Korean National

Protection Profile for

Single Sign On

V1.1

2019. 12. 11.

NSR
국가보안기술연구소
National Security Research Institute

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

Foreword

This Protection Profile has been developed with the support of National Security Research Institute (NSR) under the agreement between National Intelligence Service (NIS) and Ministry of Science and ICT (MSIT). The Protection Profile author developed the security requirements for Single Sign On 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**

1.2. TOE overview **1**

1.2.1. Single Sign On 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 4

1.3. Conventions **7**

1.4. Terms and definitions **8**

1.5. PP organization **13**

2. Conformance claim **14**

2.1. CC conformance claim **14**

2.2. PP conformance claim **14**

2.3. Package conformance claim **14**

2.4. Conformance claim rationale **14**

2.5. PP conformance statement **14**

3. Security objectives **15**

3.1. Security objectives for the operational environment **15**

4. Extended components definition **17**

4.1. Cryptographic support **17**

4.1.1. Random Bit Generation 17

4.2. Identification and authentication **18**

4.2.1. TOE Internal mutual authentication 18

4.2.2. Specification of Secrets 18

4.3. Security Management **19**

4.3.1. ID and password 19

4.4. Protection of the TSF **21**

4.4.1. Protection of stored TSF data 21

4.4.2. TSF update 22

4.5. TOE Access **23**
4.5.1. Session locking and termination 23

5. Security requirements **25**
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. Identification and authentication (FIA) 36
5.1.4. Security management (FMT) 42
5.1.5. Protection of the TSF (FPT) 46
5.1.6. TOE access (FTA) 49
5.2. Security functional requirements (Optional SFRs) **52**
5.2.1. Security audit (FAU) 52
5.2.2. Identification and authentication (FIA) 53
5.2.3. Protection of the TSF (FPT) 54
5.2.4. Trusted path/channels (FTP) 56
5.3. Security assurance requirements **59**
5.3.1. Security Target evaluation 59
5.3.2. Development 63
5.3.3. Guidance documents 64
5.3.4. Life-cycle support 65
5.3.5. Tests 66
5.3.6. Vulnerability assessment 67
5.4. Security requirements rationale **68**
5.4.1. Dependency rationale of security functional requirements 68
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 Single Sign On
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-0822a-2017
Keywords	Single Sign On, SSO

1.2. TOE overview

1.2.1. Single Sign On overview

'Single Sign On (SSO)' (hereinafter referred to as "TOE") is used to enable the user to access various business systems and use the service through a single user login without additional login action. The TOE performs user identification and authentication, authentication token(hereinafter referred to as "token") issue and validity verification according to the user authentication policy.

The TOE shall provide the user login capability using various authentication methods (e.g., ID and password, certificate, security card), issue a token during user login, and verify the issued token if accessing another business system after user login.

The primary security features provided by the TOE include user identification and authentication, token issue, storage, verification and destruction. The TOE must use a validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

1.2.2. TOE type and scope

The TOE defined by this Protection Profile is SSO that enables the user to access various business systems through a single user login, and the TOE is provided as software.

The agent and the server are the indispensable TOE component defined in this PP. The ST author that claim conformance to this PP can include a management console or client as an option, if

necessary. The TOE is composed of the server that processes user login, manages the token, and sets the policy; and the agent that is installed in each business system performs the function of token issue and verification. In addition, the agent can be one of the 'API type' composed of the library file, the 'process type' composed of the executable file, or a combination of these two types.

If a client or management console is added as a TOE component, the ST author shall define the role of the added component from the viewpoint of 'Single Sign on'.

This PP defines the minimum mandatory security functional requirements and optional security functional requirements that shall be provided by the agent and server, which are the indispensable TOE component, and the TOE shall implement those security functional requirements. If a client or management console is added to the ST that claim conformance to the PP, the mandatory security functional requirement and optional security functional requirement shall be applied to the client and management console according to the application notes.

1.2.3. TOE usage and major security features

The TOE performs user identification and authentication to enable the user to access various business systems and use the service through a single user login without additional login action, and the TOE can be supported by user identification and authentication that the external authentication systems(e.g., RADIUS, TACACS, Kerberos, or other authentication server within the organization) provide. The support by the external authentication system, however, is only allowed for the authorized end-user.

The TOE provides the security audit function that records and manages a critical events as audit data when activating the security functionality and management function, function of protecting the data that stored in the TSF controlled repository, and TSF protection function such as TSF self-testing. In addition, the TOE provides authentication failure handling, identification and authentication functions including mutual authentication between the TOE components, cryptographic support function such as cryptographic key management and cryptographic operation for issuing a token, security management function for management of security functions behaviour and configuration, and the TOE access function to manage the authorized administrator's interacting session.

In addition, the TOE can provide the function of testing the TOE's external entities, the trusted path/channels function that provides secure communication between the TOE and management access administrator, if implementation is needed.

In addition, the token requires confidentiality and integrity protection, and the TOE executable code requires integrity protection.

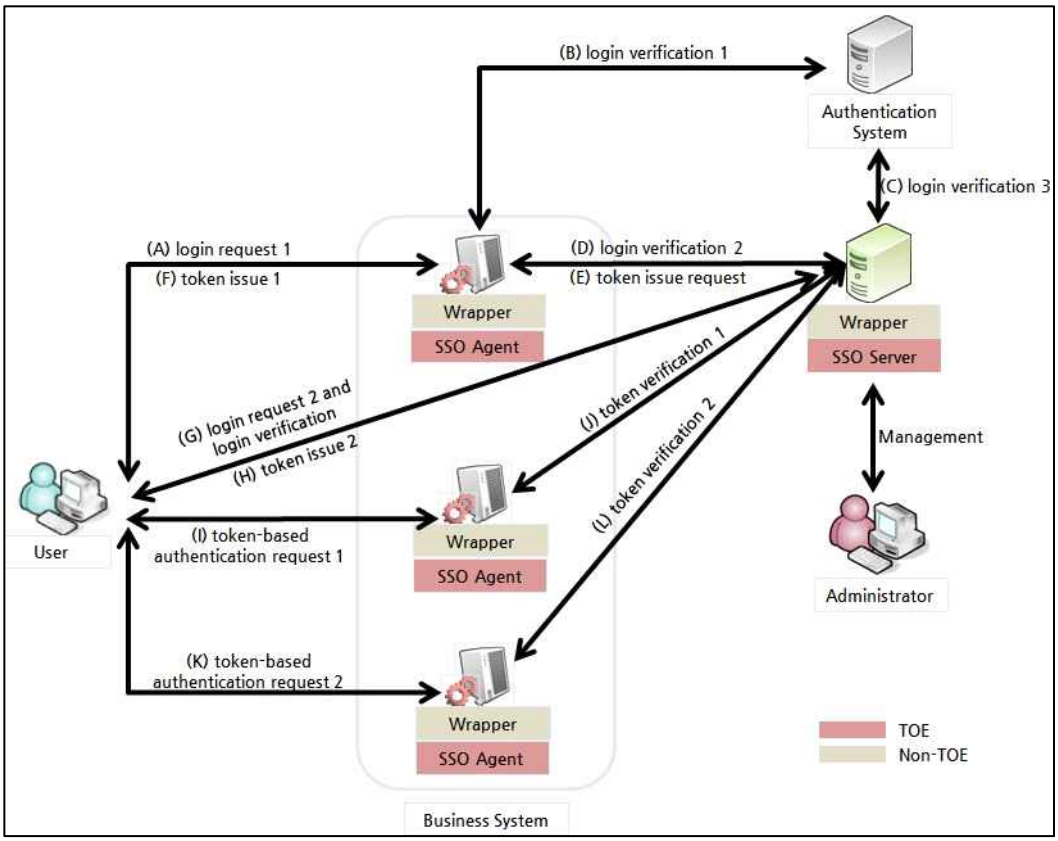
Figure 1 shows the user identification and authentication procedure of the general TOE. The detailed execution procedure can vary depending on the TOE implementation.

The user identification and authentication procedure can be grouped into the initial authentication phase using the ID/password, certificate, or security card, and the token-based authentication phase that accesses the business system using the token issued during the initial authentication procedure. The detailed execution procedure of each authentication phase can vary according to the

implementation of the TOE. The following describes one process among the general authentication procedure.

The execution procedure of the initial authentication phase is as follows. The user requests login using the ID/password or certificate, and the SSO agent that receives the login request message sends a login verification request to the SSO server, which in turn checks the authorized user status. Upon receiving the login verification request, the SSO server performs login verification directly using the user information stored in the DBMS, or by interfacing with the authentication system. The SSO server issues a token or requests token issue to the SSO agent if the login verification result is valid. The SSO server or SSO agent transfers an issued token to the user.

The token-based authentication phase is performed only when the token has been normally issued in the initial authentication phase. When the user utilizes business system services, the issued token is transferred to the SSO agent installed in the pertinent business system, and the SSO agent verifies the validity of the token by interfacing with the SSO server upon receiving the token.



[Figure 1] user identification and authentication procedure

The user identification and authentication procedure can be executed with various procedures depending on the TOE implementation. The following table shows the example of operation by phase.

authentication phase	example of operation procedure
initial authentication	(A) login request 1 → (D) login verification 2 → (E) token issue request → (F) token issue 1
	(A) login request 1 → (B) login verification 1 → (C) login verification 3 ↔ (E) token issue request → (F) token issue 1
	(A) login request 1 → (D) login verification 2 → (C) login verification 3 ↔ (E) token issue request → (F) token issue 1
	(G) login request 2 and login verification → (H) token issue 2
	(G) login request 2 and login verification → (E) token issue request → (F) token issue 1
	(G) login request 2 and login verification → (C) login verification 3 ↔ (E) token issue request → (F) token issue 1
token-based authentication	(I) token-based authentication request 1 → (J) token verification 1
	(K) token-based authentication request 2 → (L) token verification 2

[Table 1] example of operation procedure by authentication phase

In addition, the subject who issues, stores, and verifies the token can be different, depending on the implementation. The following is an example of the subject who issues, stores, and verifies the token.

- Subject who issues the token: SSO Server, SSO Server + SSO Agent, etc.
- Token storage location: User PC(Web browser/Client), User PC + SSO Agent, etc.
- Subject who verifies the token: SSO Server, SSO Server + SSO Agent, etc.

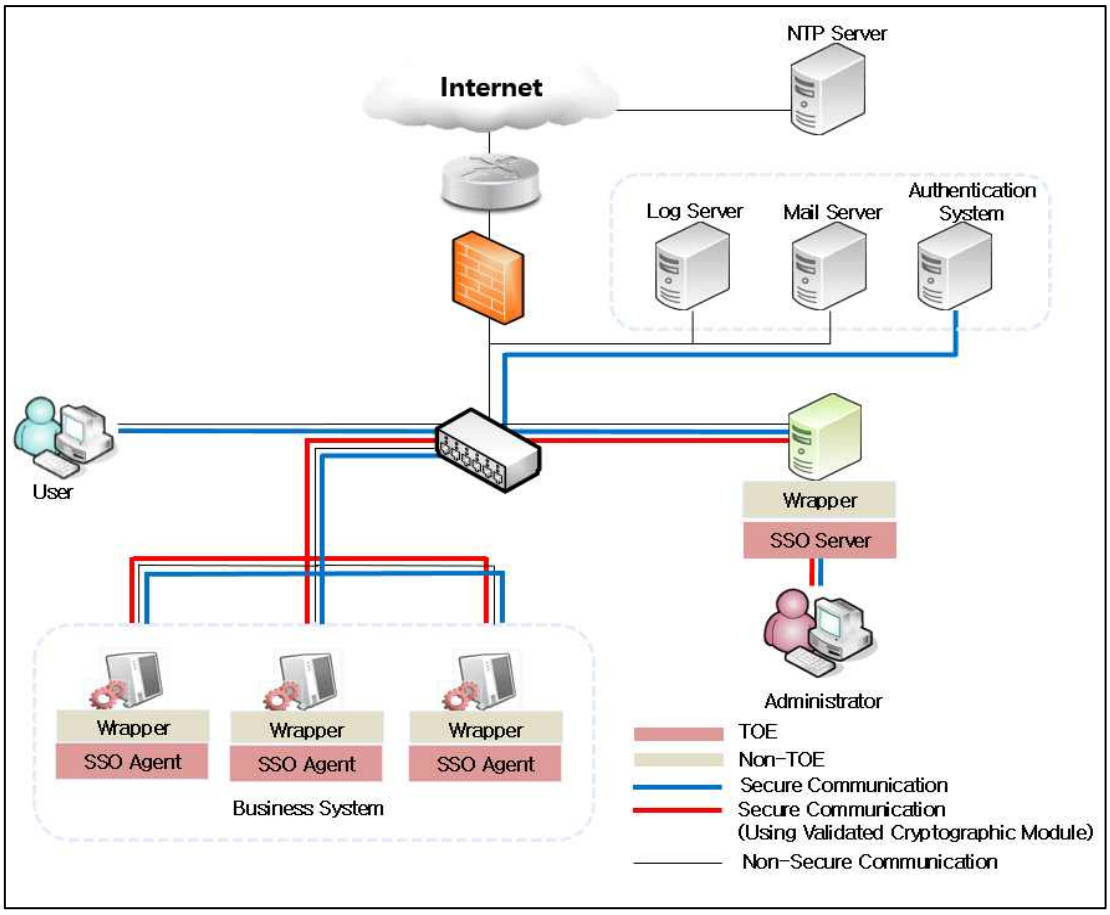
1.2.4. Non-TOE and TOE operational environment

Figure 2 shows the general TOE operational environment. Figure 2 is one of the various operational environments and is composed of the SSO server and SSO agent. The SSO server verifies user login attempts directly using the user information stored in the DBMS, or provides the user login verification resulted from the authentication system (e.g., RADIUS, TACACS, Kerberos, and other authentication servers inside the organization), the token management, and the policy configuration. The SSO agent is installed in each business system and requests user login verification to the SSO server or issues the token. In addition, the SSO agent can be one of the 'API type' composed of the library file, the 'process type' composed of the executable file, or a combination of two types. In addition, the client program that manages the token in the user PC and the management console for the TOE management can be included in the TOE component according to the implementation. Wrappers which may be used to support various types of authentication mechanisms (e.g., OTP, certificate) or compatibility with business systems are out of the TOE scope.

There may exist various external entities necessary for the operation of the TOE, including the NTP server to synchronize time, log server to store the audit data outside and manage the audit data, email server to notify the authorized administrator in case of audit data loss, and the authentication

system for the end-user identification and authentication.

The ST author, which claims conformance to this PP, shall describe any external entities that interact with the TOE.



[Figure 2] TOE operational environment

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

The ST author shall include FAU_STG.1, which is the optional security functional requirement, in the ST if the TOE implements the protected audit trail storage function. If this function is not implemented in the TOE, the operational environment shall provide the function (e.g. using DBMS, etc.) and accordingly, the security objective for the operational environment shall be added.

The ST author shall include FPT_STM.1, which is the optional security functional requirement, in the ST if the TOE implements the reliable time stamp function. If this function is not implemented in the TOE, the operational environment shall provide the function (e.g. provided by the operating system, etc.) and accordingly, the security objective for the operational environment shall be added.

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

- If the TOE provides multiple authentication mechanisms (e.g., certificate-based authentication method, OTP method) additionally, FIA_UAU.5 shall be included.

- If the authorized administrator or end-user accesses the SSO server directly using the web browser or terminal connection program, FTP_TRP.1 shall be included. If they access the SSO server via the web server, FTP_TRP.1 and FTP_ITC.1 shall be included. If direct communication between the management console and SSO server is implemented, FPT_ITT.1 shall be included. In addition, if management access is provided by communication between the web browser of the administrator PC and SSO server operating environment (web server), the ST author shall describe this security functional requirement by replacing it with the security objectives for the operational environment.

- If the SSO server is supported by the external authentication system (e.g., RADIUS, TACACS, Kerberos, and other authentication servers in the organization), FTP_ITC.1 shall be included.

- The ST author shall include FPT_TEE.1 in the ST if there is an external entity that interact with the TOE, and the major and security features of the TOE are affected by the abnormal state of the external entity (e.g., error, shutdown, etc.).

The optional security functional requirements except for the above can be selectively included in the ST if the TOE provides the security features that 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 applicable 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.

Application Programming Interface (API)
A set of software libraries that exist between the application layer and the platform system layer and facilitate the development of applications that run on the platform

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

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

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

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

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

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

Authentication Data
Information used to verify a user's claimed identity

Authentication token
Authentication data that authorized end-users use to access the business system

Authorized Administrator
Authorized user to securely operate and manage the TOE

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

Business System
An application server that authorized end-users access through 'SSO'

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

Class
Set of CC families that share a common focus

Client
Application program that can access the services of SSO server or SSO agent through network

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)

Database Management System (DBMS)
A software system composed to configure and apply the database.

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

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

Element
Indivisible statement of a security need

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

end-user
Users of the TOE who want to use the business system, not the administrators of the TOE

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

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

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

Kerberos
A centralized authentication scheme, described in RFC 1510, that provides user authentication using symmetric cryptographic technique in a distributed computing environment

Korea Cryptographic Module Validation Program (KCMVP)

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

Management access

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

Management Console

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

Object

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

Operation(on a component of the CC))

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

Operation(on a subject)

Specific type of action performed by a subject on an object

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 key

Public Security Parameters (PSP)

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

Random bit generator (RBG)

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

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

Refinement
Addition of details to a component

Remote Authentication Dial-In User Services (RADIUS)
Service to identify and authenticate users by sending information such as user ID, password and IP address to the authentication server when a remote user requests a connection

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

Secret Key
The cryptographic key which is used in symmetric cryptographic algorithm and is associated with on or more entity, it is not allowed to release

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

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

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

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

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

Sensitive Security Parameters (SSP)
critical security parameters (CSP) and public security parameters (PSP)

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

Subject
Active entity in the TOE that performs operations on objects

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

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

Terminal Access Controller Access Control System (TACACS)
Authentication protocol that is common for UNIX networks, described in RFC 1492, used by remote access server to send user login passwords to an authentication server

Threat Agent
Entity that can adversely act on assets

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

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

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

User
Refer to "External entity", authorized administrator and authorized end-user in the TOE

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

Wrapper
Interfaces for interconnection between the TOE and various types of business systems or authentication systems

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 SSO

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

2.2. PP conformance claim

This Protection Profile does not claim conformance to other PPs.

2.3. Package conformance claim

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

2.4. Conformance claim rationale

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

2.5. PP conformance statement

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

3. Security objectives

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

3.1. Security objectives for the operational environment

OE.PHYSICAL_CONTROL

The place where SSO agent and SSO server among the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.

OE.TRUSTED_ADMIN

The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidances.

OE.LOG_BACKUP

The authorized administrator shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

OE.OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

Application notes

o Depending on the implementation type of the TOE, the TOE components(SSO agent, SSO 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.

OE.SECURE_DEVELOPMENT

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

Application notes

o This security objective for the operational environment is applied when a Wrapper is used for compatibility between the SSO agent that is the TOE component and business system.

OE.AUTHENTICATION_SYSTEM_SECURITY

If TOE receives the support of the external authentication system (RADIUS, TACACS, Kerberos, or other authentication server within the organization) regarding the initial end-user identification and authentication function, the external authentication system shall support the function of storing and managing the authentication information of the authorized end-user safely.

Application notes

o This security objective for the operational environment applies only when the initial end-user identification and authentication function is supported by the external authentication system, Therefore, this does not apply to the identification and authentication of the administrator or the token-based end-user authentication.
  - FAU_GEN.1, FAU_SAA.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.7, FMT_PWD.1(Extended), FPT_PST.1(Extended), FTA_SSL.5(Extended)

o If TOE implements the initial authentication function for the end-user, the security objective for the operational environment 'OE.AUHTENTICATIO_SYSTEM_SECURITY' shall be deleted, and the following SFR related to the initial user authentication function shall be satisfied by the TOE.
  - FAU_GEN.1, FAU_SAA.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.7, FMT_PWD.1(Extended), FPT_PST.1(Extended), FTA_SSL.5(Extended)

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 Random bit generation	1

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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

4.1.1.1. FCS_RBG.1 Random bit generation

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

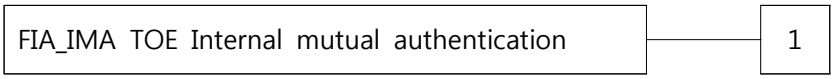
4.2. Identification and authentication

4.2.1. TOE Internal mutual authentication

Family Behaviour

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

Component leveling



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

Management: FIA_IMA.1
There are no management activities foreseen.

Audit: FIA_IMA.1

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

a) Minimum: Success and failure of mutual authentication

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

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

4.2.2. Specification of Secrets

Family Behaviour

This family defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

Component leveling

The specification of secrets family in CC Part 2 is composed of 2 components. It is now composed of three components, since this PP adds one more component as below.

※ The description on two components included in CC Part 2 is omitted.

FIA_SOS.3 Destruction of secrets requires, that the secret information be destroyed according to the specified destruction method, which can be based on the assigned standard.

Management: FIA_SOS.3
There are no management activities foreseen.

Audit: FIA_SOS.3
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimum : Success and failure of the activity

4.2.2.1. FIA_SOS.3 Destruction of Secrets

Hierarchical to	No other components.
Dependencies	FIA_SOS.2 TSF Generation of secrets
FIA_SOS.3.1	The TSF shall destroy secrets in accordance with a specified secrets destruction method [assignment: secret destruction method] that meets the following: [assignment: list of standards].

Application notes

o This SFR can be applied to the user's token.

4.3. Security Management

4.3.1. ID and password

Family Behaviour

This family defines the capability that is required to control ID and password management used

in the TOE, and set or modify ID and/or password by authorized users.

Component leveling

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

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:
a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

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

a) Minimum: All changes of the password

4.3.1.1. FMT_PWD.1 Management of ID and password

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*]. 1. [assignment: *password combination rules and/or length*] 2. [assignment: *other management such as management of special characters unusable for password, etc.*]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*]. 1. [assignment: *ID combination rules and/or length*] 2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

Application notes

- o If the TOE does not provide the capability for managing the ID and password combination rules by authorized roles, etc., 'None.' may be specified in assignment operations of FMT_PWD.1.1, FMT_PWD.1.2.
- o The ID and password combination rules that can be set by authorized roles may include minimum and maximum length setting, mixing rule setting involving English upper case/lower case/number/special characters, etc.

4.4. Protection of the TSF

4.4.1. Protection of stored TSF data

Family Behaviour

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

Component leveling

FPT_PST 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.

4.4.1.1. FPT_PST.1 Basic protection of stored TSF data

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

Application notes

- o Containers controlled by the TSF mean storage in the TOE or external entities (DBMS, etc.) that interact with the TOE.
- o Examples of TSF data to be protected as follows:
  - User password, cryptographic key (pre-shared key, symmetric key, private key, etc), TOE configuration values (security policy, environment setting, configuration parameters), audit data, etc.
- o The TSF data can be encrypted and stored to be protected from the unauthorized disclosure or modification.

4.4.2. TSF update

Family Behaviour

This family defines TOE firmware/software update requirements.

Component leveling

FPT_TUD TSF update	1

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

Management: FPT_TUD.1

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

Audit: FPT_TUD.1

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

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

4.4.2.1. FPT_TUD.1 TSF security patch update

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Application notes

- o The TSF shall provide the capability to check the current version of the TOE that most recently installed and executed by authorized roles.
- o The latest updates and security patches are essential to remove security vulnerabilities. The validity verification on the update files is required since the installation of update files without any verification can result in system malfunction, or service failures, etc.

4.5. TOE Access

4.5.1. Session locking and termination

Family Behaviour

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

Component leveling

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) Minimum: Locking or termination of interactive session

4.5.1.1. FTA_SSL.5 Management of TSF-initiated sessions

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

Application notes

o This requirement can be applied to the management access of 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 'Single Sign On'
- Optional SFRs: are not required to be mandatorily implemented in 'Single Sign On'. 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	Cryptographic key generation	Mandatory SFR
	FCS_CKM.2	Cryptographic key distribution	Mandatory SFR
	FCS_CKM.4	Cryptographic key destruction	Mandatory SFR
	FCS_COP.1	Cryptographic operation	Mandatory SFR
	FCS_RBG.1(Extended)	Random bit generation	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_SOS.2	TSF Generation of secrets	Mandatory SFR
	FIA_SOS.3(Extended)	Destruction of secrets	Mandatory SFR

Security functional class	Security functional component		Mandatory SFR / Optional SFR
	FIA_UAU.1	Timing of authentication	Mandatory SFR
	FIA_UAU.4	Single-use authentication mechanisms	Mandatory SFR
	FIA_UAU.5	Multiple authentication mechanisms	Optional 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
	FPT_TUD.1(Extended)	TSF security patch update	Optional SFR
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	Mandatory SFR
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions	Mandatory SFR
	FTA_TSE.1	TOE session establishment	Mandatory SFR
FTP	FTP_ITC.1	Inter-TSF trusted channel	Optional SFR
	FTP_TRP.1	Trusted path	Optional SFR

[Table 2] Security functional requirements

5.1. Security functional requirements (Mandatory SFRs)

The 'Single Sign On' 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

Security functional class	Security functional component	
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_RBG.1(Extended)	Random bit generation
FIA	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_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 3] 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 4] Audit events, [*assignment: other specifically defined auditable events]*].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and 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 4] Audit events, [assignment: *other audit relevant information*]].

Application Notes

o The ST author shall perform assignment operation of FAU_GEN.1.1 with the audit records supported by the TOE using following table. But, it is strongly recommended to record audit data of critical events related to the operation of the TOE security functionality.

o If the audit function is working as a part of the major process in the TOE, 'start-up' of the audit function may be recorded within the audit record which is the start-up of major processes after the initial start-up of the TOE. 'Shutdown' of the audit function may be replaced with the function-level event similar to 'start-up' (e.g. audit records of process

termination, etc.) or lower-level event (e.g. audit records of device shutdown, etc.).

- o The audit records shall include the date and time of the event, type of event, subject identity (e.g. account, connection IP, etc., if applicable, and the details of critical events and outcome (success or failure) in detail.
- o If the TOE receives the identification and authentication result from the authentication system, the audit record related to the user identification and authentication shall be recorded.
- o When TSF synchronizes reliable time information of external entity (e.g., reliable NPT server), the audit record relevant to the change of time shall be stored.
- o If the TOE includes a management console or client, the ST author shall include audit events that the management console or client shall support in the auditable events defined in FAU_GEN.1.1. It is recommended that major events related to the operation of the security functions of the TOE should be included in the auditable events and should be recorded as audit data.

Security functional component	Auditable event	Additional audit record
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (only applying to key distribution related to the TSF data encryption/decryption)	
FCS_CKM.4	Success and failure of the activity (only applying to key destruction related to the TSF data encryption/decryption)	
FCS_COP.1	Success and failure, and the type of cryptographic operation(only applying to items related to the issue, storing, verification, and destruction of a token)	
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_SOS.2	Rejection by the TSF of any tested secret	
FIA_SOS.3 (Extended)	Success and failure of the activity(applicable to the destruction of SSO token only)	
FIA_UAU.1	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the administrator identification mechanism,	

Security functional component	Auditable event	Additional audit record
	including the administrator 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 4] Audit events

5.1.1.3. FAU_SAA.1 Potential violation analysis

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events. a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation; b) [assignment: *any other rules*].

Application notes

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

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

o Authentication failure event of the administrator and end-user shall be included as audit

events defined in FAU_SAA.1.2.

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

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

5.1.1.4. FAU_SAR.1 Audit review

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [assignment: *authorized administrator*] with the capability to read [all the audit data] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

5.1.1.5. FAU_SAR.3 Selectable audit review

Hierarchical to	No other components.
Dependencies	FAU_SAR.1 Audit review
FAU_SAR.3.1	The TSF shall provide the ability to apply [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

Application notes

o Selective audit review based on logical relationships such as AND and OR, etc. shall be available.

o The audit data viewing ability that applies the sorting or ordering method on retrieved results can be provided.

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

Hierarchical to	No other components.
Dependencies	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	The TSF shall [Notification to the authorized administrator, [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*]].

Application notes

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

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

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

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 Cryptographic key generation

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 is related to the cryptographic key generation required for cryptographic operation, if there are more than one cryptographic key generation algorithms lists, it is recommended to perform iteration operations on this SFR.
The cryptographic key associated with the cryptographic operation specified in FCS_COP.1

shall be handled in this SFR.

- o Cryptographic key generation must 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 cryptographic algorithm and cryptographic key sizes shall meet the cryptographic complexity of 112 bits or more.
- o Generating an cryptographic key by deriving it from the password is not allowed, except the key encryption key (KEK).
- o When generating an key encryption key (KEK) by deriving it from the password, the safe method presented by TTAK.KO-12.0274, NIST SP 800-132, PKCS#5 must be used. In addition, if random numbers are used to generate an encryption key, an approved random number generator that has been validated by the Korea Cryptographic Module Validation Program (KCMVP) must be used.
- o When generating an key encryption key (KEK) by deriving it from the password, an 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 should be used as salt value, and at least 1,000 should be used as iteration count.
- o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.
- o If the TOE includes a client, these application notes shall be applied to the client.

5.1.2.2. 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.4.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

Application notes

- o The key distributed through the cryptographic key distribution method defined in FCS_CKM.2.1 shall be related to the key generated in FCS_CKM.1.1.
- o If the cryptographic key distribution method is used, the approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be applied.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.2.3. 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 destroy 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 When the cryptographic keys, critical security parameters, etc. being loaded on the memory are no longer used, plain type cryptographic key and critical security parameters shall be deleted. It shall also be applied to all cryptographic keys covered in FCS_CKM.1.

o If the TOE is terminated, cryptographic keys and critical security parameters loaded onto memory shall be deleted.

o If the SSO agent is an API type, the developer who develops(or modifies) the business systems of the purchaser shall implement the application to meet this requirement. Therefore, if the API type SSO agent exists as a component of the TOE, the above description shall be described in the form of notes in the manual.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.2.4. FCS_COP.1 Cryptographic operation

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 cryptographic operation related requirements such as token encryption provided by the TOE, encrypted communication between the TOE components, or encryption when

storing TSF data(e.g., token encryption key, critical security parameter, etc.)

e.g. : encryption and decryption of token / encryption key / critical security parameter / etc.

cryptographic communication used to support confidentiality and integrity between the TOE components

cryptographic communication used to support confidentiality and integrity of the management access, etc.

o In cryptographic operation, it is recommended to perform iteration operation on FCS_COP.1 according to the used cryptographic algorithm (symmetric key, asymmetric key, hash, etc.).

e.g. FCS_COP.1(1) Cryptographic operation (Symmetric key cryptographic operation)

FCS_COP.1(2) Cryptographic operation (MAC)

FCS_COP.1(3) Cryptographic operation (Hash)

FCS_COP.1(4) Cryptographic operation (Digital signature generation)

FCS_COP.1(5) Cryptographic operation (Digital signature verification)

o Cryptographic operation must be performed using the approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

o When performing cryptographic operation, the validated cryptographic module must run in approved mode of operation.

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

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

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

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

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.2.5. 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 It shall use a random bit generator validated under the Korea Cryptographic Module Verification Program (KCMVP) and the entropy of seed value in generating random numbers must be 2^{112} or higher.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3. Identification and authentication (FIA)

5.1.3.1. 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 [selection: *met, surpassed*] the TSF shall [assignment: *list of actions*].

Application notes

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

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

o The list of authentication events includes both administrator authentication attempts and end-user authentication attempts.

o Even if the TOE provides the initial end-user authentication in conjunction with the external authentication system, the end-user authentication failure handling shall be performed.

o If the number of authentication failure and actions are set differently depending on the TOE user and service(SSH, HTTPS etc.), the ST author can apply the iteration operation.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.2. FIA_IMA.1 TOE Internal mutual authentication

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

Application notes

- o This SFR is a requirement for mutual verification among the TOE components that are physically separated. The ST author is recommended to use iteration operation according to the communication sector among the TOE components.
- o This SFR shall be applied among the physically separated TOE components.
- o The ST author can specify 'None' as the assignment operation if [assignment: list os standards] does not exist.
- o The cryptographic function to perform 'mutual authentication' of this SFR must perform cryptographic operation using the approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) and the validated cryptographic module must run in approved mode of operation when performing cryptographic operation.
  - The ST author shall specify matters related to cryptographic operation in FCS_COP.1 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.
- o The ST author shall also provide the "Security policy document" of the validated cryptographic module to the evaluation facility.
- o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.3. FIA_SOS.1 Verification of secrets

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Application notes

- o Verification of secrets can be applied in password generation and change of administrator and end-user. However, verification of secrets shall be required for the administrator, but only for the TOE which provides the initial end-user authentication.
- o The information that shall meet password complexity requirements can be data as the following.
  - administrator's password, end-user'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.
- o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.4. FIA_SOS.2 TSF Generation of secrets

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_SOS.2.1	TSF shall provide a mechanism to generate **an authentication token** that meet [assignment: *a defined acceptable standard*].
FIA_SOS.2.1	TSF shall be able to enforce the use of TSF-generated **authentication token** for [assignment: *list of TSF functions*].

Application notes

- o This SFR deals with the generation of a token used by TOE, and the ST author shall describe the standard for generating a token in the TOE.
- o The subject of token generation can be the SSO server or SSO agent, depending on the TOE component.
- o The cryptographic function for generating the token of this SFR must perform cryptographic operation using the approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) and the validated cryptographic module must run in approved mode of operation when performing cryptographic operation.
  - The ST author shall specify matters related to cryptographic operation in FCS_COP.1 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.
- o Confidentiality and integrity shall be provided to information such as TSF data included in the token when generating a token, and refer to the protection of the TSF (FPT) class for parts related to storing important information such as TSF data.

5.1.3.5. FIA_SOS.3 Destruction of secrets (Extended)

Hierarchical to	No other components.
Dependencies	FIA_SOS.2 TSF Generation of secrets
FIA_SOS.3.1	The TSF shall destroy authentication tokens in accordance with a specified authentication token destruction method [assignment: secrets *destruction method*] that meets the following: [assignment: *list of standards*].

Application notes

o This SFR is a requirement related to the destruction of the token used in the TOE. Since the token can only be used until the user session is terminated, it shall be safely destroyed when a session is terminated.

o When a session is terminated, or the TOE execution is finished, all tokens loaded onto the memory shall be destructed.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.6. FIA_UAU.1 Timing of authentication

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

Application notes

o The user in the TOE refers to the authorized administrator and authorized end-user. The ST author can define the roles of administrators in detail according to the administrative function access right. When dividing the administrator roles into multiple roles, requirements shall be defined in FMT_SMR.1.

o The ID and password based authentication function for the authorized administrator and the authorized end-user shall be required in the TOE, however, for end-users, it applies only to the TOE that provides the initial authentication function.

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. Therefore, the ST author shall consider the function list according to the authentication method supported by the TOE before identification and authentication of the administrator and end-user, and perform the assignment operation.

o In case of the token-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. Therefore, the ST author shall consider the function list according to the authentication method supported by the TOE before identification and authentication of the end-user, and perform the assignment operation.

- In case of token generation, the requirements shall be defined in FIA_SOS.2, and in case of token destruction, the requirements shall be defined in FIA_SOS.3.

o The authentication function using the token must perform cryptographic operation using the approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation

Program (KCMVP) and the validated cryptographic module must run in approved mode of operation when performing cryptographic operation.

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

o 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.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.7. 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 This SFR defines the requirements for the authentication data and token of the authorized administrator and the authorized end-user.

o If authentication data for each authorized administrator and authorized end-user sessions are the same such as password-based authentication method, it is possible to bypass the authentication by obtaining the session information of that 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 password-based cryptographic authentication protocol, the time stamp, random number, etc.).

o In addition, if multiple authentication mechanisms are supported, authentication mechanisms that require the prevention of authentication data reuse (e.g., OTP, etc.) shall be identified and applied to the assignment operation. For example, the SMS authentication number method can set additional security attributes including time limitations, authentication number length, and randomness to prevent its reuse.

o Since the token issued from the TOE is included in the web browser cookie depending on the operational environment, and the token can be exposed to the outside, the token can be snatched and exploited to launch a reuse attack. Reuse of the token can be prevented by ensuring the uniqueness of each token (e.g., time stamp, including random numbers, etc.).

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.8. FIA_UAU.7 Protected authentication feedback

Hierarchical to	No other components.
종속관계	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 to make it unrecognizable(e.g., "****", etc.) 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 and changing the administrator/end-user password
- When authenticating the administrator/end-user

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 ID, You have inputted an incorrect password, etc.).

o Protected authentication feedback for the administrator shall be required in the TOE, however, for end-users, it applies only to the TOE that provides the initial authentication function of the end-user.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.3.9. FIA_UID.1 Timing of identification

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_UID.1.1	The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application notes

o This SFR defines the security requirements for identification of authorized administrator and authorized end-user (including initial authentication phase and token-based authentication phase).

o The user in the TOE refers to the authorized administrator and authorized end-user. The ST author can define the roles of administrators in detail according to the administrative function access right. When dividing the administrator roles into multiple roles, requirements shall be defined in FMT_SMR.1.

o Administrator identification and token-based user identification function shall be required, and the token-based user identification function is applicable only after initial end-user authentication phase is normally performed. Also, the end-user identification is applied when the TOE provides the initial end-user authentication.

o The user identification using the token must perform cryptographic operation using the

approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) and the validated cryptographic module must run in approved mode of operation when performing cryptographic operation.

- The ST author shall specify matters related to cryptographic operation in FCS_COP.1 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.
- The ST author shall meet the requirements defined in FIA_SOS.2 when generating the token and meet the requirements defined in FIA_SOS.3 when destructing the token.

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.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.4. Security management (FMT)

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
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_SOS.1	Management of the metric used to verify the secrets	Management of security functions
FIA_UAU.1	Management of the authentication data by an administrator, Management of the authentication data by the associated end-user	Management of TSF data
	Management of the list of actions that can be taken	Management of

Security functional component	Management function	Management type
	before the administrator and the end-user are authenticated	security functions
FIA_UID.1	Management of the administrator and end-user identities	Management of TSF data
	If an administrator and end-user 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 (Extended)	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 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 intial 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

[Table 5] Security management action and management type by component

5.1.4.1. FMT_MOF.1 Management of security functions behaviour

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MOF.1.1	The TSF shall restrict the ability to ***conduct management actions of*** the functions [assignment: *list of functions*] to [the authorized administrator].

Application notes

- o "Management action" to which a refinement operation is applied includes the ability to determine the behavior, disable, enable, modify the behavior of some functions in the TSF. This requirement shall be applied to the management access(SSH, HTTPS, etc.) supported by the TOE.
- o The action that adds, deletes or modifies conditions or rules capable of determining the

security functions behavior is included in the management of security functions behaviors. And, the action that adds, deletes or modifies behaviors taken by the TSF according to the corresponding conditions and rules is also included in the management of security functions behaviors. In addition, the action of selecting mechanism, protocol, etc., when there are variously provided to support the same purpose, is included in the management of security functions behavior because it corresponds to the modification of behavior.

- o The ST author can apply assignment operation in FMT_MOF.1.1 with reference to '[Table 5] 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 5] security management action and management type by component'. Management actions of security function can be included for the additional or extended requirements.

5.1.4.2. 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*** the [assignment: *list of TSF data*] to [assignment: *the authorized identified 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 5] security management action and management type by component', for the case that the TOE supports the TSF data management function.
- o The ST author shall refer to the roles defined in FMT_SMR.1 and perform the assignment operation by dividing the roles in FMT_MTD.1.1 when TSF data management is classified according to the roles. The TSF data which can be managed by the authorized end-user is limited to the TSF data stored in the "user device".
- o The ST author can define additional TSF data management actions for each component in addition to management function that are presented in '[Table 5] 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 administrator from deleting or modifying audit data.

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

Hierarchical to	Hierarchical to
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [the authorized administrator]. 1. [assignment: *password combination rules and/or length*] 2. [assignment: *other management such as management of special characters unusable for password, etc.*]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [the authorized administrator]. 1. [assignment: *ID combination rules and/or length*] 2. [assignment: *other management such as management of special characters unusable for ID, etc.*]
FMT_PWD.1.3	The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

Application notes

- o If the TOE does not provide the authorize administrator with the function to manage the combination rule and length for the ID and password, 'None' can 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 This requirement shall be applied to the management access(SSH, HTTPS, etc.) supported by the TOE.
- o The password combination rules that can be set by the administrator in FMT_PWD.1.1 shall be able to be composed of three combinations of English letters/numbers/special characters and support passwords of 9 characters or more in length.
- o In case of 'setting ID and password when installing, setting password when installing' presented in FMT_PWD.1.3, the function to force to change the administrator's password shall not be required
- o If the TOE includes a client, these application notes shall be applied to the client.

5.1.4.4. 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_PWD.1, etc.

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

Application notes

- o The administrator roles shall be severally divided depending on access privileges.
- 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 configuration.

5.1.5. Protection of the TSF (FPT)

5.1.5.1. FPT_ITT.1 Basic Internal TSF data transfer protection

Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_ITT.1.1	The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

Application notes

o This SFR shall be applied when transmitting TSF data between the TOE components which are physically separated regardless of operating type.

o Examples of data transmitted between the TOE components

- security policy, control command, audit data, CSP, etc.

o When implementing the encryption and message integrity verification function, the approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance 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 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.

o If the TOE includes a client, these application notes shall be applied to the client.

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

Hierarchical to	No other components
Dependencies	No dependencies.
FPT_PST.1.1	The TSF should protect the [Assignment: TSF data] stored in the repository, which is controlled by the TSF, from unauthorized exposure and modification.

Application notes

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

o Examples of TSF data to be protected as follows:

- Administrator and end-user passwords, token, cryptographic key (pre-shared key, symmetric key, private key, etc), CSP, TOE configuration values (security policy, configuration parameters, etc), audit data, etc.

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

o Confidentiality and integrity shall be provided to the generated token and important information included in the token.

o If the administrator and end-user password, token, CSP, TOE configuration value, account information used to access the external IT entity (e.g., DBMS account, etc.), are stored inside/outside of the TOE, they shall be encrypted and stored using approved cryptographic algorithms of the validated cryptographic module regardless of the storing location and type.

- 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 shall be encrypted mandatorily, the application of internally implemented encoding technique is allowed.
- The ST author shall specify matters related to cryptographic operation in FCS_COP.1 and specify related matters in FCS_CKM.1 if a cryptographic key is needed to be generated to perform the cryptographic operation function.

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

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

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.5.3. 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], TSF*].

Application notes

o It is recommended to conduct the TSF self tests of critical processes related to the operation of security functions such as identification and authentication, 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 When applying cryptographic function to implement 'the function to verify integrity' in FPT_TST.1.2, FPT_TST.1.3, approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be used and the validated cryptographic module must run in approved mode of operation when performing

cryptographic operation.

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

- The integrity of the TOE's configuration value and executable file shall be checked at the initial phase of TOE operation.
- A function that verifies the configuration value of TOE (e.g., security policy, environment configuration 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 (e.g. every one hour during normal operation or at the request of the authorized administrator) 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 functions should be notified when the error occurs after receiving the self-test result of the validated cryptographic module.

o If the TOE includes a client, operation (iteration, refinement, etc.) about the client shall be appled so that the following can be satisfied:

- The integrity of TOE's configuration value and executable file shall be checked at the initial phase of TOE operation.

5.1.6. TOE access (FTA)

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

Hierarchical to	FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies	FIA_UID.1 Timing of identification
FTA_MCS.2.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [the number of maximum concurrent sessions as 1 for administrator management access sessions, rules for the number of maximum concurrent sessions { decided by the ST author }]
FTA_MCS.2.2	The TSF shall enforce, by default, a limit of [1] sessions per user.

Application notes

o A session is presented in FMT_MCS.2 is 'user access', the number of sessions shall be 'the

number of user accesses.'

- o When restricting the number of management access sessions to the TOE by each service(e.g. SSH, HTTPS, etc.), it is defined in operation of FTA_MCS.2.1.
- o After one device makes administrator's management access, another device performs a login 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 If the TOE includes a client, these application notes shall be applied to the client.
- 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.

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

Application notes

- o This SFR shall require the capability to lock or terminate the session after a time interval of the inactivity after administrator and/or end-user login, and it shall be applied to management access(SSH, HTTPS, etc.) supported by the TOE.
  - Application target: administrator session, end-user session
- o A time interval of the authorized administrator and authorized end-user 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. But, default value shall be set within 10 minutes.

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 authorized administrator and authorized end-user and service (SSH, etc.), the ST author 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 and end-user'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.

o If the TOE includes a client, these application notes shall be applied to the client.

5.1.6.3. FTA_TSE.1 TOE session establishment

Hierarchical to	No other components.
Dependencies	No dependencies
FTA_TSE.1.1	The TSF shall be able to deny **administrator's management access** session establishment based on [connection IP, [selection: connection time, whether or not to activate the management access session of the same account, whether or not to activate the management access session of administrator account with the same privilege, [assignment: *critical management functions attribute*], None]].

Application notes

o The management access session of administrator shall be allowed only from the terminal with designated IP address for management access.

o The ST author is able to establish the number of connection IP, the default value provided by the TOE shall set at most 2.

o When establishing the administrator's connection IP, it is not allowed to add an IP address range such as 192.168.10.2 to 253, etc, individually it shall implemented to add the IP address one by one. Moreover, establishment of IPs such as 0.0.0.0, 192.168.10.*, any, etc. is not allowed.

o The ST author can add access time of the administrator, activation of management access session for the same account, etc.

5.2. Security functional requirements (Optional SFRs)

'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	
FAU	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
FIA	FIA_UAU.5	Multiple authentication mechanisms
FPT	FPT_STM.1	Reliable time stamps
	FPT_TEE.1	Testing of external entities
	FPT_TUD.1(Extended)	TSF security patch update
FTP	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

[Table 6] Optional security functional requirements

5.2.1. Security audit (FAU)

5.2.1.1. FAU_SEL.1 Selective audit

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation FMT_MTD.1 TSF Management of TSF data
FAU_SEL.1.1	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) [selection: *object identity, user identity, subject identity, host identity, event type*] b) [assignment: *list of additional attributes that audit selectivity is based upon*]

Application notes

o FAU_SEL.1 Selective audit is an optional SFR that can be optionally implemented. When

providing this capability in the TOE, the ST author shall include this requirement into SFRs.

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

5.2.1.2. FAU_STG.1 Protected audit trail storage

Hierarchical to	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

Application notes

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

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

5.2.2. Identification and authentication (FIA)

5.2.2.1. FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_UAU.5.1	TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.
FIA_UAU.5.2	TSF shall authenticate any user's claimed identity according to [assignment: rules that explain how multiple authentication mechanisms provide authentication].

Application notes

o FIA_UAU.5 Multiple authentication mechanisms are the functional requirement (“optional SFR”) that can be optionally implemented. If the TOE additionally provides the following functions, the ST author shall include this requirement in SFR.

- Additional authentication function about the administrator or end-user

o When multiple authentication mechanisms(e.g., certificate-based authentication method, OTP method) are additionally provided to the administrator or end-user, iteration operation shall be applied to each user, and the corresponding authentication mechanism is applied to the assignment operation of FIA_UAU.5.1

o If the TOE includes a client, these application notes shall be applied to the client.

5.2.3. Protection of the TSF (FPT)

5.2.3.1. FPT_STM.1 Reliable time stamps

Hierarchical to	No other components.
Dependencies	No dependencies.

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

Application notes

o FPT_STM.1 Reliable time stamps is a functional requirement ("optional SFR") that can be optionally implemented. If the TOE provides the function additionally, the ST author shall include this requirement in SFR.

o The TSF can provide all of the reliable time stamp functions or can provide a time stamp function by synchronizing the reliable time information of the external entities(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 Security objectives for the operational environment related to the reliable time stamp in the ST

o If the TOE provides a reliable time stamp function, the TOE shall be operated based on the time in the SSO server.

5.2.3.2. FPT_TEE.1 Testing of external entities

Hierarchical to	No other components.
Dependencies	No dependencies.

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

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

Application notes

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

- 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 using alarm, etc.
- o Testing 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 intial start-up, external entities affecting the critical functions and security functions of shall be tested in full.
- o The ST author can select the interval (e.g. every one hour during normal operation or at the request of the authorized administrator) of external entities testing during normal operation. However, the testing interval shall be determined within certain reasonable bounds so that they do not adversely affect when the TOE operates abnormally.
- o The capability may 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 external IT entities outside of the TOE that interacts with the TOE (e.g., NTP server, log server, DBMS) can be the target of an additional test. It is recommended to include an external entity needed for the safe and accurate operation of TOE in the test target.

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

Hierarchical to	No other components.
Dependencies	No dependencies.
FPT_TUD.1.1	The TSF shall provide the capability to view the TOE versions to [assignment: *the authorized identified roles*].
FPT_TUD.1.2	The TSF shall verify validity of the update files using digital signature verification before installing updates.

Application notes

- o FPT_TUD.1 TSF security patch update is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.
- o The TSF shall provide the capability to check the current version of TOE which most recently installed and executed by authorized administrator.
- o Updates may be available either automatically or manually. If online update is available, update files shall be transmitted through a secure communication channel to protect the file. Refer to 'Optional SFR' FTP_ITC.1 for more details.
- o If the agent receives a file from the server, it shall perform verification of digital signature on the subject of file generation to ensure non-repudiation and integrity. The certificate as well as digital signature shall be verified, and the agent should perform integrity

verification on the address of the SSO server or update server. If there are more than two servers on the file transmission route, the receiving server shall perform integrity verification on the address of the sending server.

o If the TOE includes a client and provides TSF security patch update function for the client, these application notes shall be applied to the client.

o When applying cryptographic function to verify integrity of update file, approved cryptographic algorithms of the validated cryptographic module whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP) must be used and the validated cryptographic module must run in approved mode of operation when performing cryptographic operation.

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

5.2.4. Trusted path/channels (FTP)

5.2.4.1. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to	No other components.
Dependencies	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application notes

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

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

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

o If the TSF interfaces with trusted IT product, the TSF and the IT product shall protect the

TSF data (e.g., audit data, authentication data, and TOE setting configuration file) from unauthorized disclosure and modification using the trusted channel which utilizes 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, it is recommended that the SFRs regarding cryptographic key generation (FCS_CKM.1) and cryptographic operation (FCS_COP.1), which are additionally required, are added by performing the iteration operations.

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

5.2.4.2. FTP_TRP.1 Trusted path

Hierarchical to	No other components.
Dependencies	No dependencies.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [selection: *remote, local*] users 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, local users, remote users*] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [selection: *initial user authentication,* [assignment: *other services for which trusted path is required*]].

Application notes

o FTP_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 the user access. If communication needs to be established between the user and the TOE component such as web access, terminal 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 user access, it shall support TLS 1.2 (RFC 5246)

or its successors. And, if the SSH protocol is supported, it shall support SSH v2(RFC 4251 ~ 4254) or its successors.

- If the ST author has added this SFR to the ST, it is recommended that the SFRs regarding cryptographic key generation (FCS_CKM.1) and cryptographic operation (FCS_COP.1), which are additionally required, are added by performing the iteration operations.

o In FTP_TRP.1, 'the remote user' is a human who interacts indirectly with the TOE through other IT products, the 'local user' is a human who interacts directly with the TOE through the installed device(e.g., PC, workstation). The user includes the administrator and the end-user.

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 SFR can be applied if it is implemented by communication between the web browser of the user PC and the SSO server which is a component of the TOE, and this SFR can be replaced by FTP_ITT.1 if communication between the user PC and the SSO server is implemented directly. In addition, if management access is provided by communication between the web browser of the administrator PC and SSO server 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 7] Security assurance requirements

5.3.1. Security Target evaluation

5.3.1.1. ASE_INT.1 ST introduction

Dependencies	No dependencies.
Developer action elements	
ASE_INT.1.1D	The developer shall provide an ST introduction.
Content and presentation elements	
ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C	The ST reference shall uniquely identify the ST

ASE_INT.1.3C	The TOE reference shall uniquely identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C	The TOE overview shall identify the TOE type.
ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
Evaluator action elements	
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

5.3.1.2. ASE_CCL.1 Conformance claims

Dependencies	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements
Developer action elements	
ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
Content and presentation elements	
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is

	consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
Evaluator action elements	
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.3. ASE_OBJ.1 Security objectives for the operational environment

Dependencies	No dependencies.
Developer action elements	
ASE_OBJ.1.1D	The developer shall provide a statement of security objectives.
Content and presentation elements	
ASE_OBJ.1.1C	The statement of security objectives shall describe the security objectives for the operational environment.
Evaluator action elements	
ASE_OBJ.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.4. ASE_ECD.1 Extended components definition

Dependencies	No dependencies.
Developer action elements	
ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
Content and presentation elements	

ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
Evaluator action elements	
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

5.3.1.5. ASE_REQ.1 Stated security requirements

Dependencies	ASE_ECD.1 Extended components definition
Developer action elements	
ASE_REQ.1.1D	The developer shall provide a statement of security requirements.
ASE_REQ.1.2D	The developer shall provide a security requirements rationale.
Content and presentation elements	
ASE_REQ.1.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.1.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.1.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.1.4C	All operations shall be performed correctly.
ASE_REQ.1.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.1.6C	The statement of security requirements shall be internally consistent.

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

5.3.1.6. ASE_TSS.1 TOE summary specification

Dependencies	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Developer action elements	
ASE_TSS.1.1D	The developer shall provide a TOE summary specification
Content and presentation elements	
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
Evaluator action elements	
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.3.2. 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 Labelling of the TOE

Dependencies	ALC_CMS.1 TOE CM coverage
Developer action elements	
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
Content and presentation elements	
ALC_CMC.1.1C	The TOE shall be labelled with its unique reference.
Evaluator action elements	
ALC_CMC.1.1E	The evaluator shall confirm that the information provided meet requirements for content and presentation of evidence.

5.3.4.2. ALC_CMS.1 TOE CM coverage

Dependencies	No dependencies.
Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
Evaluator action elements	
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5. Tests

5.3.5.1. ATE_FUN.1 Functional testing

Dependencies	ATE_COV.1 Evidence of coverage
Developer action elements	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
Content and presentation elements	
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
Evaluator action elements	
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2. ATE_IND.1 Independent testing - conformance

Dependencies	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.6. Vulnerability assessment

5.3.6.1. AVA_VAN.1 Vulnerability survey

Dependencies	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.4. Security requirements rationale

5.4.1. Dependency rationale of security functional requirements

The following table shows dependency of security functional requirement.

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	-
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	-
7	FAU_STG.4	FAU_STG.1	-
8	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	9, 11
		FCS_CKM.4	10
9	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	10
10	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
11	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	10
12	FCS_RBG.1	-	-
13	FIA_IMA.1	-	-
14	FIA_AFL.1	FIA_UAU.1	18
15	FIA_SOS.1	-	-
16	FIA_SOS.2	-	-
17	FIA_SOS.3	FIA_SOS.2	16
18	FIA_UAU.1	FIA_UID.1	21
19	FIA_UAU.4	-	-
20	FIA_UAU.7	FIA_UAU.1	18
21	FIA_UID.1	-	-
22	FMT_MOF.1	FMT_SMF.1	25
		FMT_SMR.1	26
23	FMT_MTD.1	FMT_SMF.1	25
		FMT_SMR.1	26

No.	Security functional requirements	Dependency	Reference No.
24	FMT_PWD.1	FMT_SMF.1	25
		FMT_SMR.1	26
25	FMT_SMF.1	-	-
26	FMT_SMR.1	FIA_UID.1	21
27	FPT_ITT.1	-	-
28	FPT_PST.1	-	-
29	FPT_STM.1	-	-
30	FPT_TST.1	-	-
31	FTA_MCS.2	FIA_UID.1	21
32	FTA_SSL.5	FIA_UAU.1 or No dependencies	18
33	FTA_TSE.1	-	-

[Table 8] Rationale for the dependency of the security functional requirements

FAU_GEN.1 has the dependency on FPT_STM.1. However, in this PP, if the pertinent function is implemented by the TOE, the ST author needs to identify the optional SFR (FPT_STM.1) as the SFR of the ST and describe the pertinent reference number. In addition, if FPT_STM.1 is supported by the operational environment, the author shall add the security objectives for the operational environment and provide justification that the dependency is satisfied.

FAU_STG.3 and FAU_STG.4 have the dependency on FAU_STG.1. However, in this PP, 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 the dependency 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
EAL	Evaluation Assurance Level
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IP	Internet Protocol
IT	Information Technology
IV	Initial Vector
KEK	Key Encryption Key
NTP	Network Time Protocol
OFB	Output Feedback
OTP	One Time Password
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMS	Short Message Service
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality