Korean National Protection Profile for Database Encryption V1.1

2019. 12. 11.

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 requirements for database encryption in conformity with the Common Criteria. And the NIS offered advise for the accurate interpretation of those 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
1.1	2019.12.11	o Correction of content reinforcement, editing error, etc.

Table of Contents

1. PP introduction **1**

1.1. PP reference **1**

1.2. TOE overview **1**

1.2.1. Database Encryption overview 1

1.2.2. TOE type and scope 1

1.2.3. TOE usage and major security features 2

1.2.4. Non-TOE and TOE operational environment 2

1.3. Conventions **6**

1.4. Terms and definitions **8**

1.5. PP organization **13**

2. Conformance claim **15**

2.1. CC conformance claim **15**

2.2. PP conformance clam **15**

2.3. Package conformance claim **15**

2.4. Conformance claim rationale **15**

2.5. PP conformance statement **15**

3. Security objectives **16**

3.1. Security objectives for the operational environment **16**

4. Extended components definition **17**

4.1. Cryptographic support **17**

4.1.1. Random Bit Generation 17

4.2. Identification and authentication **17**

4.2.1. TOE Internal mutual authentication 17

4.3. User data protection **18**

4.3.1. User data encryption 18

4.4. Security Management **19**

4.4.1. ID and password 19

4.5. Protection of the TSF **20**

4.5.1. Protection of stored TSF data 20
4.6. TOE Access 21
4.6.1. Session locking and termination 21

5. Security requirements 24
5.1. Security functional requirements (Mandatory SFRs) 26
5.1.1. Security audit (FAU) 28
5.1.2. Cryptographic support (FCS) 32
5.1.3. User data protection (FDP) 37
5.1.4. Identification and authentication 38
5.1.5. Security management 42
5.1.6. Protection of the TSF 47
5.1.7. TOE access 49
5.2. Security functional requirement (Optional SFR) 53
5.2.1. Security audit 53
5.2.2. Protection of the TSF 54
5.2.3. Trusted path/channels 55
5.3. Security assurance requirements 58
5.3.1. Security Target evaluation 58
5.3.2. Development 62
5.3.3. Guidance documents 63
5.3.4. Life-cycle support 64
5.3.5. Tests 65
5.3.6. Vulnerability assessment 66
5.4. Security requirements rationale 67
5.4.1. Dependency rationale of security functional requirements 67
5.4.2. Dependency rationale of security assurance requirements 69

References 70
Abbreviated terms 71

1. PP introduction

1.1. PP reference

Title	Korean National Protection Profile for Database Encryption
Version	1.1
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Developer	National Security Research Institute, Telecommunications Technology Association, Korea System Assurance
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	CC V3.1 r5
Certification Number	KECS-PP-0820a-2017
Keywords	Database, Encryption

1.2. TOE overview

1.2.1. Database Encryption overview

Database encryption (hereinafter referred to as "TOE") performs the function of preventing the unauthorized disclosure of confidential information by encrypting the database (hereinafter referred to as "DB").

The encryption target of the TOE is the DB managed by the database management system (hereinafter referred to as "DBMS") in the operational environment of the organization, and the protection profile (hereinafter referred to as "PP") defines the user data as all data before/after encrypted and stored in the DB. Part or all of the user data can be the encryption target, depending on the organizational security policies that runs the TOE.

The DBMS that controls the DB in the operational environment of the organization is different from the DBMS that is directly used by the TOE to control the TSF data (security policy, audit data, etc.).

1.2.2. TOE type and scope

The TOE is provided as software and shall provide the encryption/decryption function for the user data by each column. The TOE type defined in this PP can be grouped into the 'plug-in type' and 'API type', depending on the TOE operation type. The TOE can support both types. The TOE developed by the plug-in type can generally be composed of the agent and management server, whereas the TOE developed by the API type can be composed of the API module and management server.

The TOE developer can implement the management server with several TOE components by subdividing roles such as the encryption/decryption of the user data, security management function, and cryptographic key management function. For example, additional management tools developed for security management (like management console) can be included in the TOE component. In this case, the security target (hereinafter referred to as "ST") author shall identify all TOE components in the ST.

1.2.3. TOE usage and major security features

The TOE is used to encrypt the user data according to the policy set by the authorized administrator to prevent the unauthorized disclosure of the confidential information. In order that the authorized administrator can operate the TOE securely in the operational environment of the organization, the TOE provides various security features such as the security audit function that records and manages major auditable events; cryptographic support function such as cryptographic key management to encrypt the user and the TSF data, and cryptographic operation; user data protection function that encrypts the user data and protects the residual information; identification and authentication function such as verifying the identity of the authorized administrator, authentication failure handling, and mutual authentication among the TOE components; security management function for security functions, role definition, and configuration; TSF protection functions including protecting the TSF data transmitted among the TOE components, protecting the TSF data stored in the storage that is controlled by the TSF, and TSF self-test; and TOE access function to manage the access session of the authorized administrator. In addition, the TOE can provide the trusted path/channel function that provides cryptographic communication between the TOE and authorized administrator, if necessary.

The DEK (Data Encryption Key) used to encrypt/decrypt the user data is protected by encryption with the KEK (Key Encryption Key). For the requirements regarding how to generate and use the DEK and KEK, refer to 5.1.2. Cryptographic Support (FCS).

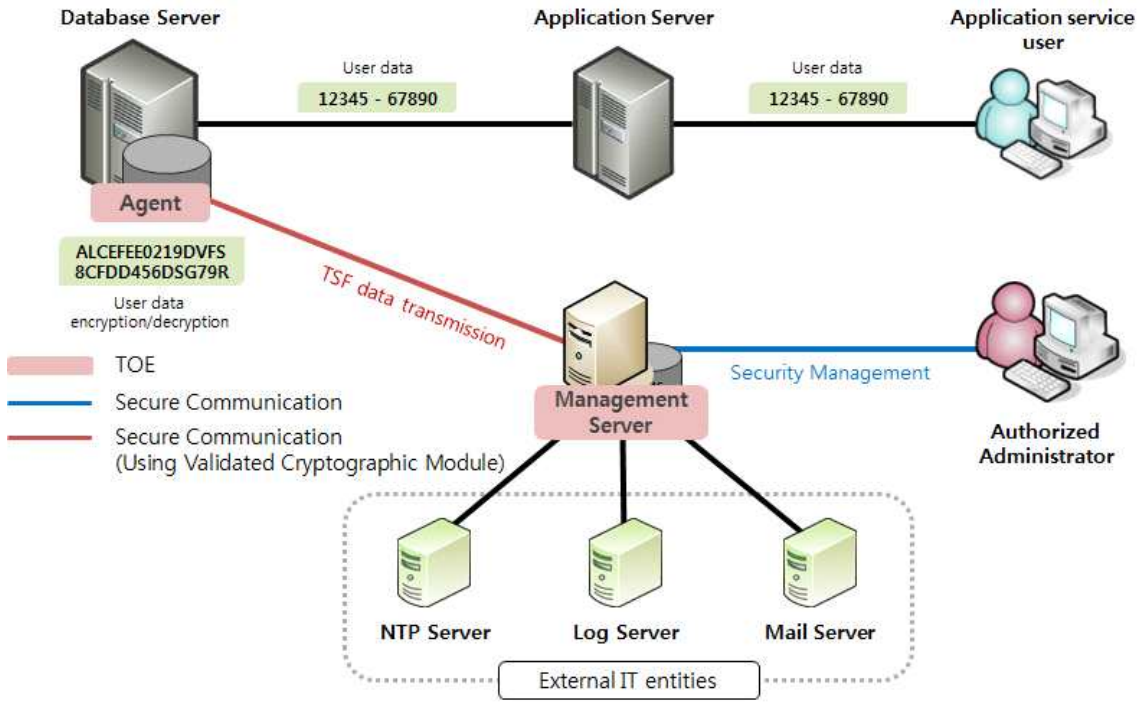
1.2.4. Non-TOE and TOE operational environment

The TOE operational environment defined in this PP can be classified into two: plug-in type and API type.

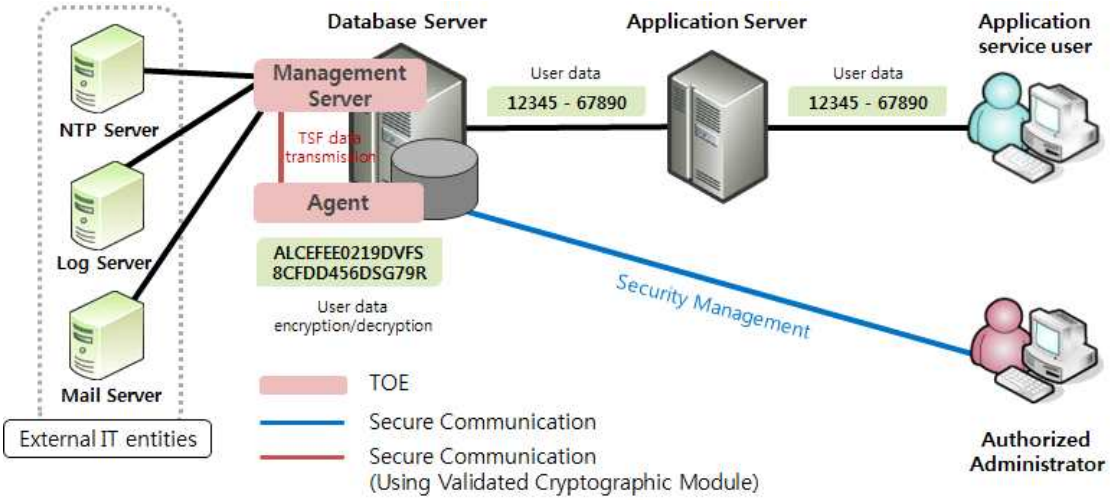
Figure 1-1 and Figure 1-2 show the general operational environment of the plug-in type. The agent, which is installed in the protected database server of the DB, encrypts the user data of the application server before storing it in the DB according to the policy configured by the authorized administrator, and decrypts the encrypted user data sent from the database server to the application server.

The authorized administrator can encrypt/decrypt the user data through the management server according to the scope of the encryption that is required by the organizational security policy. In addition, the authorized administrator can perform security management through access to the management server. The management server can be installed in the database server along with the agent, or installed separately from the agent. The ST author shall clearly identify the operating

location of the management server in the TOE operational environment, depending on the operation type of the TOE component.



[Figure 1-1] Plug-in type operational environment (Agent, management server separate type)

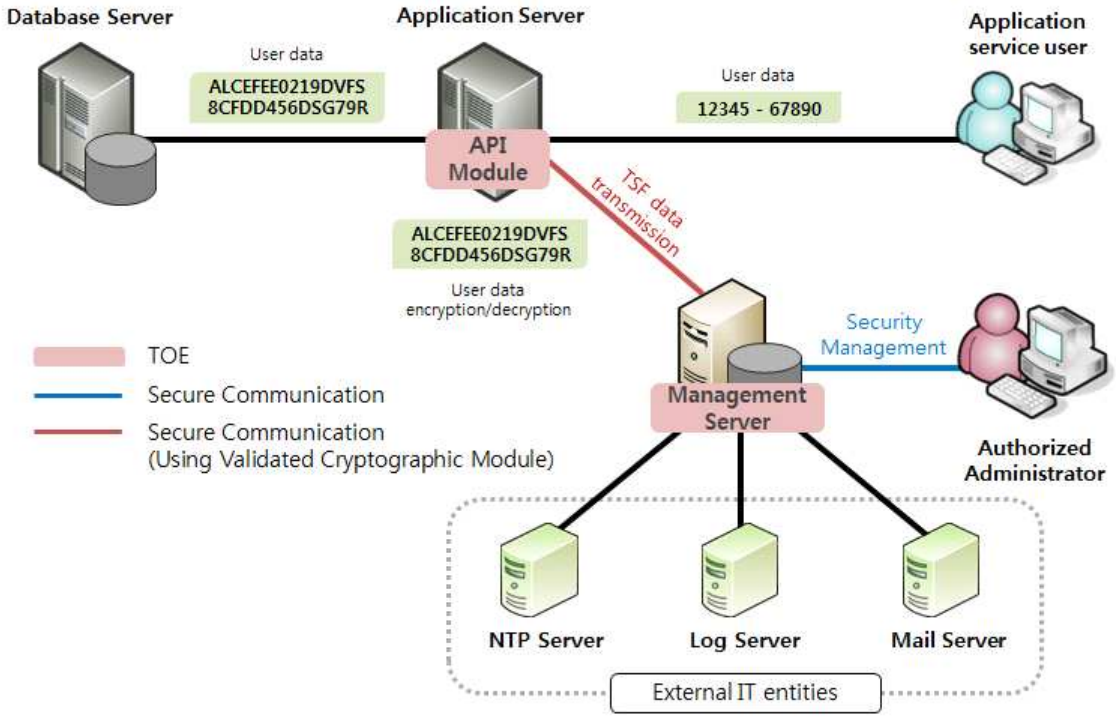


[Figure 1-2] Plug-in type operational environment (Agent, management server integrated type)

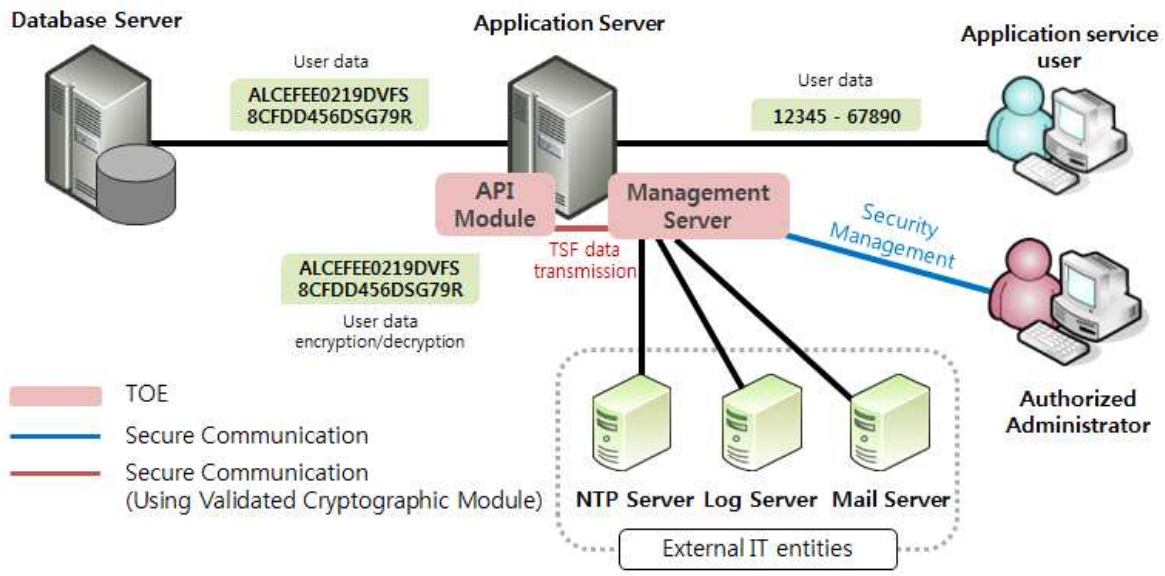
Figure 2-1 and Figure 2-2 show the general operational environment of the API type. The application, which is installed in the application server and provides application services, is developed using the API provided by API module in order to use the cryptographic function of the TOE. The API module is installed in the application server and performs encryption/decryption of the user data in accordance with the policies configured by authorized administrator. The user data entered by the application service user is encrypted by the API module, which is installed in the application server, and sent to the database server. The encrypted user data received from the

database server is decrypted by the API module, which is installed in the application server, and sent to the application service user.

The authorized administrator can encrypt/decrypt the user data through the management server according to the scope of the encryption required by the organizational security policy. In addition, the authorized administrator can perform security management through access to the management server. The management server can be installed in the application server along with the agent, or installed separately from the API module. The ST author should clearly identify the operating location of the management server in the TOE operational environment, depending on the operation type of the TOE component.



[Figure 2-1] API-type operational environment (API module, management server separate type)



[Figure 2-2] API-type operational environment (API module, management server integrated type)

The communication among the TOE components shall be based on the encrypted communication using the approved cryptographic algorithm of the validated cryptographic module. Even though the TOE is operated as an integrated type, the TSF data shall be shared among the TOE components through the encrypted communication using the validated cryptographic module. In addition, the encrypted communication shall be also applied using the validated cryptographic module when the authorized administrator accesses the management server using the TOE component that has been added separately (e.g., management console). However, the use of OpenSSL etc. that implements the security protocol is allowed only when communication is needed between the external IT entity and the TOE component (e.g., the administrator accesses the management server using the web browser).

The TOE user can be defined in various ways depending on the TOE operation and implementation. For the plug-in type, the authorized administrator who performs security management on the TOE using the management server is identified as the human user of the TOE. The DBMS that manages the DB in the database server and the application which is developed to provide application service in the application server can be the user of the TOE as the external IT entity, if the security function provided by the agent is used. For the API type, the authorized administrator who performs security management on the TOE using the management server is the human user of the TOE. The application developed to provide application service in the application server becomes the user of the TOE as the external IT entity when the security function provided by the API module is used.

The external IT entity needed to operate the TOE includes 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 author of the TOE that claims conformance to this PP shall identify all external IT entities that interact with the TOE in the ST.

The ST author shall include FAU_STG.1, an optional security functional requirement, in the ST when the protected audit trail storage function is implemented in the TOE. If the function is not implemented in the TOE, the function must be provided in the operating environment (for example:

using a DBMS, etc.), and accordingly, the security objectives for the operational environment must be added.

The ST author shall include FPT_STM.1, an optional security functional requirement, in the ST if the TOE implements a function that provides reliable time stamps. If the function is not implemented in the TOE, the function must be provided by the operating environment (for example: provided by the operating system, etc.), and accordingly, the security objectives for the operational environment must be added.

The ST author shall include the optional security functional requirements defined in this PP if the following conditions are met.

- The ST author should include FTP_TRP.1 in the ST if the authorized administrator accesses the management server through the external IT entity like a web browser.
- 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 function 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 optionally included in the ST if the TOE provides the security features that implement 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 when applying each optional security functional requirement 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.

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 *underlined and italicized.*

Refinement

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

Security Target (ST) Author

This is used to represent the final decision of attributes being made by the ST author. The ST author's operation is denoted in braces, as in {decided by the ST author}. In addition, operations of 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.

Approved cryptographic algorithm

A cryptographic algorithm selected by Korea 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

Application Server

The application server defined in this PP refers to the server that installs and operates the application, which is developed to provide a certain application service by the organization that operates the TOE. The pertinent application reads the user data from the DB, which is located in the database server, by the request of the application service user, or sends the user data to be stored in the DB to the database server.

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

Authorized Administrator

Authorized user to securely operate and manage the TOE

Authentication Data

Information used to verify the claimed identity of a user

Authorized 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

Column

A set of data values of a particular simple type, one for each row of the table in a relational database

Component

Smallest selectable set of elements on which requirements may be based

Critical Security Parameters (CSP)

Information related to security that can erode the security of the encryption module if exposed or changed (e.g., verification data such as secret key/private key, password, or Personal Identification Number).

Class

Set of CC families that share a common focus

Database

A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this PP, refers to the relational database.

Database Server

The database server defined in this PP refer to the server in which the DBMS managing the protected DB is installed in the organization that operates the TOE

DBMS (Database Management System)

A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this PP, refers to the database management system based on the relational database model.

Data Encryption Key (DEK)

Key that encrypts and decrypts 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

Encryption

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

Element

Indivisible statement of a security need

External Entity

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

Evaluation Assurance Level (EAL)

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

Family

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

Identity

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

Iteration

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

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Management access

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

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

Random bit generator

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string 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

Security Function Policy (SFP)

A Set of rules that describes the specific security action performed by TSF (TOE security functionality) and describe them as SFR (security function requirement)

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 Target (ST)

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

Security attribute

The characteristics of the subject used to define the SFR, user (including the external IT product), object, information, session and/or resources. These values are used to perform the SFR

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

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

Symmetric cryptographic technique

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

Subject

Active entity in the TOE that performs operations on objects

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 a 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

User

Refer to "External entity"

User Data

Data for the user, that does not affect the operation of the TSF

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 database 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, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security assurance components	*Conformant*
	Package	Augmented: EAL1 *augmented* (ATE_FUN.1)

2.2. PP conformance clam

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 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.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.

OE.LOG_BACKUP

The authorized administrator of the TOE 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 entities operating in the same operating system do not affect the secure operation of the TOE.

4. Extended components definition

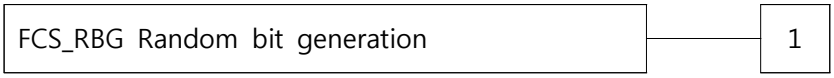
4.1. Cryptographic support

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*].

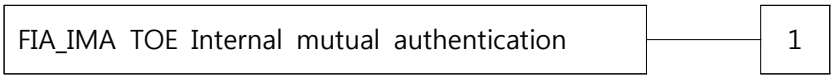
4.2. Identification and authentication

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 family is included in the PP/ST:

a) Minimal: Success and failure of mutual authentication
b) Minimal: Modification of authentication protocol

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*] using the [assignment: authentication protocol] that meets the following [assignment: *list of standards*].

4.3. User data protection

4.3.1. User data encryption

Family Behaviour

This family provides requirements to ensure confidentiality of user data.

Component leveling

FDP_UDE.1 User data encryption requires confidentiality of user data.

Management : FDP_UDE.1

The following actions could be considered for the management functions in FMT:
a) Management of user data encryption/decryption rules

Audit : FDP_UDE.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 user data encryption/decryption

4.3.1.1. FDP_UDE.1 User data encryption

Hierarchical to	No other components.
Dependencies	FCS_COP.1 Cryptographic operation
FDP_UDE.1.1	TSF shall provide TOE users with the ability to encrypt/decrypt user data according to [assignment: *the list of encryption/decryption methods]* specified.

4.4. Security Management

4.4.1. 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 ID and password	1

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.

4.4.1.1. 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.

4.5. Protection of the TSF

4.5.1. Protection of stored TSF data

Family Behaviour

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

Component leveling

FPT_PST Protection of stored TSF data	1

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

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

4.5.1.1. 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.

4.6. TOE Access

4.6.1. Session locking and termination

Family Behaviour

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

Component leveling

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

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

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

Management: FTA_SSL.5

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

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

4.6.1.1. 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 user(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 Database Encryption
- Optional SFRs: are not required to be mandatorily implemented in database 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 (User data 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 (User data 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_UDE.1(Extended)	User data encryption	**Mandatory SFR**
	FDP_RIP.1	Subset residual information protection	**Mandatory 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_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_STM.1	Reliable time stamps	Optional SFR
	FPT_TEE.1	Testing of external entities	Optional SFR
	FPT_TST.1	TSF testing	**Mandatory 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**
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 database 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	Protected audit trail storage
	FAU_STG.4	Action in case of possible audit data loss
FCS	FCS_CKM.1(1)	Prevention of audit data loss
	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 (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(Extended)	Random bit generation
FDP	FDP_UDE.1(Extended)	User data encryption
	FDP_RIP.1	Subset residual information protection
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_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_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, [selection: [assignment: *other specifically defined auditable events*], *no other components*].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Refer to the contents of "additional audit record" in [Table 3] Audit events, [selection: [assignment: *other audit relevant information*], *no other components*].

Application notes

o If FAU_GEN.1.1 cannot apply the "auditable events" in Table 3, the ST author can perform refinement operation in Table by presenting an audit event that is equal to the pertinent audit event or can be replaced with a stricter level.

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 IT entity (e.g., reliable NTP server), the audit record related to time changes shall be stored. In this case, the ST author shall perform the assignment operation to add an audit event regarding the time change, and add the ST regarding for the operational environment related to the reliable time stamp in the ST.

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(1)	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	
FCS_CKM.4	Success and failure of the activity (only applying to destruction of key related to user data encryption/decryption)	
FCS_COP.1(1)	Success and failure of the activity	
FDP_UDE.1 (Extended)	Success and failure of user data encryption/decryption	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_IMA.1 (Extended)	Success and failure of mutual authentication Modify of authentication protocol	

Security functional component	Auditable event	Additional audit record
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_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1 (Extended)	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	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 (Extended)	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

[Table 3] Audit event

5.1.1.3. FAU_SAA.1 Potential violation analysis

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

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

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

a) Accumulation or combination of [authentication failure audit event among auditable events of FIA_UAU.1, integrity violation audit event and selftest failure event of validated cryptographic module among auditable events of FPT_TST.1, [assignment: *subset of defined auditable events*]

known to indicate a potential security violation

b) [assignment: *any other rules*]

Application notes

o The ST author shall specify the result of performing the assignment operation to 'FAU_SAA.1.2 – b)' rule for the audited event assigned to 'FAU_SAA.1.2 – a)' in the PP.

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

Application notes

o Example of criteria with logical relations: AND, OR and etc.

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 Example of the pre-defined limit: 80% of audit storage capacity, 90% of audit storage capacity, etc.

o Example of response actions related to "notification to the authorized administrator": Alarm,

email sending to the administrator, etc.

o If the loss of the audit data is forecasted, the function of sending the audit data to the external log server or backup server can be provided as the response action of the TSF and/or authorized administrator. If the audit data is sent to the external log server or backup server through the trusted channel, the ST author shall include "optional SFR" FTP_ITC.1.

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 oldest stored audit records, etc.) shall be taken to prevent the loss of audit data.

5.1.2. Cryptographic support (FCS)

5.1.2.1. FCS_CKM.1(1) Cryptographic key generation (User 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(1) User data encryption". If there are more than two cryptographic key generation algorithms in the list, it is recommended to perform iteration operation on this SFR.

o It shall perform cryptographic key generation using the cryptographic algorithm validated

in Korea Cryptographic Module Validation Program (KCMVP).

- o It is not allowed to generate an cryptographic key by using the password in this SFR. If a random bit is used to generate the cryptographic key, the requirements in FCS_RBG.1 shall be satisfied.
- 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(1) User data encryption". If there are more than two cryptographic key generation algorithms in the list, it is recommended to perform iteration operation on this SFR.
- o It shall perform cryptographic key generation using the cryptographic algorithm validated in Korea Cryptographic Module Validation Program (KCMVP).
- o Generating an encryption key by deriving it from the password is not allowed, except the key encryption key (KEK).
- o When deriving an key encryption key (KEK) key from the password, a approved cryptographic algorithm like HMAC-SHA2 must 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 should be used as iteration count.
- o If random bits are used to generate encryption key, the requirements of FCS_RBG.1 shall be satisfied.
- 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 This SFR contains the cryptographic key distribution requirements that can be used to perform the function of mutual authentication among the TOE components, user data encryption, and encrypted communications among the TOE components. If the cryptographic key distribution method is more than 2, it is recommended to perform iteration operation for this SFR.
- o The key used by the cryptographic key establishment 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 implemented, the approved cryptographic algorithm of the validated cryptographic module has safety and implementation suitability 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 This SFR shall be applied to all cryptographic keys covered in FCS_CKM.1(1), FCS_CKM.1(2)

5.1.2.5. FCS_COP.1(1) Cryptographic operation (User 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 'FDP_UDE.1 User Data Encryption'. 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 ECB mode cannot be used when performing encryption using the block cipher algorithm, regardless of the size of plain text. IV in CBC, CFB, and OFB mode, as well as a counter in CTR mode, shall be used by applying the method presented in the appendix of the 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 (User Data 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 Mutual authentication among the TOE components, FPT_ITT.1 Basic protection of the internally transmitted TSF data, 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 Cryptographic operation shall be performed using the approved cryptographic algorithm of the validated cryptographic module of which safety and implementation suitabilities 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 ECB mode cannot be used when performing encryption using the block cipher algorithm, regardless of the size of plain text. IV in CBC, CFB, and OFB mode, as well as a counter in CTR mode, shall be used by applying the method presented in the appendix of the 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(2) Cryptographic key generation (TSF Data Encryption)'.
- 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 shall be performed using the approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

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

5.1.3. User data protection (FDP)

5.1.3.1. FDP_UDE.1 User data encryption (Extended)

Hierarchical to	No other components.
Dependencies	FCS_COP.1 Cryptographic operation
FDP_UDE.1.1	The TSF shall provide a function that can encrypt/decrypt the user data to the TOE user according to the specified [encryption/decryption method by column, [assignment: *List of other encryption/decryption methods*]].

Application notes

o As this SFR is related to the user data encryption/decryption function, the same ciphertext shall be generated for the same plaintext when encrypting the user data.

o If the [assignment: *list of other encryption/decryption method*] doesn't exist, the ST author can specify "None" in the assignment operation.

o The cryptographic key generation and cryptographic operation function used to implement the encryption/decryption function of this SFR shall be specified in the ST by referring to the FCS class.

5.1.3.2. FDP_RIP.1 Subset residual information protection

Hierarchical to	No other components.
Dependencies	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to, deallocation of the resource from* the following objects: [user data].

Application notes

o In FDP_RIP.1.1, 'not available' means unrecoverable deletion.

o When user data encryption/decryption are performed at the TOE operational environment (Application Server, or Database Server) by further development (or modification) of the TOE purchaser, the TOE operational environment shall be developed in accordance with the requirements provided by the TOE and this note shall be described in the TOE guidance documents.

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. This requirement shall be applied when implementing the management access (SSH, HTTPS, etc.) function provided by the TOE.
  - Number of authentication failures: five or less by default
  - List of actions: identification and authentication function inactivation (5 minutes or more by default)
- o If the number of authentication failure times and response action are set differently according to the TOE administrator and management access (SSH, HTTPS, etc.), the ST author can apply iteration operation.

5.1.4.2. FIA_IMA.1 TOE Internal mutual authentication (Extended)

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication using [assignment: *authentication protocol*] in accordance with [assignment: *list of standards*] between [assignment: *different parts of TOE*].

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 iterating operation according to the communication sector among the TOE components.
- o This SFR must be applied to the TOE components of which the TOE shape is physically separated regardless of the operating type – integrated type or separate type.

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 shall perform cryptographic operation using the approved cryptographic algorithm of the validated cryptographic 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 must run in approved operation mode.

- 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 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 Confidential information verification can be applied when generating or modifying any passwords, such as generating a new password by the administrator, changing the password, and changing the password when the administrator logs in for the first time. This requirement shall be applied when implementing the management access (SSH, HTTPS, etc.) function provided 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, etc.

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

Application notes

- o The administrator role may be divided into multiple roles depending on the management function of access privileges. When dividing the administrator roles into multiple roles, requirements shall be defined in FMT_SMR.1. This requirement shall be applied when implementing the management access (SSH, HTTPS, etc.) function provided by the TOE.
- 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, 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 user sessions are the same such as password-based authentication method, it is possible to bypass the administrator, 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.

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 and the followings are masked. Methods such as concealing user's input password on the screen are acceptable for preventing the input password disclosure.
  - When generating, changing the administrator password and authenticating the administrator
- 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 This requirement shall be applied when implementing the management access (SSH, HTTPS, etc.) function provided by the TOE.

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 **authorized administrator** to be performed before the **authorized administrator** is identified.

FIA_UID.1.2 The TSF shall require each **authorized administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **authorized administrator** , 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 end 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.) of the TOE.

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_UDE.1	Management of the user data encryption/decryption rules	Management of security attributes
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Management of TSF data threshold
	Management of actions to be taken in the event of an authentication failure	Management of security functions
FIA_IMA.1	Management of the authentication protocol for mutual authentication	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	Management of TSF data

Security functional component	Management function	Management type
	associated user	
	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_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 should 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 roles*].

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.
- 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_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*** [assignment: list of *TSF data*] to [assignment: *the authorized roles*].

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.

5.1.5.3. 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 [assignment: *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 [assignment: *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: *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 function to manage the combination rules and length for each ID and password to the authorized administrator, '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*] of FMT_PWD.1.1 including the generation and modification of administrator's password.

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.

5.1.5.4. 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.

5.1.5.5. 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 applying to this SFR in the TOE refers to the authorized administrator. The role of the administrator can be defined in detail according to the access right of management function.

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 the TSF data from *disclosure, modification* by **verifying encryption and message integrity** when the TSF data is transmitted among TOE's separated parts.

Application notes

- o This SFR must be applied to the TOE components of which the TOE shape is physically separated regardless of the operating type – integrated type or separate type – when transmitting the TSF data.
- 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 password, encryption key(pre-shared key, symmetric key, private key, etc.), CSP, TOE configuration values(security policy, configuration parameters, etc.), control command, audit data, etc.

o If the administrator password, cryptographic key, CSP, TOE configuration value, account information used to access the external IT entity (e.g., DBMS account, etc.), or DEK is stored inside/outside of the TOE, the data shall be encrypted before storing in such way that the requirements of 'FCS_COP.1(2) Cryptographic operation (TSF data encryption)' can be satisfied regardless of the storing location and type. If some of these details are included, the entire data must be encrypted.

- The mandatory encryption target information shall also be encrypted and stored in the DB that is managed by the DBMS providing the function of identification, authentication, and access control.
- If the TSF data doesn't include the information that must be encrypted, the application of internally implemented encoding technique is allowed.
- 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 encryption key (DEK) should be encrypted and saved with the approved cryptographic algorithm provided by the validated cryptographic module, using the key encryption key (KEK). KEK should be saved in a safe manner in the derivation or security token, using the password-based key derivation method.

o Cryptographic keys and key materials loaded onto memory shall not exist in plain text in memory. Note, however, that disclosure as plaintext is allowed when the encryption key and critical security parameter are used for encryption/decryption operation. If encryption/decryption is completed and not used, they should not exist as plain text.

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

5.1.6.3. 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 administrators** 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 administrators** with the capability to verify the integrity of [selection: [assignment: *parts of TSF data], TSF data*].

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, information flow 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 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 TOE shall apply operation (iteration, refinement, etc.) so that the following can be satisfied:

- The integrity of the TOE's setting value and executable file shall be checked at the initial phase of the TOE operation.
- A function that verifies the setting value of the TOE (e.g., security policy, environment setting parameter) shall be provided to the authorized administrator and 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 should receive 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 [belonging to the same **administrator** according to the rules for the list of management functions defined in FMT_SMF1.1]

a) limit the maximum number of concurrent sessions to 1 for management access by the same administrator who has the right to perform FMT_MOF.1.1 "Management actions" and FMT_MTD.1.1 "Management."

b) limit the maximum number of concurrent sessions to {what is determined

by the ST author} for management access by the same administrator who doesn't have the right to perform FMT_MOF.1.1 "Management actions" but has the right to perform a query in FMT_MTD.1.1 "Management" only

c) [assignment: *other rules for the maximum number of concurrent sessions*]

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

Application notes

- o A session is presented in FMT_MCS.2 is 'administrator access', the number of sessions should be 'the number of administrator accesses.'
- o In the FTA_MCS.2.1, the administrators corresponding to 'b)' is generally an administrator who can only monitor.
- o When restricting the number of management access sessions to the TOE by each service (e.g. SSH, HTTPS, etc.), it is defined in assignment operation of FTA_MCS.2.1.
- o After one device makes administrator's management access, another device performs a login 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.
- o In case there is no other rules for the number of maximum concurrent sessions in FTA_MCS.2.1, "None" may be specified in the assignment operation.
- o In case the TOE provides both management access and local access, the ST author shall conduct assignment operation in FTA_MCS.2.1 to specify that it is not allowed for the users with the same privilege to concurrently connect to the TOE using both management access session and local access session.

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-authenitcate the administrator before unlocking the session,*
- *terminate*] the administrator's interactive session after a [assignment: *time*

interval of the 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 local access(console port) and management access (SSH, HTTPS, etc.) supported by the TOE.
- o If 'Session termination' is selected in selection operation of FTA_SSL.5.1, "None" can be applied to the subordinate relationship of this SFR.
- o If 'Re-authentication by the administrator before locking the session and/or unlocking the session' is selected, it is not allowed to specify 'Re-authentication by the administrator before unlocking the session' by removing 'locking the session and/or.'
- 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.
- o 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 and service (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 dependencie
FTA_TSE.1.1	The TSF shall be able to refuse the **management access session of the administrator**, based on [Access IP, [Selection: *Access time, the status of activating the management access session of the administrator having the same rights*, [assignment: *attributes of other management function*], None]].

Application notes

- o The management access session of administrator shall be allowed only from the terminal with designated IP address for administrator 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 administrator IP address that can access the TOE can be specifically designated for the

administrator who has the read-only right (e.g., monitoring). However, the IP address range cannot be added by designation (e.g., 192.168.10.2~253) when setting the accessible IP of the administrator, and the IP address shall be added one by one. In addition, IP address settings like 0.0.0.0, 192.168.10.*, are not allowed, which means the entire network range.

5.2. Security functional requirement (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	
FPT	FPT_STM.1	Reliable time stamps	
	FPT_TEE.1	Testing of external entities	
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 Protection 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 implemented by can be optional 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 objectives regarding for the operational environment related to the protection of the audit trail storage in the ST.

5.2.2. Protection of the TSF

5.2.2.1. 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 said function additionally, the ST author shall include this requirement in SFRs.
- 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.

5.2.2.2. 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 FPT_TEE.1 The external entity test is a functional requirement ("optional SFR") that can be implemented optionally. The ST author shall include this requirement in SFR if there is the TOE external entity interfacing with the TOE and the major TOE functions and security functions are affected by the abnormal state of the external entity (e.g., error, shutdown, etc.).
- 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, etc) 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 IT entity 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. Trusted path/channels

5.2.3.1. 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, they shall additionally derive the security problem definition and security objectives when necessary.
- o Examples of the trusted IT product presented in FTP_ITC.1 are external log server, update server, etc.
- o If the TSF interfaces with trusted IT products, the TSF and the IT products shall protect the TSF data (e.g., audit data, authentication data, and TOE configuration file) from unauthorized disclosure and change using the cryptographic communication 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.
  - If the ST author has added this SFR to the ST, the SFR regarding cryptographic key generation (FCS_CKM.1) and cryptographic operation (FCS_COP.1), which is additionally required, shall be added by referring to the cryptographic key support (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.

5.2.3.2. 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 function additionally, the ST author shall include this requirement in the SFR.
- o The TOE shall provide a trusted channel using the cryptographic 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. If the SSH protocol is supported, it shall support SSH v2(RFC 4251 ~ 4254) or its successors.
  - 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 operating 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 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 should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security

	measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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 TOE Lavelling 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 requirements.

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	Rationale(1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	Rationale(2)
7	FAU_STG.4	FAU_STG.1	Rationale(2)
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	10, 12
		FCS_CKM.4	11
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	10, 13
		FCS_CKM.4	11
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
		FCS_CKM.4	11
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9
12	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	11
13	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	9

No.	Security functional requirements	Dependency	Reference No.
		FCS_CKM.4	11
14	FCS_RBG.1	-	-
15	FDP_UDE.1	FCS_COP.1	12
16	FDP_RIP.1	-	-
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	-	-
24	FMT_MOF.1	FMT_SMF.1	27
		FMT_SMR.1	28
25	FMT_MTD.1	FMT_SMF.1	27
		FMT_SMR.1	28
26	FMT_PWD.1	FMT_SMF.1	27
		FMT_SMR.1	28
27	FMT_SMF.1	-	-
28	FMT_SMR.1	FIA_UID.1	23
29	FPT_ITT.1	-	-
30	FPT_PST.1	-	-
31	FPT_TST.1	-	-
32	FTA_MCS.2	FIA_UID.1	23
33	FTA_SSL.5	FIA_UAU.1	20
34	FTA_TSE.1	-	-

[Table 7] Rationale for the dependency of the security functional requirements

Rationale(1) : FAU_GEN.1 has the dependency on 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_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., DBMS), the author shall add the security objectives for the operational

environment and provide justification that a subordinate relationship is satisfied.

Rationale(2) : FAU_STG.3 and FAU_STG.4 have the dependency on 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 SAR 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
IPSec	Internet Protocol Security
IT	Information Technology
IV	Initial Vector
KEK	Key Encryption Key
NTP	Network Time Protocol
OFB	Output Feedback
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