iqpad

ubCUBE v3.7

Security Target

Document Information	ubCUBE v3.7 Security Target
Version	1.2
Updated On	April 10, 2023

TABLE OF CONTENTS

List of Tables

List of Figures

1 ST introduction

This document is ubCUBE v3.7 Security Target of Iqpad, Inc. which conforms to EAL 1+ level of Common Criteria.

1.1 ST reference

Item	Specification
Title	ubCUBE v3.7 Security Target
Version	1.2
Author	Iqpad, Inc.
Updated On	April 10, 2023
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	CC V3.1 r5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Keywords	Document, Encryption

Table 1 ST reference

1.2 TOE reference

Item		Specification	
TOE		ubCUBE v3.7	
Version		3.7.0.3	
Components	Management Server	ubCUBE ubPortal v3.7.0.3	S/W (CD)
	Agent	ubCUBE Agent v3.7.0.3	
Guidance Documents		OPE-ubCUBE_v3.7_ubPortal-v1.1 OPE-ubCUBE_v3.7_Agent-v1.1	PDF (CD)
		PRE-ubCUBE_v3.7-v1.3	
Developer		Iqpad, Inc.	

Table 2 TOE reference

1.3 TOE overview

'ubCUBE' (hereinafter referred to as 'TOE') is used to protect important documents managed by the organization. The TOE encrypts electronic documents to protect the important documents managed by the organization according to the policy set by the administrator, and a document is decrypted according to the document user's request and right.

The TOE can encrypt/decrypt a document to be protected by specifying each individual document, document type (e.g., PDF document, Word document, HWP document, etc.), and document path. The entire content of the protected document, however, must be encrypted.

The primary security features provided by the TOE includes the encryption/decryption of the document to be protected and cryptographic key management. The TOE uses the 'ubXFS Cryptographic Module V1.1' validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

1.3.1 TOE type

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

The ubCUBE ubPortal and ubCUBE Agent are the indispensable TOE components that perform the security features of the TOE.

1.3.2 TOE usage and major security features

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

The TOE uses the data encryption key (hereinafter referred to as “DEK”) and key encryption key (hereinafter referred to as “KEK”) for the document encryption/decryption function. The main body of the protected document is encrypted with the DEK according to the policy set by the administrator, and the GUID linked to the DEK is stored in the header of the security document. The header of the security document is encrypted with the DEK.

The ubCUBE ubPortal generates the DEK and KEK both DEK and KEK by the symmetric key method and distributes them to the ubCUBE Agent. At this time, the cryptographic key is distributed safely by asymmetric key method. The ubCUBE Agent encrypts the main body of the protected document and decrypts the encrypted main body using the cryptographic key.

Each component of the TOE provides a cryptographic key destruction function if the cryptographic key is not used anymore.

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

1.3.3 Non-TOE and TOE operational environment

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

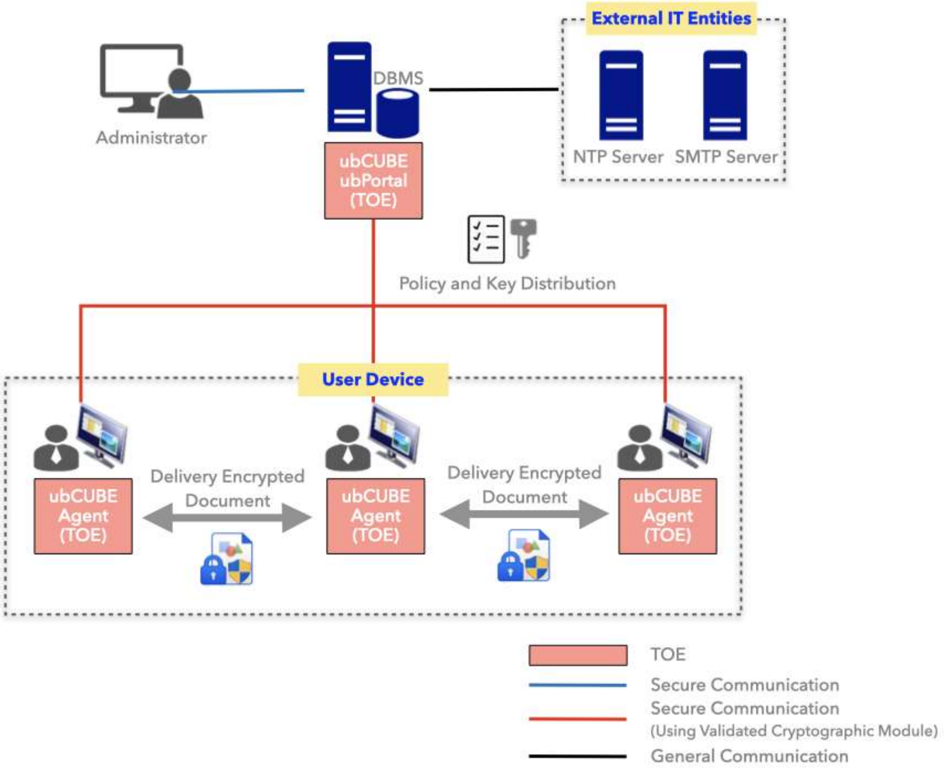


Figure 1 TOE operational environment

The TOE is composed of the ubCUBE ubPortal which manages the security policy and cryptographic key, and the ubCUBE Agent that performs Electronic Document encryption/decryption installed in the user device.

The administrator sets the policy for each document user or information system through the ubCUBE ubPortal, which distributes the policy and cryptographic key configured by the administrator to the ubCUBE Agent. The ubCUBE Agent performs Electronic Document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted/decrypted document is stored in the user PC as a file.

The ‘ubXFS Cryptographic Module V1.1’ validated cryptographic module is used for the cryptographic operation of the major security features of the TOE. For the communication between the TOE component and the administrator (e.g., the administrator accesses the ubCUBE ubPortal using the web browser to configure policies), TLS 1.2 is used.

There are external entities necessary for the operation of the TOE including the NTP server to synchronize time and email server to notify the authorized administrator in case of audit data loss.

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

Component			Requirement
	HW	CPU	Intel(R) Xeon(R) 3 GHz 6 core or higher

ubCUBE ubPortal		RAM	16 GB or higher
		HDD	100 GB or higher for the installation of TOE
		NIC	100/1000 Mbps 1 Port or higher
	OS		Microsoft Windows Server 2012 R2 Standard (64 bit)
	SW		Microsoft IIS 8.5 Microsoft .NET Framework 4.5 Microsoft .NET Framework 4.7 Microsoft ASP.NET 4.5 Microsoft SQL Server 2016
ubCUBE Agent	HW	CPU	Intel i3 Dual Core 2.50 GHz or higher
		RAM	4 GB or higher
		HDD	10 GB or higher for the installation of TOE
		NIC	100/1000 Mbps 1 Port or higher
	OS		Microsoft Windows 10 Pro (64 bit) Microsoft Windows 10 Enterprise (64 bit)
	SW		Microsoft Visual C++ 2015 Redistributable Update 3 Microsoft Office 2010, 2013, 2016, 2019 Hancom Office 2010, 2014, 2018, NEO Adobe Acrobat Reader DC

Table 3 TOE installation requirements

In addition, the 3rd-Party software as non-TOE which are necessary for the operation of the TOE are as in the following.

3rd-Party Software	Description
Microsoft SQL Server 2016	DBMS to store audit data of the ubCUBE ubPortal
Microsoft IIS 8.5	Web application server used by the ubCUBE ubPortal
Microsoft .NET Framework 4.5	Software development framework for building and running applications to operate the ubCUBE ubPortal
Microsoft .NET Framework 4.7	Software development framework for building and running applications to operate the ubCUBE ubPortal
Microsoft ASP.NET 4.5	Software framework for building web apps and services to operate the ubCUBE ubPortal
Microsoft Visual C++ 2015 Redistributable Update 3	Required library to installation of the ubCUBE Agent

Table 4 3rd-Party software requirements

The external IT entities for the operation of the TOE are as in the following.

External IT entities	Description
SMTP Server	Email server to send security alerts by email to the authorized administrator
NTP Server	Time server to synchronize time to provide reliable time stamp

Table 5 External IT entities requirements

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

Software	Description
Microsoft Edge 80.0.361.62	WEB GUI for TOE security management

Table 6 Administrator PC requirements

1.4 TOE description

1.4.1 Physical scope of the TOE

The TOE is composed of the ubCUBE ubPortal, ubCUBE Agent, and guidance documents. The ubCUBE ubPortal is software that provides functions of managing the security policy and the cryptographic key for the administrator to apply for the ubCUBE Agent. The ubCUBE Agent is software that controls the permissions to use secured documents according to the policy received from the ubCUBE ubPortal. The components of the distributed TOE are as follows.

Category	Item	Distribution	
TOE component	ubCUBE ubPortal v3.7.0.3 (ubCUBE_v3.7_ubPortal_Setup_v3.7.0.3.exe)	exe	Software (Distributed as a CD)
	ubCUBE Agent v3.7.0.3 (ubCUBE_v3.7_Agent_Setup_v3.7.0.3.exe)		
TOE guidance documents	ubCUBE v3.7 Operation Guide(ubPortal) v1.1 (ubCUBE_v3.7_ubPortal_Operation_Guide_v1.1.pdf) ubCUBE v3.7 Operation Guide (Agent) v1.1 (ubCUBE_v3.7_Agent_Operation_Guide_v1.1.pdf) ubCUBE v3.7 Preparation Procedure v1.3 (ubCUBE_v3.7_ubPortal_Preparation_Procedure_Guide_v1.3.pdf)	pdf	PDF (Distributed as a CD)

Table 7 Components of the distributed TOE

The hardware and operation system where the TOE is installed, the word processing program that the user uses, and external systems and other software necessary to operate the TOE are excluded from the scope of the TOE. The following [Figure 2] shows the physical scope of the TOE.

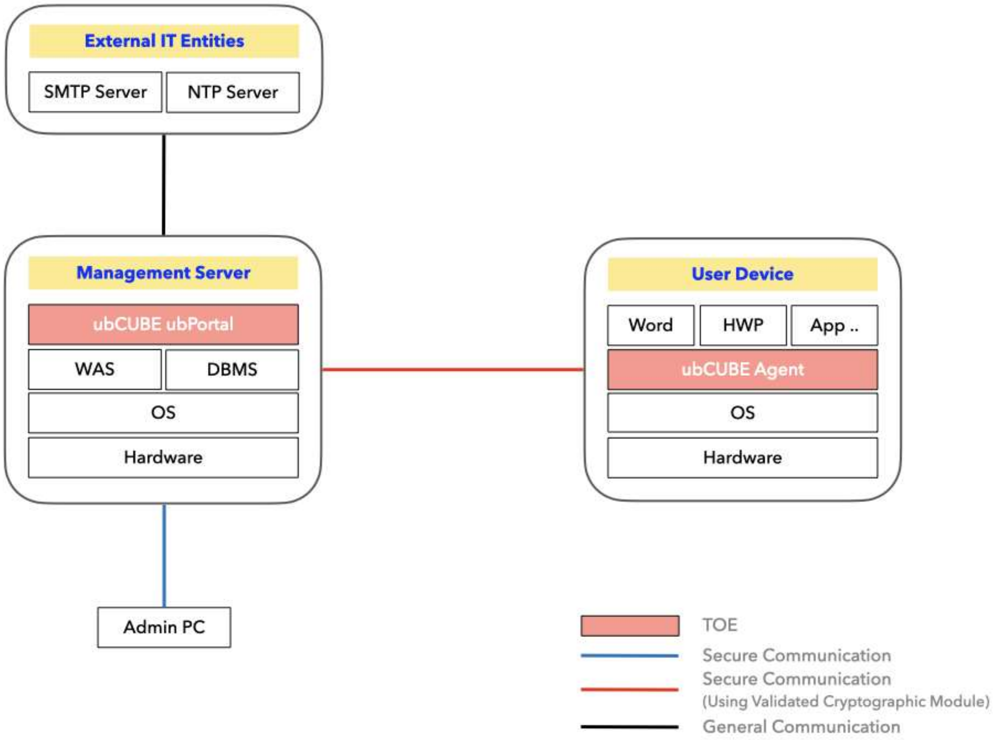


Figure 2 Physical scope of the TOE

1.4.2 Logical scope of the TOE

The following [Figure 3] shows the logical scope of the TOE.

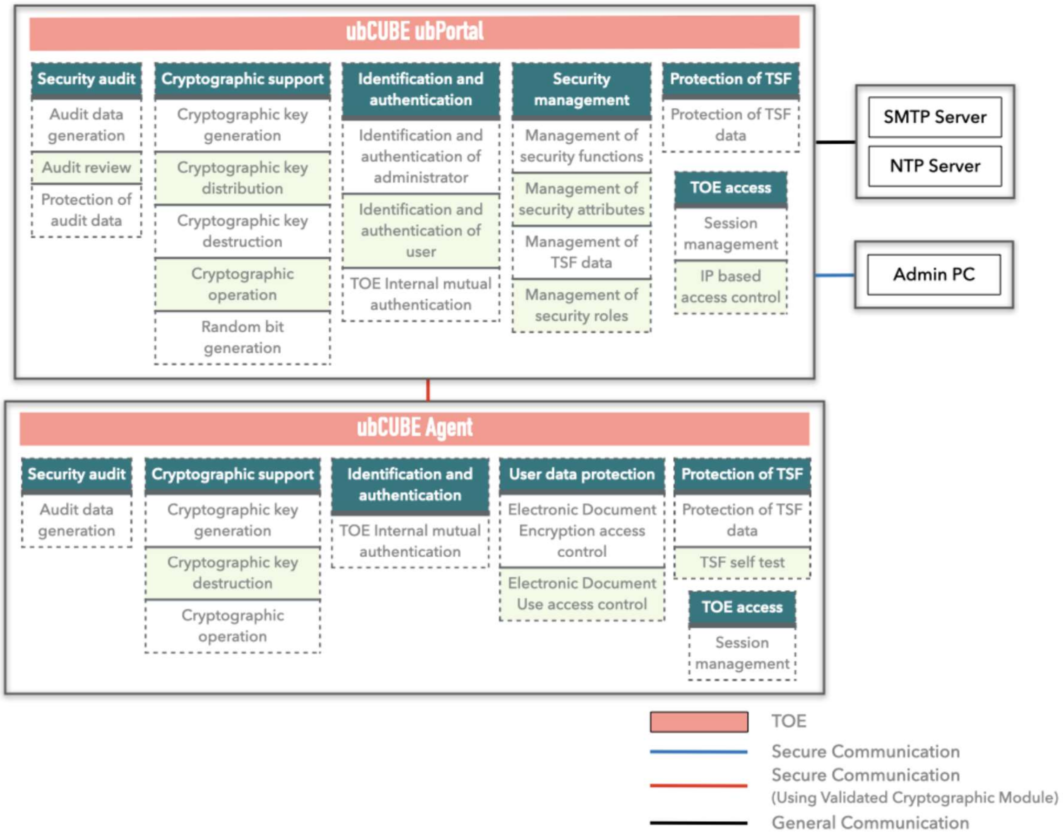

ubCUBE ubPortal
Security audit
Audit data generation
Audit review
Protection of audit data
Cryptographic support
Cryptographic key generation
Cryptographic key distribution
Cryptographic key destruction
Cryptographic operation
Random bit generation
Identification and authentication
Identification and authentication of administrator
Identification and authentication of user
TOE Internal mutual authentication
Security management
Management of security functions
Management of security attributes
Management of TSF data
Management of security roles
Protection of TSF
Protection of TSF data
TOE access
Session management
IP based access control
SMTP Server
NTP Server
Admin PC
ubCUBE Agent
Security audit
Audit data generation
Cryptographic support
Cryptographic key generation
Cryptographic key destruction
Cryptographic operation
Identification and authentication
TOE Internal mutual authentication
User data protection
Electronic Document Encryption access control
Electronic Document Use access control
Protection of TSF
Protection of TSF data
TSF self test
TOE access
Session management
TOE
Secure Communication
Secure Communication (Using Validated Cryptographic Module)
General Communication

Figure 3 Logical scope of the TOE

1.4.2.1 Security audit

The TOE creates and records audit data of the events to the DBMS when a defined audit event occurs. Information including date and time of the event, type of event, subject identity, and result of event(success or failure) are stored in an audit record. The authorized administrator can view the stored audit records and search the records by event type and search conditions. If any potential security violation such as failure of authentication, integrity violation, failure of self test, exceed of audit trail threshold, exceed of maximum size of audit trail is detected, the TOE sends an email to the administrator to inform the administrator of the potential violation. If audit trail exceeds maximum size, the TOE overwrite the oldest stored audit records to prevent a loss of audit data.

1.4.2.2 Cryptographic support

The TOE uses the ‘ubXFS Cryptographic Module V1.1’ validated cryptographic module to perform cryptographic key generation, distribution, destruction, and cryptographic operation. TOE generates 256bit DEK for document and TSF data encryption with Hash_DRBG(SHA-256), KEK for DEK encryption is generated by NIST 800-132 KDF. DEK is securely distributed with a public key algorithm(RSAES-OAEP, 3072bit) between TOE compoents. Cryptographic operation for document and TSF data is performed with a symemetric algorithm(ARIA-CBC) whose key size is 256bit. TOE mutual authentication is performed with a public key algorithm(RSAES-OAEP, 3072bit), digital signature of policy data is performed with a digital signature algorithm(RSA-PSS, 3072bit), integration check of TSF data is performed with HMAC(SHA-256), and authentication data is encrypted with SHA-256. A cryptographic key is securely destructed with zerorization in memory after use.

1.4.2.3 User data protection

The TOE performs access control of the authorized user on document encryption/decryption and use(Expiration date/Modification of permissions/Print) according to the security policy. The authorized administrator can set access control policy per document grade, user/department/group. The access control policy is set based on the security attribute of the user(ID, Allowed document grade, Department ID of the user, Group ID of the user) and the security attribute of protected a document(document type, expiration date).

The following table shows the document types that the TOE supports encryption/decryption.

Application	Document type (File extension)
MS Office Word	doc, docx
MS Office PowerPoint	ppt, pptx
MS Office Excel	xls, xlsx
Hancom Office	hwp
Adobe Acrobat Reader	pdf

Table 8 TOE supported document type

1.4.2.4 Identification and authentication

The TOE performs mutual authentication between TOE components with the internally implemented authentication protocol, provides identification and authentication of administrator and user based on ID and password. Password is set by combination of each of alphabetical, numerical, and special characters and the length is at least 9 digits and less than 30 digits. The input characters of password are masked with "●" to prevent from disclosure. No feedback is provided on a reason for the failure if authentication fails. When the defined number set by the administrator of unsuccessful authentication attempts has been met, the account is locked out. Reuse of authentication data is prevented with time stamp. The system(global) policy is applied to the user before authentication and the user can access a protected document according to a policy after authentication. The administrator is authenticated through web browser and can perform security management function after authentication.

1.4.2.5 Security management

TOE provides management of security functions, security attributes, and TSF data to the authorized administrator. The authorized administrator can manage security function including user and department, security policy, and admistrator management through web browser and can manage important TSF data including authentication data, security policy data, and cryptographic key data as well.

1.4.2.6 Protection of the TSF

The TOE communicates securely to protect transmitted data between TOE components with a public key cryptographic algorithm and assures confidentiality and integrity with a validated cryptographic module. In addition, the TOE protects TSF data that is stored in the repository controlled by the TSF with encryption and digital signature in order to prevent unauthorized disclosure and modification. The TOE runs a suite of self tests during initial start-up, periodically during normal operation to prevent unauthorized deletion of agent settings and ensure integrity. The TOE notifies the authorized administrator if an integrity violation is detected. The TOE prevents unauthorized deletion of agent files and unauthorized termination of agent processes with periodic monitoring between agent processes related to the TOE.

1.4.2.7 TOE access

The TOE provides a management function to register IP addresses that are allowed for management access and performs an access control function that management access is allowed only from a registered IP address. The TOE also restricts the number of maximum concurrent sessions belonging to the same user and permission as 1. The TOE terminates an interactive session of the authorized administrator after 5 minutes of inactivity.

1.5 Conventions

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

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

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

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

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

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

1.6 Terms and definitions

Terms used in this ST, which are the same as in the CC, must follow those in the CC.

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

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

Approved mode of operation
The mode of cryptographic module using approved cryptographic algorithm

Approved cryptographic algorithm
A cryptographic algorithm selected by Korean Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability

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

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

Public Security Parameters (PSP)
Security related public information whose modification can compromise the security of a cryptographic module

Public Key
A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity(the subject using the public key), it can be disclosed

Public Key(asymmetric) cryptographic algorithm
A cryptographic algorithm that uses a pair of public and private keys

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

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

Recommend/be recommended
The ‘recommend’ or ‘be recommended’ presented in Application notes is not mandatorily recommended, but required to be applied for secure operations of the TOE

Group Based Access Control
As the one of the discretionary access control, performing the access control for the entity based on group identity

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

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

Data Encryption Key (DEK)
Key that encrypts the data

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

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

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

Security Target (ST)
Implementation-dependent statement of security needs for a specific identified TOE

Security Policy Document
Document uploaded to the list of the validated cryptographic module with the module's name and specifying the summary for the cryptographic algorithms and operational environments of the TOE

Security Token
Hardware device that implements key generation and electronic signature generation inside the device to save/store confidential information safely

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

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

Unapproved mode of operation
The mode of cryptographic module which can use both approved cryptographic algorithms and unapproved cryptographic algorithms

Secret Key
A cryptographic key which is used in an symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

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

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

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

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

KCMVP, Korea Cryptographic Module Validation Program
A system to validate the security and implementation conformance of cryptographic modules used

for the protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions

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

Role Based Access Control (RBAC)
An access control that restricting system access by not the direct relationship (e.g., user-permission) but the role depended on the properties of the organization (e.g., user-role, permission-role), when the user access to the entity

Operation(on a component of the CC)
Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation(on a subject)
Specific type of action performed by a subject on an object

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

Threat Agent
Entity that can adversely act on assets

Authorized Administrator
Authorized user to securely operate and manage the TOE

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

Authentication Data
Information used to verify the claimed identity of a user

Application Programming Interface (API)
A set of system libraries existing between the application layer and the platform system, enables the easy development of the application running on the platform

Self-tests
Pre-operational or conditional test executed by the cryptographic module

Assets
Entities that the owner of the TOE presumably places value upon

Refinement
Addition of details to a component

Access Control List, ACL
The list including entities who are permitted to access the entity and the types of these permission

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

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

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

Subject
Active entity in the TOE that performs operations on objects

Sensitive Security Parameters (SSP)
Critical security parameter (CSP) and public security parameter (PSP)

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

Component
Smallest selectable set of elements on which requirements may be based

Class
Set of CC families that share a common focus

Key Encryption Key (KEK)
Key that encrypts another cryptographic key

Target of Evaluation (TOE)
Set of software, firmware and/or hardware possibly accompanied by guidance

Evaluation Assurance Level (EAL)
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

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

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

Shall/must
The ‘shall’ or ‘must’ presented in Application notes indicates mandatory requirements applied to the TOE

Can/could
The ‘can’ or ‘could’ presented in Application notes indicates optional requirements applied to the TOE by ST author’s choice

Critical Security Parameters (CSP)
Security-related information whose disclosure or modification can compromise the security of a cryptographic module (e.g., secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors)

TOE Security Functionality (TSF)
Combined functionality of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs

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

SSL (Secure Sockets Layer)
This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network

TLS (Transport Layer Security)
This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246

Wrapper
Interface to connect the TOE with various types of information system

1.7 ST organization

The ST are organized as follow.

Chapter 1 introduces to the Security Target, providing TOE references, TOE overview, TOE description, conventions, terms and definitions, and ST organization.

Chapter 2 provides the conformance claims to the CC, PP and package, and describes the claim's conformance rationale.

Chapter 3 describes the security objectives for the operational environment.

Chapter 4 defines the extended components for electronic document encryption.

Chapter 5 describes the security functional and assurance requirements.

Chapter 6 provides a summary of TOE security functions.

Chapter 7 provides a list of references used in the ST.

2 Conformance claim

2.1 CC conformance claim

Item	Specification
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 • Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) • Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) • Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
Part 2 Security functional components	Extended: FCS_RBG.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2, FTA_SSL.5
Part 3 Security assurance components	Conformant
Package	Augmented : EAL1 augmented(ATE_FUN.1)

Table 9 CC conformance claim

2.2 PP conformance claim

This ST claim conformance the following PP.

- Korean National Protection Profile for Electronic Document Encryption V1.1

2.3 Package conformance claim

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

- Assurance package : EAL1+ (ATE_FUN.1)

2.4 Conformance claim rationale

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

The followings are the security objectives added to 'Korean National Protection Profile for Electronic Document Encryption V1.1' by this ST.

Item	Security objectives	Rationale
Security objectives for the operational environment	OE.RELIABLE_STORAGE	The audit record where the audit trail, such as the DBMS interacting with the TOE, is saved should be protected against unauthorized deletion or modification.

	OE.RELIABLE_TIME_STAMP	The TOE shall accurately record the security related events using the reliable time stamp from the TOE operational environment.

Table 10 Conformance claim rationale

3 Security objectives

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

3.1 Security objectives for the operational environment

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

Item	Description
OE.PHYSICAL_CONTROL	The place where the management server among the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.
OE.TRUSTED_ADMIN	The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidances.
OE.LOG_BACKUP	The authorized administrator shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.
OE.OPERATION_SYSTEM_REINFORCEMENT	The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
OE.RELIABLE_STORAGE	The audit record where the audit trail, such as the DBMS interacting with the TOE, is saved should be protected against unauthorized deletion or modification.
OE.RELIABLE_TIME_STAMP	The TOE shall accurately record the security related events using the reliable time stamp from the TOE operational environment.
OE.MANAGEMENT_ACCESS	For communication between the web browser of the administrator PC and the web server which is the operation environment of the management server, TLS 1.2 shall be used to guarantee the confidentiality and integrity of the transmitted data.

Table 11 Security objectives for the operational environment

4 Extended components definition

4.1 Cryptographic support

4.1.1 Random bit generation

Family Behaviour

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

Component leveling

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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen

4.1.1.1 FCS_RBG.1 Random bit generation

Hierarchical to	No other components.
Dependencies	No dependencies.
FCS_RBG.1.1	The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: list of standards].

4.2 Identification and authentication

4.2.1 TOE Internal mutual authentication

Family Behaviour

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

Component leveling

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

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of mutual authentication

4.2.1.1 FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication between [assignment: different parts of TOE] by [assignment: authentication protocol] that meet the following: [assignment: list of standards].

4.3 Security Management

4.3.1 ID and password

Family Behaviour

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

Component leveling

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

Management: FMT_PWD.1

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

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password.

4.3.1.1 FMT_PWD.1 Management of ID and password

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [assignment: list of functions] to [assignment: the authorized identified roles]. 1. [assignment: password combination rules and/or length] 2. [assignment: other management such as management of special characters unusable for password, etc.]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [assignment: list of functions] to [assignment: the authorized identified roles]. 1. [assignment: ID combination rules and/or length] 2. [assignment: other management such as management of special characters unusable for ID, etc.]
FMT_PWD.1.3	The TSF shall provide the capability for [selection, choose one of: setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time].

4.4 Protection of the TSF

4.4.1 Protection of stored TSF data

Family Behaviour

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

Component leveling

FPT_PST Protection of the TSF
1
2

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

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

Management: FPT_PST.1, FPT_PST.2

There are no management activities foreseen.

Audit: FPT_PST.1, FPT_PST.2

There are no auditable events foreseen.

4.4.1.1 FPT_PST.1 Basic protection of stored TSF data

Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_PST.1.1	The TSF shall protect [assignment: TSF data] stored in containers controlled by the TSF from the unauthorized [selection: disclosure, modification].

4.4.1.2 FPT_PST.2 TSF Availability protection of TSF data

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

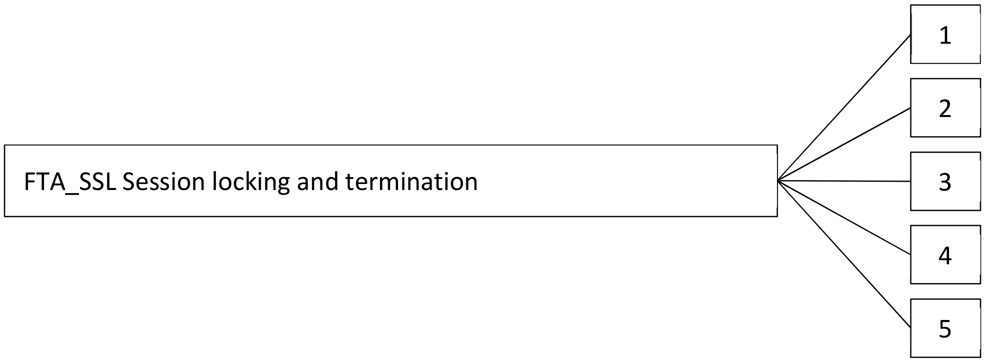
4.5 TOE Access

4.5.1 Session locking and termination

Family Behaviour

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

Component leveling



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

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

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

Management: FTA_SSL.5

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

a) Specification for the time interval of user inactivity that is occurred the session locking and

b) termination for each user

c) Specification for the time interval of default user inactivity that is occurred the session locking

d) and termination

Audit: FTA_SSL.5

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive session

4.5.1.1 FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to	No other components.
Dependencies	[FIA_UAU.1 authentication or No dependencies]
FPT_SSL.5.1	The TSF shall [selection: • *lock the session and re-authenticate the user before unlocking the* • *session,* • *terminate] an interactive session after a [assignment: time interval of user* • *inactivity]*.

5 Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.

The following table defines all the subjects, objects, operations, security attributes used in the security functional requirements.

Subject (user)	Subject (user) security attributes	Object (information)	Object (information) security attributes	Operation
Authorized administrator	User ID, Password, IP address	Security management data	-	Query, Add, Modify, Delete
		Authentication data		Query, Add, Modify, Delete
		Administrator permission setting data		Query, Add, Modify, Delete
		Security policy setting data		Query, Add, Modify, Delete
		Audit data		Query

Authorized user	User ID, Password, Department, Group, Document grade	Secured documents	Document grade, Owner ID, Permissions on User/Department/Group	Read(Decryption)
				Write(Encryption)
				Modify Permissions
				Print

Table 12 Definition of subjects, objects, relevant security properties and operations

5.1 Security functional requirements

The security functional requirements of this ST are composed by conforming ‘Korean National Protection Profile for Electronic Document Encryption’.

The following table shows the security functional requirements components used in this ST.

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation (Electronic Document Encryption)
	FCS_CKM.1(2)	Cryptographic key generation

		(TSF Data Encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Electronic Document Encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF Data Encryption)
	FCS_RBG.1(Extended)	Random bit generation
FDP	FDP_ACC.1(1)	Subset access control (Electronic Document Encryption access control)
	FDP_ACC.1(2)	Subset access control
	FDP_ACF.1(1)	Security attribute based access control (Electronic Document Encryption access control)
	FDP_ACF.1(2)	Security attribute based access control
FIA	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_PST.2(Extended)	Availability protection of TSF data
	FPT_TST.1	TSF testing
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

Table 13 Security functional requirements

5.1.1 Security audit (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to	No other components.
Dependencies	FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [sending email to the administrator] upon detection of a potential.

5.1.1.2 FAU_GEN.1 Audit data generation

Hierarchical to No other components.
Dependencies FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit; and
c) [Refer to the "auditable events" in Table 14 Audit events, [none]].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST [Refer to the contents of "additional audit record" in Table 14 Audit events, [none]].

Security functional component	Auditable event	Additional audit record
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Autom ated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption)	
FCS_CKM.4	Success and failure of the activity (applying to destruction of key related to Electronic Document Encryption)	
FCS_COP.1	Success and failure, and the type of cryptographic operation	
FDP_ACF.1	Successful request of operation execution regarding the object handled by SFP	Object identifi cationinforma tion
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_IMA.1 (Extended)	Success and failure of mutual authentication	
FIA_UAU.1	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	

FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MSA.1	All modifications to the security attributes	
FMT_MSA.3	Modifications to the basic settings of allowance or restriction rules All modifications to the initial values of security attributes	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1 (Extended)	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	TSF self test and the results of the tests	Modified TSF data or module information in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5 (Extended)	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

Table 14 Audit events

5.1.1.3 FAU_SAA.1 Potential violation analysis

Hierarchical to No other components.
Dependencies FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [

- authentication failure audit event among auditable events of FIA_UAU.1
- violation of control rules of FDP_ACF
- integrity violation audit event and self test failure event of validated cryptographic module among auditable events of FPT_TST.1
- An event that the audit trail exceeds the specified threshold among auditable events of FAU_STG.3

- An event that the audit trail is saturated among auditable events of FAU_STG.4

] known to indicate a potential security violation;

b) [none]

5.1.1.4 FAU_SAR.1 Audit review

Hierarchical to No other components.
Dependencies FAU_GEN.1 Audit data generation

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

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

5.1.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to No other components.
Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [search] of audit data based on [and operation].

Type of audit record	Search conditions
Administrator audit log	User ID, Name, IP address, Period, Success/Failure
Document encryption and use log	User ID, Name, IP address, Period, Success/Failure, Event type, Filename, Success/Failure
System access log	User ID, Name, IP address, Period, Audit type, Success/Failure

Table 15 Search conditions for audit data

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

Hierarchical to No other components.
Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [notify the authorized administrator by email, [none]], if the audit trail exceeds [the threshold set by the authorized administrator].

5.1.1.7 FAU_STG.4 Prevention of audit data loss

Hierarchical to FAU_STG.3 Action in case of possible audit data loss
Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] and [send a notification email to the authorized administrator] if the audit trail is full.

5.1.2 Cryptographic support (FCS)

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

Hierarchical to No other components.

Dependencies [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in Table 16] and a specified cryptographic key size [Cryptographic key size in Table 16] that meet the following [List of standards in Table 16].

List of standards	Cryptographic algorithm	Cryptographic key size	Purpose
ISO/IEC 18031	Hash_DRBG (SHA-256)	256bit	Document encryption DEK

Table 16 Cryptographic key generation (1)

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

Hierarchical to No other components.

Dependencies [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic key generation algorithm in Table 17] and a specified cryptographic key size [Cryptographic key size in Table 17] that meet the following [List of standards in Table 17].

List of standards	Cryptographic algorithm	Cryptographic key size	Purpose
ISO/IEC 18031	Hash_DRBG (SHA-256)	256bit	TSF data encryption DEK
NIST 800-132	KDF	256bit	TSF data encryption KEK

Table 17 Cryptographic key generation (2)

5.1.2.3 FCS_CKM.2 Cryptographic key distribution

Hierarchical to No other components.

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

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with the specified cryptographic distribution method [Cryptographic key distribution method in Table 18 Cryptographic key distribution] that meets the following [List of standards in Table 18 Cryptographic key distribution].

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

Table 18 Cryptographic key distribution

5.1.2.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components.

Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destruct cryptographic keys in accordance with the specified cryptographic key destruction method [key zeroization] that meets the following: [none].

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

Hierarchical to	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform the cryptographic operation list [Cryptographic operation list in Table 19] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in Table 19] and a specified cryptographic key size [Cryptographic key size in Table 19] that meet the following [List of standards in Table 19].

List of standards	Cryptographic algorithm	Cryptographic key size	Cryptographic operation list
KS X 1213	ARIA-CBC	256bit	Encryption/decryption of electronic documents

Table 19 Cryptographic operation (Electronic Document Encryption)

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

Hierarchical to	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform the cryptographic operation list [Cryptographic operation list in Table 20] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in Table 20] and a specified cryptographic key size [Cryptographic key size in Table 20] that meet the following [List of standards in Table 20].

List of standards	Cryptographic algorithm	Cryptographic key size	Cryptographic operation list
KS X 1213	ARIA-CBC	256bit	Encryption/decryption of TSF data
ISO/IEC 18033-2	RSAES-OAEP	3072bit	1) Mutual authentication between the ubCUBE ubPortal & ubCUBE Agent

			2) Encryption/decryption for policy and DEK distribution
ISO/IEC 14888-2	RSA-PSS	3072bit	Digital signature of policy data
ISO/IEC 9797-2	HMAC (SHA-256)	256bits	Verification of TSF data integrity
ISO/IEC 10118-3	SHA-256	N/A	Encryption of authentication data

Table 20 Cryptographic operation (TSF Data Encryption)

5.1.2.7 FCS_RBG.1 Random bit generation (Extended)

Hierarchical to No other components.
Dependencies No dependencies.

FCS_RBG.1.1 The TSF shall generate random bits using the specified random bit generator that meets the following [Table 21 Random bit generation].

List of standards	Random bit generation algorithm	Cryptographic key size
ISO/IEC 18031	Hash_DRBG (SHA-256)	256bit

Table 21 Random bit generation

5.1.3 User data protection (FDP)

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

Hierarchical to No other components.
Dependencies FDP_ACF.1 Security attribute based access control

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

a) SFP of Document grade based access control
   a. Subject: Authorized user
   b. Object: Secured document
   c. Operation: Encryption(Write), Decryption(Read)
b) SFP of User/Department/Group based access control
   a. Subject: Authorized user
   b. Object: Secured document
   c. Operation: Encryption(Write), Decryption(Read)

]

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

Hierarchical to No other components.
Dependencies FDP_ACF.1 Security attribute based access control

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

a) SFP of Document grade based access control
   a. Subject: Authorized user

   b. Object: Secured document
   c. Operation: Expiration date, Modification of permissions, Print

b) SFP of User/Department/Group based access control
   a. Subject: Authorized user
   b. Object: Secured document
   c. Operation: Expiration date, Modification of permissions, Print

]

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

Hierarchical to	No other components.
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	TSF shall enforce the [Electronic Document Encryption access control SFP] on objects based on the [list of subjects and objects controlled by the following SFP, security attribute appropriate for SFP regarding each subject and object, or group of named security attributes]: [a) Subject: Authorized user b) Security attribute of authorized user: User ID, Allowed document grade, Department ID of user, Group ID of user c) Object: Secured document d) Security attribute of secured document: Document type, Expiration date, Allow or deny of modification of permissions, Allow or deny of print]
FDP_ACF.1.2	TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) If the security attribute for the subject is included to the security attribute which is permitted to access for the object and the operation is matched with the security attribute of the object, the corresponding operation is allowed. b) [*none*]
FDP_ACF.1.3	TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [none]
FDP_ACF.1.4	TSF shall explicitly deny access of the subject to objects based on the following additional rules: [none]

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

Hierarchical to	No other components.
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

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

a) Subject: Authorized user
b) Security attribute of authorized user: User ID, Allowed document grade, Department ID of user, Group ID of user
c) Object: Secured document
d) Security attribute of secured document: Document type, Expiration date, Allow or deny of modification of permissions, Allow or deny of print

]

FDP_ACF.1.2

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

a) If the security attribute for the subject is included to the security attribute which is permitted to access for the object and the operation is matched with the security attribute of the object, the corresponding operation is allowed.
b) [*none*]

FDP_ACF.1.3

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

FDP_ACF.1.4

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

5.1.4 Identification and authentication (FIA)

5.1.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to No other components.
Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when [*an administrator configurable positive integer within [5]*] u nsuccessful authentication attempts occur related to [authentication of administrator, user].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [perform account lockout].

5.1.4.2 FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.
Dependencies No dependencies.

FIA_IMA.1.1

The TSF shall perform mutual authentication between [ubCUBE ubPortal & ubCUBE Agent] in accordance with a specified [internally implemented authentication protocol] that meets the following: [none].

5.1.4.3 FIA_SOS.1 Verification of secrets

Hierarchical to No other components.
Dependencies No dependencies.

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

[

a) Allowed characters
   a. Alphabetical characters(case sensitive): a-z, A-Z
   b. Numerical characters: 0-9
   c. Special characters: !@#$%^&*+=-

b) Combination rules
   a. Combination of each of alphabetical, numerical, and special characters
   b. At least 9 digits and less than 30 digits

]

5.1.4.4 FIA_UAU.1 Timing of authentication

Hierarchical to No other components.
Dependencies FIA_UID.1 Timing of authentication

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

[

a) Administrator: none
b) User: Self test, Password reset

]

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

5.1.4.5 FIA_UAU.4 Single use authentication mechanisms

Hierarchical to No other components.
Dependencies No dependencies.

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

5.1.4.6 FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components.
Dependencies FIA_UAU.1 Timing of authentication

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

[

a) Mask all of characters in a password with “●”

b) No feedback is provided on a reason for the failure if authentication fails except showing a message of “Please check a ID or password again.”.

]

5.1.4.7 FIA_UID.1 Timing of identification

Hierarchical to No other components.
Dependencies No dependencies.

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

[

a) Administrator: none

b) User: Self test, Password reset

]

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security management (FMT)

5.1.5.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to No other components.
Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to ***conduct administrative actions of*** [the following list of functions in Table 22] to [the authorized administrator].

Menu	Management type	Administrative behaviour
Department and User	Management of department	Add, Modify, Delete
	Management of user	Add, Modify, Delete
	Management of group	Add, Modify, Delete
	Self test of ubCUBE ubPortal	Execute
	Self test of ubCUBE Agent	Execute
Policy Management	General master policy	Modify
	Management of policy(Encryption application and document type, Watermarking application, Print-blocked application)	Add, Modify, Delete
	Encryption policy(Excluded path, Decryption)	Add, Modify, Delete
	Document access policy (Target application and document type, Default permission)	Add, Modify, Delete
	Document grade	Add, Modify, Delete
	Document template	Add, Modify, Delete
	Application and document type	Add, Modify, Delete
	Excluded folder path	Add, Modify, Delete
	Watermarking management	Add, Modify, Delete

	Setup information file	Download
Administrator	Management of administrator	Add, Modify, Delete
	Management of administrator group	Add, Modify, Delete
User	Management of user	Search
Cryptographic Key Management	Management of passphrase	Modify
	Management of cryptographic key	Add, Modify
Audit Log	Audit log of administrator	Search
	Audit log of system	Search
	Audit log of document access and usage	Search
	Audit log of security alarm mail	Query
	Management of audit setting	Modify

Table 22 List of management functions

5.1.5.2 FMT_MSA.1 Management of security attributes

Hierarchical to No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [access control SFP] to restrict the ability to *change_default, modify, delete, [add]* the security attributes of [the following] to [the authorized administrator].

[

a) Administrator permission coverage: accessible menu, scope of management

b) Administrator's management access: Allowed IP

c) Document encryption: Application, Document type, Document path

d) Policy of print-blocked and watermarking: Allow/Deny application, Watermarking template

e) Document grade

f) Attribute of document access policy: Target application and document type for document access policy, Default permission for document creator and user, Modification of access permission, Print

]

5.1.5.3 FMT_MSA.3 Static attribute initialization

Hierarchical to No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [access control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

5.1.5.4 FMT_MTD.1 TSF Data management

Hierarchical to No other components.
Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** the [the following list of TSF data in Table 23] to [the authorized administrator].

	TSF data	Administrative behaviour
Security management data	Count of authentication failure	Query, Modify
	Allowed IP for management access	Query, Add, Modify, Delete
	Count of failure of integrity violation and self test	Query, Modify
	Threshold of log trail	Query, Modify
	Maximum size of log data	Query, Modify
	Recipient of security alarm mail	Query, Modify
Authentication data	ID	Query, Modify
	Password	Modify
Administrator permission setting data	-	Query, Add, Modify, Delete
Security policy setting data	Security policy for document	Query, Add, Modify, Delete
	Security policy for permission change	Query, Add, Modify, Delete
	Security policy for print	Query, Add, Modify, Delete
Audit data	Audit log of administrator	Query
	Audit log of access/usage of document	Query
	Audit log of system	Query
	Audit log of security alarm mail	Query
Department and User data	Department data	Query, Add, Modify, Delete
	User data	Query, Add, Modify, Delete
	Group data	Query, Add, Modify, Delete
	ubCUBE ubPortal data	Query
	ubCUBE Agent data	Query
Cryptographic key data	-	Query, Modify

Table 23 List of TSF data

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

Hierarchical to No other components.
Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

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

1. [none]

2. [none]

FMT_PWD.1.2

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

1. [none]
2. [none]

FMT_PWD.1.3

The TSF shall provide the capability for [*changing the password when the authorized administrator accesses for the first time*].

5.1.5.6 FMT_SMF.1 Specification of management functions

Hierarchical to No other components.
Dependencies No dependencies.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
[

a) TSF function management: items specified in FMT_MOF.1
b) TSF security attributes management: items specified in FMT_MSA.1
c) TSF data management: items specified in FMT_MTD.1

]

5.1.5.7 FMT_SMR.1 Security roles

Hierarchical to No other components.
Dependencies FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the role of [the authorized administrator, the authorized user].

FMT_SMR.1.2

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

5.1.6 Protection of the TSF (FPT)

5.1.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to No other components.
Dependencies No dependencies.

FPT_ITT.1.1

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

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

Hierarchical to No other components.
Dependencies No dependencies.

FPT_PST.1.1

The TSF shall protect [cryptographic data, password of administrator and document user, password for device cryptographic key and TOE setting value] stored in containers controlled by the TSF from unauthorized *disclosure, modification*.

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

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_PST.2.1 TSF shall *prevent* the unauthorized deletion for [execution and setting files of ubCUBE Agent, registry keys where stores ubCUBE Agent settings].

FPT_PST.2.2 TSF shall *prevent* the unauthorized termination for [process of ubCUBE Agent].

5.1.6.4 FPT_TST.1 TSF self test

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start up, periodically during normal operation* to demonstrate the correct operation of[*TSF*].

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

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

5.1.7 TOE access (FTA)

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

Hierarchical to	FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies	FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [the number of maximum concurrent sessions as 1 for administrator management access sessions].

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

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

Hierarchical to	No other components.
Dependencies	FIA_UAU.1 Timing of authentication or No dependencies.

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

5.1.7.3 FTA_TSE.1 TOE TOE session establishment

Hierarchical to	No other components.
Dependencies	No dependencies.

FTA_TSE.5.1 The TSF shall be able to deny **administrator's management access session** establishment based on [connection IP, [*none*]].

5.2 Security assurance requirements

Assurance requirements of this Security Target are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

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

Table 24 Security assurance requirements

5.2.1 Security Target evaluation

5.2.1.1 ASE_INT.1 ST introduction

Dependencies No dependencies.

Developer action

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

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

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

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

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

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

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

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

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

Evaluator action elements

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

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

5.2.1.2 ASE_CCL.1 Conformance claims

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

Developer action

ASE_CCL.1.1D Stated security requirements

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

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

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

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

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

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

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

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

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

5.2.1.3 ASE_OBJ.1 Security objectives for the operational environment

Dependencies No dependencies.

Developer action

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

Content and presentation elements

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

Evaluator action elements

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

5.2.1.4 ASE_ECD.1 Extended components definition

Dependencies No dependencies.

Developer action

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

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

Content and presentation elements

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

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

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

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

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

Evaluator action elements

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

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

5.2.1.5 ASE_REQ.1 Stated security requirements

Dependencies ASE_ECD.1 Extended components definition

Developer action

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

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

Content and presentation elements

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

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

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

ASE_REQ.1.4C All operations shall be performed correctly.

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

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

Evaluator action elements

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

5.2.1.6 ASE_TSS.1 TOE summary specification

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

Developer action

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.2 Development

5.2.2.1 ADV_FSP.1 Basic functional specification

Dependencies No dependencies.

Developer action

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

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

Content and presentation elements

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

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

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance documents

5.2.3.1 AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action

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

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that shall be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

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

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

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

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

Evaluator action elements

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

5.2.3.2 AGD_PRE.1 Preparative procedures

Dependencies No dependencies.

Developer action

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

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

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

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

5.2.4 Life-cycle support

5.2.4.1 ALC_CMC.1 Labelling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action

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

Content and presentation elements

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

Evaluator action elements

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

5.2.4.2 ALC_CMS.1 TOE CM coverage

Dependencies No dependencies.

Developer action

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

Content and presentation elements

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

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

Evaluator action elements

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

5.2.5 Tests

5.2.5.1 ATE_FUN.1 Functional testing

Dependencies ATE_COV.1 Evidence of coverage

Developer action

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

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

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

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

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

Evaluator action elements

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

5.2.5.2 ATE_IND.1 Independent testing - conformance

Dependencies ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.6 Vulnerability assessment

5.2.6.1 AVA_VAN.1 Vulnerability survey

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

Developer action

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

Content and presentation elements

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

Evaluator action elements

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

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

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

5.3 Security requirements rationale

5.3.1 Dependency rationale of security functional requirements

The following table shows dependency of security functional requirement.

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	OE.RELIABLE_TIME_STAMP
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	OE.RELIABLE_STORAGE
7	FAU_STG.4	FAU_STG.1	OE.RELIABLE_STORAGE
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[10 or 12] 11
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[10 or 13] 11
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[– or – or 8, 9] 11
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[– or – or 8, 9]
12	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[– or – or 8] 11
13	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[– or – or 9] 11
14	FCS_RBG.1	–	–
15	FDP_ACC.1(1)	FDP_ACF.1	17
16	FDP_ACC.1(2)	FDP_ACF.1	18
17	FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	15 28
18	FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	16 28
19	FIA_AFL.1	FIA_UAU.1	22
20	FIA_IMA.1	–	–
21	FIA_SOS.1	–	–
22	FIA_UAU.1	FIA_UID.1	25
23	FIA_UAU.4	–	–
24	FIA_UAU.7	FIA_UAU.1	22
25	FIA_UID.1	–	–
26	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	31 32
27	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	[15, 16 or –] 31 32
28	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	27 32
29	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	31 32
30	FMT_PWD.1	FMT_SMF.1	31

		FMT_SMR.1	32
31	FMT_SMF.1	–	–
32	FMT_SMR.1	FIA_UID.1	25
33	FPT_ITT.1	–	–
34	FPT_PST.1	–	–
35	FPT_PST.2	–	–
36	FPT_TST.1	–	–
37	FTA_MCS.2	FIA_UID.1	25
38	FTA_SSL.5	FIA_UAU.1	22
39	FTA_TSE.1	–	–

Table 25 Dependency rationale

FAU_GEN.1 has a subordinate relationship with FPT_STM.1. However, as the TOE accurately records security related events using reliable time stamp provided in the TOE operational environment, a subordinate relationship with FAU_GEN.1 is satisfied by the security objectives for OE.RELIABLE_TIME_STAMP instead of FPT_STM.1.

FAU_STG.3 and FAU_STG.4 has a subordinate relationship with FAU_STG.1. However, as the audit trail protects the audit record from unauthorized deletion or modification (DBMS interacting with the TOE in the TOE operational environment), a subordinate relationship with FAU_STG.3 and FAU_STG.4 is satisfied by the security objectives for OE.RELIABLE_STORAGE instead of FAU_STG.1.

5.3.2 Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

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

6 TOE summary specification

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

6.1 TOE security functions

This chapter describes the security functions provided by the TOE and how the security functions of ubCUBE v3.7 satisfy all the security requirements specified in Chapter 5.

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

6.1.1 Security audit

TOE performs the following functions of security audit.

- Audit data generation
- View and search audit data
- Protection of audit data

6.1.1.1 Audit data generation

Audit data generation is a function which creates and stores audit logs regarding the events incurred from the security functions of the TOE. The audit logs are created and stored as classified into the following three categories. The document encryption and use log can be selectively collected depending on the access and use type such as document creation, document open, change permission, and document print. In addition, the TOE records an audit log and notifies the administrator by email if a potential security violation occurs.

Type of audit records	Description
Administrator audit log	Audit logs regarding changes of security policies and management of user/department performed by the administrator during ececution of security management functions.
Document encryption and use log	Audit logs regarding open, edit, print, etc on secured document performed on document user's PC.
System access log	Audit logs regarding start-up and shutdown of the ubCUBE ubPortal, cryptographic key generation, potential violations including authentication failure, integrity violation, self test failure, audit trail threshold exceeds and saturation and, etc.

Table 26 Type of audit data generation

SFR Mapping
FAU_SAA.1, FAU_ARP.1, FAU_GEN.1

6.1.1.2 View and search audit data

The TOE provides a function to view the stored audit data to the authorized administrator. The administrator can search administrator audit log, document encryption and use log, and system access log by AND operation and combination of search conditions including ID, IP address, audit type, result.

SFR Mapping
FAU_SAR.1, FAU_SAR.3

6.1.1.3 Protection of audit data

The TOE provides a function to manage a threshold per administrator audit log, document encryption/use log, system access log and notifies the administrator by email if the audit trail exceeds the threshold. The TOE overwrites the oldest stored audit records if the audit trail is full and notifies the administrator by email.

SFR Mapping
FAU_STG.3, FAU_STG.4

6.1.2 Cryptographic support

TOE performs the following functions of cryptographic support.

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

6.1.2.1 Cryptographic key generation

The TOE generates cryptographic keys for document and TSF data encryption, the information for purpose of cryptographic keys is as follows.

List of standards	Cryptographic algorithm	Cryptographic key size	Purpose
ISO/IEC 18031	Hash_DRBG (SHA-256)	256bit	Document encryption DEK
ISO/IEC 18031	Hash_DRBG (SHA-256)	256bit	TSF data encryption DEK
NIST 800-132	KDF	256bit	TSF data encryption KEK

Table 27 Information of cryptographic key

SFR Mapping
FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1

6.1.2.2 Cryptographic key distribution

The TOE performs mutual authentication between TOE components with the internally implemented authentication protocol and then distributes cryptographic key with the process that is safe from cryptographic attacks including MITM(Man In the Middle) attack, etc.

List of standards	Cryptographic algorithm	Cryptographic key size	Purpose
ISO/IEC 18033-2	Public key cryptographic method	RSAES-OAEP	3072bit

Table 28 Cryptographic key distribution

SFR Mapping
FCS_CKM.1(2), FCS_CKM.2, FIA_IMA.1

6.1.2.3 Cryptographic operation and key destruction

TOE performs cryptographic operations for document encryption and TSF data, cryptographic key is securely destructed with zerorization in memory after use. The information for cryptographic operations is as follow.

List of standards	Cryptographic algorithm	Cryptographic key size	Purpose
KS X 1213	ARIA-CBC	256bit	Encryption/decryption of electronic documents
KS X 1213	ARIA-CBC	256bit	Encryption/decryption of TSF data
ISO/IEC 18033-2	RSAES-OAEP	3072bit	1) Mutual authentication between ubCUBE ubPortal & ubCUBE Agent 2) Encryption/decryption for policy and DEK distribution
ISO/IEC 14888-2	RSA-PSS	3072bit	Digital signature of policy data
ISO/IEC 9797-2	HMAC (SHA-256)	256bits	Verification of TSF data integrity
ISO/IEC 10118-3	SHA-256	N/A	Encryption of authentication data

Table 29 Cryptographic key for document and TSF data encryption

SFR Mapping
FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2)

6.1.2.4 Random bit generation

The TOE generates a cryptographic key with the following random bit generator.

List of standards	Cryptographic algorithm	Cryptographic key size	Purpose
ISO/IEC 18031	Hash_DRBG (SHA-256)	256bit	Cryptographic key generation

Table 30 Information of random bit generator

SFR Mapping
FCS_RBG.1

The following table shows the information of validated cryptographic module used for cryptographic support function performed by the TOE.

Cryptographic Module & Version	Validation number	Date	Developer
ubXFS Cryptographic Module V1.1	CM-195-2026.11	2021-11-18	Iqpad, Inc.

Table 31 Information of validated cryptographic module

6.1.3 User data protection

TOE performs the following functions of user data protection.

- Electronic Document Encryption access control
- Electronic Document Use access control

6.1.3.1 Electronic Document Encryption access control

The authorized administrator and user can set access permissions for encryption/decryption of secured document and related policy, the access of user on secured document is controlled according to security policy set by the administrator and user. The TOE performs the access control for encryption/decryption on the secured document based on the security attributes of the user(User ID, Department, Group) and the security attributes of the document(Document grade, Owner ID, Permission per user/department/group).

SFR Mapping
FDP_ACC.1(1), FDP_ACF.1(1)

6.1.3.2 Electronic Document Use access control

The authorized administrator and user can set access permissions for document use(Expiration date, Modification of permissions, Print) of secured document, the access of user on the secured document is controlled according to security policy set by the administrator and user. The TOE performs the access control for use on the secured document based on the security attributes of user(User ID, Department, Group) and the security attributes of document(Document grade, Owner ID, Permission per user/department/group).

SFR Mapping
FDP_ACC.1(2), FDP_ACF.1(2)

6.1.4 Identification and authentication

TOE performs the following functions of identification and authentication.

- Administrator identification and authentication
- User identification and authentication
- TOE Internal mutual authentication

6.1.4.1 Administrator identification and authentication

The authentication data for administrator identification with default value is generated when the TOE is being installed, authentication data is stored to the DBMS with encryption(SHA-256). After that, the administrator shall change the default password on access for the first time.

No action can be performed before the administrator is identified and authenticated. The input characters of password masked with "●" are shown in a screen, no feedback is provided on a reason for the failure if authentication fails. When the defined number(1~5) set by the administrator of unsuccessful authentication attempts has been met, the account is locked out.

Password is set by combination of each of alphabetical, numerical, and special characters and the length is at least 9 digits and less than 30 digits. The allowed characters are as follows.

1) Alphabetical characters(case sensitive): a-z, A-Z
2) Numerical characters: 0-9
3) Special characters: !@#$%^&*+=-

SFR Mapping
FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FMT_PWD.1

6.1.4.2 User identification and authentication

The system(global) policy is applied to the user before user authentication and a policy set for the authorized user is applied after user authentication.

The TOE performs mutual authentication between TOE components with the internally implemented authentication protocol before user authentication. The TOE provides authentication based on ID and password, the input characters of password masked with "●" are shown in a screen, no feedback is provided on a reason for the failure if authentication fails. When the defined number(1~5) set by the administrator of unsuccessful authentication attempts has been met, the account is locked out.

ID and encrypted(SHA-256) password are transmitted to the server for authentication processing and reuse of authentication data is prevented with time stamp.

SFR Mapping
FIA_AFL.1, FIA_IMA.1, SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1

6.1.4.3 TOE Internal mutual authentication

The TOE performs mutual authentication between the ubCUBE ubPortal and ubCUBE Agent with the internally implemented authentication protocol.

SFR Mapping
FIA_IMA.1

6.1.5 Security management

TOE performs the following functions of security management.

- Common management

- Management of policy for document encrypton and use

6.1.5.1 Common management

The TOE provides management function of common management including department and user, administrator, cryptographic key, audit logs, etc to the authorized administrator.

6.1.5.2 Management of policy for document encrypton and use

The TOE provides management function of policy per department and user for document encryption and use to the authorized administrator.

A policy for document encryption can be set based on target application, document type, and document path. A policy for document access including modification of access permission and print can be set based on document grade and per user/department/group.

SFR Mapping
FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.1.6 Protection of the TSF

TOE performs the following functions of protection of the TSF.

- Protection of the TSF data
- TSF self test

6.1.6.1 Protection of the TSF data

The TOE protects transmitted data between TOE components with confidentiality(ARIA-CBC, 256bit) and integrity(RSA-PSS, 3072bit) of a validated cryptographic module. The following table shows the type of TSF data that is stored in the repository controlled by the TSF and how it is protected.

TOE component	TSF data	Protection method
ubCUBE ubPortal	Cryptographic key	ARIA-CBC, 256bit RSAES-OAEP, 3072bit
	Password	SHA-256
ubCUBE Agent	Cryptographic key	ARIA-CBC, 256bit RSAES-OAEP, 3072bit
	Password	SHA-256
	Policy file	ARIA-CBC, 256bit

Table 32 Type of TSF data and protection method

SFR Mapping
FPT_ITT.1, FPT_PST.1, FPT_PST.2

6.1.6.2 TSF self test

The TOE runs a suite of self tests during initial start-up, periodically during normal operation and checks integrity violation with HMAC (SHA-256). The TOE notifies the administrator modified TSF data or information of executable file by email if integrity violation is detected.

SFR Mapping

FPT_TST.1

6.1.7 TOE access

TOE performs the following functions of TOE access.

- Session management

6.1.7.1 Session management

The TOE provides a management function to register IP addresses that are allowed for management access and performs an access control function that management access is allowed only from a registered IP address. The TOE also restricts the number of maximum concurrent sessions belonging to the same user and write permission as 1. The TOE terminates an existing session if concurrent session with the same write permission is connected.

The TOE terminates an interactive session of the authorized administrator after 5 minutes of inactivity.

SFR Mapping
FTA_MCS.2, FTA_SSL.5, FTA_TSE.1

7 References

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
- Korean National Protection Profile for Electronic Document Encryption V1.1, 2019.12.11, ITSCC