Bandi SSO v7.0

ST

v006

The certified TOE's ST is written in Korean. This document is a translation of the original from Korean into English.

< Revision History >

Revision Version	Revision Date	Changes to Previous Revision
001	06-15-2020	Initial release
002	05-04-2021	Physical scope redefined and terminology consistency ensured
003	06-09-2021	TOE component identifier and document identification configuration structure modified
004	07-13-2021	Product and document version modified
005	08-17-2021	'TOE overview' modified
006	08-26-2021	'Logical scope of the TOE' modified

< Table of Contents >

1 ST Introduction

This document is the Security Target (hereinafter referred to as the "ST") of Bandi SSO v7.0 by Bandi S&C Co., Ltd. that intends to achieve EAL1+ level under the Common Criteria.

1.1 ST Reference

This ST is identified as follows:

Classification	Description
Title	Bandi SSO v7.0 ST
ST Version	v006
Developer	Bandi S&C Co., Ltd.
Publication Date	August 26, 2021
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keywords	Single Sign-On, SSO

1.2 TOE Reference

The Target of Evaluation (hereinafter referred to as the "TOE") that complies with this ST is identified as follows:

Classification		Identifier
TOE Identification		Bandi SSO v7.0
Version Detail		v7.0.1
TOE Component	SSO Server	Bandi SSO Server v7.0.3
	SSO Agent	Bandi SSO Agent v7.0.1
Guidance Document	Operational Guidance	Bandi SSO v7.0 OPE v004
	Preparative Procedure	Bandi SSO v7.0 PRE v004
Developer		Bandi S&C Co., Ltd.

1.3 TOE Overview

1.3.1 Single Sign-On overview

Bandi SSO v7.0 (hereinafter referred to as the "TOE") is a Single Sign-On (SSO) product used to enable an end user to access various business systems (systems in which the SSO Agent has been installed) to use services through a single login (Single Sign-On) without additional login actions. The TOE implements authentication tokens in accordance with universal standard specifications to ensure stronger security and higher flexibility, which makes it applicable to various types of business systems. The TOE performs the user identification and authentication, and then issues authentication tokens in accordance with the user authentication policies to identify the user and verify the validity without a separate login process.

1.3.2 TOE scope

The TOE includes the SSO Server and the SSO Agent. Major functions of each component are as follows:

SSO Server Function

- Generate, destroy and verify an authentication code
- Generate, destroy and verify an authentication token
- Provide user information upon request for information on an authorized user, using an authentication token
- Set and manage basic information (administrator, end user, agent)
- View history (login, audit, password change, authentication code history, authentication token history, integrity)

- Manage policies (operation policy, security policy, access IP, server key management)
- Manage licenses

SSO Agent Function

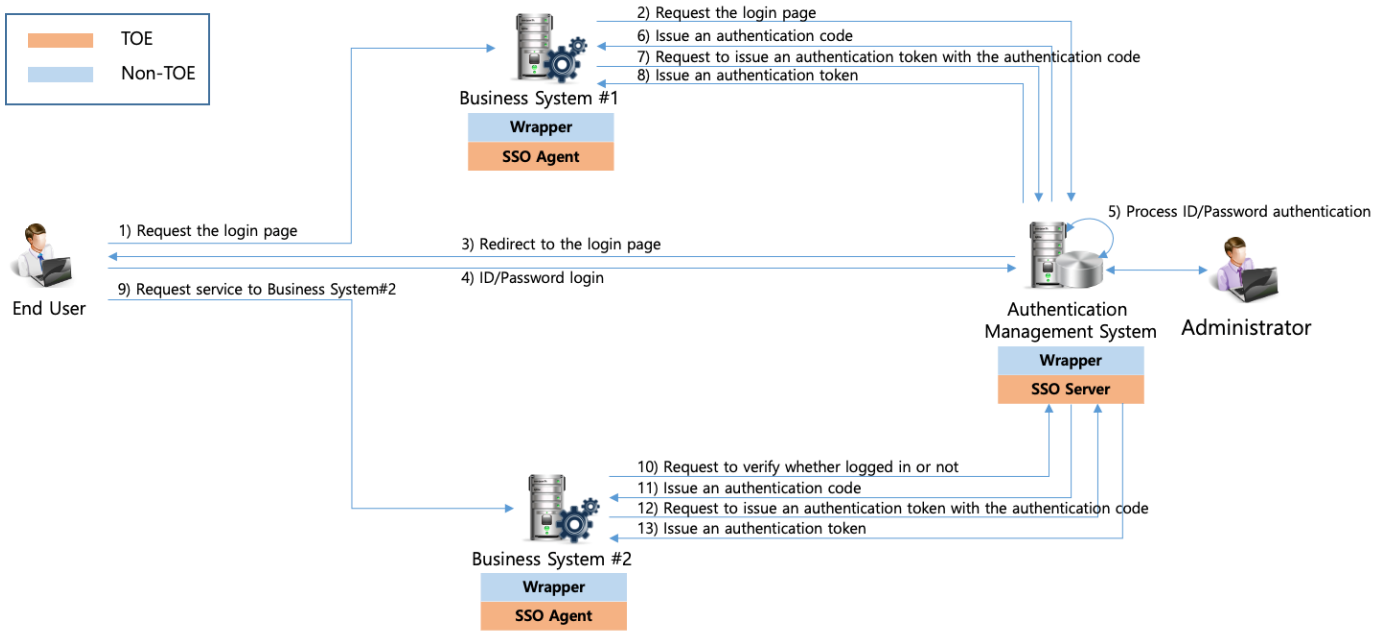
- Request the SSO Server to issue an authentication code
- Request the SSO Server to issue, destroy and verify an authentication token
- Request the SSO Server for information on a user authorized with an authentication token
- Encrypt parameters when communicating with the SSO Server

1.3.3 TOE usage and major security features

The TOE is a Single Sign-On (SSO) product provided in the form of software that permits access to various business systems with a single login by an end user. An end user using TOE requests a login with ID/password. Then, the SSO Server that interacts with a DBMS, a repository of authorized user information, performs login verification. If the login is valid, the SSO Server issues an authentication token to be stored in a business system. When the authorized user requests access to another business system through the authorized user browser and the SSO Server session, the access is controlled through the verification

Furthermore, the TOE provides the security audit function that manages major events by recording them as audit data when the security function and the management function are invoked; the identification and authentication function such as verification of an identity of an authorized user and continuous authentication failures; the cryptographic support function for secure communication and storage; the TSF protection function that ensures TOE internal communication and performs TSF self tests; the security management function that supports an authorized administrator to perform administrative functions; and the TOE access function that controls access sessions of the authorized administrator.

The user identification and authentication procedure of the TOE is shown below in [Figure 1-1] and can be largely divided into two stages: the stage in which an end user is initially authenticated by entering ID and password and then an authentication token is generated, and the stage in which the authentication token generated is verified and access to a relevant business system is made.



[Figure 1-1] Procedure for the identification and authentication of an end user

▣ Generation of an authentication token for the initial authentication of an end user

1) An end user sends a request for the login page to the business system #1.

2) The business system #1 sends a request for the login page to the SSO Server.

3) The SSO Server redirects the user to the login page.

4) The end user requests login using ID and password.

5) The SSO Server verifies ID/password and then processes the authentication.

6) The SSO Server issues an authentication code to the business system #1.

7) The business system #1 requests an authentication token to be issued by using the authentication code issued.

8) The SSO Server issues an authentication token with the authentication code requested by the business system #1.

▣ Access to the business system based on an authentication token

9) The end user accesses the business system #2.

10) The business system #2 requests to verify whether the user who accessed the SSO Server has logged in or not.

11) As the user has already logged in on the SSO Server, an authentication code is issued to the business system #2.

12) The business system #2 sends a request to issue an authentication token by using the authentication code issued.

13) The SSO Server issues an authentication token with the authentication code requested by the business system #2.

▣ Destruction of an authentication token

If a defined period of time elapses based on the validity time of authentication tokens defined by the administrator, or if the user logs out, the authentication token is automatically destroyed.

Authentication Phase	Operation Procedure
Initial authentication	1) Send a request for the login page to the business system#1 2) Send a request for the login page to the SSO Server 3) Redirect to the login page 4) Login with ID/password 5) Verify and authenticate ID/password 6) Issue an authentication code 7) Request an authentication token to be issued 8) Issue an authentication token and store the token
Authentication token-based access to the business system	9) Access to the business system 10) Request to verify whether logged in or not 11) Issue an authentication code 12) Request an authentication token to be issued 13) Issue an authentication token

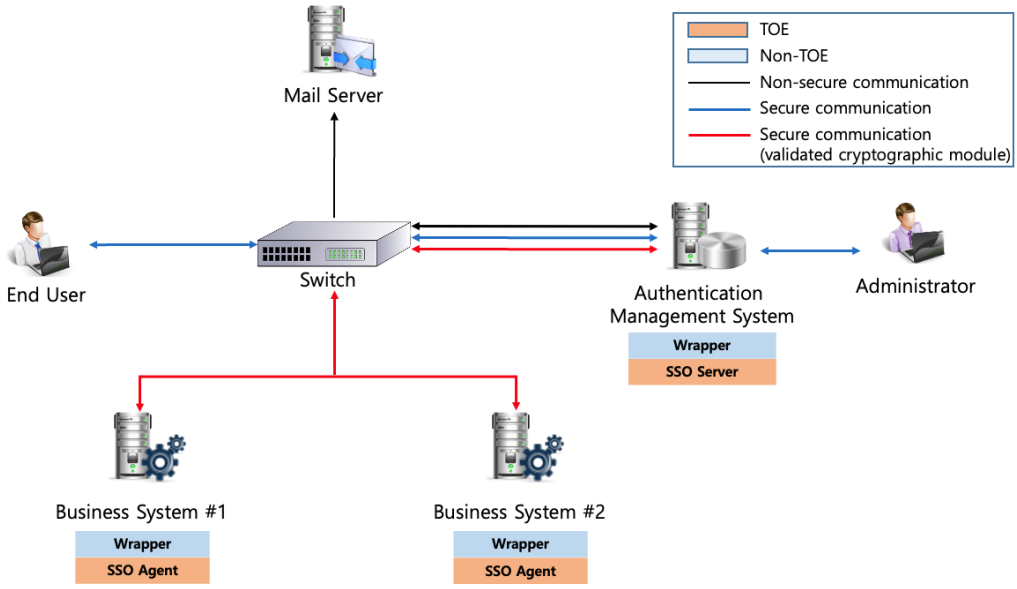
[Table 1-1] Operation procedure for each authentication phase

A subject who issues, stores and verifies the authentication token is as follows:

- A subject who issues the authentication token: SSO Server
- Authentication token storage location: Business system area where the SSO Agent is installed
- A subject who verifies the authentication token: SSO Server

1.3.4 Non-TOE and TOE operational environment

The operational environment of the TOE is shown in [Figure 1-2] TOE operational environment.



[Figure 1-2] TOE operational environment

* Non-secure communication: SMTP communication between the mail server and the SSO Server

* Secure communication: HTTPS communication

* Secure communication (validated cryptographic module): Communication among TOE components using the validated cryptographic module

The operational environment of the TOE is shown in [Figure 1-2], and consists of the SSO Server and the SSO Agent. The SSO Server uses user information stored in DBMS to provide functions such as user login verification, generation of authentication tokens and policy establishment. The SSO Agent performs functions related to request for user authentication to the SSO Server, including issuance of authentication tokens and request for verification, and is provided in the form of API, a library file format, for each business system.

Wrapper, which may be used to ensure the compatibility among the SSO Server, the SSO Agent and various types of business systems, is out of the scope of the TOE.

For the encryption of the communication used in data transfer between TOE components (including mutual authentication between components), MagicJCrypto V2.0.0.0, which is a cryptographic module validated under the Korea Cryptographic Module Validation Program (KCMVP), is used. When logging in via a web browser on a personal computer, administrators and end users communicate through a secure channel (HTTPS) supported in the operational environment for the purpose of secure communications.

The TOE is a software-type product installed on a server. The requirements for hardware and software necessary for the operation of the TOE are described below, as well as the requirements for hardware and software of a personal computer used by an end user or an administrator for the management of the TOE.

Type	Item		Minimum Specifications
SSO Server	H/W	CPU	Intel Core2Duo 2.4 GHz or higher
		HDD	1GB or higher
		RAM	8GB or higher
		NIC	10/100/1000 Mbps Ethernet * 1 port or more
	OS		Linux CentOS 7.8 (Kernel 3.10.0) 64bit
	Mandatory Software		JDK: openJDK-1.8.0-262.b10 WAS: Tomcat 9.0.50 DBMS: MariaDB 10.6.3 Stable
SSO Agent	H/W	CPU	Intel Core2Duo 2.4 GHz or higher
		HDD	1GB or higher
		RAM	8GB or higher
		NIC	10/100/1000 Mbps Ethernet * 1 port or more
	OS		Linux CentOS 7.8 (Kernel 3.10.0) 64bit
	Mandatory Software		JDK: openJDK-1.8.0-262.b10

[Table 1-2] Requirements for hardware and software necessary for the operation of the TOE

The following operational environment is required for end users and administrators.

Type	Item		Minimum Specifications
User PC and Administrator PC	H/W	CPU	Intel Core2Duo 2.4 GHz or higher
		HDD	100 GB or higher
		RAM	4GB or higher
		NIC	10/100/1000 Mbps Ethernet * 1Port or more
	OS		Windows 10 Pro 64Bit
	Mandatory Software		Chrome v83.0

[Table 1-3] Requirements for hardware and software necessary for end users and administrators

Type	Description and Roles
Mail Server	A server interlinked to send an alarm email to an administrator if an administrator authentication fails, a repository of audit trail is full, or an event that compromises the integrity is detected. The Mail Server supports general commercial mail servers.

[Table 1-4] External entity necessary for the operation of the TOE

Encryption Library	Usage		Remarks
MagicJCrypto V2.0.0.0	Asymmetric key cryptographic operation	RSA-OAEP(SHA-256)	TOE internal mutual authentication and cryptographic key exchange
	Symmetric key cryptographic operation	ARIA-256	Encryption and decryption of authentication token and TSF data
	Integrity verification of transmitted data	HMAC (SHA-512)	Verification of the integrity of the data transmitted between TOE components
	Cryptographic key generation	HMAC (SHA-512)	KEK generation
		HASH-DRBG(SHA-256)	Generation of symmetric key and authentication token cryptographic key
	Integrity verification of TSF data	SHA-512	Verification of the integrity of TSF data, critical parameters and critical operation files
	Verification of user password	SHA-512	Verification of user password
OpenJDK 1.8.0 (OpenJSSE 1.1.4)	Data protection in web communication (TLS v1.2)		User's web browser <-> Web server (WAS)

[Table 1-5] Identification of validated cryptographic module and cryptographic algorithm

1.4 TOE Description

This chapter describes the physical and the logical scope of the TOE.

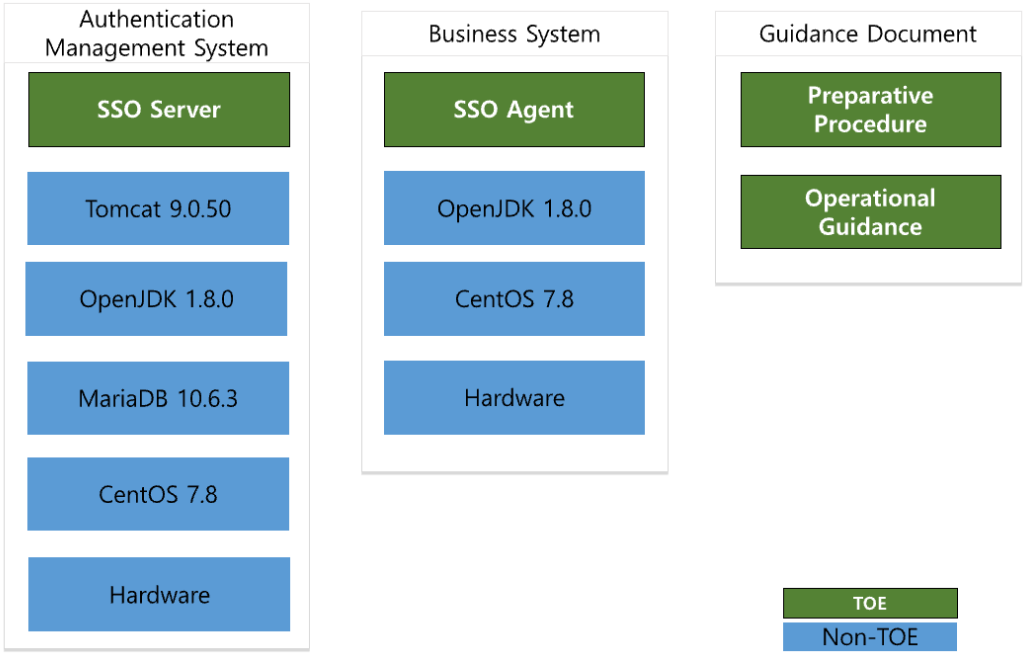
1.4.1 Physical scope of the TOE

The physical scope of the TOE includes installation files (SSO Server and SSO Agent) and guidance documents (operational guidance and preparative procedure) provided in the form of software.

Classification		Identification Information	Type	Delivery Method
TOE Component	SSO Server	Bandi SSO Server v7.0.3 (File name: Bandi_SSO_Server_v7.0.3.tar)	S/W	CD
	SSO Agent	Bandi SSO Agent v7.0.1 (File name: Bandi_SSO_Agent_v7.0.1.tar)	S/W	
Guidance Document	Operational Guidance	Bandi SSO v7.0 OPE v004 (File name: Bandi_SSO_v7.0_OPE_v004.pdf)	Electronic file (PDF)	
	Preparative Procedure	Bandi SSO v7.0 PRE v004 (File name: Bandi_SSO_v7.0_PRE_v004.pdf)	Electronic file (PDF)	

[Table 1-6] Physical scope of the TOE

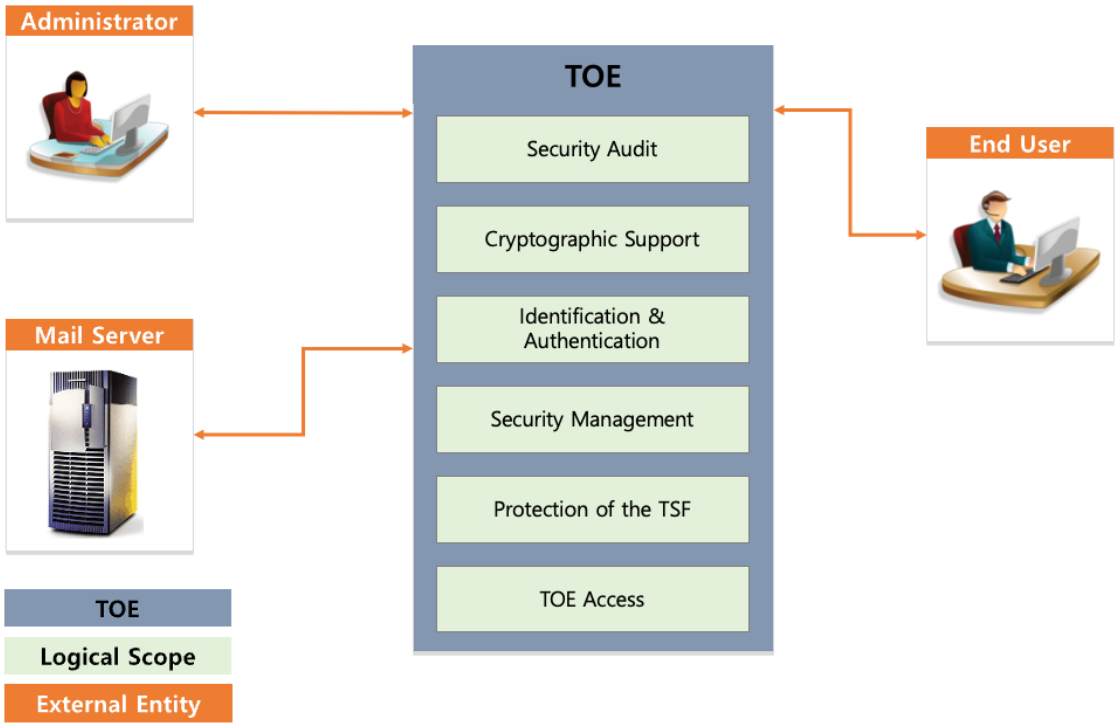
The physical scope of the TOE is shown in [Figure 1-3] below:



[Figure 1-3] Physical scope of the TOE

In [Figure 1-3] above, hardware, operating system (CentOS 7.8), DBMS (MariaDB 10.6.3), WAS (Tomcat 9.0.50) and openJDK 1.8.0 (OpenJSSE 1.1.4), which are necessary for the operation of the TOE, are out of the physical scope of the TOE.

1.4.2 Logical scope of the TOE



[Figure 1-4] Logical scope of the TOE

■ **Security Audit**

The TOE generates audit data based on the date and time of an event, a type of the event, an identity of a subject and the outcome of an auditable event, and provides an authorized administrator with a function to review audit data according to the time of occurrence, a type of an event, user IP, etc. Furthermore, if the audit data exceeds a certain threshold, thereby possibly leading to audit data loss, the TOE sends an email to the authorized administrator to take an action in case the audit trail is full.

■ **Cryptographic Support**

The TOE uses a cryptographic algorithm of the validated cryptographic module (MagicJCrypto V.2.0.0.0) whose security and implementation conformance have been validated, and performs cryptographic key management (generation, distribution and destruction) and cryptographic operation including the encryption of cryptographic keys (symmetric and asymmetric keys) used for TOE internal mutual authentication, protection of transmitted data, protection of stored TSF data (configuration files and executable files) and generation of cryptographic keys to authentication tokens.

■ **Identification and Authentication**

The TOE provides a Single Sign-On (SSO) function that enables a user to use services in various business systems in which the SSO Agent has been installed without going through additional login processes. The TOE performs the identification and authentication of an end user, and then issues an authentication token. If the end user to whom the authentication token was issued accesses business systems in which the SSO Agent has been installed, user can access those systems and uses services by using the authentication token without a login process. Upon the initial access and login to the TOE, the user is identified and authenticated, based on the user ID and password. Passwords used for the identification and authentication in the TOE shall comply with the combination rules (to use alphabet characters, numbers and special characters), password lengths (9 to 30 digits), and restrictions (use of recurring characters in a row and recently used passwords).

■ **Security Management**

The TOE provides the authorized administrator with the security management function. The authorized administrator can perform the management functions such as security policy, user management and audit data settings through a web browser, using a secure channel. The TOE also offers a function to manage valid characters, combination rules, valid lengths and so forth for user account information (ID and password) which is treated as sensitive information in this type of a SSO product. The TOE provides a function to manage user password change for the authorized administrator, and enforces users to change their passwords on a regular basis.

■ **Protection of the TSF**

The TOE performs secure communication by using a validated cryptographic module during the TOE internal communication (encrypted communication between TOE components). Important user and cryptographic information, TOE configuration data and so forth are securely stored through the encryption. The TOE verifies the integrity of configuration files and TSF executable codes, and conducts self tests (self tests of the validate cryptographic module and process availability test) to confirm the normal operation of the TOE.

■ **TOE Access**

The TOE restricts the number of concurrent sessions of the administrator login (up to 1), and prohibits concurrent connections of the same administrator. The TOE performs a function to terminate a session after a certain period of user inactivity. It manages a period of inactivity for each user (end user and administrator) separately. In the case of the administrator, the inactivity period is a fixed value of 10 minutes. For end users who relatively needs convenience, end user inactivity period can be set to 10 minutes or more (default value : 10 minutes) by the administrator. The TOE provides the function to restrict the administrator's management access sessions based on the administrator's access IP. The number of accessible IPs provided by the TOE is set as two.

1.5 Terms and Definitions

Technical terms in this ST are defined as follows. Terms used herein, which are the same as in the CC, must follow those in the CC.

Private Key

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

Object

Passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

Approved mode of operation

Operation mode of a cryptographic module using an approved cryptographic algorithm

Approved cryptographic algorithm

A cryptographic algorithm selected by an institution that validates cryptographic modules taking into account the security, credibility, interoperability and so forth with regard to block cipher, hash function, message authentication code, random bit generator, key settings, public key encryption, and digital signature cryptographic algorithms

Validated Cryptographic Module

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

Public Security Parameters (PSP)

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

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with a unique entity (the subject using the public key). It can be disclosed

Public Key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private key

Attack potential

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

Management access

Access attempts made by an administrator using HTTPS, SSH, TLS, etc. for the purpose of the management of the TOE

Management Console

Application program that provides an administrator with graphic user interface (GUI) or command line interface (CLI) for system management, configuration and so forth

Recommend/be recommended

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

Random bit generator (RBG)

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

Symmetric cryptographic technique

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

Iteration

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

Security Target (ST)

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

Security Policy Document

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

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Decryption

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

Secret Key

A cryptographic key which is used in a symmetric cryptographic algorithm and is uniquely associated with one or several entities, not to be disclosed.

User

Refer to "External entity." User in the TOE means administrator and end user.

Selection

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

Identity

Representation uniquely identifying an authorized user. The representation can be the full or abbreviated name or a pseudonym.

Encryption

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

Korea Cryptographic Module Validation Program (KCMVP)

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

Business System

Application server that an authorized end user intends to access through Single-Sign On

Element

Indivisible statement of a security need

Role

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

Operation (on a component of the CC)

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

Operation (on an object)

Specific type of action performed by a subject on an object

External entity

Entity (human or IT) interacting or possibly interacting with the TOE from outside of the TOE boundary

Threat client

Unauthorized external entity that adversely act on assets such as illegal access, modification or deletion

Authorized administrator

Authorized user to securely operate and manage the TOE

Administrator

User granted all privileges of the TOE

Authorized user

TOE user who may, in accordance with the Security Functional Requirements (SFRF), perform an operation

End user

TOE user who wants to use the business system, not the administrator of the TOE

Authentication data

Information used to verify a user's claimed identity

Authentication code

One-time code used to issue an authentication token for an end user

Authentication token

Authentication data used for access by an authorized end user to a business system

Self-test

Pre-operational or conditional test executed by the cryptographic module

Assets

Entities that the owner of the TOE presumably places value upon

Refinement

Addition of details to a component

Dependency

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

Subject

Active entity in the TOE that performs operations on objects

Sensitive Security Parameters (SSP)

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

Augmentation

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

Client

Application program that can access SSO server or a client's service through a network

Target of Evaluation (TOE)

Set of software or hardware possibly accompanied by guidance

Evaluation Assurance Level (EAL)

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

Can/could

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

Assignment

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

Shall/must

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

Critical Security Parameters (CSP)

Security-related information whose disclosure or modification can compromise the security of a cryptographic module (e.g., secret key/private key, password or authentication data such as PINs)

Application Programming Interface (API)

A set of system libraries that exist between the application layer and the platform system and enables the easy development of the application running on the platform

Database Management System (DBMS)

Software system that was built to configure and apply the database

Secure Sockets Layer (SSL)

Security protocol proposed by Netscape in order to provide the security including confidentiality and integrity in a computer network

Transport Layer Security (TLS)

Cryptographic protocol between a SSL-based server and a client, which is described in RFC 2246

TOE Security Functionality (TSF)

Combined functionality of all hardware, software and firmware of a TOE that must be relied upon for the correct enforcement of the Security Functional Requirements (SFR)

TSF data

Data generated by the TOE and for the TOE, which can affect the operation of the TOE

Wrapper

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

SSO-PP

(CC V3.1 R5) Korean National Protection Profile for Single Sign-On V1.1(KECS-PP-0822a-2017, December 11, 2019) (hereinafter referred to as "SSO-PP")

1.6 Conventions

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

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

Iteration

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

Assignment

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

Selection

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

Refinement

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

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

2 Conformance Claims

This chapter describes how this ST conforms with the CC, the PP and the package.

2.1 CC Conformance Claim

This ST conforms with the CC as follows:

Classification		Conformance
Common Criteria		Common Criteria for Information Technology Security Evaluation (Notification No. 2013-51 of the Ministry of Science, ICT and Future Planning) V3.1 R5 ■ Common Criteria Part 1: Introduction and General Model V3.1 r5 (CCMB-2017-04-001, 2017. 4) ■ Common Criteria Part 2: Security Functional Components V3.1 r5 (CCMB-2017-04-002, 2017. 4) ■ Common Criteria Part 3: Security Assurance Components V3.1 r5 (CCMB-2017-04-003, 2017. 4)
Conformance Claim	Part 2 Security Functional Requirements	Extended: FCS_RBG.1, FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security Assurance Requirements	Conformant
	Package	Augmented: EAL 1 augmented (ATE_FUN.1)

2.2 PP Conformance Claim

This ST strictly conforms to the "National Protection Profile for Single Sign-On V1.1"

- PP Title and Version: National Protection Profile for Single Sign-On V1.1
- Certification Number: KECS-PP-0822a-2017
- Publication Date: Dec. 11, 2019
- Evaluation Assurance Level: EAL1+
- Conformance Type: Strict PP conformance

2.3 Package Conformance Claim

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

- Assurance Package: EAL1 augmented (ATE_FUN.1)

2.4 Conformance Claim Rationale

Since this ST adopts the TOE type, security objectives and security requirements in the same way as the Protection Profile, it is demonstrated that this ST strictly conforms to the "National Protection Profile for Single Sign-On V1.1."

2.5 PP Conformance Statement

Since this ST adopts the TOE type, security objectives and security requirements in the same way as the Protection Profile, it is demonstrated that this ST strictly conforms to the "National Protection Profile for Single Sign-On V1.1.".

Classification	PP	ST	Rationale
TOE Type	Single Sign-On	Single Sign-On	Same as the PP
Operational Environment	OE.PHYSICAL_CONTROL	OE.PHYSICAL_CONTROL	Same as the PP
	OE.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	Same as the PP
	OE.LOG_BACKUP	OE.LOG_BACKUP	Same as the PP
	OE.OPERATION_SYSTEM _REINFORCEMENT	OE.OPERATION_SYSTEM _REINFORCEMENT	Same as the PP
	OE.SECURE_DEVELOPMENT	OE.SECURE_DEVELOPMENT	Same as the PP
	-	OE.SECURE_DBMS	As the DBMS that stores TSF data and audit data is operated in a physically secure environment, the security objective is additionally defined.
		OE.TIME_STAMP	As an audit event is accurately recorded with reliable time stamps provided in the operational environment, the security objective is additionally defined.
	-	OE.SECURE_CHANNEL	As all the information transmitted while a user

			attempts to access the TOE is securely protected, the security objective is additionally defined.
	OE. AUTHENTICATION _SYSTEM_SECURITY	-	Not supported by an external authentication system.
Security Functional Requirements	FAU_ARP.1	FAU_ARP.1	Same as the PP
	FAU_GEN.1	FAU_GEN.1	Same as the PP
	FAU_SAA.1	FAU_SAA.1	Same as the PP
	FAU_SAR.1	FAU_SAR.1	Same as the PP
	FAU_SAR.3	FAU_SAR.3	Same as the PP
	FAU_STG.3	FAU_STG.3	Same as the PP
	FAU_STG.4	FAU_STG.4	Same as the PP
	FCS_CKM.1	FCS_CKM.1	Same as the PP
	FCS_CKM.2	FCS_CKM.2	Same as the PP
	FCS_CKM.4	FCS_CKM.4	Same as the PP
	FCS_COP.1	FCS_COP.1(1)	Same as the PP
		FCS_COP.1(2)	Same as the PP
		FCS_COP.1(3)	Same as the PP
		FCS_COP.1(4)	Same as the PP
		FCS_COP.1(5)	Same as the PP
	FCS_RBG.1	FCS_RBG.1	Same as the PP
	FIA_AFL.1	FIA_AFL.1	Same as the PP
	FIA_IML.1	FIA_IML.1	Same as the PP
	FIA_SOS.1	FIA_SOS.1	Same as the PP
	FIA_SOS.2	FIA_SOS.2	Same as the PP
	FIA_SOS.3	FIA_SOS.3	Same as the PP
	FIA_UAU.2	FIA_UAU.2	Same as the PP
	FIA_UAU.4	FIA_UAU.4	Same as the PP
	FIA_UAU.7	FIA_UAU.7	Same as the PP

	FIA_UID.1	FIA_UID.1	Same as the PP
	FMT_MOF.1	FMT_MOF.1	Same as the PP
	FMT_MTD.1	FMT_MTD.1	Same as the PP
	FMT_PWD.1	FMT_PWD.1.1	Same as the PP
		FMT_PWD.1.2	Same as the PP
		FMT_PWD.1.3	Same as the PP
	FMT_SMF.1	FMT_SMF.1	Same as the PP
	FMF_SMR.1	FMF_SMR.1	Same as the PP
	FPT_ITT.1	FPT_ITT.1	Same as the PP
	FPT_PST.1	FPT_PST.1	Same as the PP
	FPT_TST.1	FPT_TST.1	Same as the PP
	FTA_MCS.2	FTA_MCS.2	Same as the PP
	FTA_SSL.5	FTA_SSL.5	Same as the PP
	FTA_TSE.1	FTA_TSE.1	Same as the PP
Assurance Requirements	ADV_FSP.1	ADV_FSP.1	Same as the PP
	AGD_OPE	AGD_OPE	Same as the PP
	ADG_PRE	ADG_PRE	Same as the PP
	ALC_CMC	ALC_CMC	Same as the PP
	ALC_CMS	ALC_CMS	Same as the PP
	ASE_CCL	ASE_CCL	Same as the PP
	ASE_ECD	ASE_ECD	Same as the PP
	ASE_INT	ASE_INT	Same as the PP
	ASE_OBJ	ASE_OBJ	Same as the PP
	ASE_REQ	ASE_REQ	Same as the PP
	ASE_TSS	ASE_TSS	Same as the PP
	ATE_FUN	ATE_FUN	Same as the PP
	ATE_IND	ATE_IND	Same as the PP
	AVA_VAN	AVA_VAN	Same as the PP

3 Security Objectives

This ST defines the security objectives for the operational environment only. The security objectives for the operational environment are those handled by IT area or non-technical/procedural methods.

3.1 Security Objectives for the Operational Environment

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

OE.PHYSICAL_CONTROL

The place where the SSO Agent and the SSO Server, among the TOE components, are installed and operated shall be equipped with access control and protection facilities so that it is accessible only by an authorized administrator.

OE.TRUSTED_ADMIN

The authorized administrator of the TOE shall not have malicious intentions, have been properly trained for the TOE management functions and shall accurately fulfill the duties in accordance with the administrator guidance.

OE.LOG_BACKUP

The authorized administrator shall check the spare space in the audit data repository on a periodic basis in preparation for audit record loss, and carry out audit data backup (external log server, separate storage device, etc.) to prevent audit data loss.

OE.OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator of the TOE shall ensure the reliability and the security of the operating system by taking reinforcement measures for the operation system on which the TOE is installed and operated to address the latest vulnerabilities.

OE.SECURE_DEVELOPMENT

A 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 specified in the guidance document provided along with the TOE.

OE. SECURE_DBMS

Security policies and audit records stored in the TOE are stored in the database. The database shall not be generated, modified or deleted without a request from the TOE.

OE.TIME_STAMP

The TOE shall accurately record security-relevant events by using reliable time stamps provided by the TOE operational environment.

OE.SECURE_CHANNEL

A secure path shall be ensured during the communication between a user and a web server that is an operational environment of the SSO Server.

4 Extended Components Definition

This ST defines the following components, in addition to the components in CC Part 2. [Table 4-1] below summarizes the extended SFR components.

Security Functional Class	Security Functional Component	
Cryptographic Support	FCS_RBG.1(Extended)	Random Bit Generation
Identification and Authentication	FIA_IMA.1(Extended)	TOE Internal Mutual Authentication
	FIA_SOS.3(Extended)	Destruction of Secrets
Security Management	FMT_PWD.1(Extended)	Management of ID and Password
Protection of the TSF	FPT_PST.1(Extended)	Basic Protection of Stored TSF Data
TOE Access	FTA_SSL.5(Extended)	Management of TSF-initiated Sessions

[Table 4-1] Extended security functional requirements

4.1 Cryptographic Support (FCS)

4.1.1 Random bit generation

Family Behaviour

This family (FCS_RBG, Random Bit Generation) family defines requirements for the capability that generates random numbers required for TOE cryptographic operation.

Component Levelling

FCS_RBG Random bit generation	1

FCS_RBG.1 Random bit generation requires the TSF to provide the capability that generates random numbers 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.

FCS_RBG.1	**Random bit generation**
	Hierarchical to: No other components.
	Dependencies: No dependencies.
FCS_RBG.1.1	The TSF shall generate random numbers by using the specified random bit generator that meets the following [assignment: *list of standards*].

4.2 Identification & Authentication (FIA)

4.2.1 TOE internal mutual authentication

Family Behaviour

This family (FIA_IMA, TOE internal mutual authentication) defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.

Component Levelling

FIA_IMA TOE internal mutual authentication	1

FIA_IMA.1 TOE Internal Mutual Authentication requires that mutual authentication between TOE components is provided in the process of user identification and authentication.

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

a) Minimal: Success and failure of mutual authentication

FIA_IMA.1	**TOE internal mutual authentication**
	Hierarchical to: No other components.
	Dependencies: No dependencies.

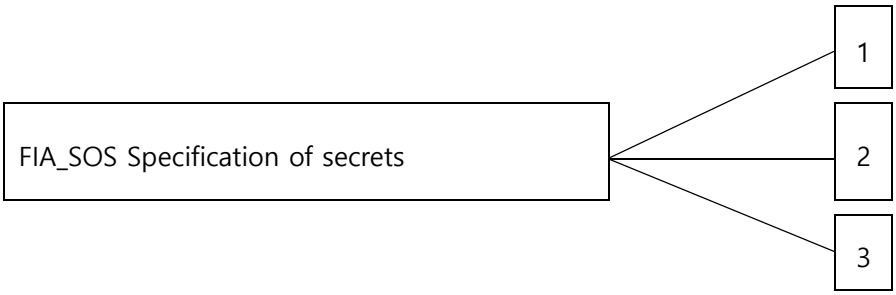
FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of the TOE*] by [assignment: *authentication protocol*] that meets the following: [assignment: *list of standards*].

4.2.2 Specification of secrets

Family Behaviour

This family (FIA_SOS, Specification of Secrets) defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

Component Levelling



In CC Part 2, the family of specification of secrets consists of two components. In this PP, it consists of three components by extending one additional component as follows.

※ Description of two components included in CC Part 2 is left out of this ST.

FIA_SOS.3 Destruction of secrets requires that secrets are destroyed in accordance with the specified destruction method. The specified destruction method may be based on the assigned standards.

Management: FIA_SOS.3

There are no management activities foreseen.

Audit: FIA_SOS.3

It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of an action

FIA_SOS.3 **Destruction of secrets**

Hierarchical to: No other components.

Dependencies: FIA_SOS.2 Generation of secrets

FIA_SOS.3.1 The TSF shall destroy secrets in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

4.3 Security Management (FMT)

4.3.1 ID and password

Family Behaviour

This family (FMT_PWD, ID and password) defines requirements for functions to control the management of ID and password that an authorized user uses in the TOE and to set or modify ID and/or password.

Component Levelling

FMT_PWD ID and password	1

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

Management: FMT_PWD.1

The following management functions could be considered in FMT.

a) Management of ID and password configuration rules

Audit: FMT_PWD.1

It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password

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 roles*] as follows:

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 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 function for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing ID and password when the administrator accesses for the first time, changing the password when the administrator accesses for the first time*].

4.4 Protection of the TSF (FPT)

4.4.1 Protection of stored TSF data

Family Behaviour

This family (FPT_PST, Protection of stored TSF data) defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component Levelling

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.

FPT_PST.1 Basic protection of stored TSF data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

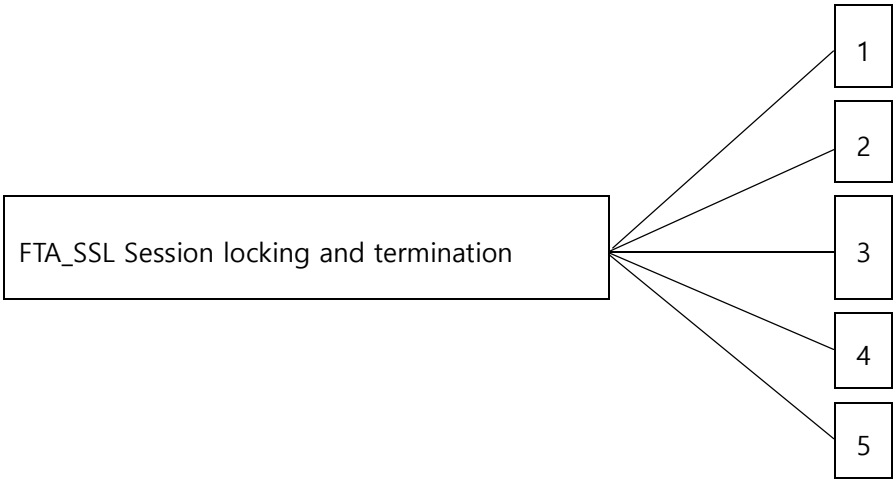
4.5 TOE Access (FTA)

4.5.1 Session locking and termination

Family Behaviour

This family (FTA_SSL, Session Locking and termination) defines requirement for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking and termination of sessions.

Component Levelling



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

※ Description of four components included in CC Part 2 is left out of this ST.

FTA_SSL.5 Management of TSF-initiated sessions provides requirements that the TSF locks or terminates the session after a specified time period of user inactivity.

Management: FTA_SSL.5

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

a) Specification of the time period of user inactivity that results in session locking or termination for each user

b) Specification of the default user inactivity period that results in session locking or termination

Audit: FTA_SSL.5

It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive sessions

FTA_SSL.5	**Management of TSF-initiated sessions**
	Hierarchical to: No other components.
	Dependencies: FIA_UAU.1 Authentication or no dependencies
FTA_SSL.5.1	TSF shall [selection:
	• *lock the session and/or re-authenticate the user before unlocking the session,*
	• *terminate]* an interactive session after a [assignment: *time period of user inactivity*].

5 Security Requirements

This chapter describes the security functional requirements and assurance requirements that must be satisfied by the TOE.

5.1 Security Functional Requirements

The security requirements included in this ST are derived from functional components in CC (V3.1) Part 2. The security functional components are summarized as follows:

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (symmetric key)
	FCS_COP.1(2)	Cryptographic operation (digital signature)
	FCS_COP.1(3)	Cryptographic operation (MAC)
	FCS_COP.1(4)	Cryptographic operation (public key)
	FCS_COP.1(5)	Cryptographic operation (hash)
	FCS_RBG.1(Extended)	Random bit generation
Identification and Authentication (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	User authentication before any action

	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (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
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF self tests
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

[Table 5-1] Security functional requirements

5.1.1 Security audit (FAU)

FAU_ARP.1 **Security alarms**

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [actions against security violations in [Table 5-2]] upon detection of a potential security violation.

[

Security Violation	Action
Accumulation of authentication failures specified in FIA_UAU.2	· Limit login attempts by an end user and the administrator for a specified period of time (default: 5 minutes) by locking the account · Send a warning email to the administrator
Integrity violation event and failure of self tests of cryptographic module specified in FPT_TST.1	· Send a warning email to the administrator

Event in which the audit trail is full specified in FAU_STG.3 and FAU_STG.4	· Send a warning email to the administrator · Overwrite the oldest records if the audit trail exceeds a pre-defined limit (default: 90%)

[Table 5-2] Security functional requirement

]

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [Refer to the "auditable events" in [Table 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 [Refer to "Additional Audit Record" in [Table 5-3], *none*].

Security Functional Component	Auditable Event	Additional Audit Record
FAU_ARP.1	Actions taken due to potential security violations	-
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	-
FAU_STG.3	Actions taken due to exceeding of a threshold	-
FAU_STG.4	Actions taken due to the audit storage failure	-
FCS_CKM.1	Success and failure of the activity	-
FCS_CKM.2	Success and failure of the activity (applied only to key distribution related to TSF data encryption/decryption)	-
FCS_CKM.4	Success and failure of the activity	-

	(applied only to key destruction related to TSF data encryption/decryption)	
FCS_COP.1	Success and failure of cryptographic operation, and the type of cryptographic operation (applied only to items related to issuance, storage, verification and deletion of authentication token)	-
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	-
FIA_SOS.2	Rejection by the TSF of any tested secret	-
FIA_SOS.3(Extended)	Success and failure of the activity (applied only to destruction of SSO authentication token)	-
FIA_UAU.1	All use of the authentication mechanism	-
FIA_UAU.4	Single-use authentication mechanisms	-
FIA_UID.1	All use of the administrator identification mechanism, including the administrator identity provided	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1(Extended)	All changes of the password	-
FMT_SMF.1	Use of the management functions	-
FMT_SMR.1	Modifications to the group of users that are part of a role	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or executable code in case of integrity violation
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions	-
FTA_SSL.5(Extended)	Locking or termination of interactive session	-
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	-

[Table 5-3] Auditable events

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 [An auditable event of authentication failure in FIA_UAU.2, Auditable events of integrity violation event of the SSO Server and self test failure of the validated cryptographic module in the SSO Server and the SSO Agent in FPT_TST.1, Audit trail exceeding the limit of disk capacity among auditable events specified in FAU_STG.3, Full audit trail specified in FAU_STG.4] known to indicate a potential security violation;

b) [None]

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [[Table 5-4] Methods of selection and ordering] of audit data based on [criteria with the following logical relations].

Type	Method of Selection per Type	Allowable Ability
Audit view	■ Event type; or ■ Server IP; or	Search, (event type, server IP, access IP, time of occurrence, success or failure) sort

	■ Access IP; or ■ Time of occurrence; or ■ Success or failure	

[Table 5-4] Methods of selection and ordering

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 [notice to the authorized administrator, [none]] if the audit trail exceeds [the percentage of the spare space out of the total capacity of the audit record storage (default value: 80%, the range of values configurable by the administrator: 60% - 80%)].

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 [none] if the audit trail is full.

5.1.2 Cryptographic support (FCS)

FCS_CKM.1 **Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1(1) Cryptographic operation (authentication token generation and verification)]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ["cryptographic key generation algorithm" in [Table 5-5] Cryptographic key generation] and specified cryptographic key sizes in ["cryptographic key sizes" in [Table 5-5] Cryptographic key generation] that meet the following ["list of standards" in [Table 5-5] Cryptographic key generation].

List of Standards	Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Usage
FIPS 198	HMAC(SHA-256)	256 bits	- Key encryption key (KEK)
ISO/IEC 18031	HASH_DRGB(SHA256)	256 bits	- Key decryption key (DEK)
ISO/IEC 18031	HASH_DRGB(SHA256)	256 bits	- Encryption/decryption of authentication token
ISO/IEC 18031	HASH_DRGB(SHA256)	256 bits	- Encryption/decryption of transmitted data
ISO/IEC 18031	HASH_DRGB(SHA256)	Public key 2048 bits	- Generation of server key for encryption/decryption
ISO/IEC 18031	HASH_DRGB(SHA256)	Public key 2048 bits	- Server key for signature

[Table 5-5] Cryptographic key generation

FCS_CKM.2 **Cryptographic key distribution**

Hierarchical to: No other components

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

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [refer to "distribution method" in [Table 5-6] Cryptographic key distribution] that meets the following [refer to "list of standards" in [Table 5-6] Cryptographic key distribution].

List of standards	Cryptographic Algorithm	Cryptographic Key Sizes	Usage
Offline release	RSAES(SHA-256)	Public key 2048 bits	- Public key encryption

[Table 5-6] Cryptographic key distribution

FCS_CKM.4 **Cryptographic key destruction**

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [refer to "destruction method" in [Table 5-7] Cryptographic key destruction] that meets the following [refer to "list of standards" in [Table 5-7] Cryptographic key destruction].

List of Standards	Method	Cryptographic Key Sizes	Usage
-	- Destruction of cryptographic key loaded on the memory if the execution of the TOE is terminated - Substitution of key values loaded on the memory with 0	-	- Destruction of key encryption key (KEK)
			- Destruction of key decryption key (DEK)
			- Destruction of encryption/decryption key of transmitted data
			- Destruction of encryption/decryption key of authentication token

[Table 5-7] Cryptographic key destruction

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 ["usage" in [Table 5-8] Symmetric key] in accordance with a specified cryptographic algorithm ["cryptographic algorithm" in [Table 5-8] Symmetric key] and cryptographic key sizes ["cryptographic key sizes" in [Table 5-8] Symmetric key] that meet the following ["list of standards" in [Table 5-8] Symmetric key].

List of Standards	Cryptographic Algorithm	Cryptographic Key Sizes	Usage
KS X 1213	- ARIA/CBC	256 bits	- DEK encryption/decryption
			- Encryption/decryption of transmitted data
			- Encryption/decryption of

			authentication token

[Table 5-8] Symmetric key

FCS_COP.1(2) **Cryptographic operation (digital signature)**

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 [refer to "usage" in [Table 5-9] Digital signature] in accordance with a specified cryptographic algorithm [refer to "cryptographic algorithm" in [Table 5-9] Digital signature] and cryptographic key sizes [refer to "cryptographic key sizes" in [Table 5-9] Digital signature] that meet the following [refer to "list of standards" in [Table 5-9] Digital signature].

List of Standards	Cryptographic Algorithm	Cryptographic Key Sizes	Usage
PKCS #1 v2.1	- RSA-PSS(SHA-256)	Public key 2048 bits	- Generation and verification of digital signature for data transmitted between the SSO Server and the SSO Agent

[Table 5-9] Digital signature

FCS_COP.1(3) **Cryptographic operation (MAC)**

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 [refer to "usage" in [Table 5-10] MAC] in accordance with a specified cryptographic algorithm [refer to "cryptographic algorithm" in [Table 5-10] MAC] and cryptographic key sizes [refer to "cryptographic key sizes" in [Table 5-10] MAC] that meet the following [refer to "list of standards" in [Table 5-10] MAC].

List of Standards	Cryptographic Algorithm	Cryptographic Key Sizes	Usage
FIPS 198	- HMAC (SHA-512)	256 bits	- KEK generation - Integrity verification of data transmitted between the SSO Server and the SSO Agent

[Table 5-10] MAC

FCS_COP.1(4) **Cryptographic operation (public 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 [refer to "usage" in [Table 5-11] Public key] in accordance with a specified cryptographic algorithm [refer to "cryptographic algorithm" in [Table 5-11] Public key] and cryptographic key sizes [refer to "cryptographic key sizes" in [Table 5-11] Public key] that meet the following [refer to "list of standards" in [Table 5-11] Public key].

List of Standards	Cryptographic Algorithm	Cryptographic Key Sizes	Usage
PKCS #1 v2.1	- RSAES(SHA-256)	Public key 2048 bits	- Encryption of transmitted data - Encryption of symmetric key

[Table 5-11] Public key

FCS_COP.1(5) **Cryptographic operation (hash)**

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_COP.1.1 The TSF shall perform [refer to "usage" in [Table 5-12] Hash function] in accordance with a specified cryptographic algorithm [refer to "cryptographic algorithm" in [Table 5-12] Hash function] and cryptographic key sizes [refer to "cryptographic key sizes" in [Table 5-12] Hash function] that meet the following [refer to "list of standards" in [Table 5-12] Hash function].

List of Standards	Cryptographic Algorithm	Cryptographic Key Sizes	Usage
FIPS 180-2	- SHA-512	-	- Integrity verification of important data - Encryption of administrator and user password

[Table 5-12] Hash function

FCS_RBG.1 **Random bit generation (Extended)**

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG.1.1 The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following ["list of standards" in [Table 5-13] Random bit generation].

List of Standards	Random Bit Generation Algorithm
ISO/IEC 18031	HASH-DRBG(SHA-256)

[Table 5-13] List of standards for random bit generation

5.1.3 Identification and authentication (FIA)

FIA_AFL.1 **Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [5]* unsuccessful authentication attempts occur related to [administrator, end user authentication attempt].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [inactivate the identification and authentication function for a period of time defined by the administrator (default value: 5 minutes) in order to prevent further login attempts by the user].

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 through [digital signature using the validated module and authentication protocol implemented by Bandi S&C Co., Ltd.] that meet [none] between [[Table 5-14] TOE components].

TOE Component	Authentication Protocol
SSO Server ↔ SSO Agent	digital signature using the validated module and authentication protocol implemented by Bandi S&C Co., Ltd.

[Table 5-14] Mutual authentication component

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 [a defined quality metric in [Table 5-15]].

Classification		Metric
Password	English letters	- Alphabet upper- and lower-case letters
	Numbers	- 0 - 9
	Special characters	- `~!@#$%^&*()-_=+[]{};:'"|,.<>/?
	Combination rule	- A password must include at least one alphabet upper-case letter, lower-case letter, number and special character, respectively. - Length: 9 – 30 digits
	Password restrictions	- The same character cannot be repeated (three letters in a row) - A password that has recently been used cannot be reused (the most recent three passwords)

[Table 5-15] End user/administrator password policy

FIA_SOS.2 **Generation of secrets**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate **authentication tokens** that meet [refer to "a defined quality metric" in [Table 5-16] Generation of secrets].

Defined Quality Metric	Description
Authentication token implementation method	Consists of header, payload and signature areas by using the JWT (json web token) specification
Authentication token component	Header area - typ: token type (default value: jwt) - alg: signature algorithm (default value: RSA-PSS SHA256) - kid: unique ID of signature key Payload area - bds:sid: session ID between the SSO Server and a user browser - exp: token expiration time - jti: token's unique ID - enc_d_a: encrypted important data - bds:chkhs: generation of hash values generated to verify the token validity (SHA-512) - client_id: ID value of the SSO Agent that requested the token - bds:encrd : random key value combined with a symmetric key when encrypting enc_d_a Signature area - Values signed with RSA-PSS SHA256 algorithm for content in the Header area and the Payload area
Confidentiality and integrity algorithm of authentication token	Confidentiality algorithm - Encryption of important data (enc_d_a) by using a cryptographic key (encrd) in the payload Integrity algorithm - Check the signature value for the Header and the Payload areas

[Table 5-16] Generation of secrets

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated **authentication tokens** for [the following TSF functions].

[

- FIA_UAU.2 User authentication before any action
- FIA_UID.1 User identification before any action

]

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 ["destruction method" in [Table 5-17] Password destruction] that meets the following [none].

Classification	Destruction Method	Timing of Destruction
Authentication token information (SSO Agent)	- When an end user logs out, the authentication token processes the destruction of the token on the SSO Server	- Destroyed when an end user logs out
Authentication token information (SSO Server)	- The authentication token becomes expired when an end user logs out - When an end user logs in, out-of-date tokens are processed to be destroyed	- Destroyed when an end user logs out - Destroyed when an authentication token of an end user expires

[Table 5-17] Password destruction

FIA_UAU.2 **User authentication before any action**

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.4 **Single-use authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [method to prevent reuse in [Table 5-18] Single-use authentication mechanisms].

Classification	Method to Prevent Reuse
Administrator authentication	- Authenticate based on password and check the number of failures - Generate a unique session ID and random bit values immediately after authentication - Store the session ID that contains authentication information on the memory
End user authentication	- Authenticate based on password and based on authentication token

[Table 5-18] Single-use authentication mechanisms

FIA_UAU.7 **Protected authentication feedback**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

[

- Passwords being entered are masked (password masked with *) to prevent them from being disclosed on the screen
- In case of failure of identification and authentication, feedback on the reason for the failure is not provided

]

FIA_UID.2 **Identification before any 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 the user.

5.1.4 Security management (FMT)

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 in [[Table 5-19] List of functions] to [the authorized administrator].

List of Functions	Criteria			
	Determine the behaviour	Determine the behaviour	Determine the behaviour	Determine the behaviour
Administrator account setting	-	○	○	-
User account setting	-	○	○	-
Basic information settings for the Agent	-	○	○	-
Server key management	-	○	○	-
Administrator policy	-	-	-	○
User policy	-	-	-	○
Password policy	-	-	-	○
Audit log policy	-	-	-	○
SSO policy	○	○	○	○
Token destruction	-	-	○	-
Integrity viewing	-	-	○	-

[Table 5-19] List of security functions behaviour

FMT_MTD.1 **Management of TSF data**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** [TSF data in [Table 5-20]] to the [administrator].

TSF Data	Ability

	Change Default	Query	Modify	Delete	Clear
Integrity verification data	-	○	-	-	-
Basic information of the administrators	-	○	○	○	-
Basic information of the users	-	○	○	○	-
Basic information of the Agent	-	○	○	○	-
Audit data	-	○	-	-	-
Login data	-	○	-	-	-
History of authorization code issuance	-	○	-	-	○
Token information	-	○	-	-	○
Token issuance history	-	○	-	-	○
Administrator policy	○	○	○	-	-
User policy	○	○	○	-	-
Password policy	○	○	○	-	-
Login policy	○	○	○	-	-
Audit log policy	-	○	○	-	-
SSO policy	○	○	○	-	-
Mail policy	○	○	○	-	-
Server key configuration information	-	○	○	○	-
Password change history	-	○	-	-	-

[Table 5-20] List of TSF data

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 [user identification and authentication functions] to [the authorized administrator]

1. [

a) At least 9 up to 30 digits (default: 9)

b) At least 9 digits that consist of a combination of four: special characters permitted by the administrator for input, upper-case alphabet characters, lower-case alphabet characters and numbers

]

2. [

a) The number of recent passwords not allowed for reuse set by the administrator

b) The number of repeated letters set by the administrator

]

FMT_PWD.1.2 The TSF shall restrict the ability to manage ID of [user identification and authentication function] to [the authorized administrator]

1. [

a) The number of alphabet characters to be included at the beginning of ID

b) A combination of at least one among upper- and lower-case alphabet characters and numbers

]

2. [Exclusion of all special characters]

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

Classification		Metric
ID	Valid characters	- Upper- and lower-case alphabet characters, numbers
	Combination rule	- Combination of at least one type of character - The number of alphabets to be included at the beginning of ID
	Valid length	- At least 5 up to 30 digits
	Change interval	- None
Password	Valid characters	- English alphabets, numbers, special characters
	Combination rule	- Combination of at least three types of characters
	Valid length	- At least 9 up to 30 digits (default: nine)
	Change interval	- A period of time defined by the administrator (default: 180)
	Reuse rule	- Not allowed to reuse the most recent three passwords
	Restriction of repeated characters	- Not allowed to use the same letter three times consecutively

	Initial access	- Guide the administrator to change the password upon the initial access - Guide users to change passwords by sending randomly issued passwords to users via email upon the user registration

[Table 5-21] User identification and authentication policy

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

[

a) Management functions of the TSF: Management functions specified in FMT_MOF.1

b) Management of TSF data: Management functions specified in FMT_MTD.1

c) Management of ID and password: Management functions specified in FMT_PWD.1

]

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 [[Table 5-22] User classification].

User Classification	Level	Security Policy	Audit Data	Remarks
Administrator	General administrator	Change default value, query, modify, delete, clear	Query	

[Table 5-22] Security roles

FMT_SMR.1.2 The TSF shall be able to associate users with **roles defined in FMT_SMR.1.1**.

5.1.5 Protection of the TSF (FPT)

FPT_ITT.1 **Basic internal TSF data transfer protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

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

[

- User account password (administrator, end user)
- DB access account information
- Cryptographic key (private key of the server)
- Critical security parameters (Secret of the SSO Agent)
- TOE set value (access information of an external entity)

]

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of *[SSO Server cryptographic module, process and SSO Agent cryptographic module in [Table 5-23]]*.

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

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

Classification	Item	Content (Role)
SSO	Cryptographic module	Self tests

Server	Process	-
SSO Agent	Cryptographic module	Self tests

[Table 5-23] Subjects of TSF self tests

5.1.6 TOE access (FTA)

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

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [restriction of the number of concurrent sessions of the management access by the administrator to one, restriction of the number of concurrent sessions of access by an end user to one, the rules on the maximum number of concurrent sessions {none}].

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

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication or no dependencies.

FTA_SSL.5.1 The TSF shall *terminate* an interactive session after

[Administrator and end-user inactivity time

a) Administrator : fixed value (10 minutes)

b) End-user : Inactivity time value set by the administrator (10 ~ 1440 minutes, default : 10 minutes)

].

FTA_TSE.1 **TOE session establishment**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **the administrator's management access session** establishment based on [administrator access IP, *whether or not to activate the management access session of the same account*].

Application notes: The default value of the number of accessible IPs provided by the TOE is set as two.

5.2 Security Assurance Requirements

Assurance requirements of this ST are composed of assurance components in CC Part 3, and the evaluation assurance level is EAL1+. [Table 5-24] below summarizes assurance components.

Assurance Class	Assurance Component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance document	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 configuration management coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

[Table 5-24] Assurance requirements

5.2.1 Security Target evaluation

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.

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.

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.

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.

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.

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

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 categorisation 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

AGD_OPE.1	**Operational user guidance**
	Dependencies: ADV_FSP.1 Basic functional specification
	Developer action elements
AGD_OPE.1.1D	The developer shall provide operational user guidance.
	Content and presentation elements
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.

Evaluator action elements

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

AGD_PRE.1 **Preparative procedure**

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.

Life-cycle support

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 meets all requirements for content and presentation of evidence.

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 followings: 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.

5.2.4 Tests

ATE_FUN.1 Evaluator action elements

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.

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.

5.2.5 Vulnerability assessment

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 preparation 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 processing Basic attack potential.

5.3 Security Requirements Rationale

5.3.1 Dependency of SFRs

The following table summarizes dependencies of the SFRs.

No	SFR	Dependencies	Reference No
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	Rationale (2)
7	FAU_STG.4	FAU_STG.1	Rationale (2)
8	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	9, 11
		FCS_CKM.4	10
9	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	10
10	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
11	FCS_COP.1 (1)-(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
		FCS_CKM.4	10
12	FCS_COP.1(5)	-	Rationale (5)
13	FCS_RBG.1(Extended)	-	-
14	FIA_AFL.1	FIA_UAU.1	Rationale (4)
15	FIA_IMA.1(Extended)	-	-
16	FIA_SOS.1	-	-
17	FIA_SOS.2	-	-
18	FIA_SOS.3(Extended)	FIA_SOS.2	17
19	FIA_UAU.2	FIA_UID.1	Rationale (3)
20	FIA_UAU.4	-	-
21	FIA_UAU.7	FIA_UAU.1	Rationale (4)
22	FIA_UID.2	-	Rationale (3)
23	FMT_MOF.1	FMT_SMF.1	26
		FMT_SMR.1	27

24	FMT_MTD.1	FMT_SMF.1	26
		FMT_SMR.1	27
25	FMT_PWD.1(Extended)	FMT_SMF.1	26
		FMT_SMR.1	27
26	FMT_SMF.1	-	-
27	FMT_SMR.1	FIA_UID.1	Rationale (3)
28	FPT_ITT.1	-	-
29	FPT_PST.1(Extended)	-	-
30	FPT_TST.1	-	-
31	FTA_MCS.2	FIA_UID.1	Rationale (3)
32	FTA_SSL.5(Extended)	FIA_UAU.1 or no dependencies	Rationale (4)
33	FTA_TSE.1	-	-

[Table 5-25] Dependencies of functional components

Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1. However, reliable time stamps provided by the security objective OE.TIME_STAMPS for the operational environment of this ST are used, thereby satisfying the dependency.

Rationale (2): FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1. However, it is protected from unauthorized deletion or modification in accordance with the security objective OE.SECURE_DBMS for the operational environment of this ST, thereby satisfying the dependency.

Rationale (3): FIA_UAU.2, FMT_SMR.1 and FTA_MCS.2 have dependencies on FIA_UID.1, which is satisfied by FIA_UID.2 hierarchical to FIA_UID.1.

Rationale (4): FIA_AFL.1, FIA_UAU.7 and FTA_SSL.5 have dependencies on FIA_UAU.1, which is satisfied by FIA_UAU.2 hierarchical to FIA_UAU.1.

Rationale (5): FSC_COP.1(5) has dependencies on FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, and FCS_CKM.4. However, it is satisfied as hash algorithms do not use cryptographic keys.

5.3.2 Dependency of SARs

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

The augmented SAR ATE_FUN.1 has a dependency on ATE_COV.1. ATE_FUN.1 has been augmented to ensure that the developer performs tests on test items correctly and documents them in the test documentation. ATE_COV.1 is not included in this ST since it is deemed not necessarily required to include ATE_COV.1 that presents the consistency between test items and TSFI.

6 TOE Summary Specification

6.1 Security Audit (FAU)

6.1.1 Audit data generation

The TOE generates audit records on results of security management functions performed and potential security violations, identification and authentication results and an event that occurs in the system, and stores them in the DBMS.

Each audit data generated include the date and time of an event, a type of the event, subject identity (if possible), and the outcome (success or failure) of the event. Selectable audit review can be performed according to an event type.

Audit data generated in the TOE are as follows:

Audit Data	Auditable Event
End user's use details	- User identification and authentication - Authentication token generation - Authentication token verification
Administrator's use details	- Administrator identification and authentication - Management of administrator, end user and agent - TSF data modification - Security settings - Session termination
System use details	- TOE start-up and termination - Self tests and integrity check - Audit storage reaches the threshold and is full

Relevant SFR: FAU_GEN.1

6.1.2 Audit data view

The TOE provides the administrator with the function to review audit data.

Audit data provided include the history of identification and authentication of the administrator and end users, the history of TSF data modification and security setting change, and the history of start-up and shutdown of the TOE, which are stored in the DBMS, an operational environment of the TOE. It is also possible to perform selectable audit review according to a combination of rules.

Potential violation can be indicated by applying a group of rules when viewing audit data.

Subject who performs potential violation analysis	Group of Rules
Administrator	- Event type - Server IP - Access IP - Time of occurrence - Success or not

Relevant SFR: FAU_SAR.1, FAU_SAR.3

6.1.3 Detection of potential security violations and actions taken due to security violation

Potential violation is detected on a periodic basis according to a batch job frequency set by the administrator.

The table below explains potential security violation items and actions taken when a violation is detected.

Actions Taken	Security Violation
Send an email in real time	- Detects that an operation file was compromised - Detects that an operation DB data were compromised - Detects self-test failure - Reaches the number of unsuccessful attempts for administrator login authentication - Reaches a disk capacity threshold (warning) (80%) - Exceeds a disk capacity threshold (full) (90%)
Overwrite the oldest audit records	- Exceeds a disk capacity threshold (full) (90%)

Relevant SFR: FAU_ARP.1, FAU_SAA.1, FAU_STG.3, FAU_STG.4

6.2 Cryptographic support (FCS)

6.2.1 Cryptographic key management and cryptographic operation

The TOE performs the function of cryptographic support by using the validated cryptographic module as follows:

Classification	Item	Value
Validated cryptographic modules	Cryptographic Module Name	MagicJCrypto V2.0.0.0
	Validation No.	CM-131-2022.10
	Developer	Dreamsecurity Co.,Ltd
	Validation Date	Oct. 16, 2017

The TOE component uses a random bit generator (HASH-DRBG (SHA256)) to generate a 256-bit cryptographic key for mutual authentication, and uses a digital signature algorithm (RSASSA-PSS (SHA256)) to perform mutual authentication between TOE components. In this case, a cryptographic key generated on the SSO Server is destroyed immediately after the use by substituting the values loaded on the memory with 0.

The TOE component generates a 256-bit cryptographic key by using a random bit generator (HASH-DRBG (SHA256)) on the SSO Agent. The cryptographic key generated uses a public key algorithm (RSAES (2048)) to encrypt a cryptographic key with a public key released offline, and exchanges cryptographic keys with the SSO Server. Then, the communication is encrypted with the symmetric key algorithm (ARIA/CBC 256bits). Also, the key changes to a new cryptographic key at a certain interval, and the previous key is destroyed immediately by substituting the values loaded on the memory with 0.

When an authentication token is issued on the SSO Server, a random bit generator (HASH-DRBG (SHA256)) is used to generate a 256-bit cryptographic key. Important data (user information) contained in the token is encrypted with a symmetric key algorithm (ARIA/CBC) 256bits).

Later, the integrity of the token is verified by using a digital signature algorithm (RSASSA-PSS(SHA256)) for the encrypted data and token information. The cryptographic key generated is immediately destroyed by substituting the values loaded on the memory with 0.

In the TSF data stored on the SSO Server (administrator and user password, operation file and setting integrity), password data are encrypted by using a function of hash code generation (algorithm: SHA-512).

Relevant SFR: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_RBG.1

6.3 Identification and authentication (FIA)

6.3.1 Authentication failure handling

If the administrator or an end user fails to be authenticated during the login for a defined number of times (5 times by default), the account is locked (5 minutes by default) and a security alarm mail is sent to the email account of the user who failed to be authenticated.

Relevant SFR: FIA_AFL.1

6.3.2 Authentication and verification

Before any action of the administrator and a user, the identification and authentication of the administrator and the end user shall be performed.

The administrator and user authentication information refers to ID and password. A password shall contain each type of characters: upper-case alphabet characters, lower-case alphabet characters, special characters and numbers. It shall not be same as the most recently used passwords (the most recent three passwords by default), nor contain repeating characters (three by default). It is possible to set at least 9 up to 30-digit password in accordance with such combination rules.

The password is masked with "*" during the authentication. In case of an authentication failure, a feedback message on a reason for failure is also protected.

Once the identification and authentication succeed, a session ID changes, and random bit values that will identify the session ID are used to prevent the authentication information from being reused. If an end user is successfully identified and authenticated, an authentication code is issued, which is used to issue an authentication token. Then, the used authentication code is destroyed.

Relevant SFR: FIA_IMA.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7

6.3.3 Management of secrets

When the initial identification and authentication of an end user are completed, an authentication code is issued, through which an authentication token is generated. Then, the used authentication code is destroyed. The authentication token consists of a signature algorithm, signature key ID, session ID, token expiration time, token ID, token's hash value (SHA-512), issuer agent ID, encrypted data (user information, etc.) and so forth, and uses digital signature (RSASSA-PSS (SHA256)) to verify the integrity of the token.

The authentication token is destroyed if the end user using the token remains inactive for a defined period of token validity time, or requests logout using the token.

Relevant SFR: FIA_SOS.2, FIA_SOS.3, FIA_UAU.4

6.3.4 Identification

Before the administrator and an end user is identified, the administrator and the end user shall be registered in the administrator page on the SSO Server. The identification of the end user is confirmed by requesting the user information of the logged-in end user by using a token issued after the login.

Relevant SFR: FIA_UID.1

6.4 Security management (FMT)

6.4.1 Security management

The TOE has the general administrator privilege only, and all the registered administrators perform the security management with the following functions on the administrator page.

- Security management settings: administrator, end user, agent, server key, policy

- History view: audit history, login history, password change history, authentication code issuance history, authentication token issuance history

- Administrator management

The TOE provides the administrator management function to perform the management function, such as managing administrators (view/register/modify/delete), designating access IP for administrator account, unlocking an administrator account and initializing an administrator password.

An administrator account can be registered in accordance with the ID policy established by the administrator [valid length (5 ~ 30 digits) and valid ID characters (upper- and lower-case alphabet characters, numbers), combination rule (a combination of one or more valid characters, the number of alphabet characters to be included at the beginning of ID)].

- End user management

The TOE provides the user management function to perform the management function, such as managing end users (view/register/modify/delete) and initializing end user passwords.

An end user account can be registered in accordance with the ID policy established by the administrator [valid length (5 ~ 30 digits) and valid ID characters (upper- and lower-case alphabet characters, number), combination rule (a combination of one or more valid characters, the number of alphabet characters to be included at the beginning of ID)].

- Agent management

The TOE provides the agent management function to manage the agent (view/register/modify/delete), manage agent URI (register/modify/delete), manage agent access IP (register/modify/delete), check the server status, reissue agent secrets and copy agent secrets.

- Server key

The TOE provides the server key management function to manage server keys used for the encryption between components and signature (view/register/destroy), and modify and copy server keys.

- Policy

The policy management function enables the TOE to perform management functions for audit policy, authentication policy, ID and password policy, alarm policy and operation policy, which are necessary for the operation of the TOE, as described below.

The audit policy allows settings for the thresholds for audit storage warnings/audit trail being full, the maximum capacity of the audit storage, and the retention period in order to protect the audit storage.

The authentication policy manages the number of unsuccessful attempts for the administrator and end user authentication, the time during which an account is locked, and the validity period of an end user's authentication token.

The ID/password policy manages the administrator and end user password policy and ID policy.

The ID policy for the administrator and end users is as follows:

Classification		Metric
ID	Valid character	- Upper- and lower-case alphabet characters, numbers
	Combination rule	- Combination of at least one type of character - The number of alphabets to be included at the beginning of ID
	Valid length	- At least 5 up to 30 digits
	Change interval	- None

The password policy for the administrator and end users is as follows:

Classification		Metric
Password	Valid characters	- English alphabets, numbers, special characters
	Combination rule	- Combination of at least three types of characters
	Valid length	- At least 9 up to 30 digits (default: nine)
	Change interval	- A period of time defined by the administrator (default: 180)
	Reuse rule	- Not allowed to reuse the most recent three passwords

	Restriction of repeated characters	- Not allowed to use the same letter three times consecutively
	Initial access	- Guide the administrator to change the password upon the initial access - Guide users to change passwords by sending randomly issued passwords to users via email upon the user registration

The alarm policy manages email addresses that will receive alarms in case of potential violations (warning for storage threshold/storage being full, self test failure, the maximum number of unsuccessful administrator authentication attempts being reached), and sender email addresses.

Relevant SFR: FMT_MOF.1, MFT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1

6.5 Protection of the TSF (FPT)

6.5.1 Protection of the TSF

The TOE performs the mutual authentication and the encrypted communication for each component in order to protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE as follow:

Protection of the TSF	Algorithm
Mutual authentication	- Public key cryptographic algorithm: RSAES(2048) - Digital signature algorithm: RSASSA-PSS(2048)
Encrypted communication	- Random bit generator: HASH-DRBG(SHA256) - Public key cryptographic algorithm: RSAES(2048) - Symmetric key algorithm: ARIA/CBC) 256 bits

In the property file encryption, DB and mail server connection information, among set values in the property files, is encrypted and managed by using the encryption function of the validated cryptographic module (algorithm: ARIA/CBC 256 bits).

Administrator and end user passwords are stored in the DBMS using a hash algorithm (SHA-512). The TOE components (the SSO Server, the SSO Agent) carry out self tests periodically after the start-up (00:00 on a daily basis).

Test items for self tests are as follows:

- Cryptographic module
  - ■ Self tests of the cryptographic module

- Process
  - ■ Integrity test of executable files and TSF data
  - ■ Token generation and verification test

Classification		Item	Description (Role)
Self Tests	SSO Server	Cryptographic module	Self tests
		Process	Self tests
	SSO Agent	Cryptographic module	Self tests
Integrity Verification	SSO Server	Configuration file	TOE configuration file and database data
		Stored TSF executable code	Execution file

Relevant SFR: FPT_ITT.1, FPT_PST.1, FPT_TST.1

6.6 TOE access (FTA)

6.6.1 Session management

The TOE provides the function to restrict the administrator's management access sessions based on the administrator's access IP, etc. The number of accessible IPs provided by the TOE is set as two.

The maximum number of concurrent sessions for the administrator and end user is enforced to one, and new access is blocked in case of the concurrent access. In the case of the administrator, if there is no interaction for a defined period of inactivity (fixed value of 10 minutes), the session is terminated, and re-authentication is required afterwards. As to an end user, if there is no interaction for a certain period (default value of 10 minutes), or if the maximum validity period of an authentication token expires (default value of one hour), the authentication token is destroyed, and re-authentication is required afterwards.

Relevant SFR: FTA_MCS.2, FTA_SSL.5, FTA_TSE.1