Security Target

iSIGN+ v4.0

2024-06-25
v1.2

Penta SECURITY

Revision History

Version	Reason for Revision	Revision Date
1.0	Draft	2023.12.26
1.1	Modified to reflect EOR	2024.05.17
1.2	Modified to reflect TOE version update	2024.06.25

Index

Figure Index

Table Index

1 Security Target introduction

This document is the security target specification for iSIGN+ v4.0 of Penta Security Inc. that complies with the **EAL1+** level of the Common Criteria.

1.1 Security Target reference

Description	Contents
Title	iSIGN+ v4.0 Security Target
ST Version	v1.2
Evaluation Assurance Level	EAL1+(ATE_FUN.)
Developer	Penta Security Inc.
Common Criteria version	CC V3.1 R5
Compliance protection profile	Korean National Protection Profile for Single Sign On V3.0
Keywords	Single Sign On, SSO

Table 1-1 Security Target reference

1.2 TOE reference

Description	Reference	
TOE Identification	iSIGN+ v4.0	
TOE Version	v4.0-r3	
TOE components	SSO Server	SS-ATH v4.0-r3
	SSO Agent	SA-WEB v4.0-r3
Guidance documents	Preparative procedure	iSIGN+ v4.0 Preparative procedures v1.2
	Operational user guidance	iSIGN+ v4.0 Operational user guidance v1.2
Developer	Penta Security Inc.	

Table 1-2 TOE reference

1.3 TOE overview

1.3.1 TOE overview

iSIGN+ v4.0 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 iSIGN+ v4.0 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), issue a token during user login, and verify the issued token if accessing another business system after user login. Authentication functions based on ID and password for authorized administrators and authorized end users in the iSIGN+ v4.0 are mandatorily required. The primary security features provided by the iSIGN+ v4.0 include user identification and authentication, token issue, storage, verification and destruction.

1.3.2 TOE type and scope

The TOE defined by this Security Target is SSO that enables the user to access various business systems through a single user login, and the TOE components are provided in the form of software. The agent and the server are the indispensable TOE component defined in this Security Target. The TOE is composed of the server that processes user login, manages the token, and sets the policy, etc; and the agent that is installed in each business system performs the function of requesting token verification, etc. The agent is composed of an 'API type' composed of library files.

1.3.3 TOE usage and major security features

The TOE performs user identification and authentication functions to provide users with a single login (Single Sign-On) to various business services without additional login actions. 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 including TSF self-testing, etc. In addition, identification and authentication functions such as mutual authentication between TOE components and authentication failure handling, cryptographic support function such as encryption key management and cryptographic calculation functions for issuing authentication tokens, etc., security management function for security function management and environment settings, etc. , TOE access function for access session management

by authorized administrators, and a secure channel to protect channel data between the TOE and the mail server. In addition, the token requires confidentiality and integrity protection, and the TOE executable code requires integrity protection.

Figure 1-1 shows the user identification and authentication procedure of the TOE. The user identification and authentication procedure can be grouped into the initial authentication phase using ID/PW and the token-based authentication phase that accesses the business system using the token issued during the initial authentication procedure.

The execution procedure of the initial authentication phase is as follows. (1) When a user accesses the business system, the SSO agent redirects to the SSO server. Afterwards, the user requests user login by entering ID/PW on the login screen of the SSO server. (2) The SSO server performs login verification using user information stored in the DBMS. The SSO server issues an authentication token if the login verification result is valid. (3) The user requests authentication token verification from the SSO agent. (4) The SSO agent requests authentication token verification from the SSO server. (5) The SSO server verifies the validity of the authentication token and returns the result. At this time, the authentication token is updated. The SSO agent allows the user to use the business system if authentication token verification is successful. (Business service login successful)

The token-based authentication phase is performed only when the token has been normally issued in the initial authentication phase. (6) When a user accesses the business system, the SSO agent redirects to the SSO server. Since an SSO session for the user already exists on the SSO server, the authentication token is extracted from the SSO session and delivered to the user. The user sends an authentication token verification request to the SSO agent. (7) The SSO agent requests authentication token verification from the SSO server. (8) The SSO server verifies the validity of the authentication token and returns the result. At this time, the authentication token is updated. The SSO agent allows the user to use the business

system if authentication token verification is successful. (Business service login successful)

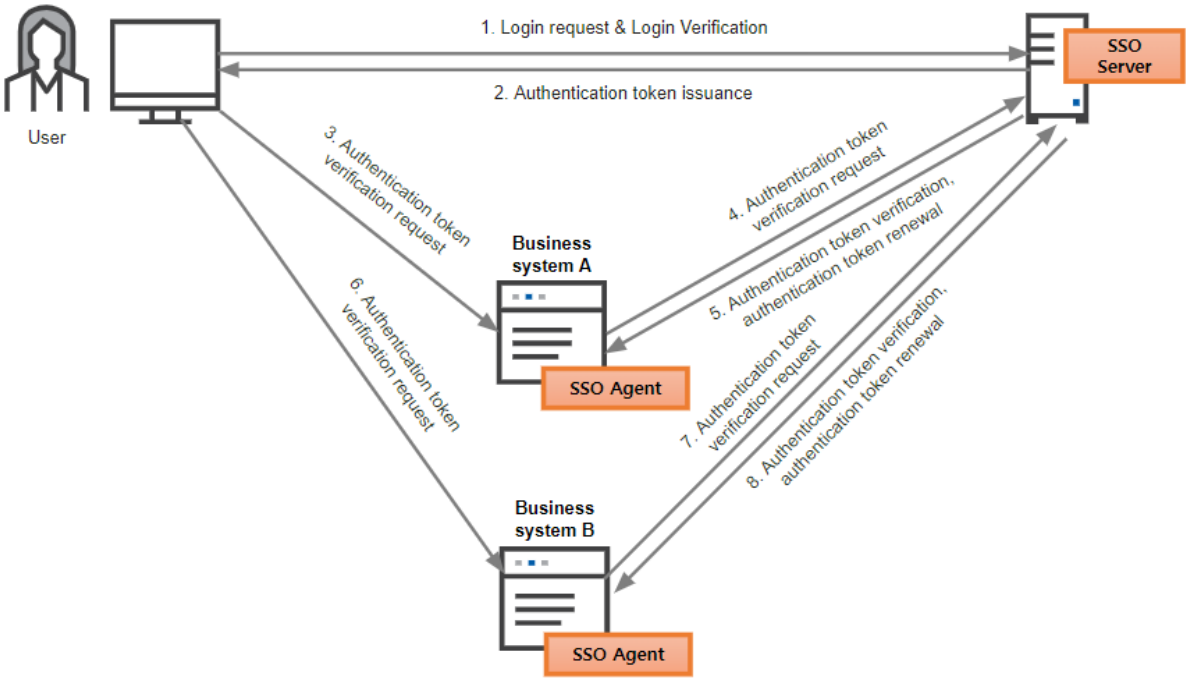


Figure 1-1 User identification and authentication procedure

1.3.4 Non-TOE and TOE operational environment

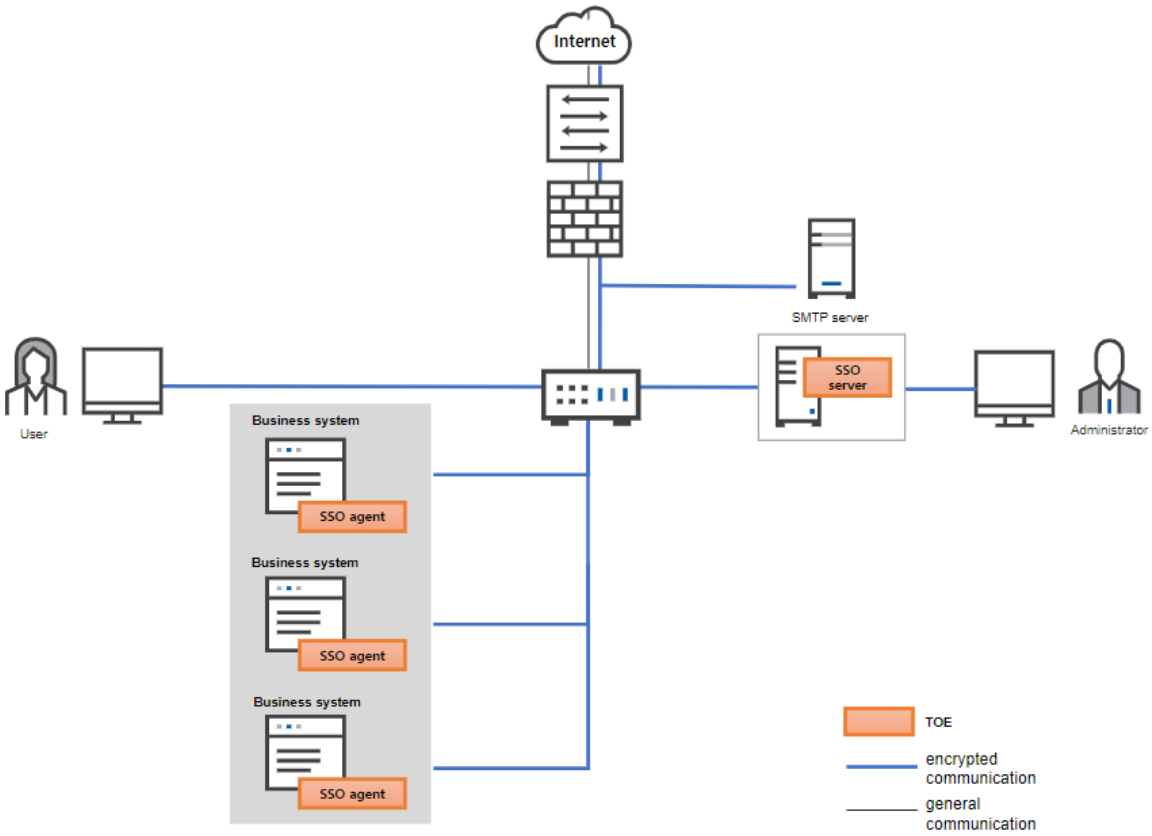


Figure 1-2 TOE operational environment

Figure 1-2 shows the general TOE operational environment. TOE is composed of the SSO server and SSO agent. The SSO server uses user information stored in the DBMS to provide functions such as direct user login verification, authentication token management, and policy settings. The SSO agent is installed in each business system and requests authentication token verification requests to the SSO server. In addition, the SSO agent can be 'API type' composed of the library file. Authorized administrators may perform security management by accessing the SSO server through web browsers.

The communication section between TOE components performs encrypted communication, and encrypted communication is also performed between the mail server and the SSO server.

The external IT entities required for TOE operation are as shown in <Table 1-3 External IT entities required for TOE operation>.

External IT entities	Contents
SMTP server	Mail server for sending emails such as administrator notifications when detect security violation

Table 1-3 External IT entities required for TOE operation

The operating environment for each component of the TOE is as follows:

Description	Software name and version	Contents
OS	Debian GNU/Linux 11(bullseye) (kernel 5.10) 64bits	Linux-based operating system that provides reliable time information
DBMS	MariaDB v10.5.23 64bits	DBMS used to safely store TOE audit data and TSF data
WAS	Apache Tomcat v10.1.19 64bits	Web Application Server to operate SSO server core logic and web-based management tools

Table 1-4 SSO server SW operating environment

Description	Specification
CPU	Intel® Core™ I3-9100 Processor 3.6GHz (4core) or higher
Memory	16GB or higher
HDD	Space required for TOE installation 1GB or higher
NIC	100/1000 Mbps x 1EA or higher

Table 1-5 HW Requirements for SSO Server

Description	SW name and version	Contents
OS	Debian GNU/Linux 11(bullseye) (kernel 5.10) 64bits	Linux-based operating system that provides reliable time information
WAS	Apache Tomcat v10.1.19 64bits	Web Application Server to operate web-based business system and SSO Agent

Table 1-6 SSO Agent SW operating environment

Description	Specification
CPU	Intel® Core™ I3-9100 Processor 3.6GHz (4core) or higher
Memory	16GB or higher
HDD	Space required for TOE installation 50MB or higher
NIC	100/1000 Mbps x 1EA or higher

Table 1-7 HW Requirements for SSO Agent

Description	SW name and version
SW	Chrome 125.0.6422.142(official build) (64bits)

Table 1-8 SW requirements for administrator and end user PCs

1.4 TOE description

1.4.1 Physical scope of the TOE

The physical scope of the TOE consists of SW and documentation as shown in <Table 1-9 Physical scope of the TOE> below.

Description		Identification	Type	Distribution method
TOE Identification		iSIGN+ v4.0		
TOE Detailed version		v4.0-r3		
TOE components	**SSO Server**	SS-ATH v4.0-r3 (iSIGN+_SS-ATH_v4.0-r3.tar)	SW	CD
	SSO Agent	SA-WEB v4.0-r3 (iSIGN+_SA-WEB_v4.0-r3.tar)	SW	CD
Guidance documents	**Preparation procedure**	iSIGN+ v4.0 Preparative procedures v1.2 (iSIGN+_v4.0_Preparative procedures_v1.2.pdf)	pdf file	CD
	Operational user guidance	iSIGN+ v4.0 Operational user guidance v1.2 (iSIGN+_v4.0_Operational user guidance_v1.2.pdf)		

Table 1-9 Physical scope of the TOE

The validated cryptographic module and software distributed and included in the SSO server and SSO agent are as follows.

Description	Contents
Validated cryptographic module	- Cryptographic module name: CIS-CC V4.0 - Verification number: CM-213-2027.10 - Verification date: 2022-10-04 - Developer: Penta Security Inc.
Software	Zulu JDK v21.32.17

Table 1-10 Validated cryptographic module and software

1.4.2 Logical scope of the TOE

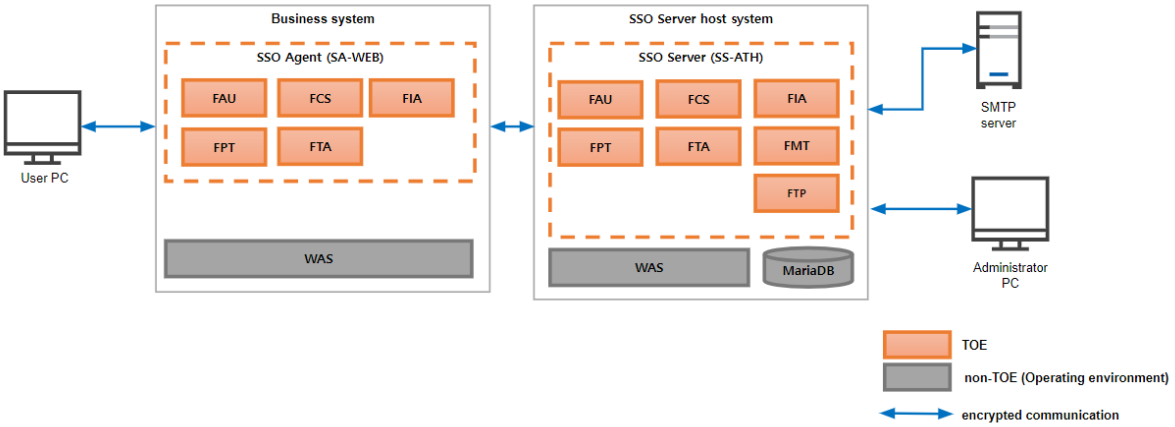


Figure 1-3 Logical scope of the TOE

As shown in <Figure 1-3 Logical scope of the TOE>, the TOE provides security functions such as **[FAU, FCS, FIA, FPT, FTA, FMT, FTP]**.

1.4.2.1 Logical scope of the SSO server

The SSO server performs user login verification, authentication token management, and policy settings. The security features provided through the SSO server are as follows.

Security audit (FAU)

Audit data generated from TOE components (SSO server, SSO agent) are stored in the DBMS of the SSO server. Authorized administrators can view all logs after successfully identifying and authenticating to the SSO server and logging into the management tool.

The SSO server periodically checks the disk usage of audit data and notifies the 0 level administrator by email if it exceeds the disk usage threshold or disk usage limit. If the disk usage limit is exceeded, the audit data is deleted file by file, starting with the oldest audit data.

If a potential security violation occurs (Audit trail storage threshold/limit exceeding event, administrator or user successive authentication failure event, self-test or integrity verification failure event) during TOE operation, response actions are taken, such as notifying the 0 level administrator by email.

Cryptographic support (FCS)

The SSO server uses a verified encryption module (CIS-CC V4.0) to generate KEK, DEK, integrity verification key, and token encryption/decryption key. KEK is used to encrypt and decrypt token encryption/decryption key/DEK/integrity verification key, DEK is used to encrypt and decrypt TSF data and mutual authentication data between TOE components, and integrity verification key is used to verify the integrity of TSF execution code and TSF data. The token encryption and decryption key is used to encrypt and decrypt the authentication token. The TOE performs encryption and decryption using the SEED (128 bits, CBC mode) encryption algorithm provided by the verified encryption module (CIS-CC V4.0). In addition, the integrity of the TSF and TSF data is verified using the HMAC SHA256 algorithm, and one-way encryption of administrator and user passwords is performed using the SHA256 algorithm.

All encryption keys created in the TOE are immediately destroyed by being overwritten 5 times (0x00) immediately after use.

Identification and authentication (FIA)

The SSO server provides an identification and authentication mechanism for administrators based on ID and password. While administrator identification and authentication are in progress, the entered password is changed to masking characters and output. Also, when processing an administrator login failure, detailed information on the reason for the failure is not provided.

When the number of administrator authentication failures reaches the allowable number of failures set by the 0~1 level administrator, the administrator account is locked for the time set by the 0~1 level administrator.

The TOE performs mutual authentication between separate TOE components (SSO server, SSO agent) using its own implemented protocol (request protocol and response protocol).

Protection of the TSF (FPT)

TSF data transmitted between separate components of the TOE (SSO server and SSO agent) is safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2).

TSF data required for the operation of the SSO server is protected from unauthorized exposure and modification by being encrypted with a verified encryption module (CIS-CC V4.0).

The SSO server performs integrity verification of all TSFs and TSF data on the SSO server at startup and upon request from the 0 level administrator. It also performs self-testing of the authentication token generation and verification process at startup and periodically.

TOE access (FTA)

The number of simultaneous sessions between 0~2 level administrators, excluding level 3 administrators, and between the same accounts is limited to a maximum of 1. And the administrator can only connect from the accessible IP set in the management tool. Additionally, the maximum number of simultaneous sessions for the same user that can use business services is limited to 1.

The session that the administrator manages and connects to the SSO server through the management tool is automatically terminated when the administrator session timeout time set in the management tool by the 0~1 level administrator has elapsed.

Security management (FMT)

Authorized administrators can perform security function management and TSF data management through management tools through the TOE identification and authentication process. For 3 level administrators, only the audit log review function can be used among the security management functions provided by the TOE, and other security management functions cannot be used.

Trusted channels (FTP)

TSF data transmitted between the SSO server and external mail servers is safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2). In addition, the SSO server forms a communication channel between itself and the mail server based on the mail server information (server address and port, mail user ID/password) set by the 0~1 level administrator in the management tool and identifies the corresponding mail server.

1.4.2.2 Logical scope of the SSO agent

The SSO agent is installed in each business service and performs authentication token verification requests, etc. The security functions provided through the SSO agent are as follows.

Security audit (FAU)

The SSO agent creates audit records during the operation process and stores them in the DBMS within the SSO server to track responsibility for security-related actions. When the connection between the SSO server and SSO agent is lost, the SSO agent records audit records in a file and transmits the audit record file to the SSO server at the time of connection.

Cryptographic support (FCS)

The SSO agent generates encryption keys and performs encryption operations using the encryption algorithm provided by the verified encryption module (CIS-CC V4.0).

The SSO agent acquires the KEK using the salt.dat file (Includes KEK_salt, encrypted DEK, encrypted integrity verification key) generated by the SSO server and distributed offline and the KEK derived password, and obtains the DEK and integrity verification key by decrypting the DEK and integrity verification key encrypted with the KEK. DEK is used to encrypt and decrypt TSF data and mutual authentication data between TOE components, and the integrity verification key is used to verify the integrity of TSF executable code and TSF data. The TOE performs encryption and decryption using the SEED (128 bits, CBC mode) encryption algorithm provided by the verified encryption module (CIS-CC V4.0), and also verifies the integrity of the TSF and TSF data using the HMAC SHA256 algorithm.

All encryption keys created in the TOE are immediately destroyed by being overwritten 5 times (0x00) immediately after use.

Identification and authentication (FIA)

The SSO agent provides an identification and authentication mechanism for users based on ID and password. In addition, users who are successfully identified and authenticated can use the authentication token to access business services assigned to the user by 0~2 level administrators. During user identification and authentication, the entered password is changed to masked characters and output, and when handling user login failure, detailed information on the reason for the failure is not provided.

When the number of user authentication failures reaches the allowable number of failures set by the 0~1 level administrator, the user account is locked for the time set by the 0~1 level administrator.

Protection of the TSF (FPT)

TSF data transmitted between the SSO server and SSO agent, which are separate components of the TOE, are safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2).

The SSO agent's TSF data is encrypted with a verified encryption module (CIS-CC V4.0) and stored in the salt.dat file to protect it from unauthorized exposure and modification. In addition, integrity verification is performed on all TSF executable files and TSF data at startup and periodically (every 6 hours).

TOE access (FTA)

Users can access business services only from the accessible IP set by the 0~2 level administrator in the management tool. In addition, users can only access business services that have been mapped to the corresponding user ID by 0~2 level administrators through management tools.

The session in which the user accesses the business service is automatically terminated when the user session timeout time set by the 0~1 level administrator in the management tool has elapsed.

1.5 Conventions

The notation, formatting and conventions used in this Security Target 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 Security Target.

Iteration

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

Assignment

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

Selection

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

Refinement

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

1.6 Terms and definitions

Among the terms used in this Security Target Specification, the terms that are the same as those used in the Common Evaluation Standard and Korean National Protection Profile for Single Sign On V3.0 follow the Common Evaluation Standard and the Protection Profile. Other terms used only in this Security Target are defined below..

- Validated Cryptographic Module

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

- Management tools

It is a web-based user interface for administrators to perform audit review and SSO server security functions and TSF data management functions, and is composed of multiple web pages.

- Administrator

An administrator who connects to the SSO server through a management tool and performs management functions, and is classified into 0~3 level administrators depending on authority.

- Integrity verification key

The key used to create the HMAC value when storing TSF data in DBMS.

- Decryption

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

- User

Authorized administrator and authorized end-user

- Manual recovery

Product recovery through reinstallation by user intervention.

- Encryption

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

- Business services ID

This is a unique number assigned when adding a service and is used when setting up the service in the business system.

- Business System

An application server that authorized users access through 'SSO'

- End User

A user who does not have authority to manage security functions or manage TSF data through management tools, and uses the TOE's initial login or SSO login function to use the business system.

- Authorized Administrator

Authorized user to securely operate and manage the TOE

■ Token encryption and decryption key

The key used to encrypt and decrypt the authentication token when generating and verifying it.

■ Token serial number

As a means of preventing the reuse of authentication tokens, a token serial number is generated for each user session. When an authentication token is created, '1' is initially given, and when the authentication token is reissued (renewed) after requesting authentication token verification, it is incremented by 1 in the authentication server.

■ Database Management System (DBMS)

A software system composed to configure and apply the database. TSF data is stored and managed in DBMS.

■ DEK

The key that encrypts user information, server and agent information, and SecureData used for mutual authentication.

■ KEK

The key that encrypts the DEK, integrity verification key, and token encryption/decryption key.

■ Transport Layer Security (TLS)

This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246. Used when transmitting TSF data between TOE.

■ TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies. This includes DEK, integrity verification keys, token encryption and decryption keys, and user information.

■ 0 level administrator

This refers to the initially created administrator. Level 0 administrators can use all management and inquiry functions.

■ 1 level administrator

This is an administrator who is allowed to use service inquiry, management, setting functions, all integrated management functions, and product registration functions. All functions except integrity verification can be used.

■ 2 level administrator

This administrator is allowed to view administrator logs and user logs, manage user identity, and manage agents.

■ 3 level administrator

Administrator log and user log inquiry TSF function is allowed.

2 Conformance claim

2.1 CC conformance claim

Description		Contents
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
	Part 3 Security assurance components	Conformant
	Package	Augmented : EAL1 augmented (ATE_FUN.1)

Table 2-1 CC conformance claim

2.2 PP conformance claim

This security target complies with the Korean National Protection Profile for Single Sign On V3.0.

2.3 Package conformance claim

This Security Target claims conformance to assurance package EAL1 augmented with ATE_FUN.1.

2.4 Conformance claim rationale

The basis for the declaration of compliance with the Korean National Protection Profile for Single Sign On V3.0 of this Security Target is as follows.

Description	Security Target	Korean National Protection Profile for Single Sign On V3.0
TOE type	Single Sign On - API type	Single Sign On - API type

Table 2-2 Conformance claim rationale

3 Security objectives

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

3.1 Security objectives for the operational environment

Category	Security purpose
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.
OE.SECURE_DEVELOPMENT	The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.
OE.RELIABLE_TIMESTAMP	The TOE must accurately record security-related events using reliable timestamps provided by the TOE operating environment.
OE.DBMS	The DBMS that interacts with the TOE must prevent unauthorized deletion or modification of audit records where audit traces are stored.
OE. MANUAL_RECOVERY	The TOE agent must be able to manually restore altered information (settings, executable files, filter drivers, etc.).
OE. SECURE PATH	Data transmitted between the web browser of the administrator's and user's PC and the web server, which is the operating environment of the TOE, must be protected through a safe channel.

Table 3-1 Security objectives for the operational environment

4 Extended components definition

The security requirements in this Security Target conform the extended component definition of "Korean National Protection Profile for Single Sign On V3.0" and define and use the following components in addition to the Common Criteria Part 2 or Part 3 components.

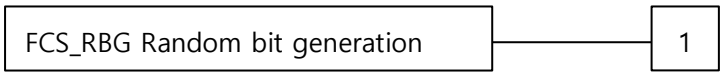
4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

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

Component leveling



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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

4.1.1.1 FCS_RBG.1 Random bit generation

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

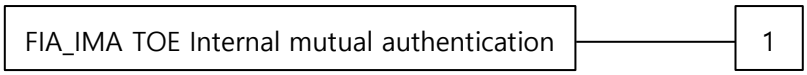
4.2 Identification and authentication

4.2.1 TOE Internal mutual authentication

Family Behaviour

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

Component leveling



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

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

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

a) Minimal: Success and failure of mutual authentication

4.2.1.1 FIA_IMA.1 TOE Internal mutual authentication

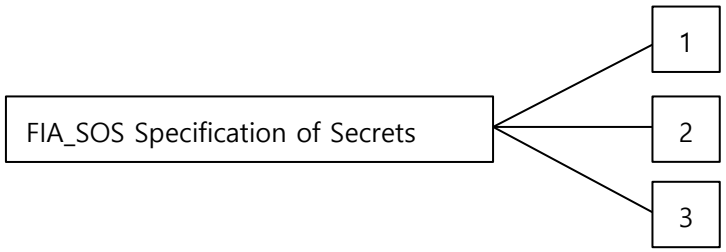
Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication between [assignment*: different parts of TOE*] using the [assignment*: authentication protocol*] that meets the following [assignment*: list of standards*].

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) Minimal : 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*].

4.3 Security Management

4.3.1 ID and password

Family Behaviour

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

Component leveling

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

Management: FMT_PWD.1

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

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

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

a) Minimal: All changes of the password

4.3.1.1 FMT_PWD.1 Management of ID and password

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment*: list of functions*] to [assignment*: the authorized identified roles*].

1. [assignment*: password combination rules and/or length*]
2. [assignment*: other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [*assignment: list of functions*] to [*assignment: the authorized identified roles*].

1. [assignment: *ID combination rules and/or length*]
2. [assignment*: other management such as management of special characters unusable for ID, etc.*]

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

4.4 Protection of the TSF

4.4.1 Protection of stored TSF data

Family Behaviour

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

Component leveling

FPT_PST Protection of 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*].

5 Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.
The security requirements of this Security Target conform the security requirements of "Korean National Protection Profile for Single Sign On V3.0".

5.1 Security functional requirements

The following <Table 5-1 Security functional requirements summary> shows a summary of the security functional requirements used in this Security Target.

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3(1)	Selectable audit review (User log)
	FAU_SAR.3(2)	Selectable audit review (Administrator log)
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation (KEK generation)
	FCS_CKM.1(2)	Cryptographic key generation (Secret key other than KEK)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Symmetric key)
	FCS_COP.1(2)	Cryptographic operation (HMAC)
	FCS_COP.1(3)	Cryptographic operation (HASH)
	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	Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.2(1)	User authentication before any action (User)
	FIA_UAU.2(2)	User authentication before any action (Administrator)
	FIA_UAU.4(1)	Single-use authentication mechanisms (ID/PW)
	FIA_UAU.4(2)	Single-use authentication mechanisms

		(Authentication token)
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before every action
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(1)	Per user attribute limitation on multiple concurrent sessions (Administrator)
	FTA_MCS.2(2)	Per user attribute limitation on multiple concurrent sessions (User)
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1(1)	TOE session establishment (Management access session)
	FTA_TSE.1(2)	TOE session establishment (User session)
FTP	FTP_ITC.1	Inter-TSF trusted channel

Table 5-1 Security functional requirements summary

5.1.1 Security audit (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to Security alarms

Dependencies FAU_SAA.1 Potential violation analysis.

FAU_ARP.1.1 The TSF shall take [Response actions of <Table 5-2 Response actions for potential security violation events>] upon detection of a potential security violation.

Security functional component	Potential security violation events	Response actions
FAU_STG.3	Audit trail storage is inspected (1 second) and the audit trail exceeds the storage capacity threshold.	1) Send email to the 0 level administrator
FAU_STG.4	Audit trail storage is inspected (1 second) and the audit trail exceeds the storage capacity limit.	1) Send email to the 0 level administrator 2) Delete the oldest audit trail
FIA_AFL.1	Administrator or user	1) Disable authentication for administrators and

	authentication failures reach 0~1 level administrator-configurable failure count	users for a period of time configurable by the 0~1 level administrator 2) Send email to the 0 level administrator
FPT_TST.1	Failure to verify integrity of TSF and TSF data on SSO server and SSO agent	1) Send email to the 0 level administrator
	SSO server self-test failure	1) Send email to the 0 level administrator

Table 5-2 Response actions for potential security violation events

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) ["Audit events " of <Table 5-3 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, ["Additional audit information" of <Table 5-3 Auditable events > reference]

Category	Sub-category	Audit events	Additional audit information
SSO Server (SSO)	**Identification and authentication**	FIA_SOS.2 Rejection by the TSF of any tested secret	
		FIA_SOS.3 (Extened) Success and failure of the activity(applicable to the destruction of SSO token only)	
		Authentication failure when attempting to reuse credentials that are prohibited from being reused	
SSO Server (excluding SSO)	**Identification and authentication**	User login and logout	
		User registration, change and deletion	
		The reaching of the threshold for the unsuccessful user authentication attempts and the actions taken	
		All changes of the password	
		Authentication failure when attempting to reuse credentials that are prohibited from being reused	
	Security	IP registration, deletion of administrative terminals	

	management	Execution of security management function and all changes and deletions of security attribute values. ** However, among the security management functions, 'Audit record inquiry' and 'TOE version information inquiry' functions are excluded	Changed security attribute data
		Default account(ID)/Password change	
		Management terminal access IP blocking	
		Changes in agent registration status	
	Trusted session management	User's session locking or termination	
		Response actions when duplicate login attempts of the same account are detected	
		Denial of new sessions based on the limit on the number of concurrent sessions	
	Cryptographic key generation	Cryptographic key generation failure	
	Cryptographic operation	Cryptographic operation failure (including cryptographic operation type)	
	Self-protection	Execution of self-test	Failed security function
		Execution of integrity verification of the TOE itself	Components with failed integrity verification
	Audit records	Response actions when audit record fails to be stored	
SSO Agent	**Self-protection**	Execution of integrity verification and its results	
	Audit records	Agent start	

Table 5-3 Auditable 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 [potential security violation events of <Table 5-2 Response actions for potential security violation events>] known to indicate a potential security violation

b) [None]

5.1.1.4 FAU_SAR.1 Audit review

Hierarchical to No other components.

Dependencies FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [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(1) Selectable audit review (User log)

Hierarchical to No other components.

Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the capability to apply [method in <Table 5-4 Criteria and methods for selecting and sequencing user-related audit logs>] of audit data based on [the logical product (AND) of one of the criteria in Selection 1, one of the criteria in Selection 2, and one of the ordering criteria in <Table 5-4 Criteria and methods for selecting and sequencing user-related audit logs>].

Category	Criteria	Method
Selection 1	Audit log creation date	Select a fixed period (today, yesterday, last week, last month, specify date)
Selection 2	Serial number (audit log storage order), user ID, user name, access IP, service name, log type, detailed information	Search substrings with user-specified search terms. If search term is not specified, search all logs
Ordering	Sequence number, audit log creation date and time, user ID, user name, access IP, service name, log type, detailed information	Sort ascending or descending

Table 5-4 Criteria and methods for selecting and sequencing user-related audit logs

5.1.1.6 FAU_SAR.3(2) Selectable audit review (Administrator log)

Hierarchical to No other components.

Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the capability to apply [the logical product (AND) of one of the criteria for selection 1, one of the criteria for selection 2, and one of the ordering criteria in <Table 5-5 Criteria and methods for selecting and sequencing administrator-related audit logs>] of audit data based on [<Table 5-5 Criteria and methods for selecting and sequencing administrator-related audit logs>].

Category	Criteria	Method

Selection 1	Audit log creation date	Select a fixed period (today, yesterday, last week, last month, specify date)
Selection 2	Serial number (audit log storage order), administrator ID, administrator name, access IP, log type, detailed information	Substring search with user-specified keywords If search term is not specified, search all logs
Ordering	Sequence number (audit log storage order number), audit log creation date and time, administrator ID, administrator name, access IP, log type, detailed information	Sort ascending or descending

Table 5-5 Criteria and methods for selecting and sequencing administrator-related audit logs

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

Hierarchical to No other components

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Notify the 0 level administrator, [none]] if the audit trail exceeds [Limit set by the 0 level administrator (30% ~ 70%, default: 60%)].

5.1.1.8 FAU_STG.4 Prevention of audit data loss

Hierarchical to FAU_STG.3 Action in case of possible audit data loss

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [Send email to 0 level administrator] if the audit trail is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 FCS_CKM.1(1) Cryptographic key generation (KEK 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 [PBKDF] and specified cryptographic key sizes [128 bits] that meet the following: [TTAK.KO-12.0334-Part1~4].

5.1.2.2 FCS_CKM.1(2) Cryptographic support (Secret key other than KEK)

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 [HASH_DRBG SHA224] and specified cryptographic key sizes [128 bits, 256 bits] that meet the following: [TTAK.KO-12.0331-Part1~4].

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 destruct cryptographic keys in accordance with a specified cryptographic key destruction method [Repeatedly overwritten with 0x00 5 times] that meets the following: [none].

5.1.2.4 FCS_COP.1(1) Cryptographic operation (Symmetric key)

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 [cryptographic operations of <Table 5-6 Cryptographic Operation (Symmetric key)>] in accordance with a specified cryptographic algorithm [SEED (Mode=CBC)] and cryptographic key sizes [128 bits] that meet the following: [TTAS.KO-12.0004/R1, KS X ISO/IEC 18033-3].

Cryptographic key name	Cryptographic operations
KEK	Encryption and decryption of Token encryption and decryption key, DEK, integrity verification key
DEK	Encryption and decryption of TSF data excluding authentication tokens and encryption keys, mutual authentication between TOE components
Token encryption/decryption key	Encryption and decryption of Authentication token

Table 5-6 Cryptographic Operation (Symmetric key)

5.1.2.5 FCS_COP.1(2) Cryptographic operation (HMAC)

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 [verification of integrity of TSF and TSF data] in accordance with a specified cryptographic algorithm [HMAC SHA256] and cryptographic key sizes [256 bits] that meet the following: [KS X ISO/IEC 9797-2].

5.1.2.6 FCS_COP.1(3) Cryptographic operation (HASH)

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 [One-way encryption (HASH) of administrator's PW and end user's PW] in accordance with a specified cryptographic algorithm [SHA256] and cryptographic key sizes [No other components] that meet the following: [ISO/IEC 10118-3].

5.1.2.7 FCS_RBG.1 Random bit generation (Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FCS_RBG.1.1 The TSF shall generate random bit required to generate an cryptographic key using the specified random bit generator that meets the following [TTAK.KO-12.0331-Part1~4].

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 *an **0~3 level administrator** configurable positive integer within [1 ~ 5]* unsuccessful authentication attempts occur related to [0~3 level administrator's authentication attempt, end user's authentication attempt].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [The authentication function for the same administrator or end user is disabled for a positive number of minutes from 5 to 90 that can be configured by the 0~1 level administrator.].

5.1.3.2 FIA_IMA.1 TOE Internal mutual authentication (Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [SSO server and SSO agent] in accordance with a specified [Self-implemented protocol] that meets the following: [none].

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 *[<Table 5-7 Password acceptance* criteria*>*].

Description	Contents
Compliance	Ensure a length of 9 to 20 characters
	Contains at least one number, uppercase letter(english), lowercase letter(english), and special character
Prohibition	Do not set the same password as the user account (ID)
	Prohibition of consecutive repeated input of the same letter/number
	Prohibit sequential input of consecutive letters or numbers on the keyboard
	Prohibition of reuse of the password used immediately before

Table 5-7 Password acceptance criteria

5.1.3.4 FIA_SOS.2 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. [Combination of SSO agent ID, user ID, timestamp, user IP, server IP, token serial number, and HMAC value]

FIA_SOS.2.2 TSF shall be able to enforce the use of TSF-generated **authentication token** for [Integrated user authentication].

5.1.3.5 FIA_SOS.3 Destruction of secrets (Extended)

Hierarchical to No other components.

Dependencies FIA_SOS.2 Generation of secrets

FIA_SOS.3.1 The TSF shall destroy **authentication tokens** in accordance with a specified **authentication token** destruction method [Repeatedly overwritten with 0x00 5 times] that meets the following: [none].

5.1.3.6 FIA_UAU.2(1) User authentication before any action (End User)

Hierarchical to FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **end user** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **end user**.

5.1.3.7 FIA_UAU.2(2) User authentication before any action (Administrator)

Hierarchical to FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrator**.

5.1.3.8 FIA_UAU.4(1) Single-use authentication mechanisms (ID/PW)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [administrator/end user password authentication mechanism].

5.1.3.9 FIA_UAU.4(2) Single-use authentication mechanisms (Authentication token)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [Authentication token authentication mechanism].

5.1.3.10 FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components.

Dependencies FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [Display masking of entered password (●), Authentication success/failure indication] to the user while the authentication is in progress.

5.1.3.11 FIA_UID.2 User identification before every action

Hierarchical to FIA_UID.1 Timing of identification

Dependencies No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security management (FMT)

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 [security

management of <Table 5-8 Managed Security Features>] to [authorized roles of <Table 5-8 Managed Security Features>].

Sub-category	Security management	Authorized roles
Identification and authentication	Registration, deletion, and modification of administrators	0~1 level administrator
	User registration, deletion, and modification	0~2 level administrator
	Grant administrator privileges	0~1 level administrator
	Setting user's password combination/length policy	0~1 level administrator
	Setting the allowed number of user's authentication failures	0~1 level administrator
	Setting the time from deactivation of user's authentication function to re-activation	0~1 level administrator
Security management	IP registration, deletion of management terminals	0~2 level administrator
	Agent inquiry - status, version, and applied security policy	0~2 level administrator
	Agent security policy management – policy settings, policy transmission	0~2 level administrator
Self-protection	Performing an integrity verification of the TOE setting values and the TOE itself by the administrator's request	0 level administrator
Safe session management	User session timeout time setting	0~1 level administrator
Audit records	Inquiry of audit records	0~3 level administrator

Table 5-8 Managed Security Features

5.1.4.2 FMT_MTD.1 TSF 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*** [TSF data of <Table 5-9 Managed TSF data>] to [[<Table 5-9 Managed TSF data>'s authorized roles].

TSF data management behavior	Authorized roles
Grant permission to administrator account (ID)	0~1 level administrator
Add, delete, and modify administrator ID	0~1 level administrator
Add, delete, or modify end user ID	0~2 level administrator
Add, delete, or modify user passwords	0~2 level administrator
Set user password combination/length policy	0~1 level administrator
Set the number of times a user is allowed to fail authentication	0~1 level administrator
Setting the time until activation of the user authentication function after it is disabled	0~1 level administrator
Setting the audit trail threshold to notify the administrator when	0 level administrator

predicting loss of audit records	
Registration and deletion of management terminal IP address	0~2 level administrator
Agent inquiry - Required information for inquiry: agent version, security policy applied to the agent, agent operation status (activation/deactivation), agent integrity verification result (success/failure)	0~2 level administrator
Agent security policy management	0~2 level administrator
Setting up authentication information for accessing external IT entities	0~1 level administrator
TOE and TOE component (server, agent) identification information inquiry	0~2 level administrator
Set automatic end time for user sessions	0~1 level administrator
Audit record inquiry	0~3 level administrator
Set predefined audit trail size limits	0~1 level administrator

Table 5-9 Managed TSF data

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

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [password creation/change function for end users and 0~3 level administrators] to [**0~1 level administrator**].

1. [Logical product (AND) of acceptance criteria for each item of <Table 5-7 Password acceptance criteria>]
2. [None]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [none] to [the authorized administrator].

1. [none]
2. [none]

FMT_PWD.1.3 The TSF shall provide the capability *changing the password when the **authorized administrator and end user** accesses for the first time.*

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: [<Table 5-8 Managed Security Features> management, <Table 5-9 Managed TSF data> management, End user and administrator ID/password management].

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 [Administrator, End user].

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

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 the TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.

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 shall protect [Administrator information (administrator ID, administrator password, administrator password salt value, administrator accessible IP, email), end user information (user ID, user password, user password salt value, user access IP usage status, email), agent information (authentication server URL, SID, library path, request data, mutual authentication validity time), authentication token, token encryption/decryption key, DEK, integrity verification key] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

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 *at the initial start-up periodically during normal operation* to demonstrate the correct operation of *TSF*.

FPT_TST.1.2 The TSF shall provide **0 level administrator** with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide **0 level administrator** with the capability to verify the integrity of *TSF*.

5.1.6 TOE access (FTA)

5.1.6.1 FTA_MCS.2(1) Per user attribute limitation on multiple concurrent sessions (administrator)

Hierarchical to FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions belonging to the same **administrator** according to the rules [limiting the maximum number of concurrent sessions to 1 for **administrator** who have the same privilege and the same **administrator**, [<Table 5-10 Concurrent session limitation rule when administrator attempts HTTPS management connection>]].

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

Category		**Existing session manager permissions**		
		0~1 level	**2 level**	**3 level**
New connection manager authority	**0~1 level**	Release existing session, Allow new connections	Release existing session, Allow new connections	Allow concurrent sessions
	2 level	Maintain existing sessions, Block new connections	Release existing session, Allow new connections	Allow concurrent sessions
	3 level	Allow concurrent sessions	Allow concurrent sessions	Allow concurrent sessions

Table 5-10 Concurrent session limitation rule when administrator attempts HTTPS management connection

5.1.6.2 FTA_MCS.2(2) Per user attribute limitation on multiple concurrent sessions (end user)

Hierarchical to FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions belonging to the same **end user** according to the rules [limiting the maximum number of concurrent sessions to 1 for same end **users**, [none]].

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

5.1.6.3 FTA_SSL.3 TSF-initiated termination

Hierarchical to No other components.

Dependencies No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [time interval of user inactivity default: 10 minutes (5~10 minutes)].

5.1.6.4 FTA_TSE.1(1) TOE session establishment (management access session)

Hierarchical to No other components.

Dependencies No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **the administrator's management access session** establishment

based on [access IP, *none*].

5.1.6.5 FTA_TSE.1(2) TOE session establishment (user session)

Hierarchical to	No other components.
Dependencies	No dependencies.
FTA_TSE.1.1	The TSF shall be able to deny **end user session** establishment based on [agent IP, agent ID].

5.1.7 Trusted path/channels (FTP)

5.1.7.1 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 *the TSF* to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [Email notification function to administrator].

5.2 Security assurance requirements

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

Security assurance class	Security assurance component
Security Target	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 5-11 Security assurance requirements

5.2.1 Security Target evaluation

5.2.1.1 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.

5.2.1.2 ASE_CCL.1 Conformance claims

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

Developer action 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.

5.2.1.3 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.

5.2.1.4 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.

5.2.1.5 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.

5.2.1.6 ASE_TSS.1 TOE summary specification

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

Developer action 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.

5.2.2 Development

5.2.2.1 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.

5.2.3 Guidance documents

5.2.3.1 AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

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

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

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

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

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

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

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

Evaluator action elements

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

5.2.3.2 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

5.2.4 Life-cycle support

5.2.4.1 ALC_CMC.1 Labelling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action 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.

5.2.4.2 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.

5.2.5 Tests

5.2.5.1 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.

5.2.5.2 ATE_IND.1 Independent testing - conformance

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

Developer action 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.

5.2.6 Vulnerability assessment

5.2.6.1 AVA_VAN.1 Vulnerability survey

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

Developer action 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.

5.3 Security requirements rationale

5.3.1 Dependency rationale of security functional requirements

The following table shows dependency of security functional requirements.

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

30	FTA_SSL.3	-
31	FTA_TSE.1(1)(2)	-
32	FTP_ITC.1	-

Table 5-12 Rationale for the dependency of the security functional requirements

FAU_GEN.1 has a dependency on FPT_STM.1. However, in the case of the TOE in this Security Target, since the corresponding function is supported by the operating environment, a security objective for the operating environment (OE.RELIABLE_TIMESTAMP) was added, and this satisfies the dependency relationship.

FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1. However, in the case of this Security Target, since the function is supported by the operating environment such as DBMS, the security objective for the operating environment (OE.DBMS) was added, and this satisfies the dependency relationship.

FIA_UAU.2(1)(2), FMT_SMR.1, and FTA_MCS.2(1)(2) have a dependency on FIA_UID.1. However, in the case of this Security Target, since FIA_UID.2, which has a hierarchical relationship with this SFR, is used for the corresponding function, the dependency relationship is satisfied.

FIA_AFL.1, FIA_UAU.7 have a dependency on FIA_UAU.1. However, in the case of this Security Target, FIA_UAU.2, which has a hierarchical relationship with this SFR, is used for the corresponding function, so the dependency relationship is satisfied.

5.3.2 Dependency rationale of security assurance requirements

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

The augmented ATE_FUN.1 has dependency on ATE_COV.1. 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 ST since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6 TOE Summary Specification

6.1 Security audit (TSS_AU)

6.1.1 Audit data generation

■ Related SFR: FAU_GEN.1

Audit data on TOE start-up and shutdown and audit data generated from each TOE component (SSO server, SSO agent) for auditable events in <Table 5-3 Auditable events> is stored in the DBMS (MariaDB) of the SSO server and as a file in the DBMS partition (/opt/penta/data1/mysql/isignplus).

The information recorded when generating audit data is the event date and time, event type, identity of the subject (if possible), and event result (success or failure). In the case of audit data for some auditable events, <Table 5-3 Auditable events> includes additional audit information.

6.1.2 Response to security violations

■ Related SFR: FAU_ARP.1, FAU_SAA.1

The TOE detects "potential security violation events" in <Table 5-2 Response actions for potential security violation events> and performs "response actions" for violation events.

When the SSO server checks the audit trail storage and exceeds the storage capacity threshold, it notifies the 0 level administrator by email as a response. If the limit is exceeded, the 0 level administrator is notified by email as a response and the oldest audit data is deleted.

If administrator or user authentication failures occur 5 times (default value, 0~1 level administrator can set within 1 to 5 times), the authentication function of the administrator or end user is disabled for 5 minutes (default value, 0~1 level administrator can set within 5 to 90 minutes), and an email is sent to the 0 level administrator.

If the SSO server's self-test for authentication token verification fails, the 0 level administrator is notified by email, and all subsequent end users' authentication requests are processed as failed.

When the SSO server and SSO agent start up, the SSO agent periodically (6 hours), and the SSO server at the request of the 0 level administrator performs integrity verification of the TSF executable code and TSF data using the HMAC SHA-256 algorithm. In case of failure, an email is sent to the 0 level administrator. In addition, the SSO server performs a self-test on all TSF execution processes at startup and periodically (1 hour), and sends an email to the 0 level administrator if the self-test fails.

6.1.3 Audit review

■ Related SFR: FAU_SAR.1, FAU_SAR.3(1), FAU_SAR.3(2)

After successfully identifying and authenticating the SSO server and logging in, the authorized administrator can view the log through the log menu of the management tool. The audit data sent and saved to the SSO server will be displayed on the management tool screen and all logs can be reviewed.

When an authorized administrator searches audit data, the TOE outputs audit data according to <Table 5-4 Criteria and methods for selecting and sequencing user-related audit logs> and <Table 5-5 Criteria and methods for selecting and sequencing administrator-related audit logs> for each item in the log, and it is ordered and searched in ascending or descending order.

6.1.4 Audit data protection and loss response

■ Related SFR: FAU_STG.3, FAU_STG.4

After the SSO server starts up, the disk usage of audit data is periodically checked by a thread that runs automatically, and if the audit data exceeds the disk usage threshold set by the 0 level administrator, response action is taken by notifying the 0 level administrator by email. The threshold setting value range is 30 to 70 (%) (default value: 60%) and can be set by the 0 level administrator.

If the audit data exceeds the disk usage limit set by the 0 level administrator, the 0 level administrator is notified by email. In addition, the oldest audit data among recent logs is deleted in file units, and deletion ends when disk usage reaches the threshold. The disk usage limit value range is (threshold setting value + 1) ~ 80(%) (default value: 70%)

6.2 cryptographic support (TSS_CS)

6.2.1 Random bit and Cryptographic key generation

■ Related SFR: FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1

The TOE uses a verified cryptographic module (CIS-CC V4.0) to generate KEK, DEK, integrity verification key, and token encryption/decryption key.

The standard list for generating KEK, encryption key generation algorithm, encryption key length, encryption key type and purpose are as follows.

List of standards	Cryptographic key generation	Cryptographic key sizes	Cryptographic key types and purposes

	algorithm		
TTAK.KO-12.0334-Part 1~4	PBKDF	128 bits	KEK - DEK and integrity verification key are encrypted and stored in DBMS, salt.dat - Encrypt the token encryption and decryption key and store it in DBMS

Table 6-1 KEK generation

The standard list for generating secret keys other than KEK, encryption key generation algorithm (random bit generator), cryptographic key sizes, cryptographic key type and purpose are as follows.

List of standards	Cryptographic key generation algorithm	Cryptographic key sizes	Cryptographic key types and purposes
TTAK.KO-12.0331-Part1~4	HASH_DRBG SHA-224	128 bits	DEK - TSF data encryption/decryption operation - Encryption/decryption operation of mutual authentication data Token encryption and decryption key - Authentication token encryption/decryption operation
		256 bits	Integrity verification key - Generate integrity verification values for TSF and TSF data

Table 6-2 Generating secret keys other than KEK

6.2.2 Cryptographic key destruction

■ Related SFR: FCS_CKM.4

The TOE destroys the cryptographic key by overwriting 0x00 for the KEK, DEK, integrity verification key, and token encryption/decryption key 5 times. All cryptographic keys are destroyed immediately after use. The cryptographic key, timing of cryptographic key destruction, and cryptographic key destruction method are as follows.

Cryptographic key	Timing of cryptographic key destruction	Cryptographic key destruction method
KEK	Destroy the plain text KEK loaded in memory immediately after encryption and decryption of	Overwrite 0x00 5 times

	DEK, token encryption and decryption key, and integrity verification key. Destruction of self-encoded KEK loaded in memory upon termination of TOE	
DEK	Destroy the plaintext DEK loaded in memory immediately after encrypting and decrypting TSF data.	Overwrite 0x00 5 times
Token encryption/decryption key	Destroy the plaintext token encryption and decryption key loaded in memory immediately after authentication token encryption and decryption.	Overwrite 0x00 5 times
Integrity verification key	Destroy the plaintext integrity verification key loaded into memory immediately after integrity verification.	Overwrite 0x00 5 times

Table 6-3 Cryptographic key destruction method

6.2.3 Cryptographic operation

- Related SFR: FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3)

- Symmetric key (KEK, DEK, token encryption and decryption key)

  Using the encryption algorithm SEED (Mode=CBC) that conforms to TTAS.KO-12.0004/R1, KS X ISO/IEC 18033-3, perform the 'cryptographic operation' in <Table 5-6 Cryptographic Operation (Symmetric key)> with an encryption key of 128 bits in length.

  During each SEED encryption operation, a 128-bit random bit is generated and used as an encryption key using HASH-DRBG SHA-224, a random bit generator subject to verification that complies with TTAK.KO-12.0331-Part1~4 of the the validated cryptographic module (CIS-CC V4.0(<Table 6-4 The validated cryptographic module>)).

- HMAC (Integrity verification key)

  The TOE verifies the integrity of the TSF executable code and TSF data using the HMAC SHA-256 algorithm that conforms to KS X ISO/IEC 9797-2 (Using CIS-CC V4.0(<Table 6-4 The validated cryptographic module>))

- HASH

  Login passwords of administrators and end users are encrypted using SHA-256, a one-way encryption algorithm that complies with ISO/IEC 10118-3. Even if the password is the same, salt is used to generate a different ciphertext each time.

- The validated cryptographic module

Cryptographic module name and version	Verification number	Verification date	Developer
CIS-CC V4.0	CM-213-2027.10	2022-10-04	Penta Security Inc.

Table 6-4 The validated cryptographic module

6.3 identification and authentication (TSS_IA)

6.3.1 identification and authentication

■ Related SFR: FIA_AFL.1, FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.4(1), FIA_UAU.7, FIA_UID.2

TOE provides identification and authentication mechanisms for administrators and end users based on ID and password. Administrators who successfully identify and authenticate can access the management tool screen and perform security management. And end users who are successfully identified and authenticated can use the authentication token to access business services assigned to the end user by 0~2 level administrators.

When the number of administrator and end user authentication failures reaches the allowable number of failures set by the 0~1 level administrator (default: 5, can be set within 1 to 5), the relevant administrator and end user accounts are locked for the time set by the 0~1 level administrator (default value: 5 minutes, can be set within 5 to 90 minutes), for locked accounts, identification and authentication requests are rejected for a specified time, and administrator and end user authentication requests are allowed after the specified time has elapsed.

When an administrator accesses a management tool or an end user accesses a business service, the password entered during identification and authentication is changed to a masking character (•) and displayed.

When processing administrator and end user login failures, 'Login failed.' is output and detailed information on the reason for the failure is not provided. Additionally, all functions provided by all TOEs cannot be used before successful login.

The SSO server generates a random value when authenticating the administrator based on ID/password, issues a session ID including UUID (Universally Unique Identifier), and stores it in the DBMS. If the session ID sent at each request after the administrator logs into the management tool does not match the administrator's session ID stored in the DBMS, the SSO server considers the session ID to have been reused and the session is blocked.

6.3.2 Mutual authentication between TOE components (SSO server and SSO agent)

■ Related SFR: FIA_IMA.1

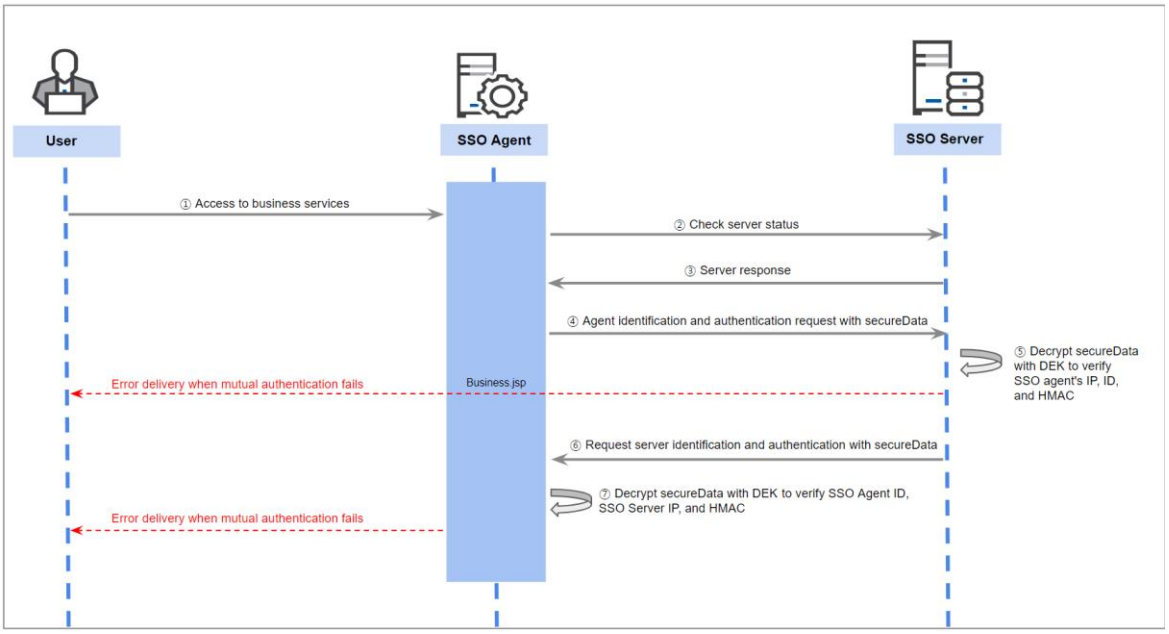


Figure 6-1 Mutual authentication

The TOE performs mutual authentication between separate TOE components (SSO server, SSO agent) using self-implemented protocol. Penta Security Inc.'s self-implemented security protocols are divided into request protocols and response protocols.

The mutual authentication mechanism is as follows. When an end user accesses a business service, the SSO agent checks the status of the SSO server, and the SSO server responds as an SSO agent. Afterwards, the SSO agent sends secureData to the SSO server to request identification and authentication. This secureData is a combination of the SSO Agent ID, SSO Agent IP, and the HMAC value of the SSO Agent ID and IP encrypted with DEK.

The SSO server decrypts the secureData in the request with DEK, identifies the SSO agent with the SSO agent's ID and IP, and verifies the HMAC value. At this time, if it is different from the agent information stored in the SSO server, an error result regarding mutual authentication failure is delivered to the end user.

If the SSO server succeeds in identifying and authenticating the SSO agent, the SSO server transmits secureData to the SSO agent to request identification and authentication of the SSO server. This secureData is a combination of the SSO agent ID, SSO server IP, and the HMAC value of the SSO agent ID and server IP encrypted with DEK.

The SSO agent decrypts the received secureData with DEK, identifies the SSO server with the SSO server IP, and verifies the HMAC value. At this time, if it is different from the SSO server IP stored in the SSO agent's salt.dat, an error result regarding mutual authentication failure is delivered to the end user.

6.3.3 Generation and destruction secrets

■ Related SFR: FIA_SOS.2, FIA_SOS.3, FIA_UAU.4(2)

The SSO server generates an authentication token after the end user logs in to the SSO agent, verifies the authentication token, and determines whether to allow access to the business service. The SSO server generates an authentication token for the end user by combining the business service ID, user ID, timestamp, user IP, token serial number, and HMAC value, encrypts it with the token encryption and decryption key, and stores it in the DBMS.

Authentication tokens are destroyed by overwriting 0x00 5 times immediately after the user logs out of the SSO agent, when the 0~2 level administrator forcibly terminates the end user's session through the management tool.

When authenticating an end user based on a token, the SSO server uses the authentication token creation time information and token serial number to prevent reuse of the authentication token. The token serial number is a value that increases by 1 each time the authentication token is verified after the authentication token is created.

6.4 Security management (TSS_MT)

6.4.1 security management function

■ Related SFR: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

In the TOE, authorized administrators can perform <Table 5-8 Managed Security Features>'s 'security function management actions' through management tools. Authorized administrators can perform management actions on security functions through the TOE identification and authentication process.

Additionally, in the TOE, authorized administrators can perform 'TSF data management actions' in <Table 5-9 Managed TSF data> through management tools. Authorized administrators can perform management actions (query, change, delete, add) on TSF data through the TOE identification and authentication process.

For 3 level administrators, only the authority to view audit logs among TSF data is granted.

6.4.2 User ID and password management

■ Related SFR: FMT_PWD.1, FMT_SMF.1, FMT_SMR.1, FIA_SOS.1

There is only one 0 level administrator account and it has a fixed ID ('adm'). When the administrator first accesses the management tool, the administrator logs in with the default password (0 level administrator)

and temporary password (1~3 level administrator). A screen is displayed forcing the administrator to change the password immediately upon successful login, and if the password is not changed, other functions of the management tool cannot be used.

The administrator's password must comply with the administrator password length and combination rules set by the 0~1 level administrator in the management tool (<Table 5-7 Password acceptance criteria>).

The rules in the table are followed when the 0 level administrator changes the default password when first logging in, when the 1~3 level administrator changes the initial temporary password, when the 0~1 level administrator creates the 1~3 level administrator account, and also when the administrator changes the password.

The end user's password must comply with the user password length and combination rules set by the 0~1 level administrator in the management tool (<Table 5-7 Password acceptance criteria>). This rule must be followed even when the initial temporary password that is automatically generated when a 0~2 level administrator creates an end user account or when the end user changes the password. When an end user first accesses a business service, the user logs in with a temporary password. As soon as the login is successful, a screen is displayed forcing the user to change the password. If the password is not changed, the user cannot log in to the business service.

6.5 Protection of the TSF (TSS_PT)

6.5.1 Internal TSF data transfer protection

■ Related SFR: FPT_ITT.1

TSF data transmitted between the SSO server and SSO agent, which are separate components of the TOE, are safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2).

Audit records generated by the SSO agent (SSO agent start-up, verifying the integrity of the SSO agent) are transmitted to the SSO server and stored in the DBMS. Audit records generated by the SSO agent while disconnected from the SSO server are stored in the form of temporary files. It is then sent to the SSO server at the time of connection to the SSO server.

In addition, when an end user accesses a business service, the TSF data transmitted during mutual authentication between the SSO agent and SSO server to generate and verify an authentication token is safely transmitted through a secure encrypted transmission protocol (TLS V1.2).

6.5.2 Protection of stored TSF data

■ Related SFR: FPT_PST.1

TSF data required for the operation of the SSO server is stored in the DBMS, the operating environment. TSF data is encrypted and stored with a verified encryption module (CIS-CC V4.0) to protect it from unauthorized exposure and modification. In the case of the SSO agent, TSF data is encrypted and stored in the salt.dat file to protect it from unauthorized exposure and modification.

TSF data		Protection mechanism
Administrator/End User Password		Store the hash value generated with SHA256 (with SALT) in DBMS DEK encrypted and stored in the salt.dat file of the SSO agent
Administrator information	**ID, salt value of password, accessible IP, email**	After encryption with DEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key. DEK encrypted and stored in the salt.dat file of the SSO agent
End User information	**ID, salt value of user password, access IP usage, email**	After encryption with DEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key.
Agent information	**Authentication server URL, SID, library path, request data, mutual authentication validity time**	After encryption with DEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key. DEK encrypted and stored in the salt.dat file of the SSO agent.
Authentication token		After encryption (SEED 128bit + CBC) with the token encryption and decryption key, the HMAC value is stored in DBMS by concatenating the integrity verification key.
Token encryption/decryption key		After encryption with KEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key.
DEK		After encryption with KEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key. DEK encrypted and stored in the salt.dat file of the SSO agent.
Integrity verification key		After encryption with KEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key. DEK encrypted and stored in the salt.dat file of the

	SSO agent.
TOE settings	After encryption with DEK (SEED 128bit + CBC), the HMAC value is stored in DBMS by concatenating the integrity verification key.
KEK	The key (KEK) derived from PBKDF is self-encoded and stored only in memory (RAM)

Table 6-5 Protection of TSF data

6.5.3 integrity verification

■ Related SFR: FPT_TST.1

The SSO server performs integrity verification of all TSFs and TSF data on the SSO server at startup and upon request from the 0 level administrator. The SSO agent performs integrity verification of all TSFs and TSF data (salt.dat) at startup and periodically (every 6 hours). At the time of verifying the integrity of the SSO server and SSO agent, the HMAC SHA256 algorithm is used to generate a hash value for the TSF executable file and TSF data to be verified and perform integrity verification by comparing it with the original hash value. If the generated hash value does not match the original hash value, it is judged as an integrity verification failure, the result is recorded in the audit log, and the management tool 0 level administrator is notified by email.

The TSF and TSF data subject to integrity verification in the SSO server and SSO agent are as shown in the table below, and in the case of TSF, integrity verification is performed on the entire TSF.

	SSO server	SSO agent
TSF	- CIS-CC V4.0 related library files - All files in path {SSO server's TOMCAT}/webapps	- CIS-CC V4.0 related library files - All files in path {SSO agent's TOMCAT}/webapps/ROOT/WEB-INF/lib - All files in path {SSO agent's TOMCAT}/webapps/ROOT/sso
TSF data	- Administrator information (administrator ID, administrator password, salt value of administrator password, administrator accessible IP, email) - End User information (user ID, user password, salt value of user password, user access IP usage, email) - Agent information (authentication server URL, SID, library path, request data, mutual authentication effective time) - Authentication token	Data in the salt.dat file

	- Token encryption/decryption key - DEK - Integrity verification key - TOE settings	

Table 6-6 Integrity verification target

6.5.4 Self-test

■ Related SFR: FPT_TST.1

The SSO server performs a self-test of the authentication token generation and verification process upon startup and periodically (every hour). An authentication token is generated with a fixed input value, the generated authentication token is verified, and if the output value matches the input value, the self-test is successful. In other cases, that is, if the input/output values do not match or the cryptographic operation performed during the self-test fails, the self-test fails.

If the SSO server fails the self-test, the results are recorded in the administrator log and notified to the 0 level administrator by email.

6.6 TOE access (TSS_TA)

6.6.1 Limit number of sessions and terminate sessions

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

0~3 Level administrators can manage and connect to the SSO server through HTTPS communication. Basically, the number of simultaneous sessions between 0~2 level administrators/same accounts excluding 3 level administrators is up to 1. Concurrent sessions are limited according to <Table 5-10 Concurrent session limitation rule when administrator attempts HTTPS management connection>. Additionally, the maximum number of simultaneous sessions for the same end user that can use business services is limited to 1.

The session is automatically terminated when the administrator and end user session timeout time (default 10 minutes, 5 to 10 minutes can be set) set by the 0~1 level administrator in the management tool has elapsed.

Administrators and end users can only access the IP address set in the management tool. When an administrator or end user attempts to log in, the SSO server uses the administrator and end user information in the DBMS to identify the administrator and end user. Afterwards, the IP information accessed by the

administrator and end users is searched and compared with the list of IPs allowed for access by the administrator and end users, and if the IP is not allowed to access, the connection is blocked.

End users can only access business services (SSO Agent IP and SSO Agent ID) that the 0~2 level administrator has mapped to the corresponding user ID through the management tool.

6.7 Trusted path/channel (TSS_TP)

6.7.1 Trusted channel

- Related SFR: FTP_ITC.1

TSF data transmitted between the SSO server and external mail servers is safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2). TSF data transmitted between the SSO server and an external mail server includes an alert email when a potential security violation occurs in the TOE and a temporary password issuance email when 1~3 level administrator and end user passwords are initialized.

Additionally, the SSO server forms a communication channel between the SSO server and the mail server and identifies the mail server based. Based on the mail server information (server address and port, mail user ID/password) set by the 0~1 level administrator in the management tool.