Magic SSO V4.0 Security Target

v1.4

< Revision History >

Version	Date	Content / Author
v1.0	2017-12-04	First Issue / Dreamsecurity Co.,Ltd., Solution-Team3
v1.1	2019-05-31	Update / Dreamsecurity Co.,Ltd., R&D-Part2 R&D-Team1
v1.2	2019-07-29	Update / Dreamsecurity Co.,Ltd., R&D-Part2 R&D-Team1
v1.3	2019-09-25	TOE detailed version change / Dreamsecurity Co.,Ltd., R&D-Part2 R&D-Team1
v1.4	2019-10-30	Update / Dreamsecurity Co.,Ltd., R&D-Part2 R&D-Team1

< Table of Contents >

1 Security Target introduction

1.1 Security Target Reference

Classification	Contents
Title	Magic SSO V4.0 Security Target
Version	v1.4
Developer	Dreamsecurity Co.,Ltd. R&D-Part2 R&D-Team1
Date	2019.10.30
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	V3.1 r5
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keywords	Single Sign On, SSO

1.2 TOE Reference

Classification		Contents
TOE Identification		Magic SSO V4.0
Detailed Version		v4.0.0.2
Component	SSO Server	Magic SSO V4.0 Server v4.0.0.2 : magicsso-server-4.0.0.2.tar
	SSO Agent	Magic SSO V4.0 Agent v4.0.0.2 : magicsso-agent-4.0.0.2.tar
Guidance's		Magic SSO V4.0 Operational Guidance v1.2 : Magic_SSO_V4.0-OPE-v1.2.pdf Magic SSO V4.0 Installation Guide v1.2 : Magic_SSO_V4.0-PRE-v1.2.pdf
Developer		Dreamsecurity Co.,Ltd. R&D-Part2 R&D-Team1

1.3 TOE overview

1.3.1 Single Sign On overview

Magic SSO V4.0 (hereinafter referred to as 'TOE') is used to enable the user to access various business systems and use the service through a single user login without additional login action. The TOE performs user identification and authentication, authentication token(hereinafter referred to as "token") issue and validity verification according to the user authentication policy.

1.3.2 TOE Type and scope

TOE is provided as software. The TOE is composed of the server that processes user login, manages the authentication token, and sets the policy(hereinafter referred to as 'SSO Server') and the agent that is installed in each business system performs the function of authentication token issue and verification(hereinafter referred to as 'SSO Agent').

The TOE uses the following validated cryptographic modules whose safety and implementation conformity are verified through KCMVP (Korea Cryptographic Module Validation Program).

- Encryption module name : MagicJCrypto V2.0.0.0
- Verification Number : CM-131-2022.10
- Verification date : 2017-10-16

1.3.3 TOE usage and major security features

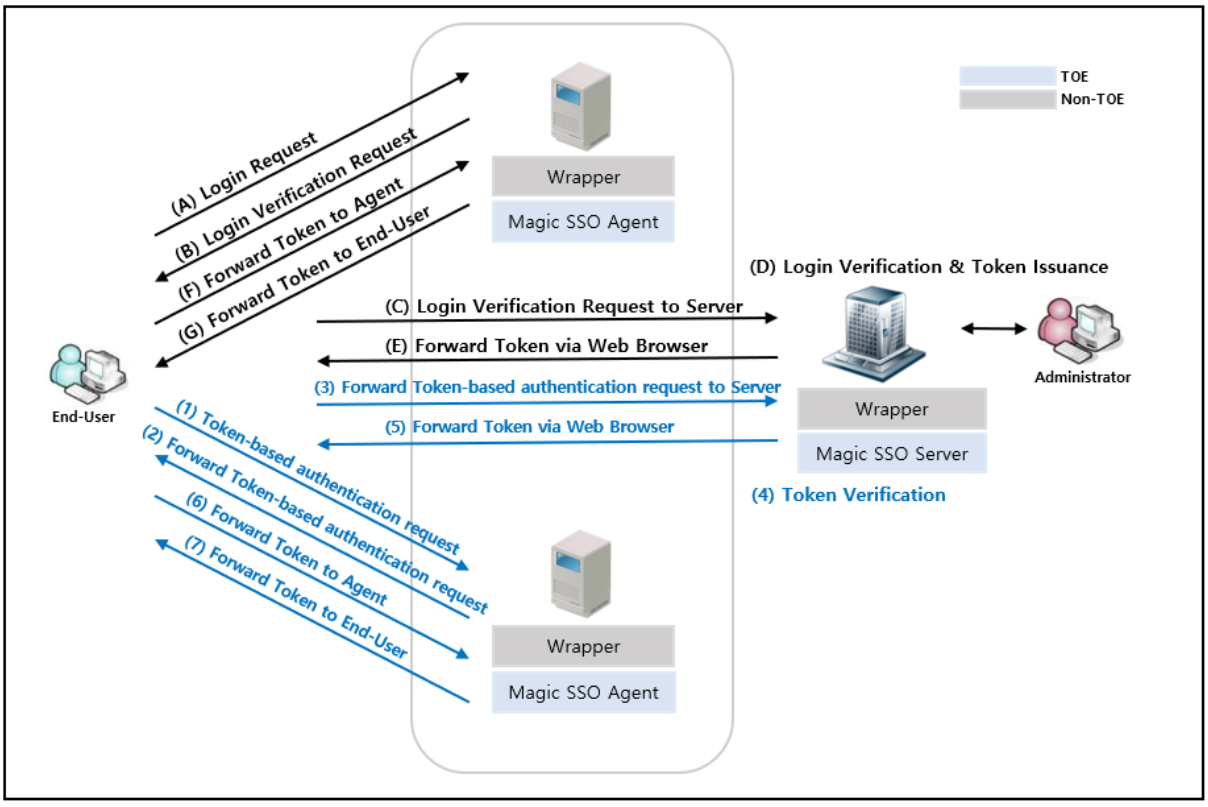
The TOE performs end user identification and authentication function through DBMS that stores end user information in order to provide service without additional login behavior to several work systems with single sign-on. The TOE provides the security audit function that records and manages a critical events as audit data when activating the security functionality and management function, function of protecting the data that stored in the TSF controlled repository, and TSF protection function such as TSF self-testing. In addition, the TOE provides authentication failure handling, identification and authentication functions including mutual authentication between the TOE components, cryptographic support function such as cryptographic key management and cryptographic operation for issuing a token, security management function for management of security functions behaviour and configuration, and the TOE access function to manage the authorized administrator's interacting session. In addition, the token requires confidentiality and integrity protection, and the TOE executable code offer integrity protection.

The end user identification and authentication procedures of the TOE are shown in [Figure 1]. The detailed procedures are divided into the initial authentication phase using the end user ID and password and the authentication token-based authentication phase that accesses the

business system using the authentication token issued during the initial authentication procedure.

Firstly, the initial authentication phase is as follows. The end user accesses the business system and enters the ID, password and the SSO agent receives a login verification request to the SSO server, which in turn checks the authorized user status. Upon receiving the login verification request, the SSO server issues an authentication token if the login verification result is valid after performing login verification using end user information stored in the DBMS. The issued token is passed to the SSO Agent. If the authentication token is verified and valid, The SSO agent transfers an issued token to the user.

Second, authentication token-based authentication steps are as follows. The authentication token-based authentication phase is performed only when has been normally issued in the initial authentication phase. The end user sends an authentication token-based authentication request to the SSO Agent installed in the business system, receiving the authentication request, the SSO agent sends an authentication token verification request to the SSO server. The SSO server that receives the authentication token verification request performs the stored authentication token verification and delivers the authentication token to the SSO agent when the verification result is valid. The SSO Agent that receives the authentication token verifies the authentication token and passes it to the end user if it is valid.

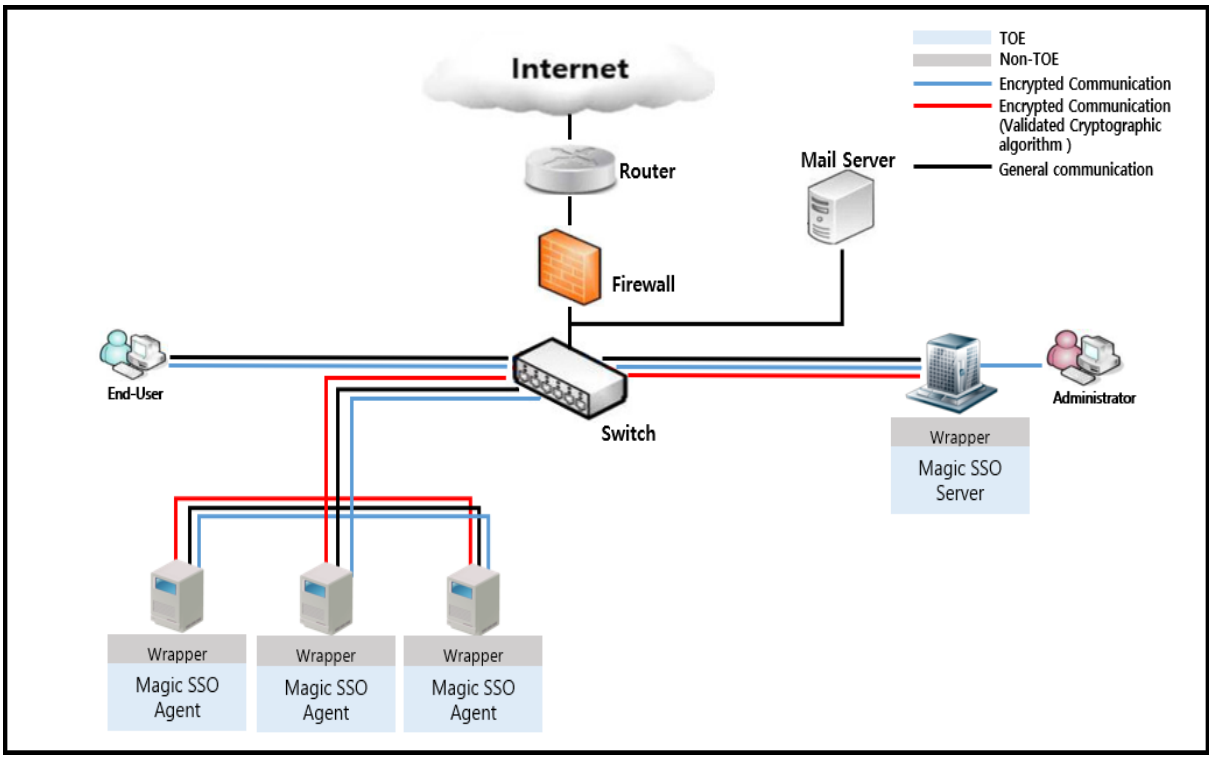


[Figure 1] End user identification and authentication procedure

Authentication phase	Example of operation procedure
Initial authentication	(A) Login request → (B) Login verification request → (C) Login verification request to server → (D) Login verification & Token issuance → (E) Forward Token via web browser → (F) Forward Token to agent → (G) Forward Token to end-user
Token-based authentication	(1) Token-based authentication request → (2) Forward Token-based authentication request → (3) Forward Token-based authentication request to server → (4) Token verification → (5) Forward Token via web browser → (6) Forward Token to agent → (7) Forward Token to end-user

1.3.4 Non-TOE and TOE operational environment

Figure 2 shows the TOE operational environment. TOE operational environment and consists of an SSO server and an SSO agent. SSO server provides login verification, authentication token issue and management, and policy setting. SSO server is mounted on Web Application Server and operates as a single web application. The SSO Agent performs normal user login verification requests, authentication token issuance, and verification request functions to the SSO server and verifies the authentication token received from the SSO server. SSO Agent is installed in each business system web application server in the form of library file API. Wrapper is used for compatibility with various business systems and Wrapper is excluded from the scope of the TOE.



[Figure 2] TOE operational environment

An administrator PC operational environment on which Internet Explorer 11 web browser that supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is required for an administrator to access the SSO server and perform security management functions such as SSO server configuration, status check and audit log search.

■ DBMS(Oracle)

SSO server and Oracle, a relational database management system, are interlinked for the purpose of the management of authentication and policy information.

■ Mail Server

A mail server is used as an external entity necessary for the operation of the TOE. The mail server is utilized to notify an authorized administrator via email in case of failed administrator authentication or possible audit data loss.

Any hardware in which the TOE is installed is non-TOE. The requirements for non-TOE hardware/software that is mandatory for the operation of the product but does not fall under the scope of the TOE are as follows:

TOE	Classification	Item	Minimum Specification
SSO Server	H/W	CPU	Intel Dual Core 2 GHz or higher
		Memory	8 GB or more
		HDD	100 GB or more of space required for TOE installation
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	S/W	OS	CentOS 6.10(Kernel 2.6.32) 64 bit
		Java	Java Runtime 1.8.0_221 Running and operating server based on Java Application
		WAS	Apache Tomcat 8.5.45 Web application server operating based on Java Application for normal operation of the TOE
		DBMS	Oracle 11g(11.2.0.1.0) Authentication and policy setting information and audit data stores
SSO Agent	H/W	CPU	Intel Dual Core 2 GHz or higher
		Memory	8 GB or more

		HDD	100 GB or more of space required for TOE installation
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	S/W	OS	CentOS 6.10(Kernel 2.6.32) 64 bit
		Java	Java Runtime 1.8.0_221 Running and operating server based on Java Application
		WAS	Apache Tomcat 8.5.45 Web application server operating based on Java Application for normal operation of the TOE
Management PC	H/W	CPU	Intel Dual Core 2 GHz or higher
		Memory	8 GB or more
		HDD	50 GB or more
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	S/W	OS	Windows 10 Pro 64 bit
		Browser	Internet Explorer 11

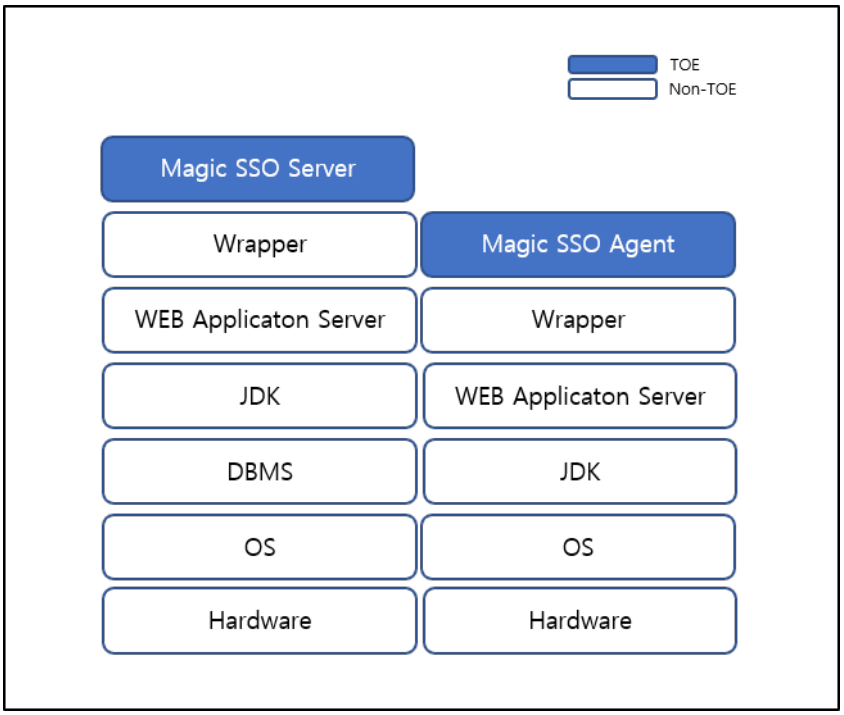
1.4 TOE description

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

1.4.1 Physical scope of the TOE

The TOE consists of SSO server, SSO agent, an operational guidance (Magic SSO V4.0 Operational Guidance v1.2, Magic_SSO_V4.0-OPE-v1.2.pdf) and an installation guide (Magic V4.0 Installation Guide v1.2, Magic_SSO_V4.0-PRE-v1.2.pdf).

The SSO server is Magic SSO V4.0 Server v4.0.0.2 that verifies end user login, manages authentication tokens and establishes policies. The SSO agent is Magic SSO V4.0 Agent v4.0.0.2 that performs the function of requesting the verification of end user login to the SSO server and requesting authentication token issuance. Any hardware and software in which the TOE is installed shall not fall under the scope of the TOE.

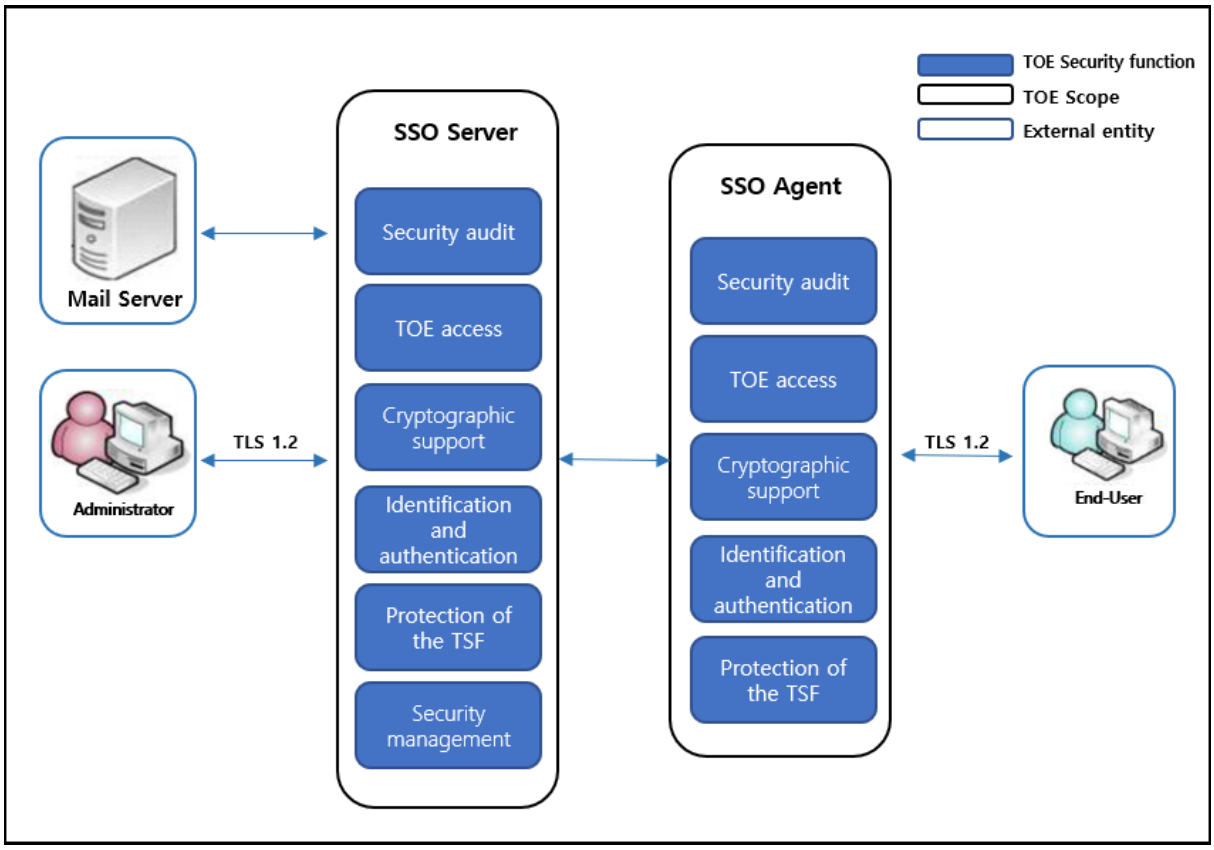


[Figure 3] Physical scope of the TOE

Magic SSO V4.0 product includes SSO server and SSO agent, which are the software developed by Dreamsecurity Co.,Ltd., together with the operational guidance and the installation guide procedure documents.

Classification	Type	Distribution type
SSO Server	S / W to install in management server (CD distribution)	Magic SSO V4.0 Server v4.0.0.2 : magicsso-server-4.0.0.2.tar
SSO Agent	S / W to install in business system (CD distribution)	Magic SSO V4.0 Agent v4.0.0.2 : magicsso-agent-4.0.0.2.tar
Guideline	Operational Guidance, Installation Guide (CD distribution)	Magic SSO V4.0 Operational Guidance v1.2 : Magic_SSO_V4.0-OPE-v1.2.pdf Magic SSO V4.0 Installation Guide v1.2 : Magic_SSO_V4.0-PRE-v1.2.pdf

1.4.2 Logical scope of the TOE



[Figure 4] Logical scope of the TOE

1) SSO Server

■ Security audit

The SSO server generates audit data on security-relevant events in order to trace the responsibility for behaviors related to the security. Audit data generated by the SSO server record the date and time of an event, the type of an event, subject identity and an outcome (success or failure) of an event. All the audit data are stored in DBMS.

An authorized administrator can review the audit data through the administrator screen and can search the audit data according to the date and time of an event, the type of an event and an outcome of an event. In addition to the super administrator, monitoring administrators authorized for audit viewing can view the audit data.

In case the audit data storage reaches a certain threshold defined by the administrator, a warning email will be sent to the administrator. Also, in case the audit storage is full, audited events are ignored and a warning message is sent to the administrator via email.

In addition, the following potential violations are analyzed, and a warning message is sent to the administrator via email.

- Authentication failure event: authentication attempts made by an end user/administrator fail consecutively for a specific number of times defined by the administrator
- Audit event on integrity violation
- Event on failed self test of the validated cryptographic module

■ TOE Access

The TOE performs per user attribute limitation on concurrent sessions, management of TSF-initiated sessions and TOE session establishment to manage access by the end users and administrators. The maximum number of concurrent sessions of management access by an administrator that belong to the same administrator is limited to one. Also, the concurrent establishment of management access session and local access session that belong to the same administrator is prohibited.

The TOE blocks new access if an administrator makes management access in one terminal and then tries to log in with the same account or the same privilege in a different terminal. An access session by an administrator/end user is terminated after a specified time period of end user inactivity (default value: 10 minutes). As to management access by an administrator, any access by IPs, other than access IPs configurable by an administrator (default value: 2 IPs), is denied.

■ Cryptographic Support

The TOE manages the security functions for generation, distribution and destruction of cryptographic key necessary for cryptographic operation, cryptographic operation and random number generation. For an algorithm applied here, MagicJCrypto V2.0.0.0, which is a validated cryptographic module, is used.

The SSO server uses a random bit generator (HASH_DRBG(SHA-256)) in generating a symmetric key necessary for encrypting authentication information sent to the SSO agent and encrypting/decrypting authentication tokens.

The SSO server performs encryption/decryption by using a symmetric key encryption algorithm (SEED/CBC 128 bits) in encrypting authentication information sent to the SSO agent and encrypting/decrypting authentication tokens.

The SSO server destroys a symmetric key that was used for encrypting authentication information sent to the SSO agent and encrypting/decrypting authentication tokens by overwriting it with '0' (0x30).

The SSO server, when sending a cryptographic key for authentication information sent to the SSO agent, uses a public key algorithm (RSAES (SHA-256)) to encrypt with a SSO agent public key and distribute it.

The SSO server uses a digital signature algorithm (RSA-PSS (SHA-256)) in generating digital signature of authentication information sent to the SSO agent and verifying digital signature of authentication information received by the SSO agent.

A random bit generator (HASH_DRBG (SHA-256)) is used for generating necessary random bits in generating symmetric key and password salts.

A message authentication code algorithm (HMAC (SHA-256)) is used for the integrity verification of the TOE module implemented by Dreamsecurity Co.,Ltd.

■ Identification and Authentication

The TOE identifies an administrator based on ID during identification and authentication attempts and performs administrator authentication before any behavior. The information provided through the GUI for identification/authentication of an administrator is ID and password, based on which an administrator is identified/authenticated.

In case administrator authentication attempts fail consecutively for a specified number of times defined by an administrator (default value: 5 times), the authentication function becomes inactivated and access is denied for a specified period of time for authentication delay defined by an administrator (default value: 5 minutes). Passwords for authentication are masked with * and only the cause information of authentication failure is provided. Thus, in case of failed identification and authentication, feedback on reasons for the failure is not provided.

An administrator password shall be generated in accordance with the password rules. Once identification and authentication are completed, the administrator can manage the security functions.

If identification and authentication of an end user are initially completed, an authentication token is generated with single-use login authentication information on the authenticated user and time stamps. Afterwards, upon authentication request based on the authentication token of the end user, the integrity verification that compares the end user's authentication token with the authentication token hash managed on the SSO server is conducted. Also, the token verification in the validity verification that compares the authentication token expirations is performed.

For the destruction of the authentication token, the authentication token managed on the SSO server is overwritten with "0" value and then destroyed.

Upon login request from an end user and upon token-based authentication request, duplication check is performed to compare Request ID in the authentication request information with Request ID managed on the SSO server in order to prevent the reuse.

TOE internal mutual authentication is performed through the protocol implemented by Dreamsecurity Co.,Ltd.

■ **Protection of the TSF**

The TOE offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the cryptographic module.

For the protection of the TSF data, the information on end user/administrator's authentication, TOE integrity verification, SSO server and SSO agent and so forth is encrypted, stored and managed in the DBMS. Authentication tokens are loaded in SSO server sessions in an end user's browser and are destroyed immediately after the use.

The SSO server runs self tests during the initial start-up and periodically during normal operation to check the process status in order to ensure that it is in a safe condition and the security function works normally. It also performs integrity monitoring of TSF data and TSF executable codes subject to the integrity verification.

■ **Security Management**

The SSO server provides the function that enables an authorized administrator to manage security roles, policies, end user information and audit information through the security management interface.

An authorized administrator can change an administrator's or an end user's password through the security management interface and verifies the validity of the password values in accordance with the password policy when creating or changing an end user's or an authorized administrator's password.

When an authorized administrator accesses the security management interface for the first time, it shall be enforced that the administrator changes the password. An audit administrator shall change the password upon access after the password is reset by an authorized administrator.

- Security Role Management: The function of the administrator role management is provided. The administrator role is classified into super administrator and monitoring administrator. A super administrator is authorized for policy management, end user information management and audit information management while a monitoring administrator is authorized for the monitoring of the TOE and audit information viewing.
- Security Policy Management: The function of the authentication policy management is provided. It performs the setting of the password validity and prevention of duplicated logins, and the establishment of end user authentication policies to define a session inactivity period. It establishes a threshold of the audit storage capacity and the audit information regarding the verification interval of the module implemented by Dreamsecurity Co.,Ltd. It sets up mail information including mail server address and mail alarm information.
- End User Information Management: It provides the function of handling unlocking of an end user account that has been locked.
- Audit Information Management: It provides the function of viewing audit information based on a search period, types of audit events and outcomes

2) SSO agent

■ Security Audit

The SSO agent generates audit data on security-relevant events in order to trace the responsibility for behaviors related to the security. Audit data generated by the SSO server record the date and time of an event, the type of an event, subject identity and an outcome (success or failure) of an event. All the audit data are transmitted to the SSO server.

■ TOE Access

Following identification and authentication of an end user, a session is terminated after a specified time period of inactivity (default value: 10 minutes). Afterwards, identification and authentication are performed through re-authentication.

■ Cryptographic Support

The TOE manages the security functions for generation, distribution and destruction of cryptographic key necessary for cryptographic operation, cryptographic operation and random number generation. For an algorithm applied here, MagicJCrypto V2.0.0.0, which is a validated cryptographic module, is used.

The SSO agent uses a random bit generator (HASH_DRBG(SHA-256)) in generating a symmetric key necessary for encrypting authentication information sent to the SSO server and encrypting/decrypting authentication tokens.

The SSO agent performs encryption/decryption by using a symmetric key encryption algorithm (SEED/CBC 128 bits) in encrypting authentication information sent to the SSO server.

The SSO agent destroys a symmetric key that was used for encrypting authentication information sent to the SSO server tokens by overwriting it with '0' (0x30).

The SSO agent, when sending a cryptographic key for authentication information sent to the SSO server, uses a public key algorithm (RSAES (SHA-256)) to encrypt with a SSO server public key and distribute it.

The SSO agent uses a digital signature algorithm (RSA-PSS (SHA-256)) in generating digital signature of authentication information sent to the SSO server and verifying digital signature of authentication information received by the SSO server.

A random bit generator (HASH_DRBG (SHA-256)) is used for generating necessary random bits in generating a symmetric key.

A message authentication code algorithm (HMAC (SHA-256)) is used for the integrity verification of the TOE module implemented by Dreamsecurity Co.,Ltd.

■ **Identification and Authentication**

The TOE identifies an end user based on ID during the initial identification and authentication attempts and performs end user authentication before any behavior. The information provided through GUI for identification/authentication of an end user is ID and password, based on which an end user is identified/authenticated.

In case end user authentication attempts fail consecutively for a specified number of times defined by an administrator (default value: 5 times), the authentication function becomes inactivated and access is denied until the administrator unlocks the end user account. Passwords for authentication are masked with * and only the cause information of authentication failure is provided. Thus, in case of failed identification and authentication, feedback on reasons for the failure is not provided.

If identification and authentication of an end user are initially completed, identification and authentication through an authentication token are performed upon token-based request.

For the destruction of the authentication token, the authentication token managed on the SSO

server is overwritten with "0" value and then destroyed.

Upon login request from an end user and upon token-based authentication request, duplication check is performed to compare Request ID in the authentication request information with Request ID managed on the SSO server in order to prevent the reuse.

TOE internal mutual authentication is performed through the protocol implemented by Dreamsecurity Co.,Ltd.

■ **Protection of the TSF**

The TOE offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the cryptographic module.

For the protection of the TSF data, the information on end user/administrator's authentication, TOE integrity verification, SSO server and SSO agent and so forth is encrypted, stored and managed in the DBMS. Authentication tokens are loaded in SSO server sessions in an end user's browser and are destroyed immediately after the use.

The SSO agent runs self tests during the initial start-up and periodically during normal operation to check the process status in order to ensure that it is in a safe condition and the security function works normally. It also performs integrity monitoring of TSF data and TSF executable codes subject to the integrity verification

1.5 Terms and definitions

Application Programming Interface (API)

A set of software libraries that exist between the application layer and the platform system layer and facilitate the development of applications that run on the platform

Approved cryptographic algorithm

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

Approved mode of operation

The mode of cryptographic module using approved cryptographic algorithm

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

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

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

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

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

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

Authorized Administrator
Authorized user to securely operate and manage the TOE

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

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

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

Class
Set of CC families that share a common focus

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

Component
Smallest selectable set of elements on which requirements may be based

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

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

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

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

Element
Indivisible statement of a security need

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

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

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

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

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

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

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

Korea Cryptographic Module Validation Program (KCMVP)
A system to validate the security and implementation conformance of cryptographic modules used for protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions

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

Monitoring administrator
As An authorized user who operates and manages the TOE securely, Only the audit log can be viewed among the security management functions

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

Operation(on a component of the CC)
Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation(on a subject)
Specific type of action performed by a subject on an object

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

Protection Profile (PP)
Implementation-independent statement of security needs for a TOE type

Public Key

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

Public Key(asymmetric) cryptographic algorithm

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

Public Security Parameters (PSP)

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

Random bit generator (RBG)

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

Recommend/be recommended

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

Refinement

Addition of details to a component

Role

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

Secret Key

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

Secure Sockets Layer (SSL)

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

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

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

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

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

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

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

Subject
Active entity in the TOE that performs operations on objects

Super administrator
As an authorized user who operates and manages the TOE securely, it can perform all security management functions

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

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

Threat Agent
Entity that can adversely act on assets

TOE Security Functionality (TSF)
Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

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

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

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

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

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

1.6 Conventions

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

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement.

Each operation is used in this PP.

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

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

Selection

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

Refinement

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

2 Conformance claim

2.1 CC, PP and security requirements package conformance

The Common Criteria and the Protection Profile, and the security requirements package that this ST and the TOE conform to are as follows:

Classification	Compliance
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 - Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
CC Part2	Extended : FCS_RBG.1, FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1, FPT_TUD.1, FTA_SSL.5
CC Part3	Conformant
PP	National Protection Profile for Single Sign On V1.0 (2017-08-18)
Security requirements package	Augmented : EAL1 augmented (ATE_FUN.1)

2.2 Conformance claim rationale

This ST strictly conforms to the "National Protection Profile for Single Sign-On V1.0," adopting the TOE type, security objectives and security requirements in the same way as the PP.

Classification	PP	ST	Rationale
TOE Type	Single sign on	Single sign on	Same as PP
Operational environment	OE.Physical control	OE.Physical control	Same as PP
	OE.Trusted admin	OE.Trusted admin	Same as PP
	OE.Log backup	OE.Log backup	Same as PP

	OE.Operation system reinforcement	OE.Operation system reinforcement	Same as PP
	OE.Secure development	OE.Secure development	Same as PP
	-	OE.Time stamp	More restrictive than the PP - Although the PP does not include security problem definitions and security requirements regarding time stamps used in audit records, this ST additionally identifies the assumptions that secure time stamps received from the TOE operational environment are used. Therefore, it is more restrictive than the PP
	-	OE.DBMS	More restrictive than the PP - Although the PP does not include security problem definitions and security requirements regarding the DBMS where audit data are recorded, this ST additionally identifies the assumptions that the DBMS safely stores and protects audit data generated in the TOE. Therefore, it is more restrictive than the PP
Security functional requirements	FAU_ARP.1	FAU_ARP.1	Same as PP
	FAU_GEN.1	FAU_GEN.1	Same as PP
	FAU_SAA.1	FAU_SAA.1	Same as PP
	FAU_SAR.1	FAU_SAR.1	Same as PP
	FAU_SAR.3	FAU_SAR.3	Same as PP
	FAU_STG.3	FAU_STG.3	Same as PP
	FAU_STG.4	FAU_STG.4	Same as PP
	FCS_CKM.1	FCS_CKM.1	Same as PP
	FCS_CKM.2	FCS_CKM.2	Same as PP
	FCS_CKM.4	FCS_CKM.4	Same as PP
	FCS_COP.1	FCS_COP.1(1)	Cryptographic operation in the PP is divided into symmetric key, digital signature, MA, public key and hash
		FCS_COP.1(2)	
		FCS_COP.1(3)	

		FCS_COP.1(4)	to perform iteration operation. This ST conforms to the security requirements equivalent to those in the PP
		FCS_COP.1(5)	
	FCS_RGB.1	FCS_RGB.1	Same as PP
	FIA_AFL.1	FIA_AFL.1(1)	Authentication failure handling in the PP is divided into that of an administrator and that of an end user to perform the iteration operation. Since the users of the TOE consist of the administrators and the end users, this ST conforms to the security requirements equivalent to those in the PP
		FIA_AFL.1(2)	
	FIA_IMA.1	FIA_IMA.1	Same as PP
	FIA_SOS.1	FIA_SOS.1	Same as PP
	FIA_SOS.2	FIA_SOS.2	Same as PP
	FIA_SOS.3	FIA_SOS.3	Same as PP
	FIA_UAU.2	FIA_UAU.2(1)	User authentication handling in the PP is divided into that of an administrator and that of an end user to perform the iteration operation. Since the users of the TOE consist of the administrators and the end users, this ST conforms to the security requirements equivalent to those in the PP
		FIA_UAU.2(2)	
	FIA_UAU.4	FIA_UAU.4	Same as PP
	FIA_UAU.7	FIA_UAU.7	Same as PP
	FIA_UID.2	FIA_UID.2(1)	User Identification processing in the PP is divided into that of an administrator and that of an end user to perform the iteration operation. Since the users of the TOE consist of the administrators and the end users, this ST conforms to the security requirements equivalent to those in the PP
		FIA_UID.2(2)	

	FMT_MOF.1	FMT_MOF.1	Same as PP
	FMT_MTD.1	FMT_MTD.1	Same as PP
	FMT_PWD.1	FMT_PWD.1	Same as PP
	FMT_SMF.1	FMT_SMF.1	Same as PP
	FMT_SMR.1	FMT_SMR.1	Same as PP
	FPT_ITT.1	FPT_ITT.1	Same as PP
	FPT_PST.1	FPT_PST.1	Same as PP
	FPT_TST.1	FPT_TST.1	Same as PP
	FTA_MCS.2	FTA_MCS.2	Same as PP
	FTA_SSL.5	FTA_SSL.5	Same as PP
	FTA_TSE.1	FTA_TSE.1	Same as PP
Warranty requirements	ADV_FSP.1	ADV_FSP.1	Same as PP
	AGD_OPE.1	AGD_OPE.1	Same as PP
	AGD_PRE.1	AGD_PRE.1	Same as PP
	ALC_CMC.1	ALC_CMC.1	Same as PP
	ALC_CMS.1	ALC_CMS.1	Same as PP
	ASE_CCL.1	ASE_CCL.1	Same as PP
	ASE_ECD.1	ASE_ECD.1	Same as PP
	ASE_INT.1	ASE_INT.1	Same as PP
	ASE_OBJ.1	ASE_OBJ.1	Same as PP
	ASE_REQ.1	ASE_REQ.1	Same as PP
	ASE_TSS.1	ASE_TSS.1	Same as PP
	ATE_FUN.1	ATE_FUN.1	Same as PP
	ATE_IND.1	ATE_IND.1	Same as PP
	AVA_VAN.1	AVA_VAN.1	Same as PP

3 Security objectives

3.1 Security objectives for the operational environment

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

OE. PHYSICAL_CONTROL

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

OE. TRUSTED_ADMIN

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

OE. LOG_BACKUP

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

OE. OPERATION_SYSTEM_REINF ORCEMENT

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

OE. SECURE_DEVELOPMENT

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

OE.TIME_STAMP

The TOE shall receive reliable time stamps from the operating environment and accurately record audit data related to the operation of the TOE.

OE.DBMS

The TOE shall receive reliable DBMS from the operational environment, store audit data related to the operation of the TOE and protect the audit data from unauthorized deletion or modification.

4 Extended components definition

4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

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

Component leveling

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

Management: FCS_RBG.1
There are no management activities foreseen

Audit: FCS_RBG.1
There are no auditable events foreseen

4.1.1.1 FCS_RGB.1 Random bit generation

Hierarchical to No other components
Dependencies No dependencies

FCS_RBG.1.1 The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

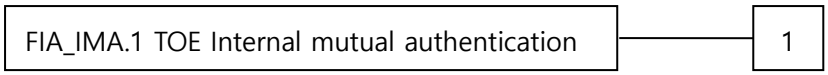
4.2 Identification and authentication

4.2.1 TOE Internal mutual authentication

Family Behaviour

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

Component leveling



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

Management: FIA_IMA.1
There are no management activities foreseen

Audit: FIA_IMA.1

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

a) Minimum: Success and failure of mutual authentication

4.2.1.1 FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to	No other components
Dependencies	No dependencies

FIA_IMA.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] using the [assignment: authentication protocol] that meets the following [assignment: *list of standards*]

4.2.2 Specification of Secrets

Family Behaviour

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

Component leveling

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

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

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

Management: FIA_SOS.3

There are no management activities foreseen

Audit: FIA_SOS.3

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

a) Minimum : Success and failure of the activity

4.2.2.1 FIA_SOS.3 Destruction of Secrets

Hierarchical to	No other components
Dependencies	FIA_SOS.2 TSF Generation of secrets

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

4.3 Security Management

4.3.1 ID and password

Family Behaviour

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

Component leveling

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

Management: FMT_PWD.1

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

Audit: FMT_PWD.1

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

a) Minimum: All changes of the password

4.3.1.1 FMT_PWD.1 Management of ID password

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

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*]
1. [assignment: *password combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: list of functions] to [assignment: the authorized identified roles]
1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters*

unusable for ID, etc]

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

4.4 Production of the TSF

4.4.1 Protection of stored TSF data

Family Behaviour

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

Component leveling

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

Management: FPT_PST.1
There are no management activities foreseen

Audit: FPT_PST.1
There are no auditable events foreseen

4.4.1.1 FPT_PST.1 Basic protection of stored TSF data

Hierarchical to No other components
Dependencies No dependencies

FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by

the TSF from the unauthorized [selection: *disclosure, modification*]

4.5 TOE Access

4.5.1 Session locking and termination

Family Behaviour

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

Component leveling

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

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

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

Management: FTA_SSL.5

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

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

Audit: FTA_SSL.5

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

a) Minimum: Locking or termination of interactive session

4.5.1.1 FTA_SSL.5 Management of TSF-initiated sessions

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

FTA_SSL.5.1	The TSF shall [selection: • *lock the session and re-authenticate the user before unlocking the session,* • *terminate] an interactive session after a [assignment: time interval of user inactivity]*

5 Security requirements

In this section specify security functional requirements and assurance requirements that must be satisfied by the TOE

5.1 Security functional requirements

The security functional requirements defined in this ST are derived from the relevant security functional components in CC Part 2 in order to satisfy the security objectives identified in Chapter 3. [Table 1] below summarizes the security functional components used in this ST.

[Table 1] Security functional requirements

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1	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_RGB.1(Extended)	Random bit generation
FIA	FIA_AFL.1(1)	Authentication failure handling(Administrator)
	FIA_AFL.1(2)	Authentication failure handling(End-user)
	FIA_IMA.1(Extended)	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.2(1)	Authenticated the user before all behavior (Administrator)
	FIA_UAU.2(2)	Authenticated the user before all behavior (End-user)
	FIA_UAU.4(1)	Single-use authentication mechanisms(Administrator)

	FIA_UAU.4(2)	Single-use authentication mechanisms(End-user)
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	Identification the user before all behavior (Administrator)
	FIA_UID.2(2)	Identification the user before all behavior (End-user)
FMT	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF testing
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

5.1.1 Security audit (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to No other components

Dependencies FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [refer to "actions" in [Table 2] list of actions against security violations] upon detection of a potential security violation.

[Table 2] List of actions against security violations

Security functional component	Security violation	Action
FIA_UAU.2(1)	- In case administrator authentication attempts fail consecutively for a defined number of times (default value: 5 times)	- Inactivate the authentication function for a defined period of time (default value: 5 minutes) - Send a warning message email to the authorized administrator
FIA_UAU.2(2)	- In case end user authentication attempts fail consecutively for a defined number of times (default value: 5 times)	- Inactivate the authentication function until the authorized administrator unlock the account
FPT_TST.1	- In case the integrity verification fails	- Send a warning message email

	- In case a self-test of the validated cryptographic module fails	to the authorized administrator
FAU_STG.3	- In case the audit trail exceeds the threshold (default value: 90%)	- Send a warning message email to the authorized administrator
FAU_STG.4	- In case the audit trail is full	- Ignore an audited event - Send a warning message email to the authorized administrator

5.1.1.2 FAU_GEN.1 Audit data generation

Hierarchical to: No other components
Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) [Refer to the "auditable events" in [Table 3] Audit events, [assignment: *No other components*]]

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Refer to the contents of "additional audit record" in [Table 4] Audit events, [assignment: other audit relevant information]]

[Table 3] Auditable events

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 the distribution of a key related to encryption/decryption of TSF data)	
FCS_CKM.4	Success and failure of the activity (applied only to the destruction of a key related to encryption/decryption of TSF data)	
FCS_COP.1(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)	
FCS_COP.1(2)	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)	
FCS_COP.1(3)	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)	
FCS_COP.1(4)	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)	
FCS_COP.1(5)	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(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_AFL.1(2)	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.2(1)	All use of the administrator authentication mechanism	
FIA_UAU.2(2)	All use of the end user authentication mechanism	
FIA_UAU.4	Single-use authentication mechanism	
FIA_UID.2(1)	All use of the administrator identification mechanism	
FIA_UID.2(2)	All use of the end user identification mechanism	

FMT_MOF.1	All modifications in the behavior 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 management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5(Extended)	Locking or termination of interactive sessions	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

5.1.1.3 FAU_SAA.1 Potential violation analysis

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

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

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

a) Accumulation or combination of [Authentication failure audit event among auditable events in FIA_UAU.2(1), Authentication failure audit event among auditable events in FIA_UAU.2(2), Integrity violation audit event and failure of self test of approved cryptographic module among auditable events in FPT_TST.1, Audit trail capacity exceeding the threshold among auditable events in FAU_STG.3, Full audit trail event among auditable events in FAU_STG.4] known to indicate a potential security violation;

b) [None]

5.1.1.4 FAU_SAR.1 Audit review

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

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

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

5.1.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [sorting in the descending order based on the time and date of events] of audit data based on [the time and date of an event AND event type AND event outcome].

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

Hierarchical to: No other components
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Notification to the authorized administrator, [N/A]] if the audit trail exceeds [the percentage of the used storage in excess of the total audit trail storage (50-90% range that can be defined by the authorized administrator, default value of exceeding the threshold: 90%)].

5.1.1.7 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *ignore audited events* and [send a warning email to the authorized administrator] if the audit trail is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ["Cryptographic algorithm" in [Table 4] List of cryptographic key generation standards] and specified cryptographic key size ["Cryptographic key size" in [Table 4] List of cryptographic key generation standards] that meet the following ["Reference standard" in [Table 4] List of cryptographic key generation standards].

[Table 4] List of cryptographic key generation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
KEK (Key Encrypt Key)	HMAC (SHA-256)	128 bit	FIPS 198
DEK (Data Encrypt Key)	HASH_DRBG (SHA-256)	128 bit	ISO/IEC 18031
Authentication token encrypting/decrypting key	HASH_DRBG (SHA-256)	128 bit	ISO/IEC 18031
Transmission information encrypting/decrypting key	HASH_DRBG (SHA-256)	128 bit	ISO/IEC 18031
Server Certificate Public / Private Key Pair for Cryptography	HASH_DRBG (SHA-256)	Public key 2048 bit	ISO/IEC 18031
Server certificate public / private key pair for Signing	HASH_DRBG (SHA-256)	Public key 2048 bit	ISO/IEC 18031

5.1.2.2 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ["Cryptographic key distribution method" in [Table 5] List of cryptographic key distribution standards] that meets the following ["Reference standard" in [Table 5] List of cryptographic key distribution standards].

[Table 5] List of cryptographic key distribution standards

Usage	Cryptographic algorithm	Cryptographic key	Reference standard

		size	
Public key cryptography	RSAES (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Cryptographic key distribution method			
- Distribution by encrypting an encryption key for the information transmitted between the SSO server and the SSO agent with the public key of the other server			

5.1.2.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ["Method" in [Table 6] List of cryptographic key destruction] that meets the following [[Table 6] List of cryptographic key destruction].

[Table 6] List of cryptographic key destruction

Usage	Method	Cryptographic key size	Reference standard
Cryptographic key destruction	Overwriting with '0' (0x30)	-	-
Function of cryptographic key destruction			
- Destruction of a symmetric key used for KEK (Key Encrypt Key) - Destruction of a symmetric key used for DEK (Data Encrypt Key) - Destruction of a symmetric key used for encryption of authentication tokens - Destruction of a symmetric key used for encryption of the information transmitted between the SSO server and the SSO agent			

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

Hierarchical to: No other components

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

FCS_COP.1.1 The TSF shall perform ["Function of cryptographic operation" in [Table 7] List of cryptographic operation standards] in accordance with a specified cryptographic algorithm ["Cryptographic algorithm" in [Table 7] List of cryptographic operation

standards] and cryptographic key sizes ["Cryptographic key size" in [Table 7] List of cryptographic operation standards] that meet the following ["Reference standard" in [Table 7] List of cryptographic operation standards].

[Table 7] List of cryptographic operation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Block cipher (symmetric key cryptography)	SEED/CBC	128 bits	TTAS.KO-12.0004
Function of cryptographic operation			
- Encryption/decryption of DEK (Data Encrypt Key) - Encryption/decryption of TSF data - Encryption/decryption of authentication tokens - Encryption/decryption of the information transmitted between the SSO server and the SSO agent			

5.1.2.5 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 ["Function of cryptographic operation" in [Table 8] List of cryptographic operation standards] in accordance with a specified cryptographic algorithm ["Cryptographic algorithm" in [Table 8] List of cryptographic operation standards] and cryptographic key sizes ["Cryptographic key size" in [Table 8] List of cryptographic operation standards] that meet the following ["Reference standard" in [Table 8] List of cryptographic operation standards].

[Table 8] List of cryptographic operation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Digital signature	RSA-PSS (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Function of cryptographic operation			
- Digital signature/verification of the information transmitted between the SSO server and the SSO agent			

5.1.2.6 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 ["Function of cryptographic operation" in [Table 9] List of cryptographic operation standards] in accordance with a specified cryptographic algorithm ["Cryptographic algorithm" in [Table 9] List of cryptographic operation standards] and cryptographic key sizes ["Cryptographic key size" in [Table 9] List of cryptographic operation standards] that meet the following ["Reference standard" in [Table 9] List of cryptographic operation standards].

[Table 9] List of cryptographic operation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Message authentication code	HMAC (SHA-256)	256 bits	FIPS 198
Function of cryptographic operation			
- Generation of a symmetric key used for KEK (Key Encrypt Key) - Integrity verification of the TOE			

5.1.2.7 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 ["Function of cryptographic operation" in [Table 10] List of cryptographic operation standards] in accordance with a specified cryptographic algorithm ["Cryptographic algorithm" in [Table 10] List of cryptographic operation standards] and cryptographic key sizes ["Cryptographic key size" in [Table 10] List of cryptographic operation standards] that meet the following ["Reference standard" in [Table 10] List of cryptographic operation standards].

[Table 10] List of cryptographic operation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Public key cryptography	RSAES (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Function of cryptographic operation			

- Encryption of a symmetric key used for encryption of authentication tokens - Encryption of a symmetric key used for encryption of the information transmitted between the SSO sever and the SSO agent

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

Hierarchical to: No other components

Dependencies: No dependencies

FCS_COP.1.1 The TSF shall perform ["Function of cryptographic operation" in [Table 11] List of cryptographic operation standards] in accordance with a specified cryptographic algorithm ["Cryptographic algorithm" in [Table 11] List of cryptographic operation standards] and cryptographic key sizes ["Cryptographic key size" in [Table 11] List of cryptographic operation standards] that meet the following ["Reference standard" in [Table 11] List of cryptographic operation standards].

[Table 11] List of cryptographic operation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Hash	SHA-256	-	FIPS 180-2
Function of cryptographic operation			
- Integrity verification of authentication tokens - Integrity verification of TSF data - Encryption of administrator and end user passwords			

5.1.2.9 FCS_RGB.1 Random bit generation (extended)

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RGB.1.1 The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following ["Reference standard" in [Table 12] List of random bit generation standards].

[Table 12] List of random bit generation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Random bit generation	HASH_DRBG (SHA-256)	-	ISO/IEC 18031

5.1.3 Identification and authentication (FIA)

5.1.3.1 FIA_AFL.1(1) Authentication failure handling (administrator)

Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *[5]* unsuccessful authentication attempts occur related to [authentication attempt in the TOE by the authorized administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [inactivate the relevant administrator's authentication function for the period configurable by the authorized administrator (positive integer number between 5 and 10, default value: 5 minutes), send a warning email to the authorized administrator].

5.1.3.2 FIA_AFL.1(2) Authentication failure handling (end user)

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 [authentication attempt in the TOE by the end user].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [inactivate the authentication function of the relevant end user so that the user cannot log in any longer until the administrator unlocks].

5.1.3.3 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 [the authentication protocol implemented by Dreamsecurity Co.,Ltd. (digital signature using the validated cryptographic module, verification)] that meets [None] between [the SSO server and the SSO agent].

5.1.3.4 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 [the following defined quality metric].

[

a) Valid characters: English alphabets (a~z, A~Z), numbers (0~9), special characters (!, @, #, $, %, ^, *, +, =, -)

b) Valid length: 9 - 16 digits

c) Combination rules: Combination of all three types of characters

]

5.1.3.5 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 **an authentication token** that meets [the acceptable standard defined below].

[

a) Subject that generates an authentication token: SSO server

b) Authentication token components:

User ID, user name, user IP, authentication time (time stamp), integrity value

c) Cryptographic algorithm of an authentication token:

Refer to the algorithm in [Table 7] List of cryptographic operation standards

d) Integrity algorithm of an authentication token:

Refer to the algorithm in [Table 9] List of cryptographic operation standards

]

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF-generated **authentication tokens** for [end user login].

[

- FIA_UAU.2(2) User authentication before any action (end user)
- FIA_UID.2(2) User identification before any action (end user)

]

5.1.3.6 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 [overwriting with "0" value] that meets the following [None].

5.1.3.7 FIA_UAU.2(1) User authentication before any action (administrator)

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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

5.1.3.8 FIA_UAU.2(2) User authentication before any action (end user)

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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

5.1.3.9 FIA_UAU.4(1) Single-use authentication mechanism (administrator)

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [the authorized administrator access session information].

5.1.3.10 FIA_UAU.4(2) Single-use authentication mechanism (end user)

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [end user access session information, authentication token generation information].

5.1.3.11 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.

[

a) Passwords being entered are masked (character "●")

b) In case of failed authentication, feedback on the reason for the failure is not provided but feedback is provided with the statement, "authentication failed"

]

5.1.3.12 FIA_UID.2(1) User identification before any action (administrator)

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

FIA_UID.2.1 The TSF shall require each **authorized administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of the **authorized administrator**.

5.1.3.13 FIA_UID.2(2) User identification before any action (end user)

Hierarchical to: FIA_UID.1 Identification
Dependencies: No dependencies

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

5.1.4 Security management (FMT)

5.1.4.1 FMT_MOF.1 Management of security functions behavior

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 13] List of security functions behavior] to the [authorized administrator].

[Table 13] List of security functions behavior

List of functions	Management behavior	Authorized administrator
Audit information viewing	Determine behaviors	Super administrator, monitoring administrator
Module verification in real time	Determine, modify behaviors	Super administrator
Audit information setting	Determine, modify behaviors	Super administrator
Mail notification setting	Determine, modify behaviors	Super administrator
User unlocking	Determine, modify behaviors	Super administrator
User policy establishment	Determine, modify behaviors	Super administrator
Administrator management	Determine, modify behaviors	Super administrator
Administrator policy establishment	Determine, modify behaviors	Super administrator
Administrator password change	Determine, modify behaviors	Super administrator, monitoring administrator

5.1.4.2 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** [[Table 14] List of TSF data] to [the authorized administrator].

[Table 14] List of TSF data

List of functions	Management	Authorized administrator
Audit information	Query	Super administrator, monitoring administrator
Audit storage capacity threshold	Query, modify	Super administrator
Cycle of integrity verification of cryptographic module and SSO module	Query, modify	Super administrator
Mail server information	Query, modify	Super administrator
Mail sending information	Query, modify	Super administrator
User policy information	Query, modify	Super administrator
Administrator information	Query, modify	Super administrator
Administrator policy establishment	Query, modify	Super administrator

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

Hierarchical to: No other components

Dependencies FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage [administrator password change] to the [authorized administrator].

1. [Password combination rules and length: English alphabet (a-Z)/number (0-9)/special character (!, @, #, $, %, ^, *, +, =, -), combination of all three types, 9-16 digits]
2. [None]

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

1. [None]
2. [None]

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

5.1.4.4 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
[list of management functions to be provided by the TSF]
[
a) List of security functions specified in FMT_MOF.1
b) List of TSF data management specified in FMT_MTD.1
c) List of functions specified in FMT_PWD.1
]

5.1.4.5 FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [the following authorized roles].

[

a) Roles of super administrator

Audit information viewing

Module verification in real time

Audit information setting

Mail notification setting

User unlocking

User policy establishment

Administrator management

Administrator policy establishment

Administrator password change

Version information

b) Roles of monitoring administrator

Audit information viewing

Administrator password change

]

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)

5.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

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

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

Hierarchical to: No other components

Dependencies: No dependencies

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

[

a) Administrator and end user password
b) Authentication token
c) Cryptographic key
d) DBMS account information
e) Server certificate password
f) Policy establishment information
g) Configuration information
]

5.1.5.3 FPT_TST.1 TSF testing

Hierarchical to: No other components
Dependencies: No dependencies

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

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

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

5.1.6 TOE access (FTA)

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

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

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [limitation on the maximum number of concurrent sessions in case of management access sessions by the administrator to one, prohibition of concurrent establishment of management access session and local access session that belong to the same administrator, { None }].

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

5.1.6.2 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 [the period of user inactivity (administrator configurable positive integer between 3 and 10, default value: 10 minutes)].

5.1.6.3 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components
Dependencies: No dependencies

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

5.2 Security assurance requirements

Security assurance requirements of this ST are composed of assurance components in CC Part 3 and the evaluation assurance level is EAL1+. [Table 15] below summarizes assurance components.

[**Table 15**] **Assurance requirements**

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 documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE configuration management coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

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 a ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain a 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 summarize 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.1D The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements

ASE_OBJ.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation 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 Security-enforcing functional specification
Dependencies: No dependencies

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

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

Evaluator action elements

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E 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 procedures
Dependencies: No dependencies

Developer action elements

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

Content and presentation elements

AGD_PRE.1.1C 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_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

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

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

5.2.4 Life-cycle support

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.

5.2.5 Tests

ATE_FUN.1 Functional testing
Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements

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

ATE_IND.1 Independent testing**:** conformance
Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements

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

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as

specified.

5.2.6 Vulnerability assessment

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

Security requirements rationale demonstrates that the SFRs described are suitable to satisfy the security objectives and consequently, appropriate to address the security problem.

5.3.1 Dependency of the SFRs

The following table shows dependency of security functional requirements.

[**Table 16**] **Dependency rationale**

No.	Security functional requirements	dependency	Reference standard
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.Time stamp
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	OE.DBMS
7	FAU_STG.4	FAU_STG.1	OE.DBMS
8	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	9, 11, 12, 13, 14
		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)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	8
		FCS_CKM.4	10
12	FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	8
		FCS_CKM.4	10
13	FCS_COP.1(3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	8
		FCS_CKM.4	10
14	FCS_COP.1(4)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	8
		FCS_CKM.4	10
15	FCS_COP.1(5)	-	-
16	FCS_RGB.1	-	-
17	FIA_AFL.1(1)	FIA_UAU.1	23
18	FIA_AFL.1(2)	FIA_UAU.1	24
19	FIA_IMA.1	-	-
20	FIA_SOS.1	-	-
21	FIA_SOS.2	-	-
22	FIA_SOS.3	FIA_SOS.2	21

23	FIA_UAU.2(1)	FIA_UID.1	28
24	FIA_UAU.2(2)	FIA_UID.1	29
25	FIA_UAU.4(1)	-	-
26	FIA_UAU.4(2)	-	-
27	FIA_UAU.7	FIA_UAU.1	23, 24
28	FIA_UID.2(1)	-	-
29	FIA_UID.2(2)	-	-
30	FMT_MOF.1	FMT_SMF.1	33
		FMT_SMR.1	34
31	FMT_MTD.1	FMT_SMF.1	33
		FMT_SMR.1	34
32	FMT_PWD.1	FMT_SMF.1	33
		FMT_SMR.1	34
33	FMT_SMF.1	-	-
34	FMT_SMR.1	FIA_UID.1	28, 29
35	FPT_ITT.1	-	-
36	FPT_PST.1	-	-
37	FPT_TST.1	-	-
38	FTA_MCS.2	FIA_UID.1	28, 29
39	FTA_SSL.5	FIA_UAU.1 or no dependencies	23, 24
40	FTA_TSE.1	-	-

FAU_GEN.1 has a dependency on FPT_STM.1. However, the TOE uses reliable time stamps provided in the TOE operational environment and accurately records audit data related to the operation of the TOE. Thus, the dependency of FAU_GEN.1 is satisfied by OE. Time Stamp, which is the security objective for the operational environment, on behalf of FPT_STM.1.

FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1. However, the TOE uses reliable DBMS provided in the TOE operational environment to store audit data related to the operation of the TOE and ensures that audit data are protected from unauthorized deletion or modification. Thus, the dependency of FAU_STG.3 and FAU_STG.4 is satisfied by OE.DBMS, which is the security objective for the operational environment, on behalf of FAU_STG.1.

FCS_COP.1(5) has a dependency on FCS_CKM.1 and FCS_CKM.4. However, the dependency of FCS_COP.1(5) is satisfied because there is no key generation and destruction due to the nature of hash algorithms.

FIA_AFL.1(1) has a dependency on FIA_UAU.1, which is satisfied by FIA_UAU.2(1) hierarchical to FIA_UAU.1.

FIA_AFL.1(2) has a dependency on FIA_UAU.1, which is satisfied by FIA_UAU.2(2) hierarchical to FIA_UAU.1.

FIA_UAU.2(1) has a dependency on FIA_UID.1, which is satisfied by FIA_UID.2(1) hierarchical to FIA_UID.1.

FIA_UAU.2(2) has a dependency on FIA_UID.1, which is satisfied by FIA_UID.2(2) hierarchical to FIA_UID.1.

FIA_UAU.7 has a dependency on FIA_UAU.1, which is satisfied by FIA_UAU.2(1) and FIA_UAU.2(2) hierarchical to FIA_UAU.1.

FMT_SMR.1 has a dependency on FIA_UID.1, which is satisfied by FIA_UID.2(1) and FIA_UID.2(2) hierarchical to FIA_UID.1.

FTA_MCS.2 has a dependency on FIA_UID.1, which is satisfied by FIA_UID.2(1) and FIA_UID.2(2) hierarchical to FIA_UID.1.

FTA_SSL.5 has a dependency on FIA_UAU.1, which is satisfied by FIA_UAU.2(1) and FIA_UAU.2(2) hierarchical to FIA_UAU.1.

5.3.2 Dependency rationale of security assurance requirements

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. However, 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

This chapter summarizes security functionality required by the TOE.

The table below is the list of security functions specified in the TOE summary specification.

[Table 1] Security functional requirements

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1	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_RGB.1(Extended)	Random bit generation
FIA	FIA_AFL.1(1)	Authentication failure handling(Administrator)
	FIA_AFL.1(2)	Authentication failure handling(End-user)
	FIA_IMA.1(Extended)	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.2(1)	Authenticated the user before all behavior (Administrator)
	FIA_UAU.2(2)	Authenticated the user before all behavior (End-user)
	FIA_UAU.4(1)	Single-use authentication mechanisms(Administrator)
	FIA_UAU.4(2)	Single-use authentication mechanisms(End-user)
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	Identification the user before all behavior (Administrator)
	FIA_UID.2(2)	Identification the user before all behavior (End-user)
FMT	FMT_MOF.1	Management of security functions behavior

	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF testing
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

6.1 Security audit

All the audit data generated during the operation of the TOE are collected by and stored in the SSO server.

As to auditable events of the TOE, audit data are generated regarding the start-up and the termination of the audit function, and "auditable events" and "additional audit records" in [Table 18] Auditable events.

[Table 18] Auditable events

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 distribution of key related to encryption/decryption of TSF data)	
FCS_CKM.4	Success and failure of the activity (applied only to destruction of key related to encryption/decryption of TSF data)	
FCS_COP.1(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)	
FCS_COP.1(2)	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)	
FCS_COP.1(3)	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)	
FCS_COP.1(4)	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)	
FCS_COP.1(5)	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(1)	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and subsequently, if appropriate, restoration to the normal state	
FIA_AFL.1(2)	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and subsequently, 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.2(1)	All use of the administrator authentication mechanism	
FIA_UAU.2(2)	All use of the end user authentication mechanism	
FIA_UAU.4(1)	Administrator single-use authentication mechanism	
FIA_UAU.4(2)	End user single-use authentication mechanism	
FIA_UID.2(1)	All use of the administrator identification mechanism	
FIA_UID.2(2)	All use of the end user identification mechanism	
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1(Extended)	All changes of the password	
FMT_SMF.1	Use of the management functions	

FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or executable code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5(Extended)	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

Audit data generated by the TOE record the date and time of an event, the type of an event, subject identity, an outcome (success or failure) of an event and further details.

The authorized administrator can review the audit data through the Web UI (Audit Information>Audit information View menu) and search the audit data according to the date and time of an event, the type of an event and an outcome of an event. Search results of the audit data are sorted and displayed in the descending order based on the time and date of events. The function of modifying/deleting the audit data is not provided.

If the storage where the audit data are stored exceeds the threshold defined by the administrator (define an integer number between 50 and 90, default value: 90, unit: %), a warning message is sent to the administrator via email. Also, if the audit data storage is full, the audited event data are ignored and a warning message is sent to the administrator via email.

Furthermore, a "security violation" in [Table 19] Actions against security violations below is detected and an "action" in [Table 19] Actions against security violations below is performed.

[Table 19] Actions against security violations

Security functional component	Security violation	Action
FIA_UAU.2(1)	- In case administrator authentication attempts fail consecutively for a defined number of times (default value: 5 times)	- Inactivate the authentication function for a defined period of time (default value: 5 minutes) - Send a warning message email to the authorized administrator
FIA_UAU.2(2)	- In case end user authentication attempts fail	- Inactivate the authentication

	consecutively for a defined number of times (default value: 5 times)	function until the authorized administrator unlock the account
FPT_TST.1	- In case the integrity verification fails - In case a self test of the validated cryptographic module fails	- Send a warning message email to the authorized administrator
FAU_STG.3	- In case the audit trail exceeds the threshold (default value: 90%)	- Send a warning message email to the authorized administrator
FAU_STG.4	- In case the audit trail is full	- Ignore an audited event - Send a warning message email to the authorized administrator

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

6.2 Cryptographic support

The TOE uses [Table 20] the validated cryptographic module used by the TOE, and generates/distributes cryptographic keys and performs cryptographic operations in accordance with a cryptographic algorithm and a cryptographic key size specified in [Table 21] List of TOE cryptographic algorithm standards. In addition, it generates random bits required to generate a cryptographic key using a specified random bit generator that meets [Table 21] List of TOE cryptographic algorithm standards.

[Table 20] TOE Use a validated cryptographic module

Encryption module name	Validation number	Developer	Validation date
MagicJCrypto V2.0.0.0	CM-131-2022.10	Dreamsecurity Co.,Ltd.	2017-10-16

[Table 21] TOE List of Cryptographic Algorithms Standards

Classification	Cryptographic algorithm	Encryption key length	Reference standard
Symmetric Key Cipher	SEED/CBC	128 Bit	TTAS.KO-12.0004
Secure hash algorithm	SHA-256	-	FIPS 180-2
Message authentication code	HMAC (SHA-256)	256 Bit	FIPS 198
Public key cipher	RSAES (SHA-256)	Public key 2048 Bit	PKCS #1 v2.1
Digital signatures	RSA-PSS (SHA-256)	Public key 2048 Bit	PKCS #1 v2.1
Random bit generation	HASH_DRBG (SHA-256)	-	ISO/IEC 18031

The TOE generates a cryptographic key when performing "the function of cryptographic key

generation" in the following [Table 22] List of cryptographic key generation standards, and generates a cryptographic key in accordance with "cryptographic algorithm" and "cryptographic key size" specified in [Table 22] List of cryptographic key generation standards.

[Table 22] List of Cryptographic Key Generation Standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
KEK (Key Encrypt Key)	HMAC (SHA-256)	128 bit	FIPS 198
DEK (Data Encrypt Key)	HASH_DRBG (SHA-256)	128 bit	ISO/IEC 18031
Authentication token encrypting/decrypting key	HASH_DRBG (SHA-256)	128 bit	ISO/IEC 18031
Transmission information encrypting/decrypting key	HASH_DRBG (SHA-256)	128 bit	ISO/IEC 18031
Server Certificate Public / Private Key Pair for Cryptography	HASH_DRBG (SHA-256)	Public key 2048 bit	ISO/IEC 18031
Server certificate public / private key pair for Signing	HASH_DRBG (SHA-256)	Public key 2048 bit	ISO/IEC 18031

The TOE generates random bits in accordance with the "reference standard" in the following [Table 23] List of random bit generation standards, and generates random bits required to generate a cryptographic key.

[Table 23] Random Bit Generation Standard List

Purpose	Cryptographic algorithm	Encryption key length	Reference standard
Random bit generation	HASH_DRBG (SHA-256)	-	ISO/IEC 18031

The TOE distributes a cryptographic key when performing "the function of cryptographic key distribution" in the following [Table 24] List of cryptographic key distribution standards and distributes a cryptographic key in accordance with the "reference standard" specified in [Table 24] List of cryptographic key distribution standards.

[Table 24] List of cryptographic key distribution standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Public key cryptography	RSAES (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Cryptographic key distribution method			
- Distribution by encrypting an encryption key for the information transmitted between the SSO server and the SSO agent with the public key of the counterpart server			

The TOE destroys a cryptographic key when performing "the function of cryptographic key destruction" in the following [Table 25] List of cryptographic key destruction standards and destroys a cryptographic key in accordance with the "reference standard" specified in [Table 25] List of cryptographic key destruction standards.

[Table 25] List of cryptographic key destruction standards

Usage	Method	Cryptographic key size	Reference standard
Cryptographic key destruction	Overwriting with '0' (0x30)	-	-
Function of cryptographic key destruction			
- Destruction of a symmetric key used for KEK (Key Encrypt Key) (upon the termination of the TOE) - Destruction of a symmetric key used for DEK (Data Encrypt Key) (upon the termination of the TOE) - Destruction of a symmetric key used for encryption of authentication tokens (upon end user logout) - Destruction of a symmetric key used for encryption of the information transmitted between the SSO server and the SSO agent (upon the completion of the encrypted transmission, upon the completion of the decryption after the reception)			

The TOE performs cryptographic operations for a symmetric key when performing "the function of cryptographic operation" in the following [Table 26] List of cryptographic operation standards for symmetric key, and performs cryptographic operations for a symmetric key in accordance with "cryptographic algorithm" and "cryptographic key size" specified in [Table 26] List of cryptographic operation standards for symmetric key.

[Table 26] List of cryptographic operation standards for symmetric key

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Block cipher (symmetric key cryptography)	SEED/CBC	128 bits	TTAS.KO-12.0004
Function of cryptographic operation			
- Encryption/decryption of DEK (Data Encrypt Key) - Encryption/decryption of TSF data - Encryption/decryption of authentication tokens - Encryption/decryption of the information transmitted between the SSO server and the SSO agent			

The TOE performs cryptographic operations for digital signature when performing "the function of cryptographic operation" in the following [Table 27] List of cryptographic operation standards for

digital signature, and performs cryptographic operations for digital signature in accordance with "cryptographic algorithm" and "cryptographic key size" specified in [Table 27] List of cryptographic operation standards for digital signature.

[Table 27] List of cryptographic operation standards for digital signature

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Digital signature	RSA-PSS (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Function of cryptographic operation			
- Digital signature/verification of the information transmitted between the SSO server and the SSO agent			

The TOE performs cryptographic operations for MAC when performing "the function of cryptographic operation" in the following [Table 28] List of cryptographic operation standards for MAC, and performs cryptographic operations for MAC in accordance with "cryptographic algorithm" and "cryptographic key size" specified in [Table 28] List of cryptographic operation standards for MAC.

[Table 28] List of cryptographic operation standards for MAC

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Message authentication code	HMAC (SHA-256)	256 bits	FIPS 198
Function of cryptographic operation			
- Integrity verification of the TOE			

The TOE performs cryptographic operations for public keys when performing "the function of cryptographic operation" in the following [Table 29] List of cryptographic operation standards for public key, and performs cryptographic operations for public keys in accordance with "cryptographic algorithm" and "cryptographic key size" specified in [Table 29] List of cryptographic operation standards for public key.

[Table 29] List of cryptographic operation standards for public key

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Public key cryptography	RSAES (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Function of cryptographic operation			
- Encryption of a symmetric key used for encryption of authentication tokens			

- Encryption of a symmetric key used for encryption of the information transmitted between the SSO server and the SSO agent

The TOE performs hash operations when performing "the function of cryptographic operation" in the following [Table 30] List of hash operation standards, and performs hash operations in accordance with "cryptographic algorithm" and "cryptographic key size" specified in [Table 30] List of hash operation standards.

[Table 30] List of hash operation standards

Usage	Cryptographic algorithm	Cryptographic key size	Reference standard
Hash	SHA-256	-	FIPS 180-2
Function of cryptographic operation			
- Integrity verification of authentication tokens - Integrity verification of TSF data - Encryption of administrator and end user passwords			

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

The TOE performs mutual authentication for the mutual authentication between the SSO server and the SSO agent by using a server certificate as specified in [Table 31] Mutual authentication mechanism.

[Table 31] Mutual authentication mechanism

Classification	Cryptographic algorithm	Cryptographic key size	Reference standard
Digital signature/verification	RSA-PSS (SHA-256)	Public key 2048 bits	PKCS #1 v2.1
Mutual authentication mechanism			
- When transmitting authentication request information from the SSO agent to the SSO server a) The SSO agent generates a digital signature with the private key of the SSO agent b) The SSO server verifies the digital signature with the public key of the SSO agent - When transmitting authentication information from the SSO server to the SSO agent a) The SSO server generates a digital signature with the private key of the SSO server b) The SSO agent verifies the digital signature with the public key of the SSO server			

In the TOE, the identification and authentication of the administrator are performed at the same time. The information provided through the screen GUI for identification/authentication of the administrator is ID and password, which are used to identify/authenticate the administrator. An action that can be taken before the administrator is identified/authenticated is communication check. The administrator can manage the security functions after the administrator is successfully identified/authenticated.

After the last successful authentication of the administrator, if authentication attempts fail consecutively for a specified number of times defined by the administrator (default value: 5 times), the TOE inactivates the authentication function and access is denied for a specified period of time for authentication delay defined by the administrator (default value: 5 minutes). Then, a warning email is sent to the authorized administrator.

In the TOE, the identification and authentication of the end user are performed at the same time. The information provided through the screen GUI for identification/authentication of the end user is ID and password, which are used to identify/authenticate the end user. An action that can be taken before the end user is identified/authenticated is mutual authentication between the SSO server and the SSO agent.

After the last successful authentication of the end user, if authentication attempts fail consecutively for a specified number of times defined by the administrator (default value: 5 times), the TOE inactivates the authentication function and access is denied until the administrator unlocks the account.

During the creation/change of administrator passwords and during the change of end user passwords, the TOE provides a mechanism to verify that the password information meets the following defined quality metric.

- Valid characters: English alphabet (a~z, A~Z), number (0~9), special character (!, @, #, $, %, ^, *, +, =, -)
- Combination rules: Combination of all three types of characters
- Valid length: 9 – 16 digits

After the end user is successfully identified/authenticated, the TOE provides a mechanism to generate an authentication token that meets the following standard. When generating an authentication token, server time information that indicates the uniqueness is encrypted.

- Subject that generates an authentication token: SSO server

- Authentication token components: User ID, user name, user IP, authentication time (time stamp), integrity value
- Cryptographic algorithm of an authentication token: Refer to the algorithm in [Table 26] List of cryptographic operation standards for symmetric key
- Integrity algorithm of an authentication token: Refer to the algorithm in [Table 28] List of cryptographic operation standards for MAC

The TOE uses a validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP).

- Cryptographic module name: MagicJCrypto V2.0.0.0
- Validation number: CM-131-2022.10
- Validation date: Oct. 16, 2017

The TOE destroys an authentication token loaded in the memory upon the termination of the end user session. It destroys an authentication token by overwriting it with "0."

The TOE prevents the reuse of authentication data related to the access session information of the authorized administrator, as well as the reuse of authentication data related to the information on the access session and authentication token generation of the end user.

The TOE provides the following feedback while the administrator/end user authentication is in progress.

- Secrets (passwords) being entered are masked (character "●")
- In case of failed authentication, feedback on the reason for the failure is not provided but feedback is provided with the statement, "authentication failed"

Relevant SFR : FIA_AFL.1(1), FIA_AFL.1(2), FIA_IMA.1, FIA_SOS.1, FIA_SOS.2, FIA_SOS.3, FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.4(1), FIA_UAU.4(2), FIA_UAU.7, FIA_UID.2(1) , FIA_UID.2(2)

6.4 Security management

The TOE provides the authorized administrator with the following [Table 32] List of security functions and [Table 31] List of TSF data. The authorized super administrator can manage all security functions and the TOE restricts the management function of the authorized monitoring administrator to the monitoring of audit information.

[Table 32] List of security functions behavior

List of functions	Management behavior	Authorized administrator
Audit information viewing	Determine behaviors	Super administrator, monitoring administrator
Module verification in real time	Determine, modify behaviors	Super administrator
Audit information setting	Determine, modify behaviors	Super administrator
Mail notification setting	Determine, modify behaviors	Super administrator
User unlocking	Determine, modify behaviors	Super administrator
User policy establishment	Determine, modify behaviors	Super administrator
Administrator management	Determine, modify behaviors	Super administrator
Administrator policy establishment	Determine, modify behaviors	Super administrator
Administrator password change	Determine, modify behaviors	Super administrator, monitoring administrator

[Table 33] List of TSF data

List of functions	Management	Authorized administrator
Audit information	Query	Super administrator, monitoring administrator
Audit storage capacity threshold	Query, modify	Super administrator
Cycle of integrity verification of cryptographic module and SSO module	Query, modify	Super administrator
Mail server information	Query, modify	Super administrator
Mail sending information	Query, modify	Super administrator
User policy information	Query, modify	Super administrator
Administrator information	Query, modify	Super administrator
Administrator policy establishment	Query, modify	Super administrator

The TOE provides the function of password change when the authorized administrator accesses for the first time, and the password rules are as follows. Only the authorized administrator is authorized to generate and change IDs and passwords of the administrator and end users.

- Password combination rules and length: 9-16 digits that combine all three types of English alphabet / number / special character
- Valid character: English alphabet (a~z, A~Z), number (0~9), special character (!, @, #, $, %, ^, *, +, =, -)

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

6.5 Protection of the TSF

The cryptographic communication of the TOE in transmitting data between the SSO server and the SSO agent is as follows:

a) A symmetric key for data encryption is generated (algorithm: SEED/CBC/128) and the data are encrypted.
b) The generated symmetric key is encrypted with the counterpart's public key (algorithm: RSAES (SHA-256)) and transmitted together with the encrypted data.
c) The counterpart uses the private key to decrypt the encrypted symmetric key (algorithm: RSAES (SHA-256)) and decrypts the transmitted data with the symmetric key (algorithm: SEED/CBC/128).

The TSF data stored in the TOE are encrypted with "cryptographic key" and "cryptographic algorithm" in the following [Table 34] TSF data protection method, thereby being protected from unauthorized disclosure and modification. A derived key used in the TOE is derived by the password-based key derivation method. The derivation method generates a key by using the password-based key derivation function 2 (PBKDF2) defined in PKCS#5.

[Table 34] How to protect TSF data

Component	Encryption Target	Encryption Key	Encryption algorithm	Storage location
SSO Server	Master Key (DEK)	Derived Key (KEK)	SEED/CBC/128	File
	Certification Private Key Password	Master Key (DEK)	SEED/CBC/128	File
	DBMS Account Information	Master Key (DEK)	SEED/CBC/128	File
	Administrator Password	-	SHA-256	DBMS
	End-user Password	-	SHA-256	DBMS
	Authentication Token	Generated Encryption Key	SEED/CBC/128	Memory
	Certification Information	Generated Encryption Key	SEED/CBC/128	Memory
	Policy Setting Information	Master Key (DEK)	SEED/CBC/128	DBMS
	Preferences Information	Master Key (DEK)	SEED/CBC/128	File
	Transmission Information Encryption Symmetric Key	Public Key	RSAES(SHA-256)	Memory
	Authentication Token Encryption Symmetric Key	Public Key	RSAES(SHA-256)	Memory
SSO Agent	Master Key (DEK)	Derived Key (KEK)	SEED/CBC/128	File
	Certification Private Key	Master Key (DEK)	SEED/CBC/128	File

	Password			
	Authentication Token	Generated Encryption Key	SEED/CBC/128	Memory
	Certification Request Information	Generated Encryption Key	SEED/CBC/128	Memory
	Preferences Information	Master Key (DEK)	SEED/CBC/128	File
	Transmission Information Encryption Symmetric Key	Public Key	RSAES(SHA-256)	Memory
	Authentication Token Encryption Symmetric Key	Public Key	RSAES(SHA-256)	Memory

The TOE provides the function of self tests during initial start-up, periodically during normal operation (select among what minute on an hourly basis, what time on a daily basis and what date on a monthly basis. Default value: 8:00 on a daily basis), and upon request of the administrator. The TOE is operated, being loaded on the Web Application Server. Therefore, self tests are determined based on whether or not there is a Web Application Server process. If a self test fails, a warning message email is sent to the administrator.

The TOE provides the function of integrity verification during initial start-up, periodically during normal operation (select among what minute on an hourly basis, what time on a daily basis and what date on a monthly basis. Default value: 8:00 on a daily basis), and upon request of the administrator. The validated cryptographic module, TOE executable codes and TOE configuration files are subject to the integrity verification. The integrity verification is performed by using the following [Table 35] TSF integrity test methods. If the integrity verification fails, a warning message email is sent to the administrator.

[Table 35] TSF Integrity Testing Method

Component	Integrity Verification Target	Test algorithm	Reference standard
SSO Server	Validated cryptographic modules	Self-test	-
	Executable code	HMAC (SHA-256)	FIPS 198
	Configuration file	HMAC (SHA-256)	FIPS 198
SSO Agent	Validated cryptographic modules	Self-test	-
	Executable code	HMAC (SHA-256)	FIPS 198
	Configuration file	HMAC (SHA-256)	FIPS 198

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

6.6 TOE access

The TOE limits the maximum number of concurrent sessions of management access by the administrator that belong to the same administrator to one. Also, the concurrent establishment of management access session and local access session that belong to the same administrator is prohibited.

The TOE blocks new access if the administrator makes management access in one terminal and then tries to log in with the same account or the same privilege in a different terminal.

An access session by the administrator/end user is terminated after a specified time period of user inactivity (positive integer number between 3 and 10 configurable by the administrator default value: 10 minutes).

As to management access by the administrator, any access by IPs other than access IPs configurable by an administrator (default value: 2 IPs) is denied.

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