Korean National

Protection Profile for Electronic Document Encryption V1.0

2017. 8. 18

국가보안기술연구소
National Security Research Institute

The certified Protection Profile is written in Korean. This document is a translation of the original from Korean into English.

Foreword

This Protection Profile has been developed with the support of National Security Research Institute (NSR) under the agreement between National Intelligence Service (NIS) and Ministry of Science and ICT (MSIT). The Protection Profile author developed the security requirement for electronic document encryption in conformity with the Common Criteria. and The NIS offered advise for the accurate interpretation of those national security requirements. The Protection Profile includes application notes which give the additional interpretation and guidance for the evaluation and certification based on the Common Criteria, and the separated guidance supporting document (Korean only) for the Protection Profile is provided.

Revision History

Version	Date	Content
1.0	2017.08.18	o First Issue

Table of Contents

1. PP introduction

1.1. PP reference

Title	Korean National Protection Profile for Electronic Document Encryption
Version	1.0
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Developer	National Security Research Institute, Telecommunications Technology Association
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	CC Version 3.1, Revision 5
Certification Number	KECS-PP-0821-2017
Keywords	Document, Encryption

1.2. TOE overview

1.2.1. Electronic Document Encryption overview

'Electronic Document Encryption' (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 must use a validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP). In addition, the encryption/decryption of the CSP (Critical Security Parameters) used by the TOE and cryptographic key management function shall use the approved cryptographic algorithm of the validated cryptographic module that security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

1.2.2. TOE type and scope

The TOE defined by this protection profile is “Electronic Document Encryption” that prevents an information leakage by encrypting/decrypting important documents within the organization and is provided as software. The TOE can be classified into “user device encryption” type or “information system encryption” type depending on the operation type, and both types can be supported.

The management server and agent are the indispensable TOE components that perform the security features defined in this PP for the user device encryption type, or the management server, agent, and API module for the information system encryption type. The management console can be included in the TOE component as an option. In this case, the ST author shall identify all TOE components in the ST. All TOE components shall be integrated with the validated cryptographic module.

Software that provides encryption/decryption capabilities which are the primary security functions of the TOE with assistance of the those capabilities of commercialized 3rd-party product (e.g., document editor that provides the encryption/decryption function, file encryption product, etc.) is not considered as a TOE defined in this PP.

This protection profile defines the common minimum security requirements that shall be provided by the indispensable TOE components for “Electronic Document Encryption~~,~~” and the TOE shall provide the security features.

The PP is written to reflect the TOE implemented in various ways. If the additional TOE component (e.g., management console) provides the security or additional function, the optional security functional requirement shall be applied. For example, the security management function of the TOE can be implemented in various ways, such as communication between the TOE component (management console) and management server, communication between the web browser of the administrator PC and the TOE component (management server), or communication between the web browser of the administrator PC and the operational environment of the management server (web server). The mandatory security functional requirements or optional security functional requirements shall be applied depending on each implementation.

1.2.3. 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 by 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.

In addition, the TOE can implement the function of testing the TOE's external entity if necessary, and it can also implement the trusted path/channel function that provides secure communication between the TOE and authorized administrator.

The document encryption/decryption and cryptographic key management function can be implemented in various ways; the general procedure is as follows.

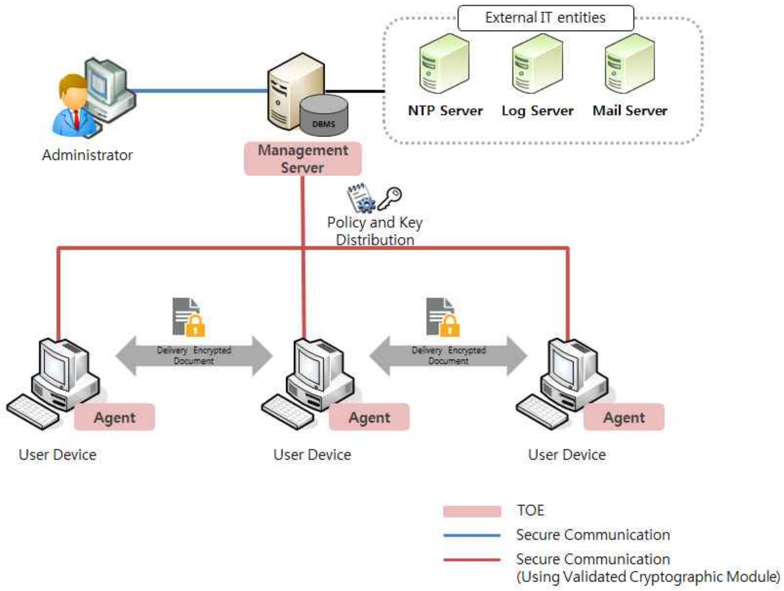
The data encryption key (hereinafter referred to as "DEK") and key encryption key (hereinafter referred to as "KEK") can be used for the document encryption/decryption function. The main body of the protected document is encrypted with the DEK according to the policy set by the administrator, and DEK is stored in the header of the security document. When the DEK is stored in the header, it is encrypted with the KEK.

The management server generates the DEK and KEK and distributes them to the agent and API module. At this time, the cryptographic key shall be distributed safely. The agent or API module encrypts the main body of the protected document and decrypts the encrypted main body using the cryptographic key. The cryptographic key like the DEK and KEK can be used by the symmetric or asymmetric key method. The KEK can be issued as a private key to a person, or a common group key for a group. The management server, agent, or API module shall provide 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 management server, and assign the document access right to the document user. Only the authorized document user can encrypt/decrypt the document, as the management server distributes a cryptographic key to the document user according to policy configured.

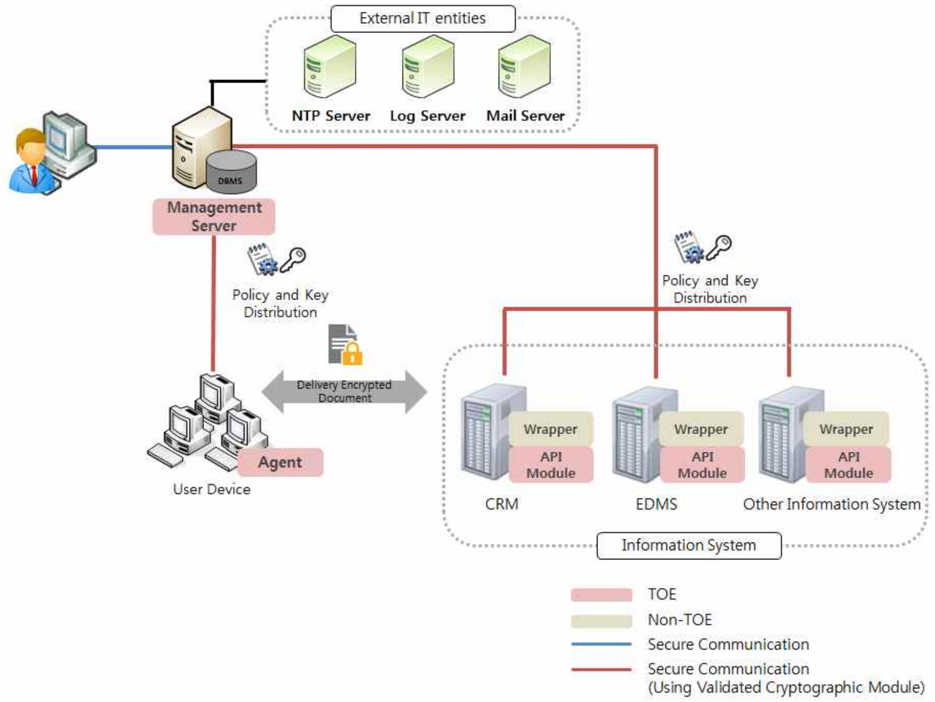
1.2.4. Non-TOE and TOE operational environment

The TOE operational environment defined by this protection profile can be classified into "user device encryption" type or "information system encryption" type.



[Figure 1] Operational environment of "user device encryption" type

[Figure 1] shows the operational environment of the “user device encryption” type. In the “user device encryption” type, the TOE can be composed of management server which manages the security policy and cryptographic key, and the agent that performs Electronic Document encryption/decryption installed in the user device. The administrator sets the policy for each document user through the management server, and the management server distributes the policy and cryptographic key configured by the administrator to the agents. The agent installed in the user device performs document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted/decrypted document is stored as a file in the user device.



[Figure 2] Operational environment of “Information system encryption” type

[Figure 2] shows the operational environment of the “information system encryption” type. In the “information system encryption” type, the TOE can be composed of management server which manages the security policy and cryptographic key, agent that performs Electronic Document encryption/decryption installed in the user device, and the API module that performs Electronic Document encryption/decryption installed in the information system in the form of API module. The administrator sets the policy for each document user or information system through the administration server, which distributes the policy and cryptographic key configured by the administrator to the agent and API module. The agent and API module perform Electronic Document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted/decrypted document is stored in the user device or information system as a file. Transferring an encrypted document is not included in the scope of this protection profile. A wrapper can be used for compatibility between the TOE and various information systems in the “information system encryption type” operational environment, but it is excluded from the scope of the TOE.

The encryption/decryption function, which is used to transfer the document to the external organization in which the agent is not installed, is not included in the scope of this PP.

The validated cryptographic module shall be used for all cryptographic operation of all security features including the primary security features in the user device encryption type and information system encryption type. The use of OpenSSL etc. that implements the security protocol, however, is allowed only when communication is needed between the administrator and the TOE component (e.g., the administrator accesses the management server using the web browser to configure policies).

There may exist various external entities necessary for the operation of the TOE, including the NTP server to synchronize time, log server to store the audit data outside and manage the audit data, and email server to notify the authorized administrator in case of audit data loss. The ST of the TOE that claims conformance to this PP shall identify all external entities that interact with the TOE.

The others such as the NTP server, log server, and email server except for the TOE correspond to the TOE operational environment. In addition, the part that is not related to a security functional requirement (hereinafter referred to as "SFR"), e.g., the function that is irrelevant to the TOE security functionality, can be classified into the non-TSF of the TOE with consideration for the physical scope of the TOE.

The ST author must have the optional security functional requirement defined in this PP, if the following conditions are met.

- If the authorized administrator or general user accesses the management server directly using the web browser or terminal connection program, FTP_TRP.1 shall be included. If they access the SSO server via the web server, FTP_TRP.1 and FTP_ITC.1 shall be included. If direct communication between the management console and SSO server is implemented, FPT_ITT.1 shall be included. However, one of the SFR (FTP_TRP.1, FPT_ITT.1) must be included.
- The ST author shall include FPT_TEE.1 in the ST if there is an external entity that interact with the TOE and the major and security features of the TOE are affected by the abnormal state of an external entity (e.g., error, shutdown, etc.).

The optional security functional requirements except for the above, can be selectively included in the ST if the TOE provides the security features that implements the pertinent security functional requirements. The ST author shall pay attention not to omit the security functional requirements for the security features provided by the TOE by referring to the application notes with regard to the applicability of the optional security functional requirements.

This PP has been developed considering various types of the TOE implementation. The ST author, which claims conformance to this PP, shall describe any non-TOE hardware, software or firmware required by the TOE to operate. In particular, if the document encryption function is implementation-dependent upon the document processing program, it must be described as software.

1.3. Conventions

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

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

Iteration

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

Assignment

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

Selection

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

Refinement

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

Security Target (ST) Author

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

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

1.4. Terms and definitions

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

Access Control List (ACL)

The list including entities who are permitted to access the entity and the types of these permission

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.

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

Approved mode of operation

The mode of cryptographic module using approved cryptographic algorithm

Assets

Entities that the owner of the TOE presumably places value upon

Assignment

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

Attack potential

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

Augmentation

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

Authentication Data

Information used to verify the claimed identity of a user

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

Can/could

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

Class

Set of CC families that share a common focus

Component

Smallest selectable set of elements on which requirements may be based

Critical Security Parameter (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)

Data Encryption Key (DEK)

Key that encrypts the data

Decryption

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

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

Element

Indivisible statement of a security need

Encryption

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

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

External Entity

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

Family

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

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

Public Security Parameter (PSP)

Security related public information whose modification can compromise the security of a cryptographic module

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.

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

Refinement

Addition of details to a component

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

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

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 Target (ST)

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

Security Token

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

Selection

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

Self-test

Pre-operational or conditional test executed by the cryptographic module

Sensitive Security Parameters (SSP)

Critical security parameter (CSP) and public security parameter (PSP)

Shall/must

The 'shall' or 'must' presented in Application notes indicates mandatory requirements applied to the TOE

SSL (Secure Sockets Layer)

This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network

Subject

Active entity in the TOE that performs operations on objects

Symmetric cryptographic technique

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

Target of Evaluation (TOE)

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

Threat Agent

Entity that can adversely act on assets

TLS (Transport Layer Security)

This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246

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

Unapproved mode of operation

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

User

See “external entity”, a user means authorized administrator and authorized document user

Validated Cryptographic Module

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

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.)

Wrapper

Interface to connect the TOE with various types of information system

1.5. PP organization

Chapter 1 introduces to the Protection Profile, providing Protection Profile references and the TOE overview.

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

Chapter 3 describes the security objectives for the operational environment.

Chapter 4 defines the extended components for the Electronic document encryption.

Chapter 5 describes the security functional and assurance requirements. If required, Application notes are provided to clarify the meaning of requirements and provide an explanation of detailed guidelines to the ST author for correct operations.

Reference describes the references for users who need more information about the background and related information than those described in this PP.

Abbreviated terms are listed to define frequently used terms in the PP.

2. Conformance claim

2.1. CC conformance claim

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)
Conformance claim	Part 2 Security functional components	Extended : FCS_RBG.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2, FPT_TUD.1, FTA_SSL.5
	Part 3 Security assurance components	*Conformant*
	Package	Augmented : EAL1 augmented(ATE_FUN.1)

2.2. PP conformance claim

This Protection Profile does not claim conformance to other PPs.

2.3. Package conformance claim

This Protection Profile claims conformance to assurance package EAL1 augmented with ATE_FUN.1.

2.4. Conformance claim rationale

Since this Protection Profile does not claim conformance to other Protection Profiles, it is not necessary to describe the conformance claim rationale.

2.5. PP conformance statement

This Protection Profile requires “strict PP conformance” of any ST or PP, which claims conformance to this PP. In addition, the security target complying with this protection profile can perform evaluation as “low assurance level security target” only.

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

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_RE-INFORCEMENT

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.

Application notes

o Depending on the implementation type of the TOE, the TOE components(agent, API module, management server) may not use the operating system independently, so care shall be taken that the operating system related settings of other external IT entities operating in the same operating system do not affect the secure operation of the TOE.

OE.SECURE_DEVELOPMENT

The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

Application notes

o The security objectives for the operational environment is applied when wrapper is used for the compatibility between API module as the components of TOE and information system in the operational environment of ‘Information system encryption‘.

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*].

Application notes

o If the TOE does not provide the capability for managing the ID and password combination rules by authorized roles, etc., 'None.' may be specified in assignment operations of FMT_PWD.1.1, FMT_PWD.1.2.

o The ID and password combination rules that can be set by authorized roles may include minimum and maximum length setting, mixing rule setting involving English upper case/lower case/number/special characters, etc.

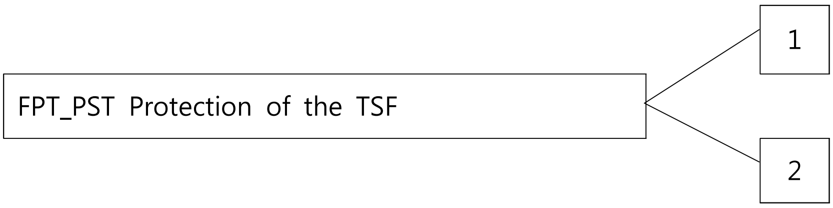
4.4. Protection of the TSF

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.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.
FPT_PST.2 Availability protection of TSF data requires the TSF to ensure the defined levels of availability for the TSF data.

Management: FPT_PST.1, FPT_PST.2

There are no management activities foreseen.

Audit: FPT_PST.1, FPT_PST.2

There are no auditable events foreseen.

4.4.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized [selection: *disclosure, modification*].

Application notes

o Containers controlled by the TSF mean storage in the TOE or external entities (DBMS, etc.)that interact with the TOE.

o Examples of TSF data to be protected as follows:

- User password, cryptographic key (pre-shared key, symmetric key, private key, etc), TOE configuration values (security policy, configuration parameters), audit data, etc.

o The TSF data can be encrypted and stored to be protected from the unauthorized disclosure or modification.

4.4.1.2. FPT_PST.2 Availability protection of TSF data

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_PST.2.1 The TSF shall [selection: *detect, prevent*] the unauthorized deletion for [assignment: *TSF data*].

FPT_PST.2.2 The TSF shall [selection: *detect, prevent*] the unauthorized termination for [assignment: *TSF data*].

Application notes

o Availability protection of TSF data includes cryptographic keys, TOE configuration values, execution files, and so on.

4.4.2. TSF update

Family Behaviour

This family defines TOE firmware/software update requirements.

Component leveling

FPT_TUD.1 TSF security patch update, requires trusted update of the TOE firmware/software including the capability to verify the validity on the update file before installing updates.

Management: FPT_TUD.1

The following actions could be considered for the management functions in FMT:
a) Management of update file verification mechanism

Audit: FPT_TUD.1

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

a) Minimal: Update file verification result (success, failure)

4.4.2.1. FPT_TUD.1 TSF security patch update

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [assignment: *the authorized identified roles*].

FPT_TUD.1.2 The TSF shall verify validity of the update files using [selection: *hash value comparison, digital signature verification*] before installing updates.

Application notes

o The TSF shall provide the capability to check the current version of the TOE that most recently installed and executed by authorized roles.

o The latest updates and security patches are essential to remove security vulnerabilities. The validity verification on the update files is required since the installation of update files without any verification can result in system malfunction, or service failures, etc.

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

FTA_SSL Session locking and termination
1
2
3
4
5

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 termination for each user

b) Specification for the time interval of default user inactivity that is occurred the session locking 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.]

FTA_SSL.5.1 The TSF shall [selection:

- *lock the session and re-authenticate the user before unlocking the session,*
- *terminate*] an interactive session after a [assignment: *time interval of user inactivity*].

Application notes

o This requirement can be applied to the management access of administrator (SSH, HTTPS, etc.).

5. Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to this PP.

The security functional requirements included in this PP are derived from CC Part 2 and Chapter 4 Extended Components Definition.

In addition, the security functional requirements are classified into mandatory SFRs and optional SFRs, as follows.

- Mandatory SFRs: are required to be mandatorily implemented in the 'Electronic Document Encryption'
- Optional SFRs: are not required to be mandatorily implemented in 'Electronic Document Encryption'. However, when the TOE additionally provides related capabilities, the ST author must include the corresponding SFRs.

The following table summarizes the security functional requirements used in the PP.

Security functional class	**Security functional component**		**Mandatory SFR / Optional SFR**
FAU	FAU_ARP.1	Security alarms	**Mandatory SFR**
	FAU_GEN.1	Audit data generation	**Mandatory SFR**
	FAU_SAA.1	Potential violation analysis	**Mandatory SFR**
	FAU_SAR.1	Audit review	**Mandatory SFR**
	FAU_SAR.3	Selectable audit review	**Mandatory SFR**
	FAU_SEL.1	Selective audit	Optional SFR
	FAU_STG.1	Protected audit trail storage	Optional SFR
	FAU_STG.3	Action in case of possible audit data loss	**Mandatory SFR**
	FAU_STG.4	Prevention of audit data loss	**Mandatory SFR**
FCS	FCS_CKM.1(1)	Cryptographic key generation (Electronic Document Encryption)	**Mandatory SFR**
	FCS_CKM.1(2)	Cryptographic key generation (TSF Data Encryption)	**Mandatory SFR**
	FCS_CKM.2	Cryptographic key distribution	**Mandatory SFR**
	FCS_CKM.4	Cryptographic key destruction	**Mandatory SFR**
	FCS_COP.1(1)	Cryptographic operation (Electronic Document Encryption)	**Mandatory SFR**
	FCS_COP.1(2)	Cryptographic operation (TSF Data Encryption)	**Mandatory SFR**

Security functional class	**Security functional component**		**Mandatory SFR / Optional SFR**
	FCS_RBG.1(Extended)	Random bit generation	**Mandatory SFR**
FDP	FDP_ACC.1(1)	Subset access control (Electronic Document Encryption access control)	**Mandatory SFR**
	FDP_ACC.1(2)	Subset access control	Optional SFR
	FDP_ACF.1(1)	Security attribute based access control (Electronic Document Encryption access control)	**Mandatory SFR**
	FDP_ACF.1(2)	Security attribute based access control	Optional SFR
FIA	FIA_AFL.1	Authentication failure handling	**Mandatory SFR**
	FIA_IMA.1(Extended)	TOE Internal mutual authentication	**Mandatory SFR**
	FIA_SOS.1	Verification of secrets	**Mandatory SFR**
	FIA_UAU.1	Timing of authentication	**Mandatory SFR**
	FIA_UAU.4	Single-use authentication mechanisms	**Mandatory SFR**
	FIA_UAU.7	Protected authentication feedback	**Mandatory SFR**
	FIA_UID.1	Timing of identification	**Mandatory SFR**
FMT	FMT_MOF.1	Management of security functions behaviour	**Mandatory SFR**
	FMT_MSA.1	Management of security attributes	**Mandatory SFR**
	FMT_MSA.3	Static attribute initialization	**Mandatory SFR**
	FMT_MTD.1	Management of TSF data	**Mandatory SFR**
	FMT_PWD.1(Extended)	Management of ID and password	**Mandatory SFR**
	FMT_SMF.1	Specification of management functions	**Mandatory SFR**
	FMT_SMR.1	Security roles	**Mandatory SFR**
FPT	FPT_ITT.1	Basic internal TSF data transfer protection	**Mandatory SFR**
	FPT_PST.1(Extended)	Basic protection of stored TSF data	**Mandatory SFR**
	FPT_PST.2(Extended)	Availability protection of TSF data	**Mandatory SFR**
	FPT_STM.1	Reliable time stamps	Optional SFR
	FPT_TEE.1	Testing of external entities	Optional SFR
	FPT_TST.1	TSF testing	**Mandatory SFR**
	FPT_TUD.1(Extended)	TSF security patch update	Optional SFR
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	**Mandatory SFR**
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions	**Mandatory SFR**
	FTA_TSE.1	TOE session establishment	**Mandatory SFR**

Security functional class	Security functional component		Mandatory SFR / Optional SFR
FTP	FTP_ITC.1	Inter-TSF trusted channel	Optional SFR
	FTP_TRP.1	Trusted path	Optional SFR

[Table 1] Security functional requirements

5.1. Security functional requirements (Mandatory SFRs)

The Electronic Document Encryption that claims conformance to this PP must meet the following 'Mandatory SFRs'.

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation (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_ACF.1(1)	Security attribute based access control (Electronic Document Encryption access control)
FIA	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication

Security functional class	Security functional component	
	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 2] Mandatory 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 [assignment: *list of actions*] upon detection of a potential security violation.

Application notes

- o It may be specified sending an alarm message to the authorized administrator, etc. in [assignment: *list of actions*]

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 3] Audit events, [assignment: *other specifically defined auditable events]*].

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

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

a) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Refer to the contents of "additional audit record" in [Table 3] Audit events, [assignment: *other audit relevant information*]].

Application notes

- o The ST author shall perform assignment operation of FAU_GEN.1.1 with the audit records supported by the TOE using following table. But, it is strongly recommended to record audit data of critical events related to the operation of the TOE security functionality.
- o If the audit function is working as a part of the major process in the TOE, 'start-up' of the audit function may be recorded within the audit record which is the start-up of major processes after the initial start-up of the TOE. 'Shutdown' of the audit function may be replaced with the function-level event similar to 'start-up' (e.g., audit records of process termination, etc.) or lower-level event (e.g., audit records of device shutdown, etc.).
- o The audit records shall include the date and time of the event, type of event, subject identity (e.g., account, connection IP, etc.), and the details of major event and outcome (success or failure) in detail.
- o If the TSF synchronizes the reliable time information of the external entities (e.g., reliable NTP server), the audit record related to time changes shall be stored.
- o If the TOE includes a management console or client, the ST author shall include audit events that the management console or client shall support in the auditable events defined in FAU_GEN.1.1. It is recommended that major events related to the operation of the security functions of the TOE should be included in the auditable events and should be recorded as audit data.

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, Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_CKM.1(2)	Success and failure of the activity	
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 identification information
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	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	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	

Security functional component	Auditable event	Additional audit record
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5	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	
FTP_TRP.1	Failures of the trusted path functions Identification of the user associated with all trusted path failures, if available	

[Table 3] 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 [assignment: *subset of defined auditable events*] known to indicate a potential security violation;
b) [assignment: *any other rules*].

Application notes

o The events of potential security violation in FAU_SAA.1.2 must include following information:

- An auditable event of authentication failure in FIA_UAU.1
- Auditable events of integrity violation and self-test failure of the validated cryptographic module, etc. in FPT_TST.1, etc.

o If the TOE includes a client, the ST author shall include the following audit events for the client in the auditable events defined in FAU_GEN.1.1.

- Auditable events of integrity violation and self-test failure of the validated cryptographic module, etc. in FPT_TST.1, etc.

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 [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

Application notes

- o Selective audit review based on logical relationships such as AND and OR, etc. shall be available.
- o The audit data viewing ability that applies the sorting or ordering method on retrieved results can be provided.

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 [Notification to the authorized administrator, [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*]].

Application notes

o The capability to notify that the amount of the audit trail exceeds the certain limit of disk capacity shall be provided for the administrator.

- Method (e.g. alarms, sending the e-mails to the administrator etc.)
- Threshold information (e.g., 80%, 90%, etc.)

o In case of possible audit data loss, the capability that audit records are transmitted to the external log server and backup server may be provided as a response action of the authorized administrator. When this capability is provided with secure communication, refer to 'Optional SFR' FTP_ITC.1 for more details.

o In case where this security functional requirement cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support actions to be taken in case of possible audit data loss.

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 [selection: *choose one of: "ignore audited events", "prevent audited events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

Application notes

o If audit storage is full, actions(e.g., overwrite the old stored audit records) shall be taken to prevent the loss of audit data. Also, in case where this SFR cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support prevention of the audit data loss.

5.1.2. Cryptographic support

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 [assignment: *cryptographic key* *generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application notes

- o This SFR refers to the cryptographic key generation requirement related to 'FCS_COP.1(1) Cryptographic operation (the electronic document encryption)'. If there are more than two cryptographic key generation algorithms in the list, it is recommended to perform repetitive iteration operation on this SFR.
- o A cryptographic key must be created using the TOE cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).
- o Generating an cryptographic key by deriving it from the password is not allowed and the cryptographic key generation method with a random number shall satisfy the requirements in FCS_RBG.1.
- o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.

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 [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application notes

- o This SFR refers to the cryptographic key generation requirement related to 'FCS_COP.1(2) Cryptographic operation (TSF data encryption)'. If there are more than two cryptographic key generation algorithms in the list, it is recommended to perform repetitive iteration operation on this SFR.
- o A cryptographic key must be created using the TOE cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).
- o The cryptographic algorithm and cryptographic key sizes are recommended to meet the

cryptographic complexity of 112 bits or more.

o Generating an encryption key by deriving it from the password is not allowed, except the key encryption key (KEK).

o When generating an key encryption key (KEK) by deriving it from the password, the safe method presented by TTAK.KO-12.0274, NIST SP 800-132, PKCS#5 shall be used. In addition, if random numbers are used to create an encryption key, it shall satisfy the requirements in FCS_RBG.1.

- When generating an cryptographic key by deriving it from the password, a verified cryptographic algorithm like HMAC-SHA2 shall be used as a pseudo random function according to the TTAK.KO-12.0274 document. In addition, at least 128-bit random value shall be used as salt value, and at least 1,000 shall be used as iteration count.

o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.

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 destruct cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application notes

o The key distributed by the cryptographic key distribution method defined in FCS_CKM.2.1 must be related to the key generated by FCS_CKM.1.1.

o If the cryptographic key distribution method is used, the validated cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be applied.

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 a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application notes

- o The SFR shall be applied to all cryptographic keys covered in FCS_CKM.1(1) and FCS_CKM.1(2).
- o When the cryptographic keys, critical security parameters, etc. being loaded on the memory are no longer used, plaintext type cryptographic key and CSP must be deleted.
- o If the TOE is terminated, cryptographic keys and key materials loaded onto memory shall be deleted.
- o Since the API method performs the encryption/decryption of important data at the application program server side by developing (or modifying) an application program for the purchaser, the application program (e.g., WAS) developer shall satisfy this requirement when implementing the application program using this information. Therefore, the API-type database encryption product shall describe the information above as notes in the product manual.

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 [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application notes

- o This SFR is the security functional requirement related to cryptographic operation required by 'FDP_ACC.1, FDP_ACF.1',. The ST author shall include all information related to the User Data Encryption function provided by the TOE in this SFR. If cryptographic algorithm or cryptographic operation has more than 2 types, it is recommended to perform iteration operation on this SFR.

o Cryptographic operation shall be performed using the approved cryptographic algorithm of the validated cryptographic module of which safety and implementation conformities are validated using the Korea Cryptographic Module Validation Process (KCMVP). When performing cryptographic operation, the validated cryptographic module must run in the approved mode of operation.

o The cryptographic algorithm and cryptographic key sizes shall meet the cryptographic complexity of 112 bits or more.

o When performing encryption using the block cipher algorithm, ECB mode cannot be used if the size of plain text is more than one block.

o The use of IV in CBC, CFB, and OFB mode and the use of the counter in CTR mode shall follow the method presented in the Appendix of NIST SP 800-38A.

o The cryptographic key generation function used for the cryptographic operation function of this SFR shall satisfy the requirements in 'FCS_CKM.1(1) Cryptographic key generation (Electronic Document Encryption)'

o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.

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 [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application notes

o This SFR is the security functional requirement related to cryptographic operation required by FIA_IMA.1 TOE internal mutual authentication, FPT_ITT.1 Basic internal TSF data transfer protection, and FPT_PST.1 Basic protection of the stored TSF data. If cryptographic or cryptographic operation has more than 2 types, it is recommended to perform iteration operation on this SFR.

o A cryptographic key must be created using the TOE cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

o The cryptographic algorithm and cryptographic key sizes are recommended to meet the cryptographic complexity of 112 bits or more.

- o When performing encryption using the block cipher algorithm, ECB mode cannot be used if the size of plain text is more than one block.
- o The use of IV in CBC, CFB, and OFB mode and the use of the counter in CTR mode shall follow the method presented in the Appendix of NIST SP 800-38A.
- o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.

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 required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

Application notes

- o Random bit generator whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be used and the entropy of seed value in generating random numbers must be 2^{112} or higher.

5.1.3. User data protection

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

FDP_ACC.1.1 TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by SFP*].

Application notes

- o This SFR specifies the requirement related to access control by encrypting/decrypting a document to be protected; the ST author is recommended to perform iteration operation according to the access control SFP supported by the TOE.
- o Example of list of subjects, objects, and operations
  - list of subjects : document user

- list of objects : documents that shall be protected
- operations : read, write

o Example of access control SFP

- Electronic document encryption access control, role-based access control, group-based access control, ACL-based access control, etc.

5.1.3.2. 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 [assignment: *access control SFP*] to objects based on [assignment: *list of subjects and objects controlled by the follow SFP, security attribute appropriate for SFP regarding each subject and object, or group of named security attributes*].

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) [selection : [assignment: *rules that control access among controlled subjects and controlled objects using controlled operation for the controlled objects*], none]

FDP_ACF.1.3 TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [assignment: *rules that authorize access of the subject to the object explicitly, based on security attributes*]

FDP_ACF.1.4 TSF shall explicitly deny access of the subject to objects based on the following additional rules: [assignment: *rules that deny access of the subject to the object explicitly, based on security attributes*]

Application notes

o This SFR specifies the requirement related to access control by encrypting/decrypting a document to be protected; the ST author is recommended to perform iteration operation according to the access control SFP supported by the TOE.

o The access control SFP enforced by TSF shall be performed through the encryption/decryption of the document to be protected, which can be done by specifying each individual document, document type (PDF document, Word document, HWP document, etc.), and document path.

o Example of list of subjects security attributes, objects security attributes, and operations

- list of subjects/security attributes : document user / document user ID, user group ID
- list of objects/security attributes : documents that shall be protected / types of document, a path of document
- operations : read, write

o The method of specifying a document to be protected can vary depending on the TOE design. When performing encryption/decryption according to the document type, however, the document type shall be recognized using the document header information, not the document extension name.

o See the FCS class for more details associated with cryptography.

5.1.4. Identification and authentication

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 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within [*assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met,* the TSF shall [assignment: *list of actions*].

Application notes

o The ST author can set the number of authentication failure and actions but the default value provided by the TOE shall be set as a follows.

- Number of authentication failures: five or less by default
- List of actions: identification and authentication function inactivation (5 minutes or more by default)

o Example of authentication events : administrator, document user(if the TOE provides the login function of document users) authentication attempts

o The authentication failure handing of administrator shall be required, however, for document users, it applies only to the TOE that provides the login function of document users.

o If the number of authentication failure and actions are set differently depending on the

TOE administrator and the management access(SSH, HTTPS etc.), the ST author can applies the iteration operation.

5.1.4.2. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to	No other components.
Dependencie	No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] in accordance with a specified [assignment: *authentication protocol*] that meets the following: [assignment: *list of standards*].

Application notes

o This SFR is a requirement for mutual verification among the TOE components that are physically separated. The ST author is recommended to use iteration operation according to the communication sector among the TOE components.

o This requirement shall be applied to physically partitioned parts of the TOE.

o If the [assignment: *list of standards*] doesn't exist, the ST author can specify "None" in the assignment operation. If the authentication protocol is internally implemented without the list of standards, the Internally Implemented Authentication Protocol can be specified as assignment operation in [assignment: *authentication protocol*].

o The cryptographic function to carry out mutual authentication in this SFR must perform cryptographic operation using the approved cryptographic algorithm of the validated cryptographic encryption module of which safety and implementation conformities are validated using the Korea Cryptographic Module Validation Program (KCMVP). When performing cryptographic operation, the validated cryptographic module shall run in approved operation mode.

- The ST author shall specify matters related to cryptographic operation in FCS_COP.1 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.

o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.

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 [assignment: *a defined quality metric*].

Application notes

- o Verification of secrets can be applied in every generation and change of all passwords, such as changing passwords, generating a password, and changing passwords at first access by the administrator and document user. The SFR shall be applied to the management access(SSH, HTTPS etc.) supported by the TOE.
- o The confidential information that must meet password complexity requirements can be authentication data such as the followings.
  - Authorized administrator's password, Authorized user's password, etc
- o The verification of secrets of administrator shall be required, however, for document users, it applies only to the TOE that provides the login function of document users.
- o The ST author are able to set the passwords combination rules and length in [assignment: *a defined quality metric*] of FIA_SOS.1.1 but the quality metric of password includes that password shall be able to be composed of three combinations of English letters/numbers/special characters and support passwords of 9 characters or more in length.
- o When deciding the password complexity verification method based on administrator-defined permission criteria, *"Administrator-defined permission criteria in FMT_PWD.1"* shall be defined in assignment operation.

5.1.4.4. FIA_UAU.1 Timing of authentication

Hierarchical to	No other components.
Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user, except for the actions specified in FIA_UAU.1.1.

Application notes

- o The user in the TOE refers to the authorized administrator and authorized document user. The role of the administrator can be defined in detail according to the access right. This requirement shall be applied to the management access(SSH, HTTPS etc.) supported by the TOE.
- o The authentication of administrator shall be required, however, for document users, it applies only to the TOE that provides the login function of document users.
- o In case of the password-based authentication method, identification and authentication are

carried out simultaneously and thus 'list of TSF mediated actions' is the same defined in FIA_UID.1. In case of the certificate-based authentication, the function that enumerates the certificate list and stored certificate location/devices selection before identification and authentication can be provided. Therefore, the ST author shall consider the function list according to the authentication method supported by the TOE before identification and authentication of the administrator and document user, and perform the assignment operation.

o If no actions are appropriate in assignment operation of FIA_UAU.1.1, it is recommended to use FIA_UAU.2 which is in a hierarchical relationship with FIA_UAU.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 [assignment: *identified authentication mechanism(s)*].

Application notes

o If authentication data for each administrator and/or document user sessions are the same such as password-based authentication method, it is possible to bypass the administrator and/or document user authentication by obtaining the session information of administrators, user illegally. Therefore, the reuse of authentication data can be prevented by encrypting the session ID or ensuring the uniqueness of the session ID for all the sessions (e.g., including the time stamp, random number, etc.). If multiple authentication mechanisms are supported, the ST author specifies authentication mechanisms required to prevent reuse of authentication data are identified(e.g., OTP, etc.) in the assignment operation. For example, the SMS authentication number method can set additional security attributes including time limitations, authentication number length, and randomness to prevent its reuse.

o The single-user authentication mechanisms of administrator shall be required, however, for document users, it applies only to the TOE that provides the login function of document users.

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 [assignment: *list of feedback*] to the user while the authentication is in progress.

Application notes

o The input password shall be masked(e.g., “****” etc.) to make it unrecognizable on the screen and the followings are masked. The method that does not display the characters entered by the administrator and/or document user on the screen as the method that prevent form the disclosure of password input values also is allowed.

- Password generation, modification of administrator and/or document user
- Authentication of administrator and/or document user

※ In the case of document user, this requirement is applied to the TOE that provides the login function of document users

o In case of identification and authentication failures, the TOE shall not provide the feedback for the cause of failure (e.g., You have inputted an incorrect account or password, etc.).

o The protected authentication feedback of administrator shall be required, however, for document users, it applies only to the TOE that provides the login function of document users.

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 [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

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.

Application notes

o The user in the TOE refers to the authorized administrator and authorized document user. The role of the administrator can be defined in detail according to the access right. When dividing the administrator roles into multiple roles, requirements shall be defined in FMT_SMR.1. This requirement shall be applied to the management access (SSH, HTTPS etc.) supported by the TOE.

o The identification of administrator shall be required, however, for document users, it applies only to the TOE that provides the login function of document users.

o If no actions are appropriate in assignment operation of FIA_UID.1.1, it is recommended to use FIA_UID.2 which is in a hierarchical relationship with FIA_UID.1.

5.1.5. Security management

Security functional component	Management function	Management type
FAU_ARP.1	Management of actions (addition, removal, modification) to be taken	Management of security functions
FAU_SAA.1	Maintenance of the rules (addition, removal and modification of the rules in the rule group)	Management of security functions
FAU_SAR.1	Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records	Management of security roles
FAU_STG.3	Maintenance of the threshold	Management of TSF data threshold
	Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure	Management of security functions
FAU_STG.4	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	Management of security functions
FDP_ACF.1	Managing the attributes used to make explicit access based decisions or denial decisions.	Management of security attributes
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Management of TSF data threshol
	Management of actions to be taken in the event of an authentication failure	Management of security functions
FIA_SOS.1	Management of the metric used to verify the secrets	Management of security functions
FIA_UAU.1	Management of the authentication data by an administrator Management of the authentication data by the associated user	Management of TSF data
	Management of the list of actions that can be taken before the user is authenticated	Management of security functions
FIA_UID.1	Management of the user identities	Management of TSF data
	If an authorized administrator can change the actions allowed before identification, the managing of the action lists	Management of security functions
FMT_MOF.1	Management of the group of roles that can interact with the functions in the TSF	Management of security roles
FMT_MSA.1	Management of the group of roles that can interact with the security attributes	Management of security roles

Security functional component	Management function	Management type
	Management of rules by which security attributes inherit specified values.	Management of security attributes
FMT_MSA.3	Management of the group of roles that can specify initial values	Management of security roles
	Management of the configuration that permit or limit the default values in accordance with given access control SFP Management of rules by which security attributes inherit specified values.	Management of security attributes
FMT_MTD.1	Management of the group of roles that can interact with the TSF data	Management of security roles
FMT_PWD.1	Management of ID and password configuration rules	Management of security functions
FMT_SMR.1	Management of the group of users that are part of a role.	Management of security roles
FPT_ITT.1	Management of the types of modification against which the TSF shall protect Management of the mechanism used to provide the protection of the data in transit between different parts of the TSF	Management of security functions
FPT_TST.1	Management of the conditions under which TSF self testing occurs, such as 'during initial start-up', 'regular interval', or 'under specified conditions' Management of the time interval (if appropriate)	Management of TSF data
FTA_MCS.2	Management of the maximum allowed number of concurrent user sessions by an administrator	Management of TSF data threshold
FTA_SSL.5	Specification of the time of user inactivity after which lock-out occurs for an individual user Specification of the default time of user inactivity after which lock-out occurs	Management of TSF data
FTA_TSE.1	Management of the session establishment conditions by the authorized administrator	Management of TSF data
FTP_TRP.1	Configuring the actions that require trusted path (if supported)	Management of security functions

[Table 4] Security management action and management type by component

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 management actions of*** the functions [assignment: *list of functions*] to [the authorized administrator].

Application notes

- o "Management action" to which a refinement operation is applied includes the ability to determine the behavior, disable, enable, modify the behavior of some functions in the TSF. This requirement shall be applied to the management access(SSH, HTTPS, etc.) supported by the TOE.
- o The action that adds, deletes or modifies conditions or rules capable of determining the security functions behavior is included in the management of security functions behaviors. And, the action that adds, deletes or modifies behaviors taken by the TSF according to the corresponding conditions and rules is also included in the management of security functions behaviors. In addition, the action of selecting mechanism, protocol, etc., when there are variously provided to support the same purpose, is included in the management of security functions behavior because it corresponds to the modification of behavior.
- o The ST author can apply assignment operation in FMT_MOF.1.1 with reference to '[Table 4] security management action and management type by component' for the case that the TOE supports management functions.
- o The ST author can define additional management actions of security function for each component in addition to management functions which are presented in '[Table 4] security management action and management type by component'. Management actions of security function can be included for the additional or extended requirements.

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 [assignment: ***access control SFP***] *to restrict the ability to* [selection: *change_default, query, modify, delete*, [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

Application notes

- o The ST author shall define FMT_MSA.1.1 assignment operation with reference to '[Table 4] security management action and management type by component' if the TOE supports security attribute management functions.
- o The ST author can define additional security attribute management actions for each component in addition to management function that are presented in '[Table 4] security management action and management type by component'. Management actions of security function can be included for the additional or extended requirements.

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 [assignment: ***access control SFP***] to provide [selection, choose one of: restrictive, permissive, [assignment: *other property*]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [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 Management of TSF data

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** the [assignment: *list of TSF data*] to [the authorized administrator].

Application notes

- o “Manage” to which a refinement operation is applied includes the ability to change default, query, modify, delete, clear, other operation, etc.
- o The ST author can apply assignment operation in FMT_MTD.1.1 with reference to '[Table 4] security management action and management type by component', for the case that the TOE supports the TSF data management function.
- o The ST author can define additional TSF data management actions for each component in addition to management function that are presented in '[Table 4] security management action and management type by component', and present TSF data management actions

for additional or extended requirements in addition to security functional requirements stated in this document. For example, the configuration of device access time limit when the unsuccessful authentication attempts can be included in management actions.

o The user interface and CLI commands related to modify audit data shall not be provided to prevent even authorized administrators from deleting or modifying audit 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 [assignment: *list of functions*] to [the authorized administrator].
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 [the authorized administrator].
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*].

Application notes

o If the TOE does not provide the management functions that administrator manage the combination rules and length of ID and password, etc., 'None' may be specified in assignment operations of FMT_PWD.1.1 and FMT_PWD.1.2.

o The ST author shall define list of functions which require the password management in [assignment: *list of function*]

o This requirement shall be applied to the management access(SSH, HTTPS, etc.) supported by the TOE.

o The password combination rules that can be set by the administrator in FMT_PWD.1.1 shall be able to be composed of three combinations of English letters/numbers/special characters and support passwords of 9 characters or more in length.

o In case of 'setting ID and password when installing, setting password when installing' presented in FMT_PWD.1.3, the function to force to change the default password shall not be required at administrator's first access.

o The management of administrator's ID and password in accordance with FMT_PWD.1.1, FMT_PWD.1.2, and FMT_PWD.1.3 is required essentially, but the management of document users' ID and password is only applied to the TOE that provides the login function of document users.

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

Application notes

o The ST author lists up all the functions that support management actions. The listed management functions in FMT_SMF.1 shall ensure that it is consistent with the management actions of TSF function, TFS data and security attributes defined in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1, FMT_PWD.1, etc.

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 roles [assignment: *the authorized identified roles*].

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

Application notes

o The user in the TOE refers to the authorized administrator and authorized document user. The role of the administrator can be defined in detail according to the access right.

o It must be noted that the ST author shall suitably assign the access privileges in accordance with the administrator's roles. For example, the administrator allowed to do monitoring only should not be able to modify the TOE's environment configuration.

5.1.6. Protection of the TSF

5.1.6.1. FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to	Hierarchical to
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.

Application notes

o This SFR shall be applied when transmitting TSF data between the TOE components which are physically separated regardless of operating type, such as user device encryption and information system encryption.

o Examples of data transmitted among the TOE components include the following: security policy, control command, audit data, and CSP, etc.

o When implementing the encryption and message integrity verification function, the approved cryptographic algorithm of the validated cryptographic module that safety and implementation conformities are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be used.

- The ST author shall specify matters related to cryptographic operation in FCS_COP.1(2) and specify related matters in FCS_CKM.1(2) if a cryptographic key is needed to be generated to perform the cryptographic operation function.

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 [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

Application notes

o Containers controlled by the TSF mean storage in the TOE or external entities (DBMS, etc.) that interact with the TOE.

o Examples of TSF data to be protected as follows:

- Administrator and/or document user password, cryptographic key (pre-shared key, symmetric key, private key, etc), CSP, TOE configuration values (security policy, configuration parameters, etc), audit data, etc.

o Administrator password and/or document user password shall not be hard-coded or stored as in plaintext (including simple encoding) in the TOE.

o When storing the TOE configuration values to the storage, the values shall be encrypted and stored with the approved cryptographic algorithm of the validated cryptographic module. When storing the audit data in the file system or registry of the document user device, the values shall be encrypted and stored with the approved cryptographic algorithm.

- If it is found that no important information (encryption key, CSP, user ID used for verification, IP/MAC information for identity check, etc.) is included, however, the internally implemented encryption encoding technique can be applied.
- The ST author shall specify matters related to cryptographic operation in FCS_COP.1(2) and specify related matters in FCS_CKM.1(2) if a cryptographic key is needed to be generated to perform the cryptographic operation function.

o The data that includes an encryption key and a CSP (directly stored value, configuration value, or value included in the audit data) must be encrypted and stored with the approved cryptographic algorithm of the validated cryptographic module, regardless of the storing location and type (file system or DMBS providing identification, authentication, and the access control function, etc.).

o The data encryption key (DEK) shall be encrypted and stored with the approved cryptographic algorithm provided by the validated cryptographic module, using the key encryption key (KEK). KEK shall be derived using the password-based key derivation method or be stored in a safe manner in security token.

o Cryptographic keys and key materials loaded onto memory shall not exist in plaintext. Note, however, that exposure as plaintext is allowed when the encryption key and CSP are used for encryption/decryption operation. If encryption/decryption is completed and not used, they shall not exist as plaintext.

o When a session is terminated or the TOE execution is finished, all the cryptographic key and CSP loaded onto the memory shall be deleted.

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 <u>*prevent*</u> the unauthorized deletion for [assignment: *TSF data*].
FPT_PST.2.2	TSF shall <u>*prevent*</u> the unauthorized termination for [assignment: *TSF data*].

Application notes

o A function that prevents the unauthorized deletion of the TOE configuration value (security policy, environment configuration parameter, etc.) shall be provided.

o A function that prevents unauthorized termination of the TOE's executable file (process) due to malicious code shall be provided. If the termination prevention function cannot be perfectly implemented, the alternative termination shall be detected and automated recovery shall be performed when alternative termination occurs.

5.1.6.4. FPT_TST.1 TSF testing

Hierarchical to	No other components.
Dependencies	No dependencies.

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

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

FPT_TST.1.3 The TSF shall provide **authorized administrator** with the capability to verify the integrity of [selection: [assignment: *parts of TSF], TSF*].

Application notes

o It is recommended to conduct the TSF self tests of critical processes related to the operation of security functions such as identification and authentication, access control, security management, etc.

o The ST author can select parts of the TSF to be tested, however, those parts of the TSF shall be tested if their abnormal operation (e.g., error, stop, etc.) affect the critical functions and security functions of the TOE.

o In the case that cryptographic functions are applied when ‘an integrity check functionality’ is implemented, the TOE cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be used.

o The TOE shall apply operation (iteration, refinement, etc.) so that the following can be satisfied.

- The integrity of the TOE’s configuration value and executable file shall be checked at the initial phase of the TOE operation.
- A function that verifies the configuration value of the TOE (e.g., security policy, environment configuration parameter) shall be provided to the authorized administrator or document user.
- Function that notifies the administrator, in real time, for result of verification of the integrity periodically during normal operation or at the request of the authorized administrator shall be provided.

o TSF testings do not need to be carried out at the same time, however, it is required to carry out each testing at certain necessary conditions per each TSF part.

- o The ST author can select the interval of TSF testing during normal operation. However, the testing interval shall be determined within certain reasonable bounds so that they do not adversely affect the TOE operates abnormally.
- o The components of the product that performs the encryption/decryption function shall be notified when the error occurs after receiving the self-test result of the validated cryptographic module.

5.1.7. TOE access

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

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

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [The maximum number of concurrent sessions for [selection: *administrator management access session, user access session*] restricted to one, prohibition of same user both concurrent connections of management access session and local access session, the maximum number of concurrent sessions for user access restricted to one, Rules on the maximum number of concurrent sessions { determined by ST author}]

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

Application notes

- o A session is presented in FMT_MCS.2 is 'administrator access', the number of sessions shall be 'the number of administrator accesses.'
- o When restricting the number of management access sessions to the TOE by each service(e.g., SSH, HTTPS, etc.), it is defined in operation of FTA_MCS.2.1.
- o After one device makes administrator's management access, another device performs a login process with the same account or privilege, the TSF shall block new connection attempts or terminate previous connection.
- o If an administrator with higher privilege has already management access, the management access of an administrator with lower privilege can be limited in accordance with the TOE's administrator role.
- o But, the duplicated login can be allowed for the administrator account carrying out monitoring for the TOE operating status, etc.
- o Even if it is logged in using the 'Same privilege', the duplication login is allowed if it is proved that there are no conflicts between the policies.

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

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

FTA_SSL.5.1 The TSF shall [selection:

- *lock the session and/or re-authenticate the* ***administrator*** *before unlocking the session,*
- *terminate*] an interactive session of the **administrator** after a [assignment: *time interval of* ***administrator*** *inactivity*].

Application notes

o This SFR shall require the capability to lock or terminate the session after a time interval of the administrator inactivity, and it shall be applied to the implementation of the management access (SSH, HTTPS, etc.) supported by the TOE.
 - subject of application: administrator session

o 'None' is applicable to the dependencies of this SFR, when 'session termination' is selected in the selection operation of FTA_SSL.5.1.

o If the ST author selects 'lock the session and/or re-authenticate the administrator before unlocking the session' in FTA_SSL.5.1, it is not permitted to specify only the statement 're-authenticate the administrator before unlocking the session' applying 'or' to the statement.

o "A time interval of the authorized administrator inactivity" can be the fixed value in the TOE (less than 10 minutes) or the TOE can provide capability to set the value to the authorized administrator. The default value shall be set within 10 minutes.

o However, the administrator account that performs monitoring only may not apply session lock or termination.

o If inactivity time and actions (session locking or session termination) are differently provided depending on the TOE administrator and management access (SSH, HTTPS, etc.), the ST authors can apply the iteration operation.

o Session Locking means that the TSF shall lock an interactive session after inactivity time by disabling any activity of the administrator's data access/display devices other than unlocking the session and clearing or overwriting display devices, making the current contents (TOE configuration values, etc.) unreadable.

5.1.7.3. FTA_TSE.1 TOE session establishment

Hierarchical to	No other components.
Dependencies	No dependencies

FTA_TSE.1.1 The TSF shall be able to deny **administrator's management access session** establishment based on [connection IP, [selection: *connection time, whether* *or not to activate the management access session of the same account, whether or not to activate the management access session of administrator* account with the same privilege, [assignment: *critical management functions attribute], None*]].

Application notes

- o The management access session of administrator shall be allowed only from the terminal with designated IP address for management access.
- o The ST author is able to establish the number of connection IP, the default value provided by the TOE shall set at most 2.
- o The IP address can be exceptionally allocated to the administrator who can access the TOE, if the administrator has the read-only right (e.g, monitoring etc.). When establishing the administrator's connection IP, it is not allowed to add an IP address range such as 192.168.10.2 to 253, etc, individually it shall implemented to add the IP address one by one. Moreover, establishment of IPs such as 0.0.0.0, 192.168.10.*, any, etc. is not allowed.
- o The ST author can add access time of the administrator, activation of management access session for the same account, etc.

5.2. Security functional requirements (Optional SFR)

'Optional SFRs' in this PP are as follows. 'Optional SFRs' are not required to be implemented mandatorily, however, when the TOE additionally provides related capabilities, the ST author must include the corresponding SFRs into the ST.

Security functional class	**Security functional component**		**Remark**
FAU	FAU_SEL.1	Selective audit	
	FAU_STG.1	Protected audit trail storage	
FDP	FDP_ACC.1(2)	Subset access control	
	FDP_ACF.1(2)	Security attribute based access control	
FPT	FPT_STM.1	Reliable time stamps	
	FPT_TEE.1	Testing of external entities	
	FPT_TUD.1(Extended)	TSF security patch update	
FTP	FTP_ITC.1	Inter-TSF trusted channel	
	FTP_TRP.1	Trusted path	

[Table 5] Optional security functional requirements

5.2.1. Security audit

5.2.1.1. FAU_SEL.1 Selective audit

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation FMT_MTD.1 TSF Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [selection: *object identity, user identity, subject identity, host identity, event type*]

b) [assignment: *list of additional attributes that audit selectivity is based upon*]

Application notes

o FAU_SEL.1 Selective audit is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.

o The ST author can select the set of events to be audited, but the default value provided by the TOE shall be set to include all auditable events defined in FAU_GEN.1.

5.2.1.2. FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

Application notes

o FAU_STG.1 Protected Audit trail storage is a functional requirement (optional SFR) that can be optionally implemented. If the TOE provides the above function additionally, the ST author shall include this requirement in the SFR.

o The TOE can use the storage managed by the DBMS as an audit trail storage. As the audit trail storage cannot be fully protected by the TSF in this case, the ST author shall add the security objective regarding for the operational environment related to the protection of the audit trail storage in the ST.

5.2.2. User data protection

5.2.2.1. FDP_ACC.1(2) Subset access control

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 TSF shall enforce the [assignment: *access control SPF*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by SFP*].

Application notes

o **FDP_ACC.1(2)** Subset access control is a functional requirement ("optional SFR") that can be implemented optionally. If the TOE provides the aforesaid function additionally, the ST author shall include this requirement in SFR.

o If the ST author includes this SFR, security problem definition and security target shall be additionally identified, if necessary.

o This SFR is a requirement related to access control regarding the printing, copy, and screen capture of the document to be protected. The ST author is recommended to perform iteration operation according to the access control SFP supported by the TOE.

o Example of access control SFP

- Role-based access control, group-based access control, ACL-based access control, etc.

5.2.2.2. FDP_ACF.1(2) Security attribute based access control

Hierarchical to No other components.

Dependencies FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 TSF shall enforce the [assignment: *access control SFP*] on objects based on [assignment: *list of subjects and objects controlled by the follow SFP, security attribute appropriate for SFP regarding each subject and object, or group of named security attributes*].

FDP_ACF.1.2 TSF shall enforce the following rules to determine whether the operations between the controlled subject and objects are allowed: [assignment: rules that control access among controlled subjects and controlled objects using controlled operation for the controlled objects]

FDP_ACF.1.3 TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [assignment: *rules that authorize access of the subject to the object explicitly, based on security attributes*]

FDP_ACF.1.4	TSF shall explicitly deny access of the subject to objects based on the following additional rules: [assignment: *rules that deny access of the subject to the object explicitly, based on security attributes*]

Application notes

- o FDP_ACF.1(2) Subset access control is a functional requirement ("optional SFR") that can be implemented optionally. If the TOE provides the aforesaid function additionally, the ST author shall include this requirement in SFR.
- o If the ST author includes this SFR, security problem definition and security target shall be additionally identified, if necessary.
- o This SFR is a requirement related to access control regarding the printing, copy, and screen capture of the document to be protected. The ST author is recommended to perform iterating operation according to the access control SFP supported by the TOE.

5.2.3. Protection of the TSF

5.2.3.1. FPT_STM.1 Reliable time stamps

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application notes

- o FPT_STM.1 Reliable time stamps are a functional requirement ("optional SFR") that can be implemented optionally. If the TOE provides the function additionally, the ST author shall include this requirement in SFR.
- o The TSF can receive the reliable time stamp function from the operational environment, such as the reliable time synchronization of the external IT entity (e.g., reliable NTP server). In this case, the ST author shall perform assignment operation of FAU_GEN.1.1 to add an audit event regarding the time change and add the security objectives for the operational environment related to the reliable time stamp in the ST, instead of applying this SFR.
- o If the TOE provides a reliable time stamp function, the TOE shall be operated based on the time in the management server.

5.2.3.2. FPT_TEE.1 Testing of external entities

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized* ***administrator****, [assignment: other conditions*]] to check the fulfillment of [assignment: *list of properties of the external entities*].

FPT_TEE.1.2 If the test fails, the TSF shall [assignment: *action(s)*].

Application notes

- o The ST author can select external entities to be tested, however, those external entities must be tested if their abnormal operation (e.g., error, stop, etc.) affect the critical functions and security functions of the network device.
- o If the test of external entities fails, the appropriate action that is suitable for the tested entities can be provided. For example, in case of external entities affecting the critical functions and security functions of the TOE, the capability can be provided so that administrators are immediately aware of abnormal status of the device's anomaly status using alarm, etc.
- o Testings of external entities do not need to be carried out at the same time, however, it is required to carry out each testing at certain necessary conditions per each external entity. For example, when initial start-up, external entities affecting the critical functions and security functions of the TOE shall be tested in full.
- o The ST author can select the interval (e.g., every one hour during normal operation or at the request of the authorized administrator) of external entities testing during normal operation. However, the testing interval shall be determined within certain reasonable bounds so that they do not adversely affect when the TOE operates abnormally.
- o The capability can be provided so that administrator directly executes the testing of external entities, and the ST author can select all or parts of external entities to be directly tested.
- o All entities outside of the TOE that interacts with the TOE (e.g., NTP server, log server, DBMS) can be the target of an additional external entities test. It is recommended to include an external entity needed for the safe and accurate operation of the TOE in the test target.

5.2.3.3. FPT_TUD.1 TSF security patch update (Extended)

Hierarchical to	No other components.
Dependencies	No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [assignment: *the authorized identified roles*].

FPT_TUD.1.2 The TSF shall verify validity of the update files using *digital signature* *verification* before installing updates.

Application notes

- o FPT_TUD.1 TSF security patch update is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.
- o The TSF shall provide the capability to check the current version of the TOE which most recently installed and executed by authorized role.
- o Updates may be available either automatically or manually. If online update is available, update files shall be transmitted through a secure communication channel to protect the file. Refer to 'Optional SFR' FTP_ITC.1 for more details.
- o When failing the update installation and update file verification of the TOE, the TOE shall be securely started and operated using a previous firmware.
- o If the agent receives a file from the server, it shall perform verification of digital signature on the subject of file generation to ensure non-repudiation and integrity. The certificate as well as digital signature shall be verified, and the agent shall perform integrity verification on the address of the management server or update server. If there are more than two servers on the file transmission route, the receiving server shall perform integrity verification on the address of the sending server. If the authorized identified roles update the TOE by hand, however, the verification of validity for the update files is allowed by comparing with hash values although it does not provide the functionality of non-reputation.
- o If the cryptographic functionality is applied to the verification of validity for the update files, this SFR shall perform the cryptographic operation using the TOE cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP), the validated cryptographic module must be operated on the approved mode of operation when the cryptographic operation is performed.
  - The ST author shall specify matters related to cryptographic operation in FCS_COP.1 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.

5.2.4. Trusted path/channels

5.2.4.1. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to	No other components.
Dependencies	No dependencies.

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

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application notes

o FTP_ITC.1 Inter-TSF trusted channel is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.

o If ST author includes this SFR, the ST author shall identify 'trusted IT products' in the TOE operational environment of the ST.

o Examples of the trusted IT product presented in FTP_ITC.1 are external log server, update server, etc.

o If the TSF interacts with the external log server or authentication server, etc., the TSF and each server shall protect the TSF data such as audit data, authentication data, TOE configuration files, etc by providing trusted channel using cryptographic protocol.

- If the TLS protocol is supported when communicating between the TSF and trusted IT product, it shall support TLS 1.2 (RFC 5246) or its successors. And, if the SSH protocol is supported, it shall support SSH v2(RFC 4251 ~ 4254) or its successors. The cryptographic communication protocol described in this SFR is recommended to remove the publicly available vulnerabilities included in the protocol for secure use.

- If the ST author add this SFR to the ST, the ST author shall add the SFR regarding the cryptographic key generation(FCS_CKM.1) and cryptographic operation(FCS_COP.1) which are additionally required with reference to the FCS class.

o If the ST author includes this SFR in the ST, the author shall perform assignment operation in the assignment operation of FMT_MOF.1 and FAU_GEN.1.1 by referring to the definition of extended components.

5.2.4.2. FTP_TRP.1 Trusted path

Hierarchical to No other components.

Dependencies No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***the management access*** **administrator** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure, [assignment: other types of integrity or confidentiality violation].*

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF,* ***the management access administrator***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *the* ***authentication of management access administrator,*** [assignment: *other services for which trusted path is required*]].

Application notes

o FAU_TRP.1 Trusted path is a functional requirement (optional SFR) that can be implemented optionally. If the TOE provides the above function additionally, the ST author shall include this requirement in the SFR.

o The TOE shall provide a trusted channel using the encrypted communication protocol in case of administrator's management access. If communication needs to be established between the management access administrator and the TOE component such as web management access, the use of OpenSSL and other means that implement the safe security protocol shall be allowed, not the approved cryptographic algorithm of the validated cryptographic module. When OpenSSL is used, the complexity of cryptographic algorithm and encryption key length shall be more than 112 bits.

- If the TLS protocol is supported for the administrator's management access, it shall support TLS 1.2 (RFC 5246) or its successors. And, if the SSH protocol is supported, it shall support SSH v2(RFC 4251 ~ 4254) or its successors. It is recommended to remove the publicly available vulnerabilities included in the protocol for secure use.
- If the ST author has added this SFR to the ST, it is recommended to perform iteration operation and add the SFR regarding cryptographic key generation (FCS_CKM.1) and cryptographic operation (FCS_COP.1), which is additionally required.

o If there is no other type of integrity or confidentiality violation in FTP_TRP.1.1, "None" can be specified in the assignment operation.

o This security functional requirement can be applied if it is implemented by communication between the web browser of the administrator PC and the TOE component (management server). If management connection is implemented by communication between the TOE component (management console) and the TOE component (management server), FTP_ITT.1 shall be applied. In addition, if management connection is provided by communication between the web browser of the administrator PC and management server's operational environment (web server), the ST author shall describe this security functional requirement by replacing it with the security objectives for the operational environment.

5.3. Security assurance requirements

Assurance requirements of this Protection Profile 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 6] Security assurance requirements

5.3.1. Security Target evaluation

5.3.1.1. ASE_INT.1 ST introduction

Dependencies No dependencies.

Developer action elements

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

Content and presentation elements

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

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

ASE_INT.1.3C The TOE reference shall 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.

5.3.1.2. 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 elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

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

Content and presentation elements

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

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

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

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

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

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

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

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

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

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

Evaluator action elements

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

5.3.1.3. ASE_OBJ.1 Security objectives for the operational environment

Dependencies No dependencies.

Developer action elements

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

Content and presentation elements

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

5.3.1.4. ASE_ECD.1 Extended components definition

Dependencies No dependencies.

Developer action elements

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

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

Content and presentation

elements

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

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

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

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

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

Evaluator action elements

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

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

5.3.1.5. ASE_REQ.1 Stated security requirements

Dependencies ASE_ECD.1 Extended components definition

Developer action elements

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

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

Content and presentation elements

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

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

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

ASE_REQ.1.4C All operations shall be performed correctly.

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

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

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

5.3.1.6. ASE_TSS.1 TOE summary specification

Dependencies	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Developer action elements	
ASE_TSS.1.1D	The developer shall provide a TOE summary specification
Evaluator action 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.

5.3.2. Development

5.3.2.1. ADV_FSP.1 Basic functional specification

Dependencies	No dependencies.
Developer action elements	
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit

categorization of interfaces as SFR-non-interfering.

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

Evaluator action elements

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

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

5.3.3. Guidance documents

5.3.3.1. AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

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

5.3.3.2. AGD_PRE.1 Preparative procedures

Dependencies No dependencies.

Developer action elements

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

Content and presentation elements

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

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

Evaluator action elements

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

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

5.3.4. Life-cycle support

5.3.4.1. ALC_CMC.1 Labelling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action elements

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

Content and presentation elements

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

Evaluator action

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

5.3.4.2. ALC_CMS.1 TOE CM coverage

Dependencies	No dependencies.
Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
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.

5.3.5. Tests

5.3.5.1. ATE_FUN.1 Functional testing

Dependencies	ATE_COV.1 Evidence of coverage
Developer action elements	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
Content and presentation elements	
ATE_FUN.1.1C	The test documentation shall consist of test 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.

5.3.5.2. 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 elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.6. Vulnerability assessment

5.3.6.1. 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 elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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

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

5.4. Security requirements rationale

5.4.1. 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	-
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	-
7	FAU_STG.4	FAU_STG.1	-
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	9, 12
		FCS_CKM.4	10
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	9, 13
		FCS_CKM.4	10
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
		FCS_CKM.4	10
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
12	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	11
13	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9
		FCS_CKM.4	11
14	FCS_RBG.1	-	-
15	FDP_ACC.1	FDP_ACF.1	16
16	FDP_ACF.1	FDP_ACC.1	15
		FMT_MSA.3	26
17	FIA_AFL.1	FIA_UAU.1	20
18	FIA_IMA.1	-	-
19	FIA_SOS.1	-	-
20	FIA_UAU.1	FIA_UID.1	23
21	FIA_UAU.4	-	-
22	FIA_UAU.7	FIA_UAU.1	20
23	FIA_UID.1	-	-

No.	Security functional requirements	Dependency	Reference No.
24	FMT_MOF.1	FMT_SMF.1	29
		FMT_SMR.1	30
25	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	15
		FMT_SMF.1	29
		FMT_SMR.1	30
26	FMT_MSA.3	FMT_MSA.1	25
		FMT_SMR.1	30
27	FMT_MTD.1	FMT_SMF.1	29
		FMT_SMR.1	30
28	FMT_PWD.1	FMT_SMF.1	29
		FMT_SMR.1	30
29	FMT_SMF.1	-	-
30	FMT_SMR.1	FIA_UID.1	23
31	FPT_ITT.1	-	-
32	FPT_PST.1	-	-
33	FPT_PST.2		
34	FPT_TST.1	-	-
35	FTA_MCS.2	FIA_UID.1	23
36	FTA_SSL.5	FIA_UAU.1	20
37	FTA_TSE.1	-	-
38	FTP_TRP.1	-	-

[표 7] 종속관계 이론적 근거

FAU_GEN.1 has a subordinate relationship with FAU_STM.1. However, as this PP is written to reflect the TOE implemented in various types, if the pertinent function is implemented by the TOE, the ST author needs to identify the optional SFR (FAU_STM.1) as the SFR of the ST and describe the pertinent reference number. In addition, if FAU_STM.1 is supported by the operational environment (e.g., operating systems), the author shall add the security objectives for the operational environment and provide justification that a subordinate relationship is satisfied.

FAU_STG.3 and FAU_STG.4 have a subordinate relationship with FAU_STG.1. However, as this PP is written to reflect the TOE implemented in various types, if the pertinent function is implemented by the TOE, the ST author needs to identify the optional SFR (FAU_STG.1) as the SFR of the ST and describe the pertinent reference number. In addition, if FAU_STG.1 is supported by the operational environment (e.g., DBMS), the author shall add the security objectives for the operational environment and provide justification that a subordinate relationship is satisfied.

5.4.2. 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. but, 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.

References

Title	Author	Remark
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) • Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002) • Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003)	CCMB	2017. 4

Abbreviated terms

CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CFB	Cipher Feedback
CTR	Counter Mode
ECB	Electronic Codebook
DEK	Data Encryption Key
EAL	Evaluation Assurance Level
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IP	Internet Protocol
IT	Information Technology
IV	Initial Vector
KEK	Key Encryption Key
NTP	Network Time Protocol
OFB	Output Feedback
OTP	One Time Password
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMS	Short Message Service
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality