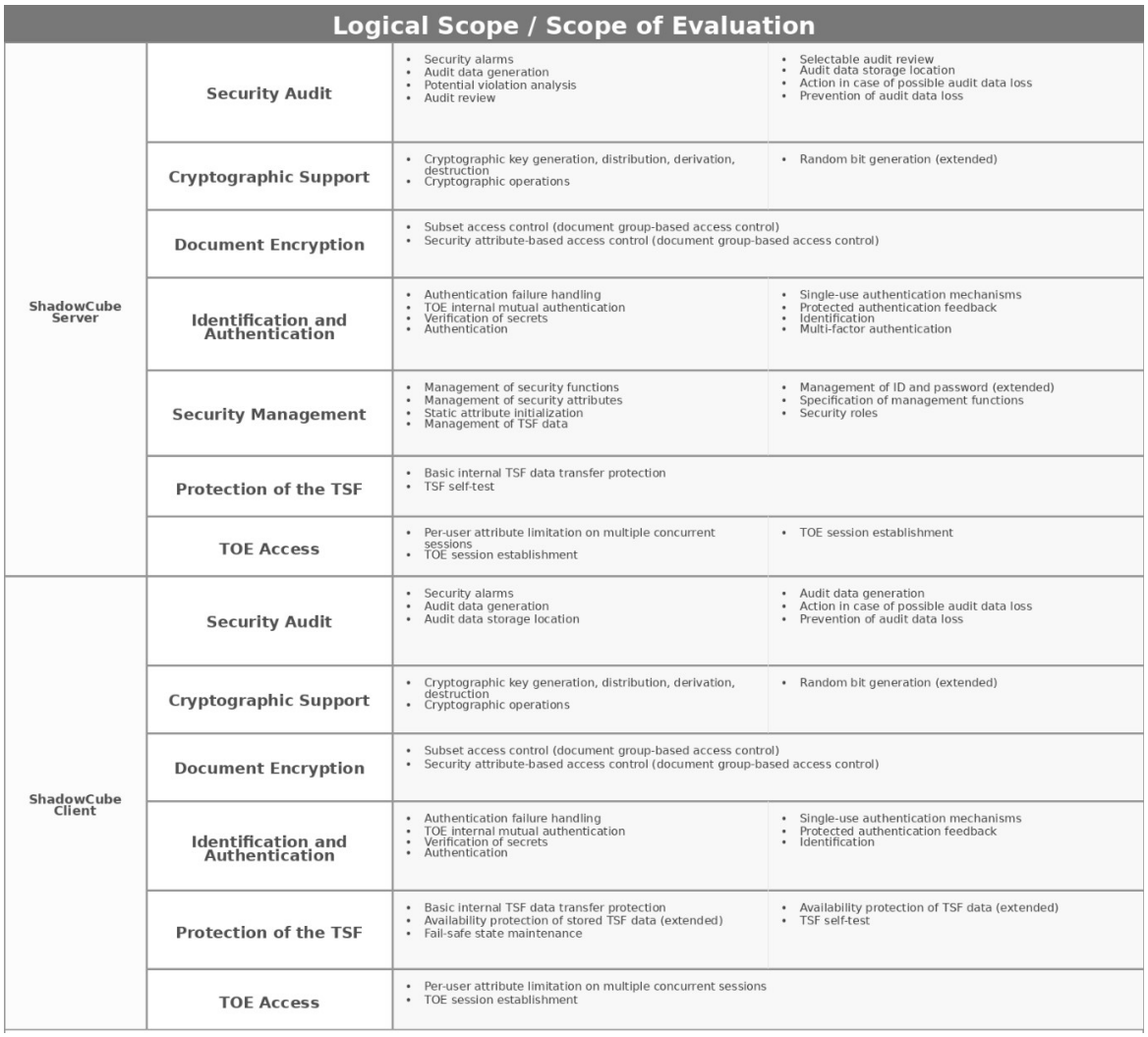
The logical scope of the TOE is as follows.

ShadowCube Server

- Security Audit
- Cryptographic Support
- Document Encryption
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

ShadowCube Client

- Security Audit
- Cryptographic Support
- Document Encryption
- Identification and Authentication
- Protection of the TSF
- TOE Access



Logical Scope / Scope of Evaluation			
ShadowCube Server	Security Audit	• Security alarms • Audit data generation • Potential violation analysis • Audit review	• Selectable audit review • Audit data storage location • Action in case of possible audit data loss • Prevention of audit data loss
	Cryptographic Support	• Cryptographic key generation, distribution, derivation, destruction • Cryptographic operations	• Random bit generation (extended)
	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 mechanisms • Protected authentication feedback • Identification • Multi-factor authentication
	Security Management	• Management of security functions • 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 self-test	
	TOE Access	• Per-user attribute limitation on multiple concurrent sessions • TOE session establishment	• TOE session establishment
ShadowCube Client	Security Audit	• Security alarms • Audit data generation • Audit data storage location	• Audit data generation • Action in case of possible audit data loss • Prevention of audit data loss
	Cryptographic Support	• Cryptographic key generation, distribution, derivation, destruction • Cryptographic operations	• Random bit generation (extended)
	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 mechanisms • Protected authentication feedback • Identification
	Protection of the TSF	• Basic internal TSF data transfer protection • Availability protection of stored TSF data (extended) • Fail-safe state maintenance	• Availability protection of TSF data (extended) • TSF self-test
	TOE Access	• Per-user attribute limitation on multiple concurrent sessions • TOE session establishment	

[Figure 2] Logical Scope of the TOE

Security Audit

The TOE generates audit data for all security function operations and, in the event of a potential security violation, sends an email alert to an authorized administrator and logs the incident.

The TOE generates audit data for each TOE components as follows.

ShadowCube Server

- Start/End of Audit Function
- Success/failure of administrator identification and authentication
- Product configuration changes history
- Security function execution history

ShadowCube Client

- Start/End of Audit Function
- Execution of operations on objects
- Successful/Failed Identification and Authentication of Document Users
- Results of TSF self-tests and integrity verification

Audit data includes detailed information on the date and time of the event, the event type, the identity of the entity that triggered the event, the operation details, and the result (success/failure).

Authorized administrators can review all audit data generated by the TOE via the GUI interface. Audit records are generated in a format suitable for interpretation by authorized administrators and allow for selective review based on logical relationship criteria such as AND and OR.

The TOE generates audit data when it predicts a loss of audit data and sends it via email to authorized administrators; to prevent the loss of audit data, it provides a function to overwrite the oldest records when the audit evidence repository becomes full and to send an email notification to authorized administrators.

Cryptographic Support

The TOE uses MagicCrypto V2.3.0, the validated cryptographic module developed by Dream Security, in order to apply encryption/decryption algorithms to TSF data according to the security policy, thereby providing assurance of confidentiality, integrity, and authentication.

The encryption/decryption algorithms used for cryptographic key generation and cryptographic key distribution, and the cryptographic key sizes, are specified below. If cryptographic keys and CSPs loaded in memory are no longer used, they are zeroized and destroyed.

ShadowCube Client: document encryption

- ARIA_CTR 128 bits

ShadowCube Client: Verification of the signature of the document file's author and the ShadowCube Client log creator

- RSA-PSS

ShadowCube Server, ShadowCube Client: Encryption of TSF data and communication data

- ARIA_CBC 256 bits
- RSAES 2048 bits

ShadowCube Server, ShadowCube Client: Hash generation

- SHA-256

ShadowCube Server, ShadowCube Client: Cryptographic Key Distribution

- ARIA_CBC 256 bits

ShadowCube Server, ShadowCube Client: Internal Mutual Authentication Key Agreement Between TOE components

- ECDH

ShadowCube Server, ShadowCube Client: KEK Generation

- PBKDF2

ShadowCube Server, ShadowCube Client: Random Bit Generation

- HASH_DRBG

Document Encryption

On ShadowCube Server, 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. ShadowCube 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 identities of administrators and document users via a GUI interface and restricts access in the event of authentication failure. It does not provide feedback on the reason for failure (e.g., ID error, password error) when identification or authentication fails. The authentication credentials of administrators and document users are processed to prevent reuse. If the number of authentication failures configured by the administrator is reached, authentication is disabled for 5 minutes for administrators and until the system is rebooted for document users.

The TOE performs mutual authentication during communication between the ShadowCube Server and the ShadowCube Client using the ECDH algorithm provided by a validated cryptographic module.

Passwords for administrators and document users must be between 9 and 16 characters long and must consist of a combination of four types of characters: uppercase and lowercase letters, numbers, and special characters.

The TOE identifies and authenticates administrators by administrator ID and email authentication code, and identifies and authenticates document users by document user certificates. In addition, the TOE prevents passwords from being displayed to administrators and users during authentication.

Security Management

The TOE provides functionality that allows authorized administrators to configure and manage security functions, security policies, and security roles via a GUI interface.

Protection of the TSF

The TOE protects TSF data from exposure and tampering by encrypting it with a validated cryptographic module when TSF data is transmitted between isolated sections of the TOE. Furthermore, it protects TSF data stored in repositories controlled by the TOE from unauthorized exposure and tampering by encrypting it with a validated cryptographic module.

The ShadowCube Server, a TOE component, performs self-tests and integrity checks at start-up, periodically during normal operation, and upon request by an authorized administrator. The ShadowCube Client, a TOE component, performs self-tests on key TOE processes and conducts integrity verification of TSF data and the TSF itself at start-up and periodically during normal operation.

Access control policies prevent unauthorized deletion of the configuration files and executable files of the ShadowCube Client, a TOE component, and prevent unauthorized termination of executable files.

The ShadowCube Server and ShadowCube Client, which are TOE components, provide a function to

query version information.

TOE Access

The TOE terminates the session of an authorized administrator who logged in via the GUI interface if the session timeout has expired. It also provides a function that allows authorized administrators to terminate their own sessions.

TOE limits the number of administrator sessions to one; if a login attempt is made from another device after an administrator has logged in, the new session is allowed, and the previous session is blocked.

Access to the ShadowCube Server is restricted to pre-registered IP addresses only. An authorized administrator can register as many IP addresses as the number of allowed connections.

1.4 Conventions

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

The Common Criteria permits the operations of iteration, assignment, selection, and refinement in security requirements. Each of these operations is used in this Security Target.

Iteration This operation is used when a single component is repeated multiple times by applying different operations. The result of an iteration operation is indicated by an iteration number in parentheses following the component identifier, i.e., (iteration number).

Assignment This operation is used to assign a specific value to an unspecified parameter (e.g., password length). The result of an assignment operation is denoted by square brackets, i.e., [assigned value].

Selection This operation is used to select one or more options provided by the Common Criteria for Information Technology Security Evaluation when stating a requirement. The result of a selection operation is indicated in underlined italics.

Refinement This operation is used to further refine a requirement by adding details. The result of a refinement operation is indicated in bold.

ST Author

This is used to represent that the final decision on attributes is made by the ST author. The ST author 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 are provided to clarify the intent of requirements, provide information for optional items in implementation, and define Pass/Fail criteria for a requirement. Application notes are provided with corresponding requirements, if necessary.

1.5 Terms and Definitions

Among the terms used in this Security Target, those that are identical to terms used in the Common Criteria follow the definitions in the Common Criteria and are not further described in this Security Target.

Private Key

A cryptographic key used in conjunction with an asymmetric Cryptographic Algorithm that is uniquely associated with a single entity (the subject using the private key) and must not be disclosed.

Object

A passive entity within the TOE that is the target of an entity's operations and that contains or receives information.

Approved Mode of Operation

Operation mode of a cryptographic module using an approved Cryptographic Algorithm

Approved Cryptographic Algorithm

Cryptographic algorithms selected by a cryptographic module validation authority based on considerations of security, reliability, interoperability, and other factors. These algorithms include block ciphers, hash functions, message authentication codes, random bit generators, key establishment algorithms, public key cryptographic algorithms, and digital signature algorithms.

Validated Cryptographic Module

A cryptographic module that has been validated and approved by a cryptographic module validation authority and assigned a validation number

Public Key

A cryptographic key used in conjunction with an asymmetric Cryptographic Algorithm that is uniquely associated with a single entity (the subject using the public key). It can be made public

Public Key (Asymmetric) Cryptographic Algorithm

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

Management Console

An application program that provides administrators with interfaces, such as a Graphical User Interface (GUI) and a Command Line Interface (CLI), for managing and configuring the system.

Random Bit Generator (RBG)

A device or algorithm that outputs a statistically independent and unbiased binary sequence. Random Bit Generators (RBGs) used for cryptographic applications generally generate bit sequences consisting of 0s and 1s, and these sequences can be combined into random bit blocks. RBGs are classified into deterministic and non-deterministic types. A deterministic RBG consists of an algorithm that generates bit sequences from an initial value called a 'seed', while a non-deterministic RBG produces output that relies on unpredictable physical sources.

Symmetric Cryptographic Techniques

A cryptographic technique that uses the same cryptographic key for both encryption and decryption; also known as secret-key cryptography.

License

This term collectively refers to various configuration information required to use ShadowCube, such as access permissions, operational environment settings, and policies. It includes user information, document group certificates and access permissions, license validity periods, application program information, and client configuration information. Licenses are granted by ShadowCube Server. They are automatically updated to the latest version when policies or configuration information change, or according to the specified license update cycle.

Document Group

This refers to an item used to grant users or departments using ShadowCube permissions such as reading, encryption (writing), and decryption for protected documents. When a user belonging to a document group creates a document, the document group information is included in the document immediately upon creation, thereby affecting the document group's permissions.

Document Group Based Access Control

A type of discretionary access control that controls access to objects based on group identifiers

Document Group Key

ShadowCube Server distributes specific keys for encrypted documents created in each document group so that only users of that group can access them. This key functions as the KEK (Key Encryption Key) for the encrypted document and is distributed as part of each user's license.

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

The use of the same component to represent two or more different requirements

Target of security

Refers to the application program for a document file that undergoes encryption/decryption using ShadowCube.

Security Target (ST)

Implementation-dependent Security Requirements specification suitable for a specific TOE

Protection Profile (PP)

Implementation-independent Security Requirements specification suitable for a TOE type

Decryption

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

Secret Key

A cryptographic key used in conjunction with a secret key Cryptographic Algorithm; it is uniquely associated with one or more entities and must not be disclosed

User License

The user license allows the user to control actions related to document processing, such as shell settings and ShadowCube Client configuration, and to configure the basic settings necessary for operating ShadowCube

Selection

The act of specifying one or more items from a list described in a component

System Unique Information

Unique information that distinguishes a system from other information systems

Korea Cryptographic Module Validation Program (KCMVP)

A scheme to validate the security and implementation conformance of cryptographic modules used to protect important but not classified information among data communicated through the information and communication networks of government and public institutions.

Encrypted File

An encrypted file.

Encryption

The process of converting plaintext into ciphertext using a cryptographic key

Role Based Access Control (RBAC)

An access control method that regulates access through user-to-role and permission-to-role assignments, using roles defined by organizational characteristics as intermediaries, rather than through a direct relationship between users and access permissions

Operation (on a component of the CC)

Modifying or iterating on a component. Permitted operations on a component include assignment, iteration, refinement, and selection.

Operation (on an object)

A specific action performed by a subject on an object

Authorized Administrator

An authorized user who safely operates and manages the TOE

Authorized Document User

A user who can execute functions in accordance with the SFR

Authentication Data

Information used to verify the claimed identity of a user

Regular File

An unencrypted file or a file that has been decrypted from an encrypted file

Application Programming Interface (API)

A set of software libraries that exists between the application layer and the platform system layer and facilitates the development of applications running on the platform

Self-tests

Pre-operation and conditional tests executed by the cryptographic module

ShadowCube Server

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

Dependencies

A Dependencies between components such that, if requirements based on a dependent component are included in a protection profile, security target, or package, then requirements based on the component on which that component depends must also be included in the PP, ST, or package

Subject

An active entity within a TOE that performs operations on objects

ShadowCube Client

Refers to the ShadowCube agent program installed on the document user's system.

File Conversion

Refers to the functionality that allows a security target file to be converted into a regular file, a secure file, or an executable secure file. File conversion is permitted only to users who have been granted decryption and export permissions for the document group.

Target of Evaluation (TOE)

A set of software, firmware, and/or hardware, accompanied by applicable documentation

Evaluation Assurance Level (EAL)

A set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale that forms an assurance package.

Family

A collection of components that share a similar purpose but differ in their focus or rigor

Hard disk serial number

A unique number assigned to each hard disk during manufacturing

TOE Security Functionality (TSF)

The 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 the SFRs 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 Problem Definition describes threats, organizational security policies, and assumptions for the TOE and TOE operational environment.

Chapter 4 Security Objectives defines the security objectives for the operational environment supported from the operational environment in order to provide TOE security functionality accurately. It also provides the rationale explaining how the security objectives for the operational environment satisfy the security problem definition.

Chapter 5 Extended Components Definition defines the extended components additionally needed according to the features of document encryption.

Chapter 6 Security Requirements describes the security functional requirements and security assurance requirements. Where necessary, application notes are provided to clarify the meaning of security

requirements and guide the ST author in correctly applying operations. It also presents the rationale explaining how the security requirements satisfy the security problem definition and dependencies.

1.7 Annex

This Security Target provides the following annex document

Validated Cryptographic Module Security Policy Document: MagicCrypto V2.3.0_SecurityPolicy.pdf

2. Conformance Claim

This chapter describes how this Security Target conforms with the CC.

2.1 CC Conformance Claim

The Common Criteria to which this Security Target and the TOE conform are as follows.

Category	Conformance
Common Criteria	Common Criteria for Information Technology Security Evaluation CC:2022, Revision 1 * Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CC:2022 R1 (CCMB-2022-11-001, November 2022) * Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CC:2022 R1 (CCMB-2022-11-002, Nov. 2022) * Common Criteria for Information Technology Security Evaluation, Part 3: Assurance Components, CC:2022 R1 (CCMB-2022-11-003, November 2022) * Common Criteria for Information Technology Security Evaluation, Part 4: Framework for Specifying Evaluation Methods and Activities, CC:2022 R1 (CCMB-2022-11-004, November 2022) * Common Criteria for Information Technology Security Evaluation, Part 5: Predefined Security Requirements Packages, CC:2022 R1 (CCMB-2022-11-005, November 2022) * Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025
Part 2: Security Functional Components	Extensions: FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2
Part 3: Security Assurance Components	Conformance
Package	Augmented: EAL1+ (ATE_FUN.1)

2.2 PP Conformance Claim

This Security Target complies with the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025).

Title	Korean National Protection Profile for Electronic Document Encryption
Version	3.1
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Author	National Security Research Institute
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of

	Science, ICT and Future Planning Notice No. 2013-51)
Common Criteria Version	CC:2022 R1
Certificate No.	KECS-PP-1349-2025
Keywords	Document, Encryption
PP Conformance Type	Strict PP conformance

2.3 Package Conformance Claim

The assurance requirement package to which this Security Target conforms is EAL1, with some additional Security Requirements defined.

* Assurance Package: EAL1 + (ATE_FUN.1)

2.4 Rationale for the Conformance Claim

Since this Security Target adopts the same TOE type, security objectives for the operational environment, security requirements, and assurance requirements as the Protection Profile, it satisfies the strict Protection Profile conformance required by the Korean National Protection Profile for Electronic Document Encryption V3.1.

2.4.1 Rationale for the TOE Type

ST	PP	Rationale
Document Encryption Product	Adopts the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)

2.4.2 Rationale for Security Objectives for the Operational Environment

ST	PP	Rationale
OE.PHYSICAL_CONTROL	Adopts the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
OE.TRUSTED_ADMIN		
OE.LOG_BACKUP		
OE.OPERATION_SYSTEM_REINFORCEMENT		
OE.SECURE_DBMS	Added	Added as a security objective for the operational environment because, in accordance with OE.SECURE_DBMS in the Korean National Protection Profile for Electronic Document Encryption, the TSF uses storage managed by a DBMS to store audit data for TOE operation and protects the audit data from unauthorized deletion or modification, thereby supporting stability.
OE.TRUSTED_PATH		Added as a security objective for the operational environment in accordance with the application notes for FTP_TRP.1, because the security management function is provided through communication between the web browser on the administrator PC and the web server, which is the operational environment of ShadowCube Server.
OE.TIME_STAMP		Added as a security objective for the operational environment because, in accordance with OE.TIMESTAMP in the Korean National Protection Profile for Electronic Document Encryption, the TSF is supported by a trusted timestamp function from the operational environment, such as synchronization with trusted time information from an external IT entity (e.g., a trusted NTP server).

2.4.3 Rationale for Security Requirements

ST		PP	Rationale
Security Audit (FAU)	FAU_ARP.1	FAU_ARP.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	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.1	FAU_STG.1	
	FAU_STG.2	FAU_STG.2	
	FAU_STG.4	FAU_STG.4	
	FAU_STG.5	FAU_STG.5	
Cryptographic Support (FCS)	FCS_CKM.1(1)	FCS_CKM.1(1)	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	FCS_CKM.1(2)	FCS_CKM.1(2)	
	FCS_CKM.2	FCS_CKM.2	
	FCS_CKM.5	FCS_CKM.5	
	FCS_CKM.6	FCS_CKM.6	
	FCS_COP.1(1)	FCS_COP.1(1)	
	FCS_COP.1(2)	FCS_COP.1(2)	
	FCS_RBG.1	FCS_RBG.1	
	FCS_RBG.3	FCS_RBG.3	
User Data Protection (FDP)	FDP_ACC.1(1)	FDP_ACC.1(1)	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	FDP_ACF.1(1)	FDP_ACF.1(1)	
Identification and Authentication (FIA)	FIA_AFL.1	FIA_AFL.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	FIA_IMA.1	FIA_IMA.1	
	FIA_SOS.1	FIA_SOS.1	
	FIA_UAU.1	FIA_UAU.1	
	FIA_UAU.4	FIA_UAU.4	
	FIA_UAU.5	FIA_UAU.5	
	FIA_UAU.7	FIA_UAU.7	
	FIA_UID.1	FIA_UID.1	
Security Management (FMT)	FMT_MOF.1	FMT_MOF.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	FMT_MSA.1	FMT_MSA.1	
	FMT_MSA.3	FMT_MSA.3	
	FMT_MTD.1	FMT_MTD.1	
	FMT_PWD.1	FMT_PWD.1	
	FMT_SMF.1	FMT_SMF.1	

	FMT_SMR.1	FMT_SMR.1	
Protection of the TSF (FPT)	FPT_FLS.1	FPT_FLS.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	FPT_ITT.1	FPT_ITT.1	
	FPT_PST.1	FPT_PST.1	
	FPT_PST.2	FPT_PST.2	
	FPT_RCV.2	FPT_RCV.2	
	FPT_TST.1	FPT_TST.1	
TOE Access (FTA)	FTA_MCS.2	FTA_MCS.2	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	FTA_SSL.3	FTA_SSL.3	
	FTA_TSE.1(1)	FTA_TSE.1(1)	
	FTA_TSE.1(2)	FTA_TSE.1(2)	

2.4.4 Rationale for Security Assurance Requirements

Security Assurance Class	Assurance Components	PP	Rationale
Security Target Evaluation	ASE_INT.1	ASE_INT.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	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 Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
Guidance	AGD_OPE.1	AGD_OPE.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	AGD_PRE.1	AGD_PRE.1	
Lifecycle Support	ALC_CMC.1	ALC_CMC.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	ALC_CMS.1	ALC_CMS.1	
Test	ATE_FUN.1	ATE_FUN.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)
	ATE_IND.1	ATE_IND.1	
Vulnerability Assessment	AVA_VAN.1	AVA_VAN.1	Equivalent to the Korean National Protection Profile for Electronic Document Encryption V3.1 (KECS-PP-1349-2025)

2.5 PP Conformance Statement

This ST strictly conforms to the Korean National Protection Profile for Electronic Document Encryption V3.1.

3. Security Problem Definition

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

3.1 Assets

The primary assets protected by document encryption are as follows.

Critical documents subject to protection that exist on user terminals and/or information systems where the TOE (agent) is installed

The TOE itself and critical data related to TOE operations (e.g., TSF data)

3.2 Threats

Threat actors are IT entities and users who attempt unauthorized access to or cause harm to the assets to be protected through abnormal means, and may pose various threats as follows. In this context, threat actors targeting the TOE possess a basic level of expertise, resources, and motivation.

3.2.1 Unauthorized Access

T. Session Hijack (T.SESSION_HIJACK)

A threat actor can gain user privileges by accessing a user's screen left unattended while logged in or by exploiting a user session that has not been terminated after the user has logged out.

T. Repeated Authentication Attempts (T.RETRY_AUTH_ATTEMPT)

A threat actor can gain TOE Access by successfully authenticating using information obtained through repeated authentication attempts and then impersonating an authorized user.

T. Impersonation (T.IMPERSONATION)

A threat actor can gain access to the TOE by impersonating an authorized user, a TOE component, or another entity.

T. Replay (T.REPLAY)

A threat actor can obtain and copy authentication credentials, then reuse them to access the TOE.

T. Weak Password (T.WEAK_PASSWORD)

A threat actor may acquire a poorly managed password, such as by using a default password, impersonate an authorized user, and gain access to the TOE.

If a weak password rule is applied, the threat actor may also impersonate an authorized user and gain access to the TOE.

3.2.2 Information Leakage

T. Unauthorized Information Leakage (T.UNAUTHORIZED_INFO_LEAK)

An attacker may leak important documents stored on user terminals and/or information systems in an unauthorized manner.

T. Stored Data Leakage (T.STORED_DATA_LEAKAGE)

A threat actor may leak sensitive data (e.g., cryptographic keys, TOE configuration values, etc.) stored within the TOE or in external entities interacting with the TOE (e.g., DBMS) in an unauthorized manner.

T. Transmission Data Compromise (T.TRANSMISSION_DATA_DAMAGE)

A threat actor may expose or modify data transmitted between TOE components and external IT entities in an unauthorized manner.

T.Weak Cryptographic Protocol (T.WEAK_CRYPTO_PROTOCOL)

A threat actor can analyze traffic that uses weak cryptographic protocols or has low cryptographic strength to infer cryptographic key information or determine the contents of encrypted messages.

3.2.3 Compromise of TOE Functionality

T.TSF Compromise (T.TSF_COMPROMISE)

A threat actor can compromise the TSF through unauthorized access or other means, causing the TOE to malfunction or rendering it inoperable.

3.3 Organizational Security Policies

P. Audit (P.AUDIT)

Security-related events shall be recorded and maintained to track responsibility for security-related actions, and the recorded data shall be reviewed. In addition, the available space of the disk used to store audit data shall be checked regularly to prevent audit data loss, and stored audit data shall be protected against unauthorized modification and deletion.

P. Secure Operation (P.SECURE_OPERATION)

Management means shall be provided so that administrators can securely configure the TOE in compliance with the organization's security policies and accurately operate the TOE in accordance with the TOE operation manual.

P. Cryptographic Strength (P.CRYPTO_STRENGTH)

The organization shall apply encryption measures to storage and transmission sections for critical data, such as passwords for user authentication, and shall use secure Cryptographic Algorithms.

3.4 Assumptions

It is assumed that the following conditions exist in the TOE operational environment that adopts this Security Target.

A. Physical Security (A.PHYSICAL_CONTROL)

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

A. Trusted Administrator (A.TRUSTED_ADMIN)

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

A. Secure Development (A.SECURE_DEVELOPMENT)

Developers who use the TOE to integrate document encryption/decryption functions in the operational environment of an information system shall comply with the requirements in the guidance documentation provided with the TOE so that the TOE security functions are applied securely.

A. Operation System Reinforcement (A.OPERATION_SYSTEM_REINFORCEMENT)

Reinforcement measures shall be performed for the latest vulnerabilities of the operating system on which the TOE is installed and operated, thereby ensuring the reliability and security of the operating system.

4. Security Objectives

The following security objectives for the operational environment shall be addressed by technical and procedural measures supported by the operational environment so that the TOE can accurately provide its security functions.

4.1 Security Objectives for the Operational Environment

ShadowCube Server

OE. Physical Security (PHYSICAL_CONTROL)

The location where ShadowCube Server is installed and operated shall be equipped with access control and protection facilities so that only authorized administrators can access it.

OE. Trusted Administrator (TRUSTED_ADMIN)

Authorized administrators shall not have malicious intentions, shall be properly trained on ShadowCube Server management functions, and shall accurately perform their duties in accordance with administrator guidance.

OE. Log Backup (LOG_BACKUP)

Authorized administrators shall periodically check the available space in the audit data repository in preparation for loss of audit records and perform audit record backups (external log server, separate

storage device, etc.) to prevent audit records from being exhausted.

OE. Operation System Reinforcement (OPERATION_SYSTEM_REINFORCEMENT)

Authorized administrators shall perform reinforcement measures to address the latest vulnerabilities of the operating system on which ShadowCube Server is installed and operated, thereby ensuring the reliability and security of the operating system.

OE. Secure DBMS (SECURE_DBMS)

Authorized administrators shall ensure that the DBMS used by the TOE stores audit data regarding TOE operations and protects the audit data from unauthorized deletion or modification, thereby ensuring stability.

OE. Trusted Path (TRUSTED_PATH)

Authorized administrators shall be provided with security management functions through secure communication between the web browser on the administrator PC and the web server, which is the operational environment of ShadowCube Server.

OE. Timestamp (TIME_STAMP)

The TOE shall accurately record security-related events using the trusted timestamp provided by the OS of ShadowCube Server.

OE. Secure Development (SECURE_DEVELOPMENT)

Developers who use the TOE to integrate document encryption/decryption functions in the operational environment of an information system shall comply with the requirements in the guidance documents provided with the TOE so that the TOE security functions are securely applied.

ShadowCube Client

OE. Trusted Administrator (TRUSTED_ADMIN)

Authorized administrators shall not have malicious intentions, shall be properly trained on ShadowCube Client management functions, and shall accurately perform their duties in accordance with administrator guidance.

OE. Operation System Reinforcement (OPERATION_SYSTEM_REINFORCEMENT)

Authorized administrators shall perform reinforcement measures to address the latest vulnerabilities of the operating system on which ShadowCube Client is installed and operated, thereby ensuring the reliability and security of the operating system.

4.2 Rationale for Security Objectives

4.2.1 Rationale for Security Objectives for the Operational Environment

[Table 6] Relationship between ShadowCube Server Security Problem Definition and Security Objectives for the Operational Environment

	OE. LOG_BACKUP	OE. PHYSICAL_CONTROL	OE. TRUSTED_ADMIN	OE. SECURE_DEVELOPMENT	OE. OPERATION_SYSTEM_REINFORCEMENT	OE. SECURE_DBMS	OE. TRUSTED_PATH	OE. TIME_STAMP
P.AUDIT	O					O		O
P.SECURE_OPERATION			O				O	
A.PHYSICAL_CONTROL		O						
A.TRUSTED_ADMIN	O		O			O		
A.SECURE_DEVELOPMENT				O				
A.OPERATION_SYSTEM_REINFORCEMENT					O			

P.Audit OE.LOG_BACKUP, OE.SECURE_DBMS, OE.TIME_STAMP
P.Audit is carried out through **OE.LOG_BACKUP, OE.SECURE_DBMS, OE.TIME_STAMP**.

OE.LOG_BACKUP not only supports the TOE operation but also ensures that administrators periodically inspect audit data storage space. To ensure that audit records are not lost, regular log backups or transfer of logs to an external log server are performed.
OE.SECURE_DBMS safely stores audit data generated during TOE operation in the database and ensures the integrity and reliability of audit records by protecting them so that unauthorized users cannot arbitrarily delete or modify the data.
OE.TIME_STAMP uses reliable time information provided by the ShadowCube Server OS to record all security-related events, ensuring the precise timing of audit logs and enabling subsequent tracking and analysis.

P.SECURE_OPERATION OE.TRUSTED_ADMIN, OE.TRUSTED_PATH
P.SECURE_OPERATION is carried out by **OE.TRUSTED_ADMIN, OE.TRUSTED_PATH.**

OE.TRUSTED_ADMIN ensures that administrators operate the TOE correctly according to the organization's document encryption security policies and operation manuals.
OE.TRUSTED_PATH encrypts the communication channel between the administrator PC and ShadowCube Server to prevent information leakage and tampering, thereby ensuring that authorized administrators can safely perform security management functions.

A.PHYSICAL_CONTROL OE.PHYSICAL_CONTROL
A.PHYSICAL_CONTROL is supported by **OE.PHYSICAL_CONTROL.**

OE.PHYSICAL_CONTROL places the management server in a facility equipped with protective measures and controls access so that only authorized administrators may enter.

A.TRUSTED_ADMIN OE.TRUSTED_ADMIN, OE.LOG_BACKUP, OE.SECURE_DBMS
A. TRUSTED_ADMIN is supported by **OE.TRUSTED_ADMIN, OE.LOG_BACKUP, OE.SECURE_DBMS**.

OE.TRUSTED_ADMIN ensures that administrators are not malicious, have been properly trained on TOE management functions, and accurately perform their duties in accordance with administrator guidance.
OE.LOG_BACKUP ensures that authorized administrators periodically check the available space in the audit data repository to prevent the loss of audit records and perform audit record backups (to external log servers, separate storage devices, etc.) so that audit records are not exhausted.
OE.SECURE_DBMS provides an environment where authorized administrators can securely store and manage audit data, and ensures that security management duties are properly performed by preventing arbitrary deletion or modification of data caused by abuse of administrator authority.

A.SECURE_DEVELOPMENT OE.SECURE_DEVELOPMENT
A.SECURE_DEVELOPMENT is supported by **OE.SECURE_DEVELOPMENT.**

OE.SECURE_DEVELOPMENT ensures that developers who integrate document encryption/decryption functions into the operational environment of an information system using the TOE comply with the requirements in the guidance documents provided with the TOE so that the TOE security functions are securely applied.

A.OPERATION_SYSTEM_REINFORCEMENT OE.OPERATION_SYSTEM_REINFORCEMENT
A.OPERATION_SYSTEM_REINFORCEMENT is supported by **OE.OPERATION_SYSTEM_REINFORCEMENT**

OE.OPERATION_SYSTEM_REINFORCEMENT ensures the reliability and security of the operating system by performing reinforcement measures to address the latest vulnerabilities of the operating system on which the TOE is installed and operated.

[Table 7] Relationship between ShadowCube Client Security Problem Definition and Security Objectives for the Operational Environment

	OE.TRUSTED_ADMIN	OE.OPERATION_SYSTEM_REINFORCEMENT
A.TRUSTED_ADMIN	O	
A.OPERATION_SYSTEM_REINFORCEMENT		O

A.TRUSTED_ADMIN OE.TRUSTED_ADMIN

A.TRUSTED_ADMIN is supported by **OE.TRUSTED_ADMIN.**

OE.TRUSTED_ADMIN ensures the reliability of the client operational environment by ensuring that authorized administrators properly manage security settings of user devices on which ShadowCube Client is installed, provide users with correct usage guidance and training, and accurately perform management duties according to administrator guidance.

A.OPERATION_SYSTEM_REINFORCEMENT OE.OPERATION_SYSTEM_REINFORCEMENT

A.OPERATION_SYSTEM_REINFORCEMENT is supported by **OE.OPERATION_SYSTEM_REINFORCEMENT.**

OE.OPERATION_SYSTEM_REINFORCEMENT ensures the reliability and security of the operating system by performing reinforcement measures to address the latest vulnerabilities in the operating system on which the TOE is installed and operated.

5. Extended Components Definition

5.1 Identification and Authentication (FIA)

5.1.1 TOE Internal Mutual Authentication

Family Behaviour

The TOE Internal Mutual Authentication (FIA_IMA) family requires that TOE components provide internal mutual authentication capabilities during the user identification and authentication process.

Component Hierarchy and Description

FIA_IMA.1 Internal Mutual Authentication Between TOE components requires that the internal mutual authentication function between TOE components be provided during the user identification and authentication process.

Management: FIA_IMA.1

No management activities are foreseen.

Audit: FIA_IMA.1

When the FAU_GEN security audit data generation family is included in a PP, PP module, function package, or ST, it is recommended that the following actions be audited.

a) Minimum: Success/failure of mutual authentication

5.1.1.1 FIA_IMA.1 TOE Internal Mutual Authentication

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FIA_IMA.1.1

The TSF shall perform mutual authentication between [Assignment: *Separate parts of the TOE*] using [Assignment: *Authentication protocols*] that comply with [Assignment: *Standard list*].

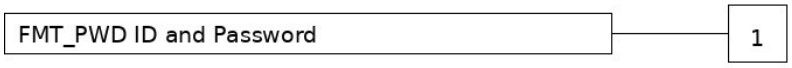
5.2 Security Management (FMT)

5.2.1 ID and Password

Family Behaviour

The ID and Password (FMT_PWD) family is defined to require the ability to control the management of IDs and passwords used by authorized users within the TOE, as well as the ability to set or change IDs and/or passwords

Component Hierarchy and Description



FMT_PWD.1 ID and Password Management requires that the TSF provide ID and password management functions.

Management: FMT_PWD.1

The following management functions may be considered in the FMT:

a) Management of rules for setting IDs and passwords

Audit: FMT_PWD.1

If the FAU_GEN security audit data generation family is included in the PP/ST, it is recommended that the following actions be audited.

a) Minimum: All changes to passwords

5.2.1.1 FMT_PWD.1 Management of ID and Password

Component Relationships

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 passwords in [Assignment: List of Functions] to [Assignment: Authorized Roles] as follows.

1. [Assignment: *Password Combination Rules and/or Length*]

2. [Assignment: *Other management tasks, such as managing special characters to be excluded from passwords*]

FMT_PWD.1.2

The TSF shall restrict the ability to manage IDs in [Assignment: *List of Functions*] to [Assignment: *Authorized Roles*] as follows.

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

2. [Assignment: *Other management tasks, such as managing special characters to be excluded from IDs*]

FMT_PWD.1.3

The TSF shall provide a function to [*select one of the following: set the ID and password during installation; set the password during installation; have an authorized administrator change the ID and password upon first login; or have an authorized administrator change the password upon first login*].

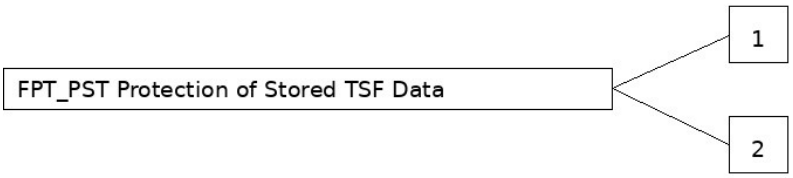
5.3 Protection of the TSF (FPT)

5.3.1 Protection of Stored TSF Data

Family Behaviour

The Protection of Stored TSF Data (FPT_PST) family defines rules to protect TSF data stored in repositories controlled by the TSF from unauthorized modification or exposure.

Component Hierarchy and Description



FPT_PST.1 Basic protection of stored TSF data requires that TSF data stored in a repository controlled by the TSF be protected.

FPT_PST.2 The availability protection for TSF data requires that the TSF ensure the availability of TSF data at a defined level.

Management: FPT_PST.1, FPT_PST.2

No management activities are foreseen

Audit: FPT_PST.1, FPT_PST.2

No auditable events are foreseen

5.3.1.1 FPT_PST.1 Basic Protection of Stored TSF Data

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_PST.1.1

The TSF shall protect [Assignment: *TSF data*] stored in repositories controlled by the TSF from unauthorized [Selection: *exposure, modification*].

5.3.1.2 FPT_PST.2 Availability Protection of TSF Data

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_PST.2.1

TSF must [Selection: *Detect or Prevent*] unauthorized deletion of [Assignment: *TSF data*].

FPT_PST.2.2

The TSF shall [Selection: *Detect or Prevent*] unauthorized termination of [Assignment: *TSF data*].

6. Security Requirements

This section describes the Security functional Requirements and assurance requirements that must be met by the TOE.

[Table 8] Terms and Definitions of Subjects, Objects, and Related Security Attributes and Operations

Subject (User)		Object (Information)		Operation	Related SFR
List	**Security attribute**	**List**	**Security attribute**		
Document user	• Document User ID • Password	• Documents to Be Protected	• Document group ID • Document Name • Document Type • Document Path	• If the user has read and encryption (write) permissions, allow the document to be read and save it in an encrypted format using document encryption • If the user has decryption permissions, decrypt the document	• FDP_ACC.1 • FDP_ACF.1(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
		• IP Connection Settings	-	• Query, Modify, Delete, Add	• FMT_MTD.1
		• Session Timeout • Maximum Number of Failed Login Attempts • Minimum Password Length	-	• Threshold Specifications • Change	• FMT_MTD.1
		• TSF data	-	• Integrity Verification	• FPT_TST.1

		• security attribute	-	• Default Value Query, Delete, Add	• FMT_MSA.1
		• security function	-	• Determine the behaviour of, disable, enable, or modify the behaviour of	• FMT_MOF.1

※ Only one type of authorized administrator is provided in the TOE; this is the web administrator designated during TOE installation.

6.1 Security Functional Requirements

The TOE satisfies the mandatory SFRs listed in the following table.

[Table 9] Security functional Requirements

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security Alerts
	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1	Potential Violations Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Optional Audit Review
	FAU_STG.1	Audit Data Storage Location
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic Key Generation (Document Encryption)
	FCS_CKM.1(2)	Cryptographic Key Generation (TSF data encryption)
	FCS_CKM.6	Cryptographic Key Destruction Timing and Events
	FCS_COP.1(1)	Cryptographic Operations (Document Encryption)
	FCS_COP.1(2)	Cryptographic Operations (TSF data Encryption)
	FCS_RBG.1	Random Bit Generation (RBG)
	FCS_RBG.3	Random bit generation (internal seeding – single source)
Document Encryption (FDP)	FDP_ACC.1(1)	Subset access control (Document Group-Based Access Control)
	FDP_ACF.1(1)	Security attribute-based access control (Document Group-Based Access Control)
Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_IMA.1	(Extended) Internal Mutual Authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Authentication
	FIA_UAU.4	Single-use Authentication Mechanism

(FIA)	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.1	Timming 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 initialisation
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1	Management of ID and password (Extended)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1	Basic protection of stored TSF data (Extended)
	FPT_PST.2	Availability protection of TSF data (Extended)
	FPT_TST.1	TSF testing
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions (ShadowCube Server)
	FTA_TSE.1(1)	TOE session establishment

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_ARP.1 Security Alerts

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential Violation Analysis

FAU_ARP.1.1

If the TSF detects a potential security violation, it must take the actions listed in [[Table 10], [Table 11] List of Response Actions].

[Table 10] Send an email to an authorized administrator upon detection of a potential security violation

ShadowCube Server	ShadowCube Client
• When the threshold for failed authentication attempts is reached • Upon failure of self-tests or integrity verification • When a self-test of a validated cryptographic module fails • When the audit log threshold is predicted to be exceeded • When the audit log threshold is exceeded	• When the limit for failed authentication attempts is reached • When self-tests or integrity verification fail • When the self-test of a validated cryptographic module fails • In the event of a violation of the control rules

[Table 11] Disable authentication when the configured number of authentication failures is reached

ShadowCube Server	ShadowCube Client
Identification and authentication disabled for 5 minutes	Reboot the PC and disable identification and authentication for 5 minutes

If the ShadowCube Client fails a self-test, reboot the system and stop the ShadowCube service
If the ShadowCube Client fails the integrity check, send an email to an authorized administrator and perform recovery using the automatic recovery feature

6.1.1.2 FAU_GEN.1 Audit Data Generation

Component Relationships

Hierarchical to: No other components

Dependencies: FPT_STM.1 Trusted Timestamp

FAU_GEN.1.1

The TSF shall be capable of generating audit records for the following auditable events:

1. Start-up and shutdown of the audit function
2. *Not specified* All auditable events according to the audit level
3. [See [Table 11] "Auditable Events" for auditable events]

FAU_GEN.1.2

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

1. Event date and time, event type, subject identity (if possible), operation details, event outcome (success or failure)
2. For each audit event type, based on the definitions of auditable events for functional components included in the PP/ST [see [Table 12] "Additional Audit Log Content" for auditable events]

[Table 12] Auditable Events

TOE component	Security Function Component	auditable event	Additional Audit Log Content
ShadowCube Server	FAU_ARP.1	Countermeasures Taken in Response to a Potential Security Violation	
	FAU_SAA.1	Initiation and suspension of analysis mechanisms, and automated responses via tools	
	FAU_STG.4	Response Actions When Threshold Exceedance Is Predicted	
	FAU_STG.5	Response Actions When Thresholds Are Exceeded	
	FCS_CKM.1(2)	* Success and failure of cryptographic key generation * Success and failure of encryption operations * Success and failure of cryptographic key distribution	
	FCS_CKM.2	Success and failure of key distribution related to document encryption and decryption	
	FCS_CKM.6	Success and Failure in Cryptographic Key Destruction	
	FCS_COP.1	Success and Failure of Cryptographic Operations, Types of Cryptographic Operations	
	FIA_AFL.1	Reaching the Threshold for Failed Authentication Attempts and Corresponding Actions Taken	
	FIA_IMA.1 (Extended)	Success/Failure of Mutual Authentication	
	FIA_UAU.1	All Results of Administrator Authentication	
	FIA_UAU.4	Attempts to Reuse Email Authentication Codes	
	FIA_UID.1	Any use of the user identification mechanism, including the provided user identity	

	FMT_MOF.1	* Add/modify/delete departments * Add/modify/delete users * Add/modify/delete document groups * Changing default license policy property values * View Certificate Issuance Status and Revoke Certificates * Configure ShadowCube Server self-testing and integrity verification * Configure connection IP, client connection IP, session timeout, maximum number of failed login attempts, and minimum password length in the environment settings	
	FMT_MSA.1	* Add, modify, or delete document groups * Add/Remove Departments and Users from Document Groups * Add/Remove Security Targets to Document Groups * Set read, write, and decryption permissions for document groups	Changed security attribute values
	FMT_MSA.3	Changes to the default settings for permission or restriction rules, or changes to the default values of security attributes	Changed security attribute values
	FMT_MTD.1	* Authorized administrator - Document user certificates, audit data, IP address settings, session timeout settings, maximum number of failed login attempts, and minimum password length * Document User - Issuing document user certificates, updating licenses	Changed TSF data values
	FMT_PWD.1 (Extended)	Changes to password combination rules	
	FMT_SMF.1	* Events related to the management function for security functions listed in [Table 12] - Changes to object settings, policy settings, authentication management, and environment settings * Events involving the execution of management functions for items related to TSF data in [Table 14] - Configuration by authorized administrators of	

		document user certificates, audit data, access IP settings, session timeouts, login failure limits, and minimum password length requirements - Issuance of document user certificates and license updates by document users * Events involving the execution of management functions for security attributes in [Table 13] - Changes to document user IDs, document group IDs, and security attributes by authorized administrators	
	FPT_TST.1	* Results of the TSF self-test and integrity verification * Results of failed self-tests and integrity verification for validated cryptographic modules	Executable file with integrity violation
	FTA_MCS.2	Termination of an existing connection based on the limit on the number of concurrent sessions	
	FTA_SSL.3	Administrative session terminated due to exceeding the allowed inactivity period for authorized administrators	
	FTA_TSE.1	Reject administrator management session requests based on the connecting IP address	
ShadowCube Client	FCS_CKM.1(2)	* Success and failure of cryptographic key generation * Successful and failed key distribution * Success and failure of encryption operations * Success and failure of cryptographic key destruction	
	FCS_CKM.2	Success and failure of key distribution related to document encryption and decryption	
	FCS_CKM.6	Success and failure of cryptographic key destruction	
	FCS_COP.1	Success and Failure of Cryptographic Operations, Types of Cryptographic Operations	
	FDP_ACF.1(1)	* An incident in which a document user with permissions successfully accessed, read, wrote to, or decrypted an encrypted document in a document group * An event in which a document user attempted to access an encrypted document in a document group for which they lacked permissions and was denied access due to a violation of control rules	Object Identification Information
	FIA_AFL.1	Reaching the threshold for failed authentication attempts and the corresponding actions taken	

	FIA_IMA.1 (Extended)	Success/failure of mutual authentication	
	FIA_UAU.1	* Document User Certificate Request * Request to Enter Email Authentication Code * Document User Certificate Creation * Request for Identification and Authentication Procedures	
	FIA_UAU.4	Attempt to reuse an email authentication code	
	FIA_UID.1	Any use of the user identification mechanism, including the provided user identity	
	FPT_TST.1	* Results of the TSF self-test and integrity verification * Results of failed self-tests and integrity verification for validated cryptographic modules	Executable File with Integrity Violation

6.1.1.3 FAU_SAA.1 Potential Violation Analysis

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAA.1.1

When the TSF examines audited incidents, it must be able to apply a set of rules and, based on these rules, identify potential violations regarding the performance of the SFR.

FAU_SAA.1.2

When examining audited events, the TSF must apply the following rules.

1. Known events indicating potential security violations, including authentication failure auditable events among the auditable events in [FIA_UAU.1], FPT_TST.1 auditable events indicating integrity violations, self-test failures of validated cryptographic modules, FAU_STG.4 auditable events where the audit repository has reached a specified threshold, FAU_STG.5 auditable events where the audit repository has reached saturation, and FDP_ACF.1 auditable events indicating control rule violations]
2. [None]

6.1.1.4 FAU_SAR.1 Audit Review

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1

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

FAU_SAR.1.2

The TSF shall provide audit records in a format suitable for interpretation by **authorized administrators**.

6.1.1.5 FAU_SAR.3 Selectable Audit Review

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit Review

FAU_SAR.3.1

The TSF shall provide the capability to apply [search or ascending/descending sorting methods] to audit data based on [[Table 13] Audit Data Types and Audit Data Type Selection].

[Table 13] Audit Data Types and Selection of Audit Data Types

Audit Data Types	audit record	Based on Logical Relationships	Sequencing Method
User Audit	Category, Date/Time of Action, IP, MAC, Department Code, Department Name, Employee ID, user name, job title, Module, Message, Date/Time of Record	All combinations of audit record fields (AND)	Search
		Combinations of category records (OR)	Search
		Based on 1 selected item from the audit records	Sort
Administrator Audit	Category, Menu, Date/Time of Action, IP, Department Code, Department Name, Employee ID, Manager, Position, Action Details	All combinations in audit records (AND)	Search
		Combinations of category records (OR)	Search
		Combinations of menu records (OR)	Search
		Based on one item selected from the audit record	Sort
System Audit	Date and Time of Operation, IP, Operation Details	Operation Date	Search
		Based on 1 item selected from the audit records	Sort
Document Log	Document Group, Security Object, Task Date/Time, Department Code, Department Name, Employee ID, User Name, Job Title, Total, Created, Read	All combinations in audit records (AND)	Search
		Combinations of document group records (OR)	Search
		Combinations of Security Object Records (OR)	Search
		Based on one item selected from Department Code, Department Name, Employee ID, user name, job title, Total, Created, or Reading	Sort
Document Details Log	Operation Date/Time, License, Category, IP, MAC, Department Code, Department, Employee ID, User, Job Title, Program Name, Version, Storage Medium, File Name, Full Path, Document Group	All combinations of audit records (AND)	Search
		Combinations of license records (OR)	Search
		Combinations of Category Records (OR)	Search
		Based on one item selected from the audit record	Sort

Decryption Log	Document Group, Date/Time, Department Code, Department Name, Employee ID, User Name, Job Title, Number of Decryption Occurrences	All combinations in the audit record (AND)	Search
		Based on one selected item from Department Code, Department Name, Employee ID, user name, job title, or Number of Decryption Occurrences	Sort
Decryption Details Log	Date and Time, License, Category, IP, MAC, Department Code, Department, Employee ID, User, Job Title, File Name, Size	All combinations in audit records (AND)	Search
		Combinations of license records (OR)	Search
		Combinations of Category Records (OR)	Search
		Based on 1 item selected from the audit records	Sort
Integrity Verification History	Operation Date/Time, PC Name, IP, MAC, Verification File, Message, Log Date/Time	All combinations in audit records (AND)	Search
		Based on one selected item from the audit records	Sort
Login history by period	Login, Logout, IP, MAC, Host Name, Hard Drive Serial Number, Department Code, Department Name, Employee ID, user name, job title, Login Method, Log Date and Time	All combinations of audit records (AND)	Search
		Combinations of login method records (OR)	Search
		Based on one selected item from the following: Login, Logout, IP, MAC, Host Name, Hard Disk Serial Number, Department Code, Department Name, Employee ID, User Name, Position, Login Method, or Log Date and Time	Sort
Last Login Information by User	Department code, department, employee ID, user, job title, last login date and time	All combinations in the audit record (AND)	Search
		Based on one selected item from the audit records	Sort

6.1.1.6 FAU_STG.1 Audit Data Storage Location

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_STG.1.1

The TSF shall be able to store the generated audit data within the *TOE itself* or *[in other storage locations]*.

Stored within the TOE itself

- ShadowCube Client - C:₩ProgramData₩ShadowCube₩UserAccount₩ShadowCube.2026xxxx.adt

Storing in other location(s)

- ShadowCube Server: ShadowCube Server installation path₩data

6.1.2 Cryptographic Support (FCS)

The TOE's cryptographic functions use the validated Cryptographic Algorithms of the validated cryptographic module (MagicCrypto V2.3.0) as listed below.

[Table 14] Algorithms Subject to Validation in the Validated Cryptographic Module

Standard List	Encryption Method	Cryptographic Algorithm	Key Length	Purpose
KS X 1213-1	Block cipher	ARIA_CTR	128	User Data Encryption • ShadowCube Client: Electronic document encryption when saving protected documents

		ARIA_CBC	256	TSF data Encryption
				• ShadowCube Server
				  • DB Password Encryption
				  • Document Group Key Encryption
				• ShadowCube Client
				  • Document User Certificate Encryption of the document user's private key
				  • Document User License Encryption
				  • Encryption of Log Files and Configuration Files
				  • Encryption of Memory Data for TSF Data Storage
				• Common
				  • Protection of Data in Transit Between TOE components

ISO/IEC 11770-3	Key Generation	ECDH	256	Key Agreement for Mutual Authentication Among TOE components

TTAS.KO-12.0334	Key Derivation	PBKDF2	256	• ShadowCube Server
				  • Derivation of the KEK for the DB Password Cryptographic Key
				• ShadowCube Client
				  • Derivation of the KEK for the Private

				Key Encryption Key of the Document User Certificate • Derivation of the KEK for TSF data protection
ISO/IEC 18031	random bit generator	HASH_DRBG	256	• TSF data and document encryption key • ShadowCube Server: Generate DB password cryptographic key • ShadowCube Client: Document Cryptographic Key Generation • Generate DEK for TSF data protection • Generating Cryptographic Keys for User Certificate Private Keys • Random Bit Generation When Creating RSA and ECC Key Pairs • Generating email authentication codes • Email authentication code for web administrator login • Email authentication code for user certificate issuance
ISO/IEC 18033-2	Public key cryptography	RSAES	2048	• KEK in the cryptographic document • Protection of data transmitted between TOE components (including user licenses)
ISO/IEC 10118-3	Hash function	SHA-256	256	• ShadowCube Server • Store the web

				administrator password in the database (with a salt) • Store hashes for integrity verification targets • ShadowCube Client • Verify the hash for items subject to integrity verification
ISO/IEC 14888-2	Digital Signatures	RSA-PSS	2048	• ShadowCube Server: Signature verification for the audit log creator • ShadowCube Client: Signatures for the author of the document file and the audit log creator

6.1.2.1 FCS_CKM.1(1) Cryptographic Key Generation (Document Encryption)

Component Relationships

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution or FCS_COP.1 Cryptographic Operations] or FCS_CKM.5 Cryptographic Key Derivation, FCS_RBG.1 (Extended) Random Bit Generation, or FCS_CKM.6 Cryptographic Key Destruction Timing and Events

FCS_CKM.1.1

The TSF shall generate the **Data Encryption Key (DEK)** and the **Key Encryption Key (KEK)** in accordance with the specified [Cryptographic Algorithm] and the specified [key length] that comply with the following [Standard List].

[Table 15]

Standard List	Generation Algorithm	Key Length	Purpose
ISO/IEC 18031	HASH_DRBG	128 bits	Document Cryptographic Key (DEK)
ISO/IEC 18031	HASH_DRBG	256 bits	Random bit generation during RSA key generation
ISO/IEC 18033-2	RSA	2048 bits	Document Encryption DEK Cryptographic Key Generation (KEK)

6.1.2.2 FCS_CKM.1(2) Cryptographic Key Generation (TSF data encryption)

Component Relationships

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution or FCS_COP.1 Cryptographic Operations] or FCS_CKM.5 Cryptographic Key Derivation, FCS_RBG.1 (Extended) Random Bit Generation, or FCS_CKM.6 Cryptographic Key Destruction Timing and Events

FCS_CKM.1.1

The TSF shall generate a cryptographic key in accordance with the specified [Cryptographic Algorithm] and specified [key length] that comply with the following [Standard List].

[Table 16] ShadowCube Server

Standard List	Cryptographic Algorithm	Key Length	Purpose
ISO/IEC 18031	HASH_DRBG	256 bits	Generation of DB password cryptographic keys
ISO/IEC 18031	HASH_DRBG	256 bits	Random bit generation when generating RSA and ECC key pairs
ISO/IEC 15946	ECC	256 bits	Generation of public and private keys for ECDH key agreement
ISO/IEC 18033-2	RSA	2048 bits	Encryption and decryption of each user's license data during communication, and verification of the log generator's signature

[Table 17] ShadowCube Client

Standard List	Cryptographic Algorithm	Key Length	Purpose
ISO/IEC 18031	HASH_DRBG	256 bits	Generation of DEK for TSF data protection
ISO/IEC 18031	HASH_DRBG	256 bits	Generating a key for encrypting the user certificate's private key
ISO/IEC 18031	HASH_DRBG	256 bits	Random bit generation when generating RSA and ECC key pairs
ISO/IEC 15946	ECC	256 bits	Generation of public and private keys for ECDH key agreement
ISO/IEC 18033-2	RSA	2048 bits	Encryption and decryption of license data and log signing during communication

6.1.2.3 FCS_CKM.6 Cryptographic Key Destruction Timing and Events

Component Relationships

Hierarchical to: No other components

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

FCS_CKM.6.1

When TSF *is no longer needed*, it must destroy the [DEK, KEK, session key, ECDH key pair, RSA key pair, certificate key pair, and certificate private key cryptographic key].

[Table 18] ShadowCube Server

Key Generation Algorithm	Key Length	Purpose	Destruction Timing
HASH_DRBG	256 bits	DEK	Upon IIS shutdown or system shutdown
PBKDF2	256 bits	KEK	
RSA	2048 bits	RSA key pair	
ECC	256 bits	ECDH key pair	

[Table 19] ShadowCube Client

Category	Key Generation Algorithm	Key Length	Purpose	Destruction Time
Document Encryption	HASH_DRBG	128 bits	DEK	When the application program (document program) closes
	RSA	2048 bits	KEK	When the user logs out or the system shuts down
TSF data Encryption	HASH_DRBG	256 bits	DEK	When a user logs out or the system shuts down
	PBKDF2	256 bits	KEK	
	RSA	2048 bits	Certificate Key Pair	When deleting or revoking a user certificate
	HASH_DRBG	256 bits	Certificate private key cryptographic key	
	ECC	256 bits	ECDH key pair	Upon system shutdown

* The HASH_DRBG random bits used to generate RSA and ECC keys are destroyed when each key is

discarded

FCS_CKM.6.2

TSF must destroy the cryptographic keys and key materials specified in FCS_CKM.6.1 in accordance with the specified cryptographic key destruction method [DEK, KEK, and security-critical parameters are overwritten with '0' three times], which complies with the following [None].

6.1.2.4 FCS_COP.1(1) Cryptographic Operations (Document Encryption)

Component Relationships

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 User Data Inflow without Security Attributes or FDP_ITC.2 User Data Inflow with Security Attributes or FCS_CKM.1 Cryptographic Key Generation] or FCS_CKM.5 Cryptographic Key Derivation, FCS_CKM.6 Cryptographic Key Destruction Timing and Events

FCS_COP.1.1

The TSF shall perform [document encryption/decryption] in accordance with the specified Cryptographic Algorithms [ARIA_CTR, RSAES] and the specified cryptographic key lengths [128 bits, 2048 bits] that comply with the following [Standard List].

[Table 20]

Standard List	Cryptographic Algorithm	Key Length	Purpose
KS X 1213-1	ARIA_CTR	128 bits	Document Encryption/Decryption
ISO/IEC 18033-2	RSAES	2048 bits	KEK

6.1.2.5 FCS_COP.1(2) Cryptographic Operation (TSF data encryption)

Component Relationships

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 User Data Inflow Without Security Attributes or FDP_ITC.2 User Data Inflow With Security Attributes or FCS_CKM.1 Cryptographic Key Generation or FCS_CKM.5 Cryptographic Key Derivation], FCS_CKM.6 Cryptographic Key Destruction Timing and Events

FCS_COP.1.1

TSF must perform [TSF data encryption/decryption] in accordance with the specified Cryptographic Algorithms [ARIA_CBC, RSAES, RSA-PSS, SHA-256] and specified cryptographic key lengths [256 bits, 2048 bits] that comply with the following [Standard List].

[Table 21] ShadowCube Server

Standard List	Cryptographic Algorithms	Key Length	Purpose
KS X 1213-1	ARIA_CBC	256 bits	• Protection of data transmitted between TOE components • DB Password Encryption • Document group key encryption
ISO/IEC 18033-2	RSAES	2048 bits	Protection of data transmitted between TOE components
ISO/IEC 14888-2	RSA-PSS	2048 bits	Signature verification for audit log generators
ISO/IEC 10118-3	SHA-256	256 bits	• Store web administrator passwords in the database (with SALT) • Storing the hash of the integrity verification target

[Table 22] ShadowCube Client

Standard List	Cryptographic Algorithms	Key Length	Purpose
KS X 1213-1	ARIA_CBC	256 bits	• Protection of data transmitted between TOE components • Encryption of the document user's certificate private key • Encryption of the document user's license • Encryption of log files and configuration files

			• Encryption of memory data for TSF data storage
ISO/IEC 18033-2	RSAES	2048 bits	Protection of data transmitted between TOE components
ISO/IEC 14888-2	RSA-PSS	2048 bits	Signature of the document author and audit log creator
ISO/IEC 10118-3	SHA-256	256 bits	HASH verification of the subject of integrity verification

6.1.2.6 FCS_RBG.1 Random Bit Generation (RBG)

Component Relationships

Hierarchical to: No other components

Dependencies: FPT_FLS.1 Failure with preservation of secure state; FPT_TST.1 TSF self-test; FCS_RBG.3 Random Bit Generation (Internal Seeding: Single Source)

FCS_RBG.1.1

After initialization, the TSF must perform a deterministic Random Bit Generation service using [HASH_DRBG] in accordance with [ISO/IEC 18031].

[Table 23] ShadowCube Server

Standard List	Cryptographic Algorithm	Key Length	Purpose
ISO/IEC 18031	HASH_DRBG	256 bits	Generation of DB password cryptographic keys
ISO/IEC 18031	HASH_DRBG	128 bits	Generate administrator login email authentication code
ISO/IEC 18031	HASH_DRBG	128 bits	Generate email authentication code when issuing a user certificate
ISO/IEC 18031	HASH_DRBG	128 bits	Random bit generation when creating RSA and ECC key pairs

[Table 24] ShadowCube Client

Standard List	Cryptographic Algorithm	Key Length	Purpose
ISO/IEC 18031	HASH_DRBG	128 bits	Document Encryption Key Generation
ISO/IEC 18031	HASH_DRBG	256 bits	TSF data cryptographic key

			generation
ISO/IEC 18031	HASH_DRBG	256 bits	User Certificate Cryptographic Key Generation
ISO/IEC 18031	HASH_DRBG	128 bits	Random bit generation when generating RSA and ECC key pairs

FCS_RBG.1.2

The TSF shall use the *TSF* interface *to obtain entropy* for initialization and seeding.

FCS_RBG.1.3

The TSF shall update the DRBG state by *reseeding* using the *TSF interface [MC_Initialize] to obtain entropy* in accordance with [ISO/IEC 18031] in the following situations.

- The following situations: *Upon request*

6.1.3 Document Encryption (FDP)

6.1.3.1 FDP_ACC.1 Subset access control (Document Group-Based Access Control)

Component Relationships

Hierarchical to: No other components

Dependencies: FDP_ACF.1(1) Security attribute-based access control

FDP_ACC.1.1

TSF must enforce [document group-based access control] regarding [document users' ability to read, encrypt (write), and decrypt protected documents].

1. Subject: Document users who perform encryption/decryption of information through the TOE
2. Object: Protected documents
3. Operations: Read, Encryption (Write), Decryption

Document group-based access control refers to assigning permissions such as read, encryption (write), and decryption to document users on a document group basis and performing document encryption/decryption in accordance with the configured policy.
Reading refers to opening a protected document as a file. Document encryption (Write) refers to encrypting a protected document when saving it after editing. Decryption refers to decrypting an encrypted protected document into plaintext.

6.1.3.2 FDP_ACF.1(1) Security attribute-based access control (Document Group-Based Access Control)

Component Relationships

Hierarchical to: No other components

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

FDP_ACF.1.1

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

Subject

- A document user who performs encryption/decryption of information via the TOE

Subject Security Attribute

- Document User ID
- Document group ID

Object

- Document to be protected

Object Security Attributes

- Document group ID
- Document Name
- Document Type
- Document Path

FDP_ACF.1.2

The TSF shall enforce the following rules to determine whether to permit an operation between a controlled subject and a controlled object: [

- a) The operation shall be permitted only if the subject's security attributes are included in the object's access-permitted security attributes and the operation matches the object's operation security attributes
- b) *None*

]

FDP_ACF.1.3

TSF must explicitly authorize the subject's access to the object based on the following additional rules: [None]

FDP_ACF.1.4

The TSF shall explicitly deny a subject's access to an object based on the following additional rules: [None]

Document group-based access control refers to the process of assigning permissions, such as read, encryption (write), and encryption/decryption, to document users on a document group basis and performing document encryption/decryption in accordance with the configured policy.

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication Failure Handling

Component Relationships

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Authentication

FIA_AFL.1.1

The TSF shall detect when the number of failed authentication attempts related to [the following list of authentication events] reaches *an administrator-configurable positive integer between [1 and 5]*.

- Administrator authentication via the ShadowCube Server GUI
- Document User Authentication via the ShadowCube Client GUI

FIA_AFL.1.2

When the defined number of failed authentication attempts has been *met*, the TSF shall perform the actions listed in [[Table 25] List of Response Actions].

[Table 25]

Authentication Event	Response
Administrator authentication via the ShadowCube Server GUI	• Reactivate the account 5 minutes after it has been locked (no configurable range) • Record an audit log and send an email to an authorized administrator
Document user authentication via the ShadowCube Client GUI	• Authentication enabled after the document user's PC has been rebooted and 5 minutes have passed since the account was locked • Audit logs are recorded and emailed to authorized administrators

The number of authentication failure attempts that an authorized administrator can configure ranges from 1 to 5, with a default value of 3.

6.1.4.2 FIA_IMA.1 TOE (Extended) Internal Mutual Authentication

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FIA_IMA.1.1

TSF must perform mutual authentication using the Cryptographic Algorithms provided by the validated cryptographic module, which comply with the standards listed in [[Table 26] Standards for Cryptographic Algorithms Provided by Validated Cryptographic Modules] and are part of the TOE components listed in [[Table 26] TOE components of Cryptographic Algorithms Provided by Validated Cryptographic Modules].

[Table 26] Cryptographic Algorithms Provided by Validated Cryptographic Modules

TOE component	Cryptographic Algorithm	Identification	Standard
ShadowCube Server	ECDH (Prime-256)	ShadowCube Client Allowed IP Addresses	ISO/IEC 11770-3
ShadowCube Client		Configuration Information (ShadowCube Server IP)	

6.1.4.3 FIA_SOS.1 Verification of secrets

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1

TSF must provide a mechanism to verify that confidential information meets [the following defined acceptance criteria].

- Composed of a combination of four elements: uppercase and lowercase letters, numbers, and special characters (!, @, #, $, %, ^, *, -, _, +, =)
- Passwords shall be between 9 and 16 characters in length.
- Passwords must not be the same as the user account (ID)
- Prohibits the consecutive repetition of the same character or digit
- Prohibited: Sequential entry of consecutive letters or numbers on the keyboard
- Do not reuse a previously used password

6.1.4.4 FIA_UAU.1 Authentication

Component Relationships

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] to be performed on behalf of the user before the user is authenticated .

Administrator Authentication

- Request to enter an email authentication code
- Request for Identification and Authentication (Login Screen)

Document User Authentication

- Certificate Issuance
  - Document User Certificate Request
  - Request to Enter Email Authentication Code
  - Document User Certificate Creation
  - Request for Identification and Authentication Procedures (Login Screen)
- After Certificate Issuance
  - Selecting a Document User Certificate
  - Request for Identification and Authentication Procedures (Login Screen)

FIA_UAU.1.2

The TSF shall successfully authenticate the user before allowing any actions other than those specified in FIA_UAU.1.1 that the TSF mediates on behalf of the user.

6.1.4.5 FIA_UAU.4 Single-use authentication mechanism

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.4.1

The TSF shall prevent the reuse of authentication data associated with [[Table 27] Identified Authentication Mechanism(s)] .

[Table 27]

Authentication Subject	Authentication Mechanism
Administrator Authentication	Email Authentication Code
Issuance of Document User Certificates	Email Authentication Code

An email authentication code is a one-time password (OTP) that cannot be reused after authentication.
Document user authentication is performed using a certificate stored in the document user system and encrypted with the ARIA_CBC (256-bit) Cryptographic Algorithm. Since the password cannot be verified, this ensures session uniqueness in the ShadowCube Client environment.

6.1.4.6 FIA_UAU.7 Protected Authentication Feedback

Component Relationships

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Authentication

FIA_UAU.7.1

During the authentication process, TSF must provide the user with only the [following list of feedback]

ShadowCube Server

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

ShadowCube Client

- Document user certificate
- Hidden password
- Email Authentication Code
- Authentication Failure Feedback (Message)
  - Authentication Failed

※ Precautions for Implementation: In the event of identification or authentication failure, feedback regarding the reason for the failure (e.g., ID error, password error) must not be provided.

6.1.4.7 FIA_UID.1 Timing of identification

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1

Before identifying a user, TSF must authorize the [following list of TSF-mediated actions] to be performed on the user's behalf.

- Administrator Authentication: Request for identification and authentication procedures (login screen)
- Document User Authentication: Request to select a document user certificate

FIA_UID.1.2

The TSF shall successfully identify each user before authorizing any TSF-mediated actions on the user's behalf other than those specified in FIA_UID.1.1.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1 Management of security functions behaviour

Component Relationships

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 perform *management actions* for the functions in [Table 28] Security Functions and Management Capabilities to [authorized administrators]

[Table 28] Security Functions and Management Capabilities

Administrator Category	Classification	Security Function	Capabilities			
			Determine the behaviour	Disable	Enable	Modify the behaviour
Authorized Administrator	Object Settings	Department Management	O	-	-	O
		User Management	O	-	-	O
	Policy Settings	Document Group Policy	O	-	-	O
		Security Object Policy	O	-	-	O

		Default License Policy	-	-	-	O
		Multi-License Policy	-	-	-	O
	Certificate 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	-	-	-
	Settings	Settings	-	-	-	O
		Check Disk Capacity	-	-	-	O
		Testing and Integrity Verification of the ShadowCube Server Itself	-		O	O

※ 'O' indicates that a management capability is provided, while '-' indicates that no management capability is provided.

6.1.5.2 FMT_MSA.1 Management of security attributes

Component Relationships

Hierarchical to: No other components

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

FMT_MSA.1.1

The TSF shall enforce [Document Group-Based Access Control] to restrict the ability to *query, delete, [add]* the security attributes in [[Table 29] Security Attributes and Access Control SFP] to [authorized administrators].

[Table 29] Security Attributes and Access Control SFP

Access Control SFP	Security Attributes	Capability			
		Query	Modify	Delete	Add
Document Group-Based Access Control	Document User ID	O	-	O	O
	Document group ID	O	-	O	O
	Security Target	O	-	O	O

* "O" indicates that a management capability is provided, while "-" indicates that no management capability is provided.

6.1.5.3 FMT_MSA.3 Static attribute initialisation

Component Relationships

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [Document Group-Based Access Control Policy] to provide restrictive default values for security attributes used to enforce the SFP.

FMT_MSA.3.2

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

6.1.5.4 FMT_MTD.1 Management of TSF data

Component Relationships

Hierarchical to: No other components

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

FMT_MTD.1.1

TSF must restrict the ability to *manage* [[Table 30] TSF data and management capabilities] to [[Table 30] Authorized Roles for TSF Data and Management Capabilities].

[Table 30] TSF Data and Management Capabilities

Authorized Roles	TSF Data	Capabilities			
		Query	Modify	Delete	Add
Authorized Administrator	Document User Certificate	O	-	O	-
	Audit Data	O	-	-	-
	IP Address Settings	O	O	O	O
	Session Timeout	O	O	-	-
	Maximum Failed Login Attempts	O	O	-	-
	Minimum Password Length	O	O	-	-
Document User	Document User Certificate	O	O	O	O
	License	O	O	-	-
	Settings	O	-	-	-

※ "O" indicates that a management capability is provided, while "-" indicates that no management capability is provided.
※ The document user certificate deletion management capability for authorized administrators refers to certificate revocation.
※ The document user's certificate deletion management capability refers to the deletion or revocation of issued certificates.
※ "License change" refers to a license update.
※ "Environment Settings" refers to license information.

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

Component Relationships

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 passwords in accordance with [the following password composition rules and length requirements] to [authorized administrators] as follows.

1. [Password Composition Rules and Length Requirements]

- Passwords shall consist of a combination of four types of characters: uppercase and lowercase English letters, numbers, and special characters (!, @, #, $, %, ^, *, -, _, +, =).
- Passwords shall be between 9 and 16 characters in length.

2. [None]

FMT_PWD.1.2

The TSF shall restrict the ability to manage IDs in [None] to [authorized administrators] as follows.

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

FMT_PWD.1.3

The TSF shall provide a function to *set an ID and password during the installation process*.

6.1.5.6 FMT_SMF.1 Specification of management functions

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [list of management functions provided by the TSF].

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

6.1.5.7 FMT_SMR.1 Security roles

Component Relationships

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the [Authorized Administrator, Document User] role.

FMT_SMR.1.2

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

※ Only one type of administrator is provided for managing TOE products. The authorized administrator designated as the web administrator during TOE product installation manages security management functions via the web interface (HTTPS).

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_FLS.1 Failure with preservation of secure state

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_FLS.1.1

The TSF shall maintain a safe state when the following types of failures occur: [List of TSF Failure Types].

- Failure of Noise Source Integrity Test (RCT, APT)
- Failure of integrity verification and failure of the algorithm self-test (KAT)

6.1.6.2 FPT_ITT.1 Basic internal TSF data transfer protection

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1

The TSF shall protect TSF data from *exposure, alteration* when it is transmitted between separate parts of the TOE.

[Table 31]

Category	Encryption Target	Encryption Method	Algorithm	Data Storage Location	Standard List
Transmission between ShadowCube Server and ShadowCube Client	Security Policy Data	Block Cipher	ARIA_CBC	Packet	KS X 1213-1
	Security Policy Data	Public Key Cryptography	RSAES	Packet	ISO/IEC 18033-2

* Key destruction timing: ShadowCube Server destroys keys when IIS is shut down or the system is shut down; ShadowCube Client destroys keys when the system is shut down.

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

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_PST.1.1

The TSF shall protect [[Table 32] Stored TSF data], which is stored in a repository controlled by the TSF, from unauthorized *exposure*.

[Table 32] Stored TSF data

TOE component	DBMS	File System
ShadowCube Server	Administrator Password, Email OTP	N/A
	Document User Certificate	
	License	
	Settings	
	Audit Data	
ShadowCube Client	N/A	Document User Certificate
		Document User Private Key
		TOE configuration file
		Audit Data

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

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_PST.2.1

Unauthorized deletion of [TSF, TSF data] must be *detected*.

ShadowCube Client executable

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

FPT_PST.2.2

[TSF] must *prevent* unauthorized agents from **being terminated**.

ShadowCube Client executable

- scmain.exe

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

6.1.6.5 FPT_TST.1 TSF testing

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TST.1.1

To verify the proper operation of *[TSF Components]*, the TSF must perform the following self-tests [List of TSF-initiated self-tests] *periodically at start-up and during regular operation*.

[Table 33]

TOE component	TSF	Role
ShadowCube Server	ShadowCubeSelfTest.exe	Processes related to operation of the security function
ShadowCube Client	scmain.exe	Processes for user GUI support
	scboots64.exe	Process for running user security management

FPT_TST.1.2

TSF must provide **authorized administrators** with the ability to verify the integrity of *TSF data*.

[Table 34]

TOE component	TSF	Role
ShadowCube Server	config.ini	Configuration file used when initializing the ShadowCube Server in a web service
	db.config	Configuration file used by the web service to connect to the DBMS
	log4net.xml	Configuration file used for logging settings in the web service
	web.config	Web service configuration file

FPT_TST.1.3

TSF must provide **authorized administrators** with the ability to verify the integrity of *TSF*.

[Table 35]

TOE component	TSF	Role
ShadowCube Server	admin.dll	Management of security attributes
	scbase.dll	License-Related Management of

		security attributes
	scpclib.dll	Database-Related Management of security attributes
	scpcws.dll	Management of ShadowCube Client-related security functions
	ssDeulmeori.dll	Process for identity and authentication management
	ssJikimi.dll	Process for using a validated cryptographic module
	ssNeobi.dll	Utility process for management console support
	ssNeonadeuli.dll	Encryption and Decryption Processing
	ssServerHelper.dll	Process for managing cryptographic functions
	MagicCryptoV230.dll	Validated Cryptographic Module
ShadowCube Client	scboot.exe, scboot64.exe, scboots64.exe	Processes Related to the Security Function
	sccm.exe	Certificate Management Console
	scconv.exe	File encryption and decryption management console
	scmain.exe	Management console for user GUI support
	scsysinfo.exe, scsysinfo64.exe	Processes related to the operation of the security function
	scewvsc.dll, scewvsc64.dll, scewvsd.dll, scewvsd64.dll, scewvsp.dll, scewvsp64.dll, scewwss.dll, scewwss64.dll	Processes for access control rules
	scshell.dll, scshell64.dll	Processes for Windows Explorer integration
	scwinui.dll, scwinui64.dll	Processes for identification and authentication support
	ssDeulmeori.dll	Process for identity and authentication management
	ssJikimi.dll	Process for Using a Validated Cryptographic Module
	ssMigratorHelp.dll	Process for Supporting ShadowCube Version Compatibility
	ssNeobi.dll	Utility process for management console support
	ssNeonadeuli.dll	Process for encryption and decryption
	ssServerHelper.dll	Process for managing cryptographic

		functions
	MagicCryptoV230.dll MagicCrypto32V230.dll	Validated Cryptographic Module

6.1.7 TOE Access (FTA)

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

Component Relationships

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 limit the maximum number of concurrent sessions belonging to the same user in accordance with the rule [For authorized administrator management access sessions, the maximum number of concurrent sessions is limited to 1; the maximum number of concurrent sessions for an authorized administrator is limited to 1].

※ The ShadowCube Client supports certificate-based user login and is dependent on the environment in which the certificate was generated; therefore, certificates cannot be issued in other environments, and duplicate login attempts are not possible.

FTA_MCS.2.2

By default, TSF must enforce a session limit of [1] per user.

6.1.7.2 FTA_TSE.1(1) TOE session establishment

Hierarchical to: No other components

Dependencies: No dependencies

FTA_TSE.1.1

The TSF shall be able to reject the **management access session settings of authorized administrators** based on [access IP, none].

Two access IPs are provided by default, and authorized administrators can configure between 2 and 5 access IPs.

6.2 Security Functional Requirements (Conditionally Mandatory SFRs)

The "Conditionally Mandatory SFRs" in this Security Target are as follows.

[Table 36] Conditionally Mandatory SFRs

Function Class	Security Function Component		Additional SFR Terms	Remarks
Security Audit (FAU)	FAU_STG.2	Protection of Audit Data Repository	When the TOE server stores audit records in a local storage	
	FAU_STG.4	Response Actions in the Event of Anticipated Audit Data Loss	When the TOE server stores audit records in local storage	
	FAU_STG.5	Preventing audit data loss	When the TOE server stores audit logs in local storage	
Cryptographic Support (FCS)	FCS_CKM.5	Cryptographic Key Derivation	When the TOE provides a cryptographic key derivation function (e.g., KEK generation using a password-based key derivation standard)	
	FCS_RBG.3	Random Bit Generation (Internal Seeding Single Source)	When generating random bits in FCS_RBG.1, if the TSF uses a single entropy source to provide a seed value to the DRBG	
Identification and Authentication (FIA)	FIA_UAU.5	Multiple authentication mechanisms	When a TOE server supports additional identification and authentication functions on its own, in addition to ID and password-based authentication methods	
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination	When the TOE provides session termination functionality	
	FTA_TSE.1(2)	TOE session establishment	When users on the agent, management console, and ShadowCube Client that make up the TOE must be identified and authenticated	
Protection of the TSF (FPT)	FPT_RCV.2	Automated recovery	When the TOE components include an document encryption/decryption agent	

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_STG.2 Protection of Audit Data Repository

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_STG.2.1

The TSF shall protect the audit data stored in the audit trail from unauthorized deletion.

ShadowCube Client

Nothing other than the product executable file can be deleted.

ShadowCube Server

The DBMS audit log table can be protected from deletion by unauthorized users through the DBMS's identification and authentication functions.

FAU_STG.2.2

TSF must *prevent* unauthorized modifications to audit data stored in the audit trail.

ShadowCube Client

No reading or modification is permitted except for the product executable file.

ShadowCube Server

The audit log table in a DBMS prevents unauthorized users from making changes through the DBMS's identification and authentication functions.

6.2.1.2 FAU_STG.4 Action in case of possible audit data loss

Component Relationships

Hierarchical to: No other components

Dependencies: FAU_STG.2 Protection of Audit Data Repository

FAU_STG.4.1

ShadowCube Server

The TSF shall take [notification to the authorized administrator, [none]] if the audit trail exceeds [10% less than the capacity set by the authorized administrator].

- Default: 70% of the audit data repository (configurable range: 50% to 90% of the audit repository)

The capacity set by the authorized administrator is the audit evidence saturation threshold, and the point at which the audit data store's capacity reaches "-10% of the set audit evidence saturation threshold" is deemed the audit evidence saturation prediction point.
Notifications to authorized administrators are sent via email.

ShadowCube Client

If the audit data repository exceeds 80% capacity, TSF must [notify authorized administrators, [None]] .

- Fixed value: 80%

Notification to authorized administrators shall be delivered via email.

6.2.1.3 FAU_STG.5 Prevention of Audit Data Loss

Component Relationships

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 Protection of Audit Data Repository

FAU_STG.5.1

ShadowCube Server

When the audit data repository is full, TSF *overwrites the oldest audit records* and [records the audit log and sends an email to authorized administrators].

ShadowCube Client

If the audit data repository is full, TSF **automatically reboots the system, stops the ShadowCube service**, and performs [audit log recording and email transmission to authorized administrators].

- Default value: 90%

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.5 Cryptographic Key Derivation

Component Relationships

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution or FCS_COP.1 Cryptographic Operations, FCS_CKM.6 Cryptographic Key Destruction Timing and Events

FCS_CKM.5.1

The TSF shall derive a cryptographic key [Key Type] from [Input Parameters] according to the specified key [Derivation Algorithm] and the specified [Cryptographic Key Length] that comply with the following [Standard List].

[Table 37] ShadowCube Server

Standard List	Cryptographic Algorithms	Key Length	Purpose	Parameters	Key Type
TTA.SKO-12.0334	PBKDF2	256 bits	Derivation of the KEK for the DB Password Encryption Cryptographic Key	Key derivation from the password entered during web administrator login	KEK

[Table 38] ShadowCube Client

Standard List	Cryptographic Algorithms	Key Length	Purpose	Parameters	Key Type
TTA.SKO-12.0334	PBKDF2	256 bits	KEK derivation for TSF data protection	Key derivation from the password entered during user login	KEK
TTA.SKO-12.0334	PBKDF2	256 bits	Deriving the KEK from the certificate's private key cryptographic key	Deriving the key from the password entered during user login	KEK

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

Component Relationships

Hierarchical to: No other components

Dependencies: FCS_RBG.1 Random Bit Generation (RBG)

FCS_RBG.3.1

The TSF shall be capable of seeding the DRBG using a *TSF software-based entropy source* [CryptGenRandom] with a minimum entropy of at least [128] bits.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_UAU.5 Multiple Authentication Mechanisms

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.5.1

To support user authentication, the TSF must provide [password authentication mechanism, [email OTP authentication mechanism]].

FIA_UAU.5.2

The TSF shall authenticate the requested identity of all users in accordance with the [rule that authentication is successful only when both the password mechanism and the email OTP authentication mechanism are successful for administrators and general users].

6.2.4 TOE Access (FTA)

6.2.4.1 FTA_SSL.3 TSF-initiated termination

Component Relationships

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles

FTA_SSL.3.1

The TSF shall terminate an interactive session after [10 minutes].

- Inactivity Period
  - Minimum: 1 minute
  - Maximum: 10 minutes
  - Default: 10 minutes

6.2.4.2 FTA_TSE.1(2) TOE Session Establishment

Component Relationships

Hierarchical to: No other components

Dependencies: No dependencies

FTA_TSE.1.1

The TSF shall be able to reject session setup based on [the user PC's IP address and the user PC's MAC address].

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_RCV.2 Automated recovery

Component Relationships

Hierarchical to: No other components

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.2.1

If automatic recovery from [None] is not possible, the TSF must enter a management mode that provides functionality to return the TOE to a safe state.

FPT_RCV.2.2

The TSF shall use an automated procedure to ensure that the TOE is restored to a secure state in the event of [TOE cryptographic client file tampering].

6.3 Security Functional Requirements (Optional SFRs)

The "Optional SFRs" in this Security Target are as follows.

[Table 39] Optional SFRs

Function Class	Security Function Component	
Cryptographic Support (FCS)	FCS_CKM.2	Cryptographic Key Distribution

6.3.1 Cryptographic Support (FCS)

6.3.1.1 FCS_CKM.2 Cryptographic Key Distribution

Component Relationships

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 User data ingestion without security attributes, or FDP_ITC.2 User data ingestion with security attributes, or FCS_CKM.1(1) Cryptographic key generation (document encryption), FCS_CKM.1(2) Cryptographic key generation (TSF data encryption), FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [ECDH] that meets the following: [Standard List].

[Table 40]

Category	Standard List	Cryptographic Algorithm	Key Length	Distribution Method

Session Key	ISO/IEC 11770-3	ECDH	256 bits	Session key agreement using a key pair generated by the ECC algorithm

6.4 Security Assurance Requirements

The Security Requirements in this Security Target consist of the assurance components defined in Part 3 of the Common Criteria, and the evaluation assurance level is EAL1+. [Table 18] summarizes the security assurance requirements included in this Security Target.

[Table 41] Assurance Requirements

Assurance Class	Assurance Components	
Evaluation of the Security Target	ASE_INT.1	Introduction to ST
	ASE_CCL.1	Conformance Claim
	ASE_OBJ.1	Security Objectives for the Operational Environment
	ASE_ECD.1	Extension Component Terms and Definitions
	ASE_REQ.1	Directly Derived Security Requirements
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance	AGD_OPE.1	User Operation Guidance
	AGD_PRE.1	Preparation Procedures
Life Cycle Support	ALC_CMC.1	TOE Labeling
	ALC_CMS.1	TOE CM Scope
Test	ATE_FUN.1	Functional Test
	ATE_IND.1	Independent Test: Functional Verification
Vulnerability Assessment	AVA_VAN.1	Vulnerability Investigation

6.4.1 Security Target Evaluation

6.4.1.1 ASE_INT.1 ST Introduction

Dependencies: No dependencies

Developer Requirements

ASE_INT.1.1D
The developer must provide an ST Introduction.

Evidence Requirements

ASE_INT.1.1C
The ST introduction must include the ST reference, TOE Reference, TOE overview, and TOE description.

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

ASE_INT.1.3C
The TOE Reference must uniquely identify the TOE.

ASE_INT.1.4C
The TOE overview must summarize the TOE's intended use and key security characteristics.

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

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

ASE_INT.1.7C
In the case of a multi-assurance ST, the TOE overview shall describe the TSF configuration with respect to the sub-TSFs defined in the PP-composition for which the ST makes a Conformance Claim.

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

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

Evaluator Requirements

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

ASE_INT.1.2E

The evaluator must verify that the TOE Reference, TOE overview, and TOE description are consistent with one another.

6.4.1.2 ASE_CCL.1 Conformance Claim

Dependencies: ASE_INT.1 ST Introduction, ASE_ECD.1 Extended Component Definition, ASE_REQ.1 Directly Derived Security Requirements

Developer Requirements

ASE_CCL.1.1D

The developer must provide a Conformance Claim.

ASE_CCL.1.2D

The developer must provide the rationale for the Conformance Claim.

Evidence Requirements

ASE_CCL.1.1C

The Conformance Claim must identify the CC publication information with which the ST and TOE comply.

ASE_CCL.1.2C

The Conformance Claim shall describe the ST's Conformance Claim for Part 2 of the CC as either "Part 2 Conformity" or "Part 2 Extension."

ASE_CCL.1.3C

A Conformance Claim must describe ST's conformance with Part 3 of the CC as either "Part 3 conformance" or "Part 3 extension."

ASE_CCL.1.4C

The Conformance Claim must be consistent with the extension component definition.

ASE_CCL.1.5C

The Conformance Claim must identify the PP-composite for which the ST makes the Conformance Claim, or all PPs and Security Requirements packages.

ASE_CCL.1.6C

The Conformance Claim must describe the ST's compliance with the packages as "package-compliant" or "package-additional."

ASE_CCL.1.7C

The conformance claim must describe ST's conformity with PPs as "PP-conformity."

ASE_CCL.1.8C

The rationale for a Conformance Claim must demonstrate that the TOE type of the ST is consistent with the TOE type of the PP-composite or PP for which the ST makes a Conformance Claim.

ASE_CCL.1.9C

The rationale for the Conformance Claim must demonstrate that the description of the security objectives in the Security Target is consistent with the description of the security objectives in the protection profile to which the Security Target declares conformance.

ASE_CCL.1.10C

The rationale for a Conformance Claim must demonstrate that the description of the security objectives of an ST is consistent with the descriptions of the security objectives of the PP-composite, PP, and functional packages for which the ST makes a Conformance Claim.

ASE_CCL.1.11C

The rationale for a Conformance Claim must demonstrate that the description of the ST's Security Requirements is consistent with the descriptions of the Security Requirements for the PP-composite, PP, and functional packages for which the ST makes a Conformance Claim.

ASE_CCL.1.12C

A Conformance Claim for a PP(s) or PP-composite must be either exact compliance, strict conformance, or demonstrable compliance, or a list of compliance types.

ASE_CCL.1.13C

If a conformance claim identifies a set of evaluation methods and evaluation activities derived from the CEM work units to be used in the TOE evaluation, this set must include all those contained in the PP modules of the package, PP, or PP-composite for which the ST declares conformance; nothing else is permitted.

Evaluator Requirements

ASE_CCL1.1E

The evaluator shall verify that the information provided satisfies all evidence requirements.

6.4.1.3 ASE_OBJ.1 Security Objectives for the Operational Environment

Dependencies: ASE_SPD.1 Security Problem Definition

Developer Requirements

ASE_OBJ.1.1D

The developer must provide a description of the security objectives for the operational environment.

ASE_OBJ.1.2D

The developer must provide the rationale for the security objectives of the operational environment.

Evidence Requirements

ASE_OBJ.1.1C

The description of security objectives must outline the security objectives for the operational environment.

ASE_OBJ.1.2C

The rationale for security objectives must trace each security objective for the operational environment to the threats addressed by that security objective, the OSPs performed to achieve that security objective, and the assumptions supported by that security objective.

ASE_OBJ.1.3C

The rationale for security objectives must demonstrate that the security objectives for the operational environment support all assumptions.

Evaluator Requirements

ASE_OBJ.1.1E

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

6.4.1.4 ASE_ECD.1 Extended Component Definition

Dependencies: No dependencies

Developer Requirements

ASE_ECD.1.1D

The developer must provide a description of the Security Requirements.

ASE_ECD.1.2D

The developer must provide an extension component definition.

Evidence Requirements

ASE_ECD.1.1C

The description of Security Requirements must identify all extended Security Requirements.

ASE_ECD.1.2C

The extended component definition must define an extended component for each extended Security Requirements.

ASE_ECD.1.3C

The definition of an extension component must describe how each extension component relates to existing CC components, families, and classes.

ASE_ECD.1.4C

Extension component definitions must be expressed using existing CC components, families, and classes, as well as the methodology, as models.

ASE_ECD.1.5C

Extension components must consist of measurable and objective elements so that compliance for each element can be demonstrated.

Assessor Requirements

ASE_ECD.1.1E

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

ASE_ECD.1.2E

The evaluator must verify that the extended component cannot be clearly expressed using existing components.

6.4.1.5 ASE_REQ.1 Direct Evidence Security Requirements

Dependencies: ASE_ECD.1 Extended Component Definition, ASE_SPD.1 Security Issue Definition, ASE_OBJ.1 Security Objectives for the Operational Environment

Developer Requirements

ASE_REQ.1.1D

The developer must provide a description of the Security Requirements.

ASE_REQ.1.2D

The developer must provide the rationale for the Security Requirements.

Evidence Requirements

ASE_REQ.1.1C

The description of Security Requirements must include the SFR and SAR.

ASE_REQ.1.2C

For a single-assurance ST, the Security Requirements description must define a set of global SARs that apply to the entire TOE.

The set of SARs must be consistent with the PP or PP composite on which the ST makes a Conformance Claim.

ASE_REQ.1.3C

For a multi-assurance ST, the Security Requirements description must define a set of global SARs applicable to the entire TOE and a set of SARs applicable to the sub-TSF. The SAR set must be consistent with the multi-assurance PP composition for which the ST makes a Conformance Claim.

ASE_REQ.1.4C

All subjects, objects, operations, security attributes, external entities, and other terms used in the SFR and SAR must be defined.

ASE_REQ.1.5C

The description of Security Requirements must identify all operations related to those Security Requirements.

ASE_REQ.1.6C

All operations must be performed accurately.

ASE_REQ.1.7C

Each Dependencies of a Security Requirements must be satisfied; if not, a justification must be provided in the rationale for the Security Requirements.

ASE_REQ.1.8C

The rationale for Security Requirements must be traceable from each SFR to the threats addressed by the SFR and the OSPs performed by the SFR. The rationale for Security Requirements must demonstrate that the SFR addresses all threats to the TOE (along with the security objectives for the operational environment).

ASE_REQ.1.9C

The rationale for Security Requirements must demonstrate that the SFR performs all OSPs for the TOE (along with the security objectives for the operational environment).

ASE_REQ.1.10C

The rationale for the Security Requirements must explain why the SAR was selected.

ASE_REQ.1.11C

The justification for the Security Requirements must be internally consistent.

ASE_REQ.1.12C

If an ST defines a set of SARs that extends the set of SARs in the PP or PP-composite for which it makes a Conformance Claim, the rationale for the Security Requirements must include the rationale for the assurance requirements that justifies the consistency of the extension and provides the rationale for the treatment of the assessment methods and assessment activities identified in the compliance methods affected by the extension of the SAR set.

Assessor Requirements

ASE_REQ.1.1.E

The assessor shall verify that the information provided satisfies all evidence requirements.

6.4.1.6 ASE_TSS.1 TOE Summary Specification

Dependencies: ASE_INT.1 ST Introduction, ASE_REQ.1 Directly Derived Security Requirements, ADV_FSP.1 Basic Functional Specification

Developer Requirements

ASE_TSS.1.1D

The developer shall provide a TOE summary specification.

Evidence Requirements

ASE_TSS.1.1C

The TOE summary specification must describe how the TOE satisfies each SFR.

Assessor Requirements

ASE_TSS.1.1E

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

ASE_TSS.1.2E

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

6.4.2 Development

6.4.2.1 ADV_FSP.1 Basic Functional Specification

Dependencies: No dependencies

Developer Requirements

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

ADV_FSP.1.2D
The developer must provide traceability from the functional specifications to the SFR.

Evidence Requirements

ADV_FSP.1.1C
The functional specification must describe the purpose and usage of each SFR-executing and SFR-supporting TSF.

ADV_FSP.1.2C
The functional specification must identify all parameters associated with each SFR-executing and SFR-supporting TSF.

ADV_FSP.1.3C
The functional specification shall provide the rationale for classifying the interface as SFR-non-interfering.

ADV_FSP.1.4C
Traceability must demonstrate that the SFR is traceable to the TSF within the functional specification.

Evaluator Requirements

ADV_FSP.1.1E
The evaluator shall verify that the information provided satisfies all evidence requirements.

ADV_FSP.1.2E
The evaluator must determine whether the functional specification accurately and completely embodies the SFR.

6.4.3 Guidance Documents

6.4.3.1 AGD_OPE.1 User Operations Guidance

Dependencies: ADV_FSP.1 Basic Functional Specification

Developer Requirements

AGD_OPE.1.1D
The developer must provide a user operation manual.

Evidence Requirements

AGD_OPE.1.1C

The user operating manual must describe, for each user role, the functions and privileges accessible to users that must be controlled within a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

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

AGD_OPE.1.3C

The user operating manual shall describe the available functions and interfaces for each user role. In particular, it shall appropriately indicate secure values for all security parameters under the user's control.

AGD_OPE.1.4C

The User Operation Guide must clearly specify, for each user role, the types of security-related events associated with the security functions the user is authorized to perform. This must also include changes to the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The User Operation Guide shall identify all possible operating modes of the TOE (including operation following a failure or an operational error), their implications, and the relevant considerations for maintaining safe operation.

AGD_OPE.1.6C

The User Operation Guide shall describe, for each user role, the security controls that must be followed to satisfy the security objectives for the operational environment, as specified in the ST.

AGD_OPE.1.7C

The User Operation Guide shall be clear and valid.

Evaluator Requirements

AGD_OPE.1.1E

The assessor must verify that the information provided satisfies all evidence requirements.

6.4.3.2 AGD_PRE.1 Preparation Procedures

Dependencies: No dependencies

Developer Requirements

AGD_PRE.1.1D

The developer must provide the TOE, including the preparation procedures.

Evidence Requirements

AGD_PRE.1.1C

The preparation procedure must describe all steps necessary for the secure acceptance of the deployed TOE in a manner consistent with the developer's deployment procedure.

AGD_PRE.1.2C

The preparation procedure must describe all steps necessary for the secure installation of the TOE and the secure preparation of the operational environment, consistent with the security objectives for the operational environment as described in the ST.

Evaluator Requirements

AGD_PRE.1.1E

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

AGD_PRE.1.2E

The evaluator shall apply the preparation procedures to verify that the TOE can be safely prepared for operation.

6.4.4 Life-cycle Support

6.4.4.1 ALC_CMC.1 TOE Labeling

Dependencies: ALC_CMS.1 TOE CM Scope

Developer Requirements

ALC_CMC.1.1D

The developer must provide the TOE and references to it.

Evidence Requirements

ALC_CMC.1.1C

The TOE must be labeled for unique identification.

Evaluator Requirements

ALC_CMC.1.1E

The assessor shall verify that the information provided satisfies all evidence requirements.

6.4.4.2 ALC_CMS.1 Scope of TOE Configuration Management

Dependencies: No dependencies

Developer Requirements

ALC_CMS.1.1D

The developer must provide a configuration list for the TOE.

Evidence Requirements

ALC_CMS.1.1C

The configuration list must include the evaluation evidence required by the TOE and SFR.

ALC_CMS.1.2C

The configuration list must uniquely identify each configuration item.

Evaluator Requirements

ALC_CMS.1.1E

The evaluator must verify that the information provided meets all evidence requirements.

6.4.5 Tests

6.4.5.1 ATE_FUN.1 Functional Testing

Dependencies: Evidence for ATE_COV.1 Test Scope

Developer Requirements

ATE_FUN.1.1D

The developer shall test the TSF and document the results.

ATE_FUN.1.2D

The developer must provide test documentation.

Evidence Requirements

ATE_FUN.1.1C

The test documentation must consist of the test plan, expected test results, and actual test results.

ATE_FUN.1.2C

The test plan must identify the test items to be performed and describe the scenarios for each test. These scenarios must include any Dependencies on other test results.

ATE_FUN.1.3C

Expected test results shall present the outcomes anticipated from the successful execution of the tests.

ATE_FUN.1.4C

Actual test results must be consistent with the expected test results.

Evaluator Requirements

ATE_FUN.1.1E

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

6.4.5.2 ATE_IND.1 Independent Testing: Functional Verification

Dependencies: ADV_FSP.1 Basic Functional Specification, AGD_OPE.1 User Operating Instructions, AGD_PRE.1 Preparation Procedures

Developer Requirements

ATE_IND.1.1D

The developer shall provide the TOE to be tested

Evidence Requirements

ATE_IND.1.1C

The TOE must be suitable for testing.

Evaluator Requirements

ATE_IND.1.1E

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

ATE_IND.1.2E

The evaluator must test a portion of the TSF to verify that it operates as specified.

6.4.6 Vulnerability Assessment

6.4.6.1 AVA_VAN.1 Vulnerability Investigation

Dependencies: ADV_FSP.1 Basic Functional Specification, AGD_OPE.1 Operational user guidance, AGD_PRE.1 Preparation Procedures

Developer Requirements

AVA_VAN.1.1.D

The developer shall provide the TOE to be tested.

Evidence Requirements

AVA_VAN.1.1C

The TOE must be suitable for testing.

Evaluator Requirements

AVA_VAN.1.1E

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

AVA_VAN.1.2E

The evaluator must conduct an investigation of the public domain to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

To determine whether the TOE is resistant to attacks carried out by an attacker with a baseline probability of success, the evaluator must conduct a penetration test based on the identified potential vulnerabilities.

6.5 Rationale for Security Requirements

6.5.1 Rationale for Security Functional Requirements

The rationale for Security Requirements demonstrates the following:

- Each threat and the organization's security policy is addressed by at least one Security Requirements for a security function.
- Each Security Requirements is traceable to at least one threat or the organization's security policy.

[Table 42] Security Problem Definition and Corresponding Security Requirements for Security Functions

Security Functional Requirements	T. Session Hijacking	T. Repeated Authentication Attempts	T. Impersonation	T. Replay	T. Weak Password	T. Unauthorized Information Leakage	T. Stored Data Leakage	T. Transmission Data Compromise	T. Weak Cryptographic Protocol	T. TSF Compromise	P. Audit	P. Secure Operation	P. Cryptographic Strength
FAU_ARP.1										O			
FAU_GEN.1											O		
FAU_SAA.1										O			
FAU_SAR.1											O		
FAU_SAR.3											O		
FAU_STG.1											O		
FAU_STG.2											O		
FAU_STG.4											O		
FAU_STG.5											O		
FCS_CKM.1(1)						O							O
FCS_CKM.1(2)							O	O	O				O
FCS_CKM.2						O	O	O	O				O
FCS_CKM.5						O	O	O	O				O
FCS_CKM.6						O	O	O	O				O
FCS_COP.1(1)						O							O
FCS_COP.1(2)							O	O	O				O
FCS_RBG.1						O	O	O	O				O
FCS_RBG.3						O	O	O	O				O
FDP_ACC.1(1)						O							
FDP_ACF.1(1)						O							
FIA_AFL.1		O	O							O			
FIA_IMA.1			O										
FIA_SOS.1					O								
FIA_UAU.1			O							O			
FIA_UAU.4			O	O						O			

FIA_UAU.5			O							O			
FIA_UAU.7			O		O					O			
FIA_UID.1			O							O			
FMT_MOF.1										O		O	
FMT_MSA.1										O		O	
FMT_MSA.3										O		O	
FMT_MTD.1										O		O	
FMT_PWD.1					O					O		O	
FMT_SMF.1										O		O	
FMT_SMR.1										O		O	
FPT_FLS.1						O	O	O	O				O
FPT_ITT.1								O					
FPT_PST.1							O						
FPT_PST.2										O			
FPT_RCV.2										O			
FPT_TST.1						O	O	O	O	O			O
FTA_MCS.2	O												
FTA_SSL.3	O												
FTA_TSE.1(1)	O												
FTA_TSE.1(2)	O												

T. Session Hijacking (FTA_MCS.2, FTA_SSL.3, FTA_TSE.1(1), FTA_TSE.1(2)**)**

FTA_MCS.2 prevents duplicate access to the TOE using the same user account or the same privileges, thereby addressing T. Session Hijacking.

FTA_SSL.3 ensures that interactive sessions are terminated after a period of inactivity by an authorized user, thereby countering T. Session Hijacking.

FTA_TSE.1(1) and FTA_TSE.1(2) counter T. Session Hijacking by ensuring that the establishment of an authorized user's access session is determined based on factors such as IP address.

T. Repeated Authentication Attempts (FIA_AFL.1)

FIA_AFL.1 defines the number of failed authentication attempts allowed for an authorized user and ensures the ability to take appropriate action when that limit is reached, thereby addressing T. Repeated Authentication Attempts.

T. Impersonation (FIA_AFL.1, FIA_IMA.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.7, FIA_UID.1)

FIA_AFL.1 defines the number of failed authentication attempts by an authorized user and ensures the ability to take appropriate action when that defined number is reached; therefore, it corresponds to T. Impersonation.

FIA_IMA.1 addresses T. Impersonation by ensuring that internal mutual authentication is performed between TOE components.

FIA_UAU.1, FIA_UAU.4, and FIA_UAU.5 address T. Impersonation by ensuring that users attempting to

access the TOE are successfully authenticated.

FIA_UAU.7 addresses T. Impersonation by ensuring that only masked values are displayed or not displayed to the user during authentication, and that no feedback regarding the reason for failure is provided in the event of authentication failure.

FIA_UID.1 addresses T. Impersonation by ensuring that users attempting TOE Access are successfully identified.

T. Replay (FIA_UAU.4)

FIA_UAU.4 ensures the ability to prevent the reuse of authentication data, thereby addressing T. Replay.

T. Weak Password (FIA_SOS.1, FIA_UAU.7, FMT_PWD.1)

FIA_SOS.1 verifies compliance with password complexity rules, thereby addressing T. Weak Password.

FIA_UAU.7 ensures that only masked values are displayed or not displayed to the user during the authentication process, thereby addressing T. Weak Password.

FMT_PWD.1 addresses T. Weak Password by ensuring that the default password provided by the system is forced to be changed upon the first login by an authorized administrator.

T. Unauthorized Information Leakage (FCS_CKM.1(1), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(1), FCS_RBG.1, FCS_RBG.3, FDP_ACC.1(1), FDP_ACF.1(1), FPT_FLS.1, FPT_TST.1)

FCS_CKM.1(1), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, and FPT_TST.1 ensure that cryptographic keys are generated and distributed in accordance with secure Cryptographic Algorithms and key lengths during document encryption and decryption, thereby addressing T. Unauthorized Information Leakage.

FCS_CKM.6 ensures that cryptographic keys and related information are destroyed in accordance with the key destruction method after document encryption and decryption are complete, thereby addressing T. Unauthorized Information Leakage.

FCS_COP.1(1) ensures that cryptographic operations are performed in accordance with the specified secure Cryptographic Algorithms and cryptographic keys during document encryption and decryption, thereby addressing T. Unauthorized Information Leakage.

FDP_ACC.1(1) and FDP_ACF.1(1) address T. Unauthorized Information Leakage by ensuring document encryption and decryption to control user access to protected documents.

T. Stored Data Leakage (FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, FPT_PST.1, FPT_TST.1)

FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, and FPT_TST.1 ensure that cryptographic keys are generated and distributed according to secure Cryptographic Algorithms and key lengths when encrypting stored data, thereby addressing T. Stored Data Leakage.

FCS_CKM.6 ensures that cryptographic keys and related information are destroyed in accordance with the specified key destruction method upon termination of stored data encryption, thereby addressing T. Stored Data Leakage.

FCS_COP.1(2) ensures that cryptographic operations are performed in accordance with the specified secure Cryptographic Algorithms and cryptographic keys during the encryption of stored data, thereby addressing T. Stored Data Leakage.

FPT_PST.1 ensures that TSF data stored through methods such as encryption and access control is

protected from the threat of leakage, thereby addressing T. Stored Data Leakage.

T. Transmission Data Compromise (FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, FPT_ITT.1, FPT_TST.1)

FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, and FPT_TST.1 ensure that cryptographic keys are generated and distributed in accordance with secure Cryptographic Algorithms and key lengths during encrypted communication; therefore, they address T. Transmission Data Compromise.

FCS_CKM.6 ensures that cryptographic keys and related information are destroyed in accordance with the specified key destruction method upon termination of encrypted communication, thereby addressing T. Transmission Data Compromise.

FCS_COP.1(2) ensures that cryptographic operations are performed in accordance with the specified secure Cryptographic Algorithms and cryptographic keys during encrypted communication, thereby addressing T. Transmission Data Compromise.

FPT_ITT.1 ensures the confidentiality and integrity of data transmitted between TOE components, thereby addressing T. Transmission Data Compromise.

T. Weak Cryptographic Protocol (FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, FPT_TST.1)

FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, FPT_TST.1 complies with T. Weak Cryptographic Protocol because it ensures that cryptographic keys are generated and distributed in accordance with the Cryptographic Algorithms and key lengths required by standard Cryptographic Algorithms with a security strength of 112 bits or more when encrypting transmitted data.

FCS_CKM.6 ensures that cryptographic keys and related information are destroyed in accordance with the specified destruction method, thereby addressing T. Weak Cryptographic Protocol.

FCS_COP.1(2) ensures that, when encrypting transmitted data, cryptographic operations are performed in accordance with standard Cryptographic Algorithms having a security strength of at least 112 bits and the specified cryptographic key length; therefore, it addresses T. Weak Cryptographic Protocol.

T. TSF Compromise (FAU_ARP.1, FAU_SAA.1, FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1, FPT_PST.2, FPT_TST.1, FPT_RCV.2)

FAU_ARP.1 ensures the ability to take corrective action when security violations, such as TOE integrity compromise, are detected, thereby addressing T. TSF Compromise.

FAU_SAA.1 ensures the ability to examine audited events and identify security violations, such as TOE integrity compromise, and thus addresses T. TSF Compromise.

FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.7, and FIA_UID.1 ensure that access to the TOE is permitted only after successful user identification and authentication, thereby preventing unauthorized access by threat actors; thus, they address T. TSF Compromise.

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, and FMT_SMR.1 distinguish between authorized user roles, administrators and general users, when accessing and configuring management functions. By providing security policies and security functions based on these roles, they ensure that unauthorized access by threat actors is blocked, thereby addressing T. TSF Compromise.

FPT_TST.1 ensures that the TSF performs self-tests to guarantee the accurate operation of the TOE and provides a function for authorized administrators to verify the integrity of TSF data and the TSF itself,

thereby addressing T. TSF Compromise.

FPT_RCV.2 ensures that the TOE agent can recover tampered information, thereby addressing T. TSF Compromise.

P. Audit (FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.2, FAU_STG.4, FAU_STG.5)

FAU_GEN.1 satisfies P. Audit by ensuring that audit records are generated for auditable events, such as the start and stop of audit functions, as well as the success or failure of administrator identification and authentication.

FAU_SAR.1 satisfies P. Audit because it provides authorized administrators with the ability to view audit records and ensures that audit records are presented in a format suitable for interpretation by administrators.

FAU_SAR.3 satisfies P. Audit by providing a selective audit review function for audit data based on logical relationship criteria.

FAU_STG.1 satisfies P. Audit because, in the case of a TOE server, it stores audit data in local storage.

FAU_STG.2 satisfies P. Audit by providing protection against unauthorized modification or deletion of stored audit data.

FAU_STG.4 satisfies P. Audit by ensuring that appropriate corrective actions are taken if the audit evidence on the TOE server exceeds the storage capacity limit.

FAU_STG.5 satisfies P. Audit by ensuring the ability to take appropriate countermeasures when the TOE server's audit trail becomes saturated.

P. Secure Operation (FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1)

FMT_MOF.1 satisfies P. Secure Operation because it ensures that only authorized users can manage security functions.

FMT_MSA.1 satisfies P. Secure Operation because it ensures that only authorized administrators have the ability to manage security attributes.

FMT_MSA.3 satisfies P. Secure Operation because it ensures that the default values of security attributes are appropriately permitted or restricted, and guarantees that only authorized administrators can specify initial values to override the default values.

FMT_MTD.1 ensures that only authorized users have the ability to manage TSF data, thereby satisfying P. Secure Operation.

FMT_PWD.1 satisfies P. Secure Operation because it ensures that only authorized administrators have the ability to manage rules and lengths for ID and password combinations, and provides functions such as password changes upon an authorized user's first login.

FMT_SMF.1 requires the specification of management functions, such as the security functions and security attributes that the TSF must perform, as well as TSF data, and therefore satisfies P. Secure Operation.

FMT_SMR.1 ensures that authorized roles related to security management are specified, thereby satisfying P. Secure Operation.

P. Cryptographic Strength (FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(1),

FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, FPT_TST.1)

FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FPT_FLS.1, FPT_TST.1) ensure that the cryptographic keys required for standard Cryptographic Algorithms with a security strength of 112 bits or more are securely generated and distributed during data encryption, thereby satisfying the P. Cryptographic Strength requirement

FCS_COP.1(1) and FCS_COP.1(2) satisfy the P. Cryptographic Strength requirement by ensuring that cryptographic operations are performed in accordance with standard Cryptographic Algorithms having a security strength of 112 bits or more and the appropriate cryptographic keys during data encryption.

6.5.2 Rationale for Security Assurance Requirements

The evaluation assurance level for this Security Target has been set to EAL1+ (ATE_FUN.1).

EAL1 can be applied in cases where a certain level of confidence in correct operation is required, but security threats are not severe. If the system was developed in accordance with the development methodologies typically used by the developer, EAL1 does not require additional effort from the developer to prepare evaluation submissions. In other words, it does not require a greater investment of cost or time to prepare for evaluation.

EAL1 provides a basic level of assurance by analyzing the Security Requirements included in a limited security objective statement using functional and interface specifications and documentation to understand security behavior.

This analysis is supported by independent testing of the TSF and the identification of potential vulnerabilities in the public domain (functional testing and penetration testing).

EAL1 does not require evidence of tests performed by the developer based on functional specifications; however,
ATE_FUN.1 has been added to enable developers to independently test whether the TSF has been implemented correctly and whether any defects exist, and to document the results.

6.5.3 Security Functional Requirements Dependencies

The following table shows the dependencies among Security Requirements.

[Table 43] Dependencies: Rationale

Number	Functional Component	Dependencies	Reference Number	SFR Type
1	FAU_ARP.1	FAU_SAA.1	3	Required
2	FAU_GEN.1	FPT_STM.1	Rationale (1)	Required
3	FAU_SAA.1	FAU_GEN.1	2	Required
4	FAU_SAR.1	FAU_GEN.1	2	Required
5	FAU_SAR.3	FAU_SAR.1	4	Required
6	FAU_STG.1	FAU_GEN.1	2	Required
		FTP_ITC.1	Rationale (2)	
7	FAU_STG.2	FAU_GEN.1	2	Conditional Requirement

8	FAU_STG.4	FAU_STG.2	7	Conditionally Required
9	FAU_STG.5	FCS_STG.2	7	Conditionally Required
10	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1]	12, 13, 15	Required
		[FCS_RBG.1 or FCS_RNG.1]	17	
		FCS_CKM.6	14	
11	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1]	12, 13, 16	Required
		[FCS_RBG.1 or FCS_RNG.1]	17	
		FCS_CKM.6	14	
12	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	10, 11, 13	option
13	FCS_CKM.5	[FCS_CKM.2 or FCS_COP.1]	12, 15, 16	Conditionally Required
		FCS_CKM.6	14	
14	FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	10, 11, 13	Required
15	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	10, 13	Required
		FCS_CKM.6	14	
16	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	11, 13	Required
		FCS_CKM.6	14	
17	FCS_RBG.1	FPT_FLS.1	36	Required
		FPT_TST.1	41	
		FCS_RBG.3	18	
18	FCS_RBG.3	FCS_RBG.1	17	Conditionally Required
19	FDP_ACC.1(1)	FDP_ACF.1	20	Required
20	FDP_ACF.1(1)	FDP_ACC.1	19	Required
		FMT_MSA.3	31	
21	FIA_AFL.1	FIA_UAU.1	24	Required
22	FIA_IMA.1	-	-	Required
23	FIA_SOS.1	-	-	Required
24	FIA_UAU.1	FIA_UID.1	28	Required
25	FIA_UAU.4	-	-	Required
26	FIA_UAU.5	-	-	Conditionally Required
27	FIA_UAU.7	FIA_UAU.1	24	Required
28	FIA_UID.1	-	-	Required

29	FMT_MOF.1	FMT_SMF.1	34	Required
		FMT_SMR.1	35	
30	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	19	Required
		FMT_SMF.1	34	
		FMT_SMR.1	35	
31	FMT_MSA.3	FMT_MSA.1	30	Required
		FMT_SMR.1	35	
32	FMT_MTD.1	FMT_SMF.1	34	Required
		FMT_SMR.1	35	
33	FMT_PWD.1	FMT_SMF.1	34	Required
		FMT_SMR.1	35	
34	FMT_SMF.1	-	-	Required
35	FMT_SMR.1	FIA_UID.1	28	Required
36	FPT_FLS.1	-	-	Required
37	FPT_ITT.1	-	-	Required
38	FPT_PST.1	-	-	Required
39	FPT_PST.2	-	-	Required
40	FPT_RCV.2	AGD_OPE.1	-	Conditionally Required
41	FPT_TST.1	-	-	Required
42	FTA_MCS.2	FIA_UID.1	28	Required
43	FTA_SSL.3	FMT_SMR.1	35	Conditionally Required
44	FTA_TSE.1(1)	-	-	Required
45	FTA_TSE.1(2)	-	-	Conditionally Required

※ Rationale (1): Although FAU_GEN.1 is dependent on FPT_STM.1, it satisfies this Dependencies because it uses the trusted timestamps provided by the security objective "OE.Timestamp" for the operational environment described in this Security Target.
※ Rationale (2): FAU_STG.1 is a function that stores audit data in the local DBMS within the TOE, and the storage process takes place within the TSF. Accordingly, the Dependencies with FTP_ITC.1, a security functional requirement for the transmission channel, is not required.

6.5.4 Security Assurance Requirements Dependencies

Since the dependencies among the assurance packages provided by the Common Evaluation Criteria for Information Security Systems are already satisfied, the rationale for this is omitted.

The added assurance requirement, ATE_FUN.1, includes ATE_COV.1 as a Dependencies. ATE_FUN.1 was added to verify that developers accurately performed tests for each test item and recorded the results in the test report; however, since ATE_COV.1 which demonstrates the consistency between test items and the TSF was deemed not strictly necessary, it was not included in this Security Target.

This Security Target conforms with the EAL1 assurance package; however, ASE_OBJ.1 includes ASE_SPD.1, which is absent from the EAL1 assurance package due to a Dependencies. However, this Security Target includes a security problem definition, and ASE_OBJ.1 provides indirect assurance regarding the security problem definition for example, by requiring an investigation into whether the security objectives for the TOE operational environment are traceable to the security problem definition. Therefore, it was determined that ASE_SPD.1, which relates to the description requirements, is not strictly necessary for the security problem definition, and it was not included in this Security Target.

ASE_REQ.1 also includes ASE_SPD.1, which is absent from the EAL1 assurance package due to a Dependencies. However, this Security Target includes the security problem definition, and ADE_REQ.1 provides indirect assurance regarding the security problem definition for example, by requiring an investigation into whether the SFR is traceable to the security problem definition. Therefore, it was determined that ASE_SPD.1, which relates to the descriptive requirements for the security problem definition, is not strictly necessary and has not been included in this Security Target.

7. TOE Summary Specification

This chapter specifies the security function of the TOE that satisfies the Security Requirements.

7.1 Security Audit

The TOE sends an alarm email to the administrator upon detection of a potential security violation, generates audit data, allows authorized administrators to review the generated audit data, and provides functions to protect the audit data.

Security Alerts

When an event deemed a potential security violation occurs, the TOE generates audit data for the event and sends an alarm email to an authorized administrator.

- Authentication Failure Events
- Control rule violation events
- Self-test failure and integrity violation events
- Self-test failure of a validated cryptographic module
- Event where the audit repository has reached its specified threshold
- Audit repository saturation event

Audit Data Generation and Review

When an auditable event listed in the following table occurs, the TOE generates an audit record (event date and time, event type, subject identity, and event result) and records the event date and time in the audit log by synchronizing with trusted time information. Audit logs are stored in an audit evidence repository managed by the DBMS, protecting audit data from unauthorized deletion or modification. The system provides authorized administrators with the ability to view administrator audits, user audits, system audits, document logs, decryption logs, integrity verification history, and login history via a GUI, presenting audit records in a format suitable for interpretation by authorized administrators. Audit records can be reviewed by applying criteria with logical relationships such as AND or OR, based on selectable audit data types including type, operation date and time, department name, user name, and message and each audit record can be sorted in ascending or descending order.

TOE Section Components	Functional Components	auditable event	Additional audit record details
ShadowCube Server	FAU_ARP.1	Response Actions Taken Due to a Potential Security Violation	
	FAU_SAA.1	Initiation and suspension of analysis mechanisms, and automated responses via tools	
	FAU_STG.4	Response Actions When Threshold Exceedance Is Predicted	
	FAU_STG.5	Response Actions When Thresholds Are Exceeded	
	FCS_CKM.1(2)	* Success and failure of cryptographic key generation * Success and failure of encryption operations	

		* Success and failure of cryptographic key distribution	
	FCS_CKM.2	Successes and Failures in Key Distribution for Document Encryption and Decryption	
	FCS_CKM.6	Successes and Failures in Cryptographic Key Destruction	
	FCS_COP.1	Success and Failure of Cryptographic Operations, Types of Cryptographic Operations	
	FIA_AFL.1	Reaching the Threshold for Failed Authentication Attempts and Corresponding Actions Taken	
	FIA_IMA.1 (Extended)	Success/Failure of Mutual Authentication	
	FIA_UAU.1	All Results of Administrator Authentication	
	FIA_UAU.4	Attempts to Reuse Email Authentication Codes	
	FIA_UID.1	Any use of user identification mechanisms, including the provided user identity	
	FMT_MOF.1	* Add/modify/delete departments * Add/modify/delete users * Add/modify/delete document groups * Changing default license policy property values * View Certificate Issuance Status and Revoke Certificates * Configure ShadowCube Server self-testing and integrity verification * Configure connection IP, client connection IP, session timeout, maximum number of failed login attempts, and minimum password length in the environment settings	
	FMT_MSA.1	* Add, modify, or delete document groups * Add/Remove Departments and Users from Document Groups * Add/Remove Security Targets to Document Groups * Set read, write, and decryption permissions for document groups	Changed security attribute values
	FMT_MSA.3	Changes to the default settings for permission or restriction rules, or changes to the default values of security attributes	Changed security attribute values
	FMT_MTD.1	* Authorized Administrator - Document user certificates, audit data, IP	Changed TSF data values

		address settings, session timeout settings, maximum number of failed login attempts, and minimum password length * Document User - Issuing document user certificates, updating licenses	
	FMT_PWD.1 (Extended)	Changes to password combination rules	
	FMT_SMF.1	* Events related to the management function for security functions listed in [Table 12] - Changes to object settings, policy settings, authentication management, and environment settings * Events involving the execution of management functions for items related to TSF data in [Table 14] - Configuration by authorized administrators of document user certificates, audit data, access IP settings, session timeouts, login failure limits, and minimum password length requirements - Issuance of document user certificates ( ) and license updates by document users * Events involving the execution of management functions for the security attributes in [Table 13] - Changes to document user IDs, document group IDs, and security attributes by authorized administrators	
	FPT_TST.1	* Results of the TSF self-test and integrity verification * Results of failed self-tests and integrity verification for validated cryptographic modules	Executable file with integrity violation
	FTA_MCS.2	Termination of an existing connection based on the limit on the number of concurrent sessions	
	FTA_SSL.3	Administrative session terminated due to exceeding the authorized administrator inactivity period	
	FTA_TSE.1(1)	Reject administrator management session requests based on the connection IP	
ShadowCube Client	FCS_CKM.1(2)	* Success and failure of cryptographic key generation * Success and failure of encryption operations * Success and failure of cryptographic key	

		distribution * Success and failure of cryptographic key destruction	
	FCS_CKM.2	Success and failure of key distribution related to document encryption and decryption	
	FCS_CKM.6	Success and Failure of Actions	
	FCS_COP.1	Success and Failure of Cryptographic Operations, Types of Cryptographic Operations	
	FDP_ACF.1(1)	* An incident in which a document user with permissions successfully accessed, read, wrote to, or decrypted an encrypted document in a document group * An event in which a document user attempted to access an encrypted document in a document group for which they lacked permissions and was denied access due to a violation of control rules	Object-Specific Information
	FIA_AFL.1	Reaching the threshold for failed authentication attempts and the corresponding response actions taken	
	FIA_IMA.1 (Extended)	Success/failure of mutual authentication	
	FIA_UAU.1	* Document User Certificate Request * Request to enter email authentication code * Document User Certificate Creation * Request for Identification and Authentication Procedures	
	FIA_UID.1	All uses of the user identification mechanism, including the provided user identity	
	FPT_TST.1	* Results of the TSF self-test and integrity verification * Results of failed self-tests and integrity verification for validated cryptographic modules	Executable files with integrity violations

Prediction and Prevention of Audit Data Loss (ShadowCube Server)

When TOE predicts that the audit repository will reach the specified limit (specified limit - 10%), it generates audit data and sends an alarm email to authorized administrators. If the audit repository exceeds the specified limit, it overwrites the oldest records and sends an alarm email to administrators. The specified limits are as follows.

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

Audit Data Loss Prediction and Prevention (ShadowCube Client)

When the audit repository reaches 80% capacity, the TOE generates audit data and sends an authorized administrator an alarm email. If the audit repository exceeds the 90% threshold, the

system automatically reboots, the ShadowCube service is stopped, and an alarm email is sent to the administrator.

Audit Data Storage Location and Repository Protection

ShadowCube Server Data is stored in the ₩data directory of the ShadowCube Server installation path and is protected against deletion or modification by unauthorized users using the DBMS's identification and authentication features.

ShadowCube Client: Stored in C:₩ProgramData₩ShadowCube₩UserAccount₩ShadowCube.2026xxxx.adt and protected against deletion or modification through ARIA_CBC 256-bit encryption.

Related SFRs: FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.2, FAU_STG.4, FAU_STG.5

7.2 Cryptographic Support

To support document encryption in TOE and TSF data encryption including cryptographic key generation, key distribution, key destruction, cryptographic operations, and random number generation validated cryptographic modules whose security and implementation compliance have been verified through the Cryptographic Module Verification Program (KCMVP) are used.

Validated Cryptographic Module

- Cryptographic Module Name: MagicCrypto V2.3.0
- Validation Number: CM-263-2030.1
- Developer: Dream Security Co., Ltd.
- Validation Date: January 24, 2025
- Expiration Date: 2030-01-24

Validated Cryptographic Modules and Their Algorithms

Standard List	Encryption Method	Cryptographic Algorithm	Key Length	Purpose
KS X 1213-1	Block Cipher	ARIA_CTR	128	User Data Encryption • ShadowCube Client: Electronic document encryption when saving protected documents

		ARIA_CBC	256	TSF data Encryption
				• ShadowCube Server
				  • DB Password Encryption
				  • Document Group Key Encryption
				• ShadowCube Client
				  • Document User Certificate Encryption of the document user's private key
				  • Document User

				License Encryption • Encryption of Log Files and Configuration Files • Encryption of Memory Data for TSF Data Storage • Common • Protection of Data in Transit Between TOE components
ISO/IEC 11770-3	Key Generation	ECDH	256	Key Agreement for Mutual Authentication Among TOE components
TTAS.KO-12.0334	Key Derivation	PBKDF2	256	• ShadowCube Server • Derivation of the KEK for the DB Password Cryptographic Key • ShadowCube Client • Derivation of the KEK for the Private Key Encryption Key of the Document User Certificate • Derivation of the KEK for TSF data protection
ISO/IEC 18031	random bit generator	HASH_DRBG	256	• TSF data and document encryption key • ShadowCube Server: Generate DB password cryptographic key • ShadowCube Client: Document Cryptographic Key Generation • Generate DEK for TSF data protection • Generating Cryptographic Keys for User Certificate Private Keys • Random Bit Generation When Creating RSA and

				ECC Key Pairs
				• Generating email authentication codes
				  • Email authentication code for web administrator login
				  • Email authentication code for user certificate issuance

ISO/IEC 18033-2	Public-key cryptography	RSAES	2048	• KEK in the cryptographic document • Protection of data transmitted between TOE components (including user licenses)

ISO/IEC 10118-3	Hash function	SHA-256	256	• ShadowCube Server
				  • Store the web administrator password in the database (with a salt)
				  • Store hashes for integrity verification targets
				• ShadowCube Server
				  • Verify hashes for integrity verification targets

ISO/IEC 14888-2	Digital Signatures	RSA-PSS	2048	• ShadowCube Server: Signature verification for the audit log creator • ShadowCube Client: Signatures for the author of the document file and the audit log generator

Cryptographic Key Destruction

ShadowCube Server

Key Generation Algorithm	Key Length	Purpose	Destruction Timing
HASH_DRBG	256 bits	DEK	Upon IIS shutdown or system

PBKDF2	256 bits	KEK	shutdown
RSA	2048 bits	RSA key pair	
ECC	256 bits	ECDH key pair	

ShadowCube Client

Category	Key generation algorithm	Key Length	Purpose	Destruction Time
Document Encryption	HASH_DRBG	128 bits	DEK	When the application program (document program) closes
	RSA	2048 bits	KEK	When the user logs out or the system shuts down
TSF data Encryption	HASH_DRBG	256 bits	DEK	When a user logs out or the system shuts down
	PBKDF2	256 bits	KEK	
	RSA	2048 bits	Certificate Key Pair	When deleting or revoking a user certificate
	HASH_DRBG	256 bits	Certificate private key cryptographic key	
	ECC	256 bits	ECDH key pair	Upon system shutdown

* The HASH_DRBG random bits used to generate RSA and ECC keys are destroyed when each key is destroyed

Cryptographic Operations

TOE uses the following methods to ensure that document encryption and TSF data processing are performed in accordance with the standard.

Document Encryption

Standard List	Cryptographic Algorithm	Key Length	Purpose
KS X 1213-1	ARIA_CTR	128 bits	Document Encryption/Decryption
ISO/IEC 18033-2	RSAES	2048 bits	KEK

TSF data Encryption

ShadowCube Server

Standard List	Cryptographic Algorithms	Key Length	Purpose
KS X 1213-1	ARIA_CBC	256 bits	• Protection of data transmitted between TOE components • DB Password Encryption • Document group key encryption
ISO/IEC 18033-2	RSAES	2048 bits	Protection of data transmitted between TOE components
ISO/IEC 14888-2	RSA-PSS	2048 bits	Signature verification for audit log generators
ISO/IEC 10118-3	SHA-256	256 bits	• Store the web administrator password in the database (with a salt) • Store hashes for items subject to integrity verification

ShadowCube Client

Standard List	Cryptographic Algorithms	Key Length	Purpose
KS X 1213-1	ARIA_CBC	256 bits	• Protection of data transmitted between TOE components • Encryption of the document user's certificate private key • Encryption of the document user's license • Encryption of log files and configuration files • Encryption of memory data for TSF data storage
ISO/IEC 18033-2	RSAES	2048 bits	Protection of data transmitted between TOE components
ISO/IEC 14888-2	RSA-PSS	2048 bits	Signature of the author of a document file and the creator of an audit log
ISO/IEC 10118-3	SHA-256	256 bits	HASH verification of the subject of integrity verification

Random Bit Generation

The TOE uses the random bit generator (HASH_DRBG) provided by the validated cryptographic module MagicCrypto V2.3.0. This random bit generator provides a security strength of at least 112 bits, which is required for cryptographic key generation.

Related SFRs: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.6, FCS_COP.1(1), FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3, FCS_CKM.5

7.3 Document Encryption

The TOE performs encryption/decryption of protected documents for document users in accordance with document group-based access control rules set by an authorized administrator.

Subset Access Control

When a document user accesses a protected document, the TOE performs document group-based access control functions that restrict reading, encryption (writing), and decryption of the protected document based on the following security attributes set by an authorized administrator.

- Document group ID
- Document User ID
- Security Target

Security Attribute-Based Access Control

The TOE allows document users to read, encrypt (write), and decrypt protected documents when permitted by the policy set by an authorized administrator, and restricts such actions when the policy is violated.

Subject (User)		Object (Information)		Operation
List	**security attribute**	**List**	**security attribute**	
document user	• Document User ID • Password	• Documents to Be Protected	• Document group ID • Document Name • Document Type • Document Path	• If the user has read and encryption (write) permissions, allow the document to be read and save it in an encrypted format using document encryption • If the user has decryption permissions, decrypt the document

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

7.4 Identification and Authentication

The TOE provides identification and authentication functions for administrators and document users, and performs internal mutual authentication among the TOE components.

Identification and Authentication of Administrators

The TOE must allow the following actions prior to administrator authentication, and must allow administrator authentication via the "Identification and Authentication Procedure Request (Login Screen)" before identifying the administrator.

- Request to Enter Email Authentication Code
- Request for Identification and Authentication Procedure (Login Screen)

TOE grants or denies administrator access through an identification and authentication process. If an authorized administrator exceeds the configurable number of failed login attempts (default: 3; configurable range: 1 to 5), identification and authentication are disabled for 5 minutes.

TSF successfully authenticates the administrator before allowing any other actions mediated by TSF on the administrator's behalf. A validation mechanism is provided to ensure that passwords meet the requirement of 9 to 16 characters, consisting of a combination of four types: uppercase and lowercase letters, numbers, and special characters (!, @, #, $, %, ^, *, -, _, +, =). When an administrator logs in, a one-time authentication code generated by the random bit generator in the validated password module is sent to their email address; the administrator must use this code to prevent the reuse of authentication credentials. During the authentication process, only the administrator ID and the masked administrator password are displayed; no feedback regarding the reason for authentication failure (e.g., ID error, password error) is provided.

Identification and Authentication of Document Users

The TOE must allow the following actions prior to authenticating the document user, and must allow authentication of the document user by selecting the document user's certificate before identifying the document user.

- Certificate Issuance
  - Document User Certificate Request
  - Request to Enter Email Authentication Code
  - Document User Certificate Creation
  - Request for Identification and Authentication Procedures (Login Screen)
- After Certificate Issuance
  - Selecting a Document User Certificate
  - Request for Identification and Authentication Procedure (Login Screen)

The TOE grants or denies access to document users through the identification and authentication process. If the number of failed login attempts exceeds the limit set by an authorized administrator (default: 3 attempts; configurable range: 1 to 5 attempts), the document user's PC is rebooted, and identification and authentication are disabled for 5 minutes.

TSF successfully authenticates the document user on their behalf before allowing any other actions mediated by TSF. A verification mechanism is provided to ensure that passwords meet the requirement of being 9 to 16 characters long and consisting of a combination of uppercase and lowercase letters, numbers, and special characters (!, @, #, $, %, ^, *, -, _, +, =). When generating a document user's certificate, a one-time authentication code generated by the random bit generator of a validated cryptographic module is sent to the user's email address and used to prevent the reuse of authentication information. During the authentication process, only the document user's certificate and the obfuscated password are displayed; no feedback regarding

the reason for authentication failure (e.g., ID error, password error) is provided.

TOE Internal Mutual Authentication

Before performing encrypted communication between components, the TOE performs internal mutual authentication between the ShadowCube Server and the ShadowCube Client; during HTTP communication, this is handled through the ECDH algorithm key agreement process of a validated cryptographic module. Internal mutual authentication between TOE components is performed upon completion of the boot process for each ShadowCube Server and ShadowCube Client system.

Multiple Authentication Mechanisms

When logging into the ShadowCube Server, the administrator enters their ID and clicks the "Send Email OTP" button; login is successful only if both the email authentication code and the password are entered correctly.

When applying for a certificate, a document user must accurately enter the ID and name generated by the ShadowCube Server and create a password that complies with the password rules. An email authentication code is then sent, and the user enters the received code to successfully obtain the certificate.

Authentication Subjects	Authentication Mechanism
Administrator Authentication	Email Authentication Code
Document User Certificate Issuance	Email Authentication Code

Related SFRs: FIA_AFL.1, FIA_IMA.1 (Extended), FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1, FIA_UAU.5

7.5 Security Management

The TOE provides security management functions that allow authorized administrators and document users to configure and manage TOE security functions and TSF data.

Security Management by Authorized Administrators

Only one type of administrator role is provided, and the ability to manage the following security functions is restricted to authorized administrators.

Classification	Security Function	Capability			
		Determine the behaviour	Disable	Enable	Modify the behaviour
Object Settings	Department Management	O	-	-	O
	User Management	O	-	-	O
Policy Settings	Document Group Policy	O	-	-	O
	Security Object Policy	O	-	-	O
	Default License Policy	-	-	-	O

	Multi-License Policy	-	-	-	O
Certificate 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	-	-	-
Settings	Settings	-	-	-	O
	Check Disk Capacity	-	-	-	O
	Testing and Integrity Verification of the ShadowCube Server Itself	-		O	O

Authorized administrators can query, delete, and add security attributes, such as document user IDs, document group IDs, and security targets, as follows to configure document group-based access control rules. When assigning a document user to a document group, read/write (encrypted) permissions are provided by default, and authorized administrators can configure read/write (encrypted) and decryption permissions for the document user regarding the document group.

Access Control SFP	**Security Attribute**	**Capabilities**			
		Query	**Modify**	**Delete**	**Add**
Document Group-Based Access Control	Document User ID	O	-	O	O
	Document group ID	O	-	O	O
	Security Target	O	-	O	O

Authorized administrators can query, modify, delete, and add the following TSF data.

TSF Data	Capabilities			
	Query	Modify	Delete	Add
Document User Certificate	O	-	O	-
Audit Data	O	-	-	-
IP Address Settings	O	O	O	O
Session Timeout	O	O	-	-
Maximum Failed Login Attempts	O	O	-	-
Minimum Password Length	O	O	-	-

During the TOE installation process, you can set an administrator ID and password. Authorized administrators can set and change the password length, which must follow a combination of four rules: uppercase and lowercase letters, numbers, and special characters (!, @, #, $, %, ^, *, -, _, +, =).

- Minimum: 9 (characters)
- Maximum: 16 (characters)
- Default: 9 characters

Security Management for Document Users

Document users can query, modify, delete, and add the following TSF data.

TSF Data	Capabilities			
	Query	Modify	Delete	Add
Document User Certificate	O	O	O	O
License	O	O	-	-
Environment Settings	O	O	-	-

When creating a certificate for a document user, you can set a password that meets the following four combination rules: a mix of uppercase and lowercase letters, numbers, and special characters (!, @, #, $, %, ^, *, -, _, +, =). The password must be between 9 and 16 characters in length.

Related SFRs: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1 (Extended), FMT_SMF.1, FMT_SMR.1

7.6 Protection of the TSF

The TOE protects the TSF and performs self-tests and integrity verification.

TSF Data Protection

Protects TSF data transmitted between isolated parts of the TOE or stored in storage controlled by the TSF from unauthorized exposure or modification.

Transmission Data Protection

Category	Encryption Target	Encryption Method	Algorithm	Data Storage Location	Standard List
Transmission between ShadowCube Server and ShadowCube Client	Security Policy Data	Block Cipher	ARIA_CBC	Packet	KS X 1213-1
	Security Policy Data	Public-Key Cryptography	RSAES	Packet	ISO/IEC 18033-2

Audit Data, Account Information Protection

Category	Encryption Targets	Encryption Methods	Algorithm	Data Storage Location	Standard List
ShadowCube Server	Administrator Password	HASH	SHA-256 + SALT	DBMS	ISO/IEC 10118-3
				File	
ShadowCube Client	Document User Certificate	Block Cipher	ARIA_CBC	File	KS X 1213-1
	Document User Private Key				
	TOE Configuration File				
	Audit data	Electronic Signature	RSA-PSS	File	ISO/IEC 14888-2

TSF Data Protection

Encryption Targets	Encryption Method	Algorithm	Data Storage Locations	Standard List
KEK	Block Cipher	ARIA_CBC	Memory	KS X 1213-1
DEK	Block Cipher	ARIA_CBC	Memory, File	KS X 1213-1
Transmitted Data	Block Cipher	ARIA_CBC	Packet	KS X 1213-1

	Public-key cryptography	RSAES		ISO/IEC 18033-2

Key for Key Encryption (KEK)

Category	Algorithm	Standard List	Purpose
KEK	PBKDF2	TTAS.KO-12.0334	Deriving a key from the password entered during login

Availability protection of TSF data

ShadowCube Client, a TOE component, detects the deletion or tampering of executable files through integrity checks, and immediately detects such events when a process terminates, restoring the system by restarting the process or rebooting the system.

Detection Targets	Targets for Termination Prevention	Termination Prevention Mechanism
• sccm.exe • scconv.exe • scmain.exe • scboots64.exe • scboot64.exe • scboot.exe • scsysinfo.exe • scsysinfo64.exe	• scmain.exe • scboots64.exe • scboot64.exe • scboot.exe	• Restart the process: scmain.exe, scboots64.exe • Recover by rebooting the system: scboot64.exe, scboot.exe

TSF Testing

ShadowCube Server and ShadowCube Client perform self-tests at start-up and periodically to verify proper operation. If a self-test fails, an alarm email is sent to authorized administrators.

TOE Section Components	Item	Timing	Description (Role)
ShadowCube Server	ShadowCubeSelfTest.exe	• At start-up • Periodically (every 60 minutes)	Processes related to operation of the security function
ShadowCube Client	scmain.exe	• At start-up • Periodically (every 10 minutes)	Process for the GUI used for user security management
	scboots64.exe		Process for running user security management

Performs integrity verification by checking the integrity target information using SHA256-processed hash values. ShadowCube Server performs integrity verification on the TSF and TSF data at start-up and at intervals set by the administrator. ShadowCube Client performs integrity verification on the TSF and TSF data at start-up and periodically every 10 minutes; when booting in Safe Mode, the system automatically reboots, so integrity verification is performed only at start-up. If integrity verification fails, an alarm email is sent to authorized administrators.

TOE Module Compone	Item	Timing	Description (Role)

nts			

ShadowCube Server	config.ini	• At start-up
		• According to the schedule set by an authorized administrator
		  • Minimum: 1 (hour)
		  • Max: 24 (hours)
		  • Default: 24 (hours)
		  • Upon request by an authorized administrator during operation
			The configuration file used by the web service when initializing ShadowCube Server

	db.config		Configuration file used by the web service to connect to the DBMS
	log4net.xml		Configuration file used for logging settings in web services
	web.config		Web service configuration file
	admin.dll		Management of security attributes
	scbase.dll		License-Related Management of security attributes
	scpclib.dll		Database-Related Management of security attributes
	scpcws.dll		Management of ShadowCube Client-related security functions
	ssDeulmeori.dll		Process for identity and authentication management
	ssJikimi.dll		Process for using a validated cryptographic module
	ssNeobi.dll		Utility process for management console support
	ssNeonadeuli.dll		Process for encryption and decryption
	ssServerHelper.dll		Process for managing cryptographic functions
	MagicCryptoV230.dll		Validated Cryptographic Module
ShadowCube Client	scboot.exe, scboot64.exe, scboots64.exe	• At start-up • Periodically (every 10 minutes)	Processes related to security functions
	sccm.exe		Certificate Management Console
	scconv.exe		File Encryption and Decryption Management Console
	scmain.exe		Management console for user GUI support
	scsysinfo.exe, scsysinfo64.exe		Processes related to the operation of the security function

	scewvsc.dll, scewvsc64.dll, scewvsd.dll, scewvsd64.dll, scewvsp.dll, scewvsp64.dll, scewwss.dll, scewwss64.dll		Processes for document group-based access control rules
	scshell.dll, scshell64.dll		Processes for Windows Explorer integration
	scwinui.dll, scwinui64.dll		Processes for identification and authentication support
	ssDeulmeori.dll		Identification and authentication management process
	ssJikimi.dll		Process for using a validated cryptographic module
	ssMigratorHelp.dll		Process for supporting ShadowCube version compatibility
	ssNeobi.dll		Utility Process for Management Console Support
	ssNeonadeuli.dll		Encryption and Decryption Process
	ssServerHelper.dll		Process for managing cryptographic functions
	MagicCryptoV230.dll MagicCrypto32V230.dll		Validated Cryptographic Module

Failure with preservation of secure state

If the Adaptive Probability Test (APT) fails during the random bit generator noise source integrity test, the TSF considers this a temporary error caused by the surrounding environment and, rather than immediately terminating, performs a certain number of retries or retries for a certain period of time to determine whether a secure state can be maintained. If the retry results are consistently determined to be failures, the TSF immediately blocks all random number output to prevent abnormal random numbers from being used in cryptographic operations and transitions to a serious error state (MC_FAIL, 0x00011) where the cryptographic module cannot be used, thereby maintaining a secure state. The list of failure types is as follows.

- Failure of the Random Source Integrity Test (RCT, APT)
- Failure of integrity verification and failure of the algorithm self-test (KAT)

ShadowCube Client Automated Recovery

In accordance with FPT_TST.1, periodic integrity checks are performed on the client executable and key files; if tampering is detected, the integrity status attribute of the file is set to abnormal, and the recovery process is initiated. ShadowCube Client requests the transmission of legitimate installation files to the ShadowCube Server via a trusted secure communication channel. After verifying the integrity of the received files and confirming that the validated legitimate files have been obtained, the system reinstall is performed, and all security functions of the TOE are restored to their normal state prior to tampering by rebooting the system.

Related SFRs: FPT_ITT.1, FPT_PST.1 (Extended), FPT_PST.2 (Extended), FPT_TST.1, FPT_FLS.1, FPT_RCV.2

7.7 TOE Access

ShadowCube Server, a TOE component, performs session termination to control an administrator's TOE Access.

Session Management for Authorized Administrators

TOE limits the maximum number of concurrent sessions for a single administrator account to one if a successful login is made with that account after the initial login. If a login is attempted again with the same account on a different management console after an administrator has logged in, TOE terminates the previous session.

TOE terminates a session if there is no activity for the duration of the session timeout set by an authorized administrator after the administrator has logged in. The administrator's session timeout is as follows.

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

TOE allows access to the ShadowCube Server only from management consoles with pre-registered IP addresses. The maximum number of pre-registered IP addresses is as follows:

- Minimum: 2
- Max: 5
- Default: 2 (excluding localhost)

Session Management for Authorized Users

Derive a certificate key by combining the user's password with their IP address and MAC address. This ensures that if the IP address and MAC address do not match during login, unauthorized access is denied.

Related SFRs: FTA_MCS.2, FTA_SSL.3, FTA_TSE.1(1), FTA_TSE.1(2)