TOUCHEN Wiseaccess v1.4

Security Target

The Security Target related to the certified TOE. This Security Target is written in Korean and translated from Korean into English.

RAON SECURE

Revision History

Configuration document no.	Detail	Data	Created by
v1.4.0	Initial Registration	2022-06-10	RAONSECURE Co., Ltd.
v1.4.1	Modification of security requirements	2023-01-25	RAONSECURE Co., Ltd.
v1.4.2	SFR change	2023-04-24	RAONSECURE Co., Ltd.
v1.4.3	Operating environment version update	2023-05-08	RAONSECURE Co., Ltd.
v1.4.4	Modify Overview	2023-05-31	RAONSECURE Co., Ltd.

Contents

1. ST Introduction

1.1 ST reference

Item	Specification
Title	TouchEn Wiseaccess v1.4 Security Target
Document Identification	wiseaccess-D-ST v1.4.4
Version	v1.4.4
Publication Date	2023-05-31
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	v3.1 R5
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Author	RAONSECURE Co., Ltd.
Keywords	integrated authentication, SSO(Single Sign-On), single authentication, Authentication token

1.2 TOE reference

Item		Specification
TOE		TouchEn Wiseaccess v1.4
Version		v1.4.4.3
Components	SSO Server	· TouchEn Wiseaccess v1.4 Server v1.4.4.3 : wiseaccess_server_v1.4.4.3_linux.tar.gz
	SSO Agent	· TouchEn Wiseaccess v1.4 Agent v1.4.4.3 : wiseaccess_agent_v1.4.4.3_linux.tar.gz
	Manual	· TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3 : TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3.pdf · TouchEn Wiseaccess v1.4 API Manual v1.4.2 : TouchEn Wiseaccess v1.4 API Manual v1.4.2.pdf · TouchEn Wiseaccess v1.4 Installation Guide v1.4.3 : TouchEn Wiseaccess v1.4 Installation Guide v1.4.3.pdf
Developer		RAONSECURE Co., Ltd.

1.3 TOE overview

This Security Target defines the security functional requirements and assurance requirements of TouchEn Wiseaccess v1.4 which provides services for End user with Single Sign-On.

TouchEn Wiseaccess v1.4 (hereinafter referred to as "TOE") provides the ID/PW based user log-in

function and issues an authentication token when a user initially attempts to log in. The TOE issues a token during user log-in, and verify the issued token if accessing another business system after user log-in.
The TOE sets the ID and PW policy for identifying and authenticating End User. It also manages various business systems by registering services. The TOE provides separate access by business system to control the single authentication function. To do so, an issued/saved/validated/discarded authentication token must use a validated cryptographic module whose security and implementation conformance are validated by the Korean Cryptographic Module Validation Program (KCMVP).

The TOE uses the following validated cryptographic modules.

Item	Specification
cryptographic module name	Key# Crypto V1.5
Developer	RAONSECURE Co., Ltd.
verification date	2022-11-02
expiration date	2027-11-02
verification number	CM-220-2027.11

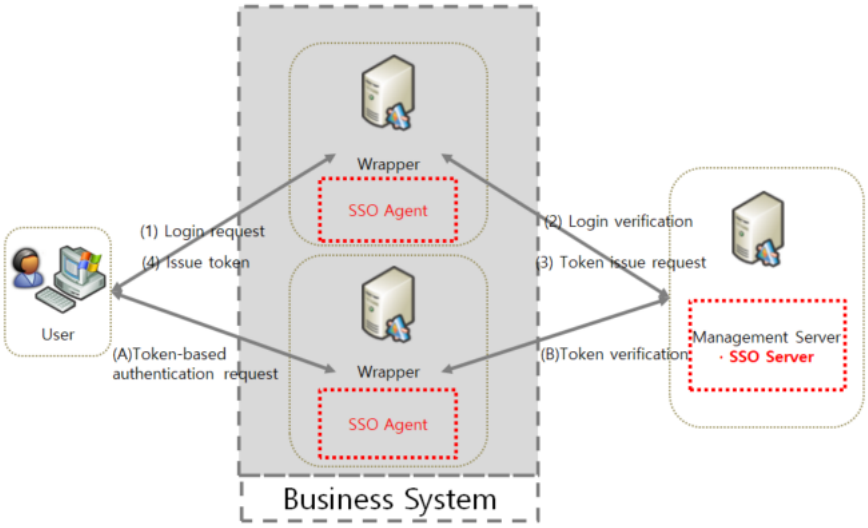
The TOE provides the security audit function that records and manages critical events as audit data when activating the security functionality and management function, function of protecting the data that stored in the TSF controlled repository, and TSF protection function such as TSF self-testing. In 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 behavior 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 requires integrity protection.

For End User identification and authentication process, it has two phases; the initial authentication phase using the ID and PW; the token-based authentication phase that accesses the business system using the token issued during the initial authentication procedure.
The initial authentication process is as follows.
The user requests log-in using the ID/PW, and the SSO Agent that receives the log-in request message sends a log-in verification request to the SSO Server to check the authorized user status. The SSO Server performs log-in verification using the user information stored in the DBMS. The

SSO Server requests token issue to the SSO Agent if the log-in verification result is valid.
The SSO Agent issues the authentication token accordingly.

The token-based authentication phase is performed only when the toke has been normally issued in the initial authentication phase. When an End User uses business system services, the SSO Agent verifies the validity of the token and decides the access accordingly.

- Authentication Token Issuer: SSO Agent
- Authentication token storage location: User PC
- Authentication token verification subject: SSO Agent



[Figure 1] end-user identification and authentication process

Authentication Phase	Operation Procedure
Initial authentication	(1) Login request -> (2) Login verification -> (3) Token issue request -> (4) Issue token
Token-based authentication	(A) Token-based authentication request -> (B) Token verification

[Table 1] Authentication step operation procedure

The TOE is an 'integrated authentication' solution which allows an End User to access to various business systems with a single log-in. SSO Agent is a combination of the 'API type' composed of the library file and the 'process type' composed of the executable file.

The TOE is composed of the SSO Server that manages security and the SSO Agent that is installed

in a business system.

▣ SSO Server

Check the integrity when running a SSO Server. Perform identification and authentication when the administrator attempts to log-in and perform the authentication failure correspondence function accordingly. Limit the number of concurrent sessions to one to access to the security management view via web browser.

Manage organization, service and configuration for the security function management.

The authorized administrator set an organization and authorization for service usage, and sets the ID/PW policy applied to users in the organization.

Set a threshold to protect the audit data storage and notification on potential security violations. Calculate the disk capacity where DBMS is installed, and create an event when exceeding the threshold (warning notification, delete past records) or failing audit storage and generate an audit log.

Encrypt a channel for mutual authentication and security communications between the SSO Server and the SSO Agent and transfer the data between the SSO Server and the SSO Agent via secure links.

The SSO Server identifies and authenticates the end-user with the user's authentication information (ID/password) when getting the request of identification and authentication attempts from the end-user.

After successfully authenticating the end-user with the authentication information, request the SSO Server to generate the session to generate the authentication token of the SSO Agent. Send the needed information(such as Token ID, user ID, token generation time, expiration date, etc.) for authentication token generation.

When the SSO Agent requests session generation, generate the session for the requested end-user and check duplication log-in. TokenID is generated when generating the session.

▣ SSO Agent

The SSO Agent installed in the business system verifies the authentication token when authenticating the user.

If there is no authentication token information during user's initial log-in attempt, get the information for authentication token generation (such as Token ID, user ID, token generation time, expiration date, etc.) from the SSO Server and generate the authentication token. Send the authentication token to the business system via the SSO Agent.

When calling the SSO Agent function from the business system, get the authentication

information of the user, the authentication token information or the authentication result (success/failure).

The requirements for hardware, software and operating system to install the TOE are as in the following.

• The requirements for hardware, software and operating system to install the TOE

1) SSO Server

Item		Specification
Hardware	CPU RAM	· Intel(R) Xeon(R) 2.8GHz or higher · 8GB or higher
	HDD	· Space required for TOE installation is 1GB or higher
	NIC	· 100/1000 Ethernet Port x 1EA or higher
Software	OS	· Oracle Linux 8.7 (64bit) (Kernel 5.15.0)
	DBMS	· MySQL 8.0.33
	Etc.	· Apache Tomcat 8.5.88 (64bit)
		· OpenJDK 1.8.0_372 (64bit)

2) Managed PC

Item	Specification
Software	· Chrome 112.0

3) SSO Agent

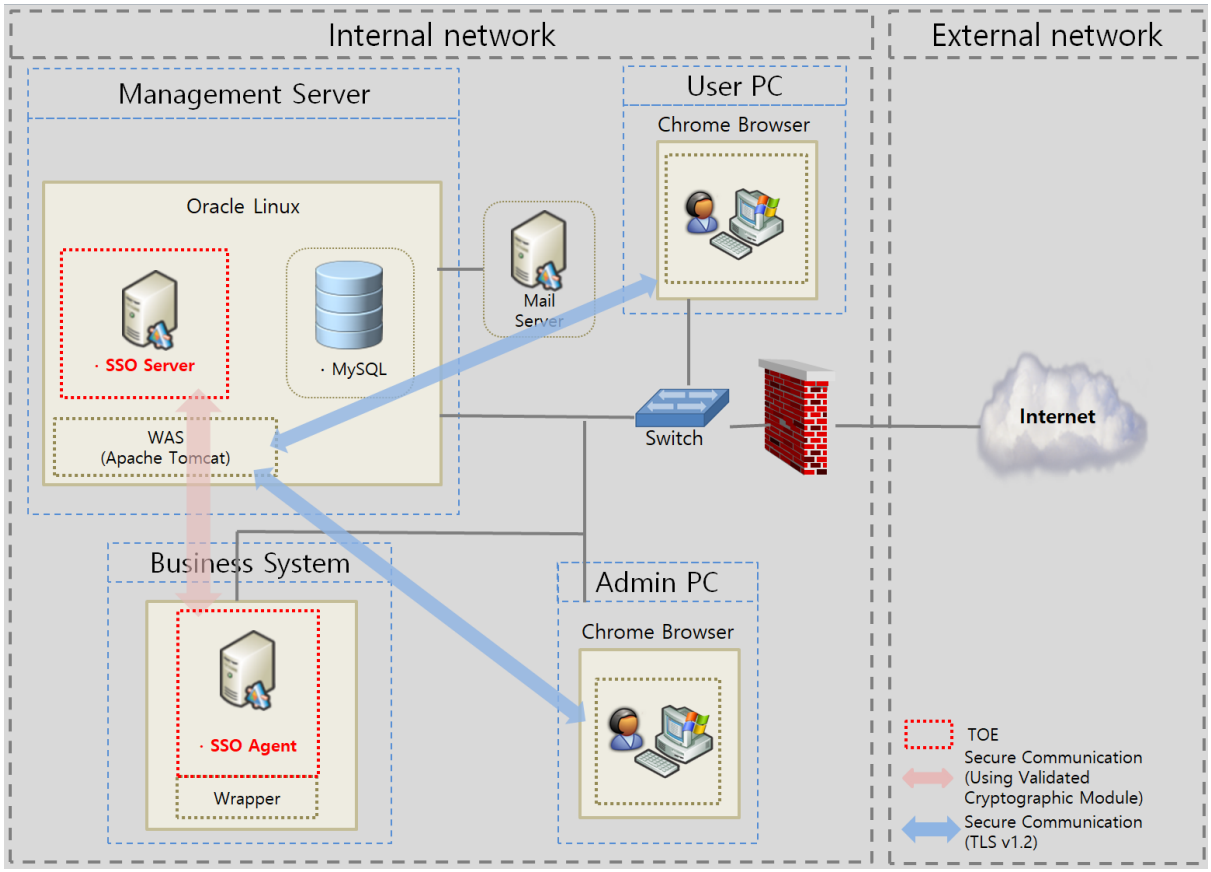
Item		Specification
Hardware	CPU	· Intel(R) Xeon(R) 2.8GHz or higher
	RAM	· 8GB or higher
	HDD	· Space required for TOE installation is 1GB or higher
	NIC	· 100/1000 Ethernet Port x 1EA or higher
Software	OS	· Oracle Linux 8.7 (64bit) (Kernel 5.15.0)
	Etc.	· Apache Tomcat 8.5.88(64bit)
		· OpenJDK 1.8.0_372 (64bit)

4) External Entity

Item	Specification
Mail Server	Sends an e-mail about potential security violations to the authorized administrator on the designated receiving side

	from the SSO server.

[Figure 2] shows the operational environment where the TOE is operated.



[Figure 2] Operational environment of the TOE

The operational environment of the TOE is composed of the SSO server that is installed in the management server and the SSO Agent that is installed in the business system.
The TOE is provided in software form.
The SSO Server is installed in the form of a process composed of executable files on the management server to perform security management, and the SSO Agent is installed in the form of a library module and process in each business system to perform functions such as issuance and verification of authentication tokens.

The SSO Server performs the security management of the TOE via web browser which supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). A Wrapper is used for compatibility with various business systems, out of the TOE scope.

▣ DBMS(MySQL)

MySQL, an open source relational database management system, is installed in the DBMS. When

SSO Server requests data inquiry/modification using arbitrary conditions, TSF data and audit data stored in the DBMS are searched, sorted, ordered, and statistically processed.

▣ Web Server (Apache Tomcat)

It is used to provide web-based management functions through a web browser.

▣ Tomcat Encryption Function

The authorized administrator communicates using the SSO Server which is run on Apache Tomcat that supports HTTPS protocol and browser.

- Confidentiality : AES 128 bit
- Integrity : SHA 256 bit
- Key exchange : RSA 2048 bit

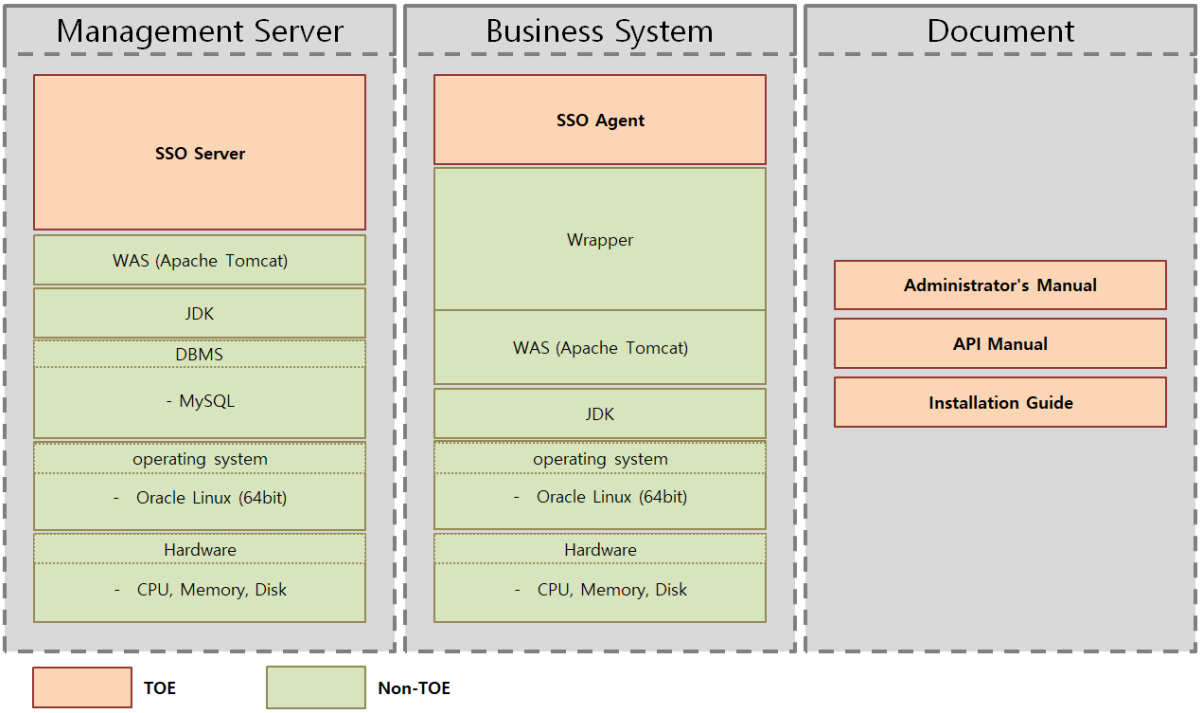
1.4 TOE description

In this part, the physical scope of the TOE such as TOE components, hardware, software, firmware and guidelines are described and security features provided by the TOE are explained in detail in the logical scope of the TOE.

1.4.1 Physical scope

The physical scope of the TOE consists of the SSO Server, SSO Agent and manuals(Administrator manual, API manual, Installation guidance). Verified Cryptographic Module(Key# Crypto V1.5) is embedded in the TOE components.

Hardware, OS, DBMS, WAS, JDK and Wrapper are out of the physical TOE scope.

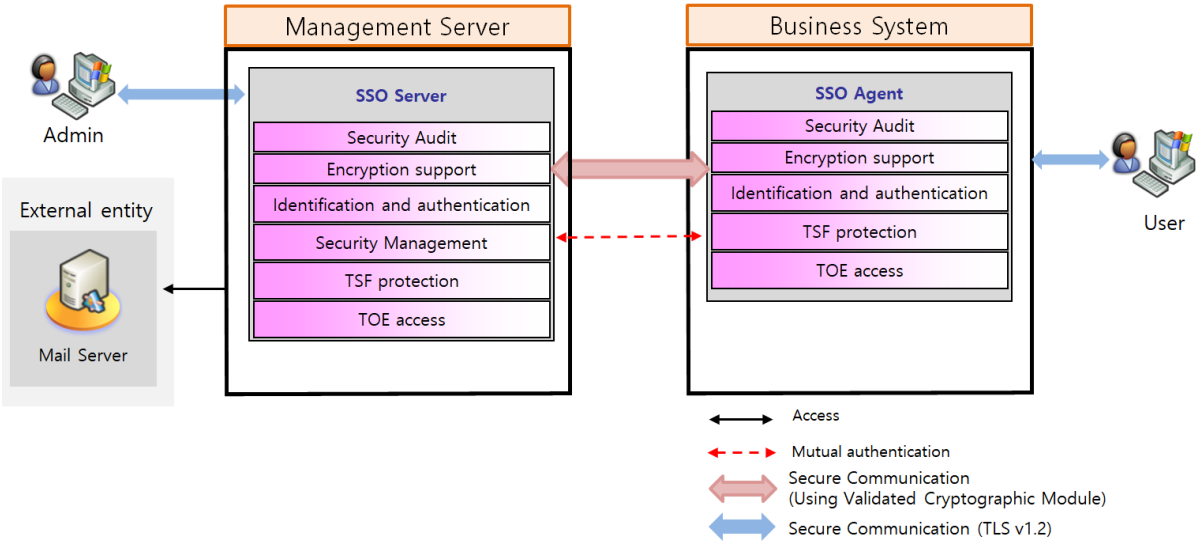


[Figure 3] Physical scope of the TOE

Type	Detail	Distribution Type
SSO Server	· TouchEn Wiseaccess 1.4 Server v1.4.4.3 : wiseaccess_server_v1.4.4.3_linux.tart.gz	CD-ROM
SSO Agent	· TouchEn Wiseaccess v1.4 Agent v1.4.4.3 : wiseaccess_agent_v1.4.4.3_linux.tar.gz	
Manual	· TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3 : TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3.pdf · TouchEn Wiseaccess v1.4 API Manual v1.4.2 : TouchEn Wiseaccess v1.4 API Manual v1.4.2.pdf · TouchEn Wiseaccess v1.4 Installation Guide v1.4.3 : TouchEn Wiseaccess v1.4 Installation Guide v1.4.3.pdf	

1.4.2 Logical scpoe

The logical scope of the TOE is as in [Figure 4] below.



[Figure 4] Logical scope of the TOE

Includes logical scopes in each module.

▣ Security Audit

[SSO Server]

SSO Server manages the TSF data from browser and generates the audit data on security management. Generate the audit data about management and security setting, information change of the TSF data, identification and authentication, integrity test, start/termination of the audit function and security violation.

The TOE corresponds to security violations and mutual authentication between the SSO Server and SSO Agent. Generate the audit data about cryptographic key management, integrity test and start/termination of the audit function accordingly.

The audit data includes log generation time, identity of the subject, result of the event (success or failure), type of the event and additional audit data.

The audit data is stored in the DBMS. The audit data is provided in a manner suitable for the authorized administrator. Protect the data from unauthorized users to delete.

Only the top-level administrator can search the audit data.

SSO Server shall periodically check audit data storage according to the setting and send a warning email to the administrator when the audit data storage exceeds the threshold. Delete the past records in the DBMS if the past records exceed the deletion threshold.

In addition, perform corresponding actions (send a warning email to the authorized administrator) on security violations (self-test failure of the validated cryptographic module 'Key# Crypto V1.5', exceed the audit storage, self-verification and integrity test failure of the SSO Server and the SSO Agent, the audit storage failure, exceeding the number of authentication failures (administrator/end-user)).

[SSO Agent]

SSO Agent generates the audit data about the mutual authentication between the SSO Agent and the SSO Server, authentication token generation/operation/destruction using the cryptographic key, cryptographic key management, integrity test and start/termination of the audit function.

The audit data includes log generation time, subject's identity, event result (success or failure), items about event type and additional audit data.

▣ Cryptographic support

[SSO Server]

SSO Server generates random numbers with the RBG for mutual authentication and verifies signature with the digital signature algorithm. After completing mutual authentication, distribute cryptographic key to the SSO Agent. Use Key# Crypto V1.5, a validated cryptographic module. Do not save the encryption key but destory it.

[SSO Agent]

SSO Agent generates random bits with the RBG for mutual authentication with the SSO Server. During mutual authentication, user the digital signature algorithm to perform signature verification. After mutual authentication, use the symmetric algorithm and the MAC algorithm to generate and manage the authentication token. Use the validated cryptographic module, Key# Crypto V1.5, as a cryptographic algorithm. Do not save the encryption key but destory it.

▣ Identification and authentication

[SSO Server]

Identify the administrator with ID when attempting identification and authentication, and perform administrator authentication before all the actions. Present the password with '•' to prevent the password from being exposed by providing the information of authentication failure reason.

SSO Server provides the function to prevent reuse of authentication information related to the administrator.

Set administrator's password according to the password rule. If identification and authentication succeeds, the administrator maintains the security management authority.

If the number of authentication attempts via the SSO Server exceeds the allowed number of authentication failures (5 times), lock the account for 10 minutes as the administrator sets.

Perform mutual authentication via implemented protocol for safe communication among TOE components.

[SSO Agent]

SSO Agent identifies the end-user with ID when the end-user initially attempts to identify and

authenticate. Perform the end-user authentication before all the actions. Present the password as '•' to prevent the password from being exposed by providing the information of authentication failure.

After completing the initial identification and authentication of end user, issue an authentication token depending on the implementation and performs identification and authentication with the authentication token. Onetime Token prevents the authentication from being reused. Do not save the authentication token but destroy it

If the end-user exceeds the allowed number of authentication failures (5 times), lock the end-user's account for the set time interval of user lock.

▣ Security management

[SSO Server]

Conduct security management via SSO Server.

Set security policy for single authentication with organization/service.

Forced to change the password when the authorized administrator accesses for the first time to the security management interface.

There is only top-level administrator who can set and perform all the policy of security management functions.

▣ Protection of the TSF

[SSO Server]

SSO Server shall protect the TSF data stored within containers controlled by the TSF and transferred between the TOE components. Run TSF testing to check major security function process. SSO Server shall run self-test for major processes and ensure the integrity of the TOE configuration files and major process periodically during initial start-up and operation. If integrity is compromised, send a warming email to the administrator.

SSO Server safely store and manage the authentication information of end user and administrator in the DBMS.

[SSO Agent]

When transmitting data between separate parts of the TOE, protects the data from disclosure and modification using the secure channel. Check integrity periodically.

SSO Agent shall protect the TSF data stored within containers controlled by the TSF and transferred between the TOE components. Run TSF testing to check major security function process. The TOE shall run self-test for major processes and ensure the integrity of the TOE configuration files and major process periodically during initial start-up and operation. If integrity is compromised, send a warming email to the administrator.

The authentication token is temporarily saved in the user's PC memory and destructed

immediately right after the use.

▣ TOE Access

[SSO Server]

For the time interval of SSO Server inactivity, the administrator performs the automated termination of sessions function. In order to reuse, reauthentication is required.

In addition, limit the maximum number of session connection for the administrator session of security management to 1 to avoid duplication log-in. After the authorized administrator logs in, another administrator PC performs a log-in with the same account, the previous connection will be terminated.

Able to set the allowed IP addresses for administrator to 2. Output 'Access Denied Error!' when accessing from an IP not in the allowed list.

[SSO Agent]

After the end-user's identification and authentication, terminates the session when the idle time of authentication token exceeds. Re-authenticate the user and perform identification and authentication.

1.5 Operation

This security Target objectives uses English for some abbreviations and clear meaning. The notation, form and preparation rules used follow the common evaluation criteria.

Iteration

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

Assignment

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

Selection

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

Refinement

This is used to add details and thus further restrict a requirement. The result of refinement is

shown in **bold text.**

1.6 Terms and definitions

Terms used in this PP, which are the same as in the CC, must follow those in the CC.

Term	Description
API (Application Programming Interface)	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, hash function, 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-user access through 'integrated authentication'.
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)
DBMS (Database Management System)	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 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.
Encryption key	Values to encrypt and decrypt an authentication token.
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 rigor.
Identity	Representation uniquely identifying authorized users. It can be user's real name, nickname or false name.
Iteration	Use of the same component to express two or more distinct requirements.
Kerberos	A centralized authentication scheme, described in RFC 1510, that provides user authentication using symmetric cryptographic technique in a distributed computing environment.
Korea Cryptographic Module Validation Program (KCMVP)	A system to validate the security and implementation conformance of cryptographic modules used for protection of important but not classified information among the data communicated through the

	information and communication network of the government and public institutions.
Management access	The access to the TOE by using the HTTPS, SSH, TLS, etc. to manage the TOE by administrator, remotely.
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, 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.
RADIUS (Remote Authentication Dial-In User Services)	Service to identify and authenticate users by sending information such as user ID, password and IP address to the authentication server when a remote user requests a connection.
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 generated 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.
Random key	Random values to be generated by RBG.
Recommend/be recommended	The ‘recommend’ or ‘be recommended’ presented in Applicate 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 allowd to release.
Security Policy Document	Document uploaded to the list of 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.
SSL (Secure Sockets Layer)	This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network.
Subject	Active entity in the TOE that performs operations on objects.
Symmetric cryptographic technique	Encryption scheme that uses the same secrete key in mode of encryption and decryption, also known as secrete key cryptographic technique.
TACACS (Terminal Access Controller Access Control System)	Authentication protocol that is common for UNIX networks, described in RFC 1492, used by remote access server to send user login passwords to an authentication server.
Target of Evaluation (TOE)	Set of software, firmware and/or hardware possibly accompanied by guidance.
Threat Agent	Entity that can adversely conduct actions such as unauthorized access, modification and deletion on assets
TLS (Transport Layer Security)	This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246.
TOE Security Functionality (TSF)	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
TSF Data	Data for the operation of the TOE upon which the enforcement of the SFR relies.
User	Refer to "External entity", 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.

1.7 Structure of Security Target

Chapter 1 introduces the Security Target and provides ST reference, TOE reference, TOE overview, TOE description, and writing rules.
Chapter 2 declares conformity to the Common Criteria, Protection Profile, and Package as a conformance declaration, and describes the rationale for the conformance declaration.
Chapter 3 describes the security objectives for the TOE operating environment.
Chapter 4 defines new components that are not included in Part 2 or Part 3 of the CC among the components described in this Security Target as extension component definition.
Chapter 5 describes security functional requirements and assurance requirements to satisfy security objectives as security requirements.
Chapter 6 describes how the TOE satisfies all security functional requirements.

2. Conformance claims

2.1 CC conformance claim

This security target claims conformance the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5.

CC

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017)
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017)
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)

Conformance claim

- Common Criteria for Information Technology Security Evaluation part 2 expansion : FCS_RBG.1, FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
- Common Criteria for Information Technology Security Evaluation part 3 : Conformant

2.2 PP conformance claim

This security target claim conformance the following protection profile.

- Korean national protection profile for Single Sign On V1.1 (2019.12.11)

2.3 Package conformance claim

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

2.4 Conformance claim rationale

Since the security target specification equally accepts the TOE type, security objectives and security requirements of the protection profile, the conformance declaration of the 'Korean national protection profile for Single Sign On V1.1' is 'strict protection profile conformance'.

2.4.1 Rationale

Since the protection profile that this Security Target conforms to requires strict compliance, the rationale for the conformance declaration is not required.

2.5 Conformance Statement

The security target specification requires strict compliance of the conforming protection profile, so all security objectives for the TOE must be included, but it was confirmed that there are security objectives that can be excluded for the following reasons.

In the case of
OE. Authentication System Security defined for the security purpose of the protection profile operating environment, if the TOE uses an external authentication system (RADIUS, TACACS, Kerberos, and other authentication servers within the organization) in the first authentication step, the external authentication system is safely authorized. This is a security objective to support the function of storing and managing authentication information of a general user.
However, since the TOE implements the user's initial authentication function directly in the TOE, it is correct that the security objective OE.Authentication System Security is not derived because it is not related to the TOE.
In addition, it was confirmed that OE.TIME_STAMP, OE.DBMS, and OE.MANAGEMENT_ACCESS were included as security objectives for the operating environment, as it is allowed to include security objectives for the operating environment additional to the TOE in strict compliance.
The additional security objectives of OE.TIME_STAMP and OE.DBMS were confirmed to be appropriate as security objectives for the operating environment.

Korean national protection profile	Security Target

for Single Sign On	
OE.PHYSICAL_CONTROL	OE.PHYSICAL_CONTROL
OE.TRUST_ADMIN	OE.TRUST_ADMIN
OE.LOG_BACKUP	OE.LOG_BACKUP
OE.OPERATION_SYSTEM_REINFORCEMENT	OE.OPERATION_SYSTEM_REINFORCEMENT
OE.SECURE_DEVELOPEMENT	OE.SECURE_DEVELOPEMENT
OE.Authentication System Security	-
-	OE.TIME_STAMP
-	OE.DBMS
-	OE.MANAGEMENT_ACCESS

* OE.TIME_STAMP : The TOE is used to receive a reliable timestamp (FPT_STM.1) so that it can accurately record security-related events included in audit records, so the added security objectives for the operating environment are reasonable.

* OE.DBMS: As the TOE uses a secure DBMS to protect audit records from unauthorized deletion, the added security objective for the operating environment is reasonable.

* OE.MANAGEMENT_ACCESS : Since the user's safe communication path is provided through communication between the web browser of the user's PC and the web server, which is the operating environment of the management server (SSO server), the security objective for the added operating environment is reasonable.

3. Security objectives for the operational environment

3.1 Security objectives for the operational environment

OE. PHYSICAL_CONTROL

The place where the TOE is installed shall be equipped with access control and protection facilities so that only authorized administrator can access.

OE. TRUST_ADMIN

The authorized administrator of the TOE shall be non-malicious, 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_REINFORCEMENT

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

OE. SECURE_DEVELOPEMENT

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

TOE shall accurately record security related events with reliable time stamps provided by the TOE operation environment.

OE.DBMS

The DBMS that saves the TSF data and the audit data shall be physically, safely operated.

OE. MANAGEMENT_ACCESS

All the information sent to the SSO Server which is a component of the TOE shall be safely protected.

4. Extended components definition

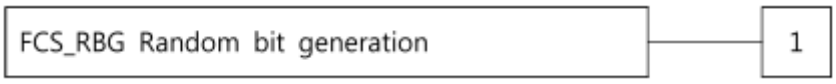
4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

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

Component leveling



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

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

Audit: FCS_RBG.1
There are no auditable events foreseen.

4.1.1.1. FCS_RBG.1 Random bit generation

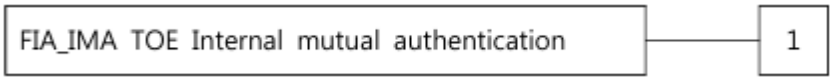
Hierarchical to No other components.
Dependencies No dependencies.
FCS_RBG.1.1The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: list of standards].

4.2 Identification and authentication

4.2.1 TOE Internal mutual authentication

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

Component leveling



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

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

Audit: FIA_IMA.1
The following actions are recommended to record if FAU_GEN Security audit data generation is

included in the PP/ST:

a) Minimum: Success and failure of mutual authentication

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.

Dependencies No dependencies.

FIA_IMA.1.1The 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.3.1The TSF shall destroy secrets in accordance with a specified secrets destruction method [assignment: secret destruction method] that meets the following: [assignment: list of standards].

4.2.2.1. FIA_SOS.3 Destruction of Secrets

Hierarchical to No other components.
Dependencies FIA_SOS.2 TSF Generation of secrets
FIA_SOS.3.1The 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 and password

Hierarchical to No other components.

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

FMT_PWD.1.1The 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.1.2The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

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

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

4.4 Protection of the TSF

4.4.1 Protection of stored TSF data

Family Behaviour

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

Component leveling

FPT_PST.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.1.1The 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.5.1The 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

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.

The security functional requirements included in this PP are derived from CC Part 2 and Chapter 4 Extended Components Definition.

5.1 Security functional requirements

The following table summarizes the security functional requirements used in the ST.

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
	FUA_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation(1)
	FCS_CKM.1(2)	Cryptographic key generation(2)
	FCS_CKM.1(3)	Cryptographic key generation(3)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction

	FCS_COP.1(1)	Cryptographic operation(1)
	FCS_COP.1(2)	Cryptographic operation(2)
	FCS_COP.1(3)	Cryptographic operation(3)
	FCS_COP.1(4)	Cryptographic operation(4)
	FCS_COP.1(5)	Cryptographic operation(5)
FIA	FIA_AFL.1(1)	Authentication failure handling(1)
	FIA_AFL.1(2)	Authentication failure handling(2)
	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	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF testing
FTA	FTA_MCS.2	Per user attribute Limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

5.1.1 Security audit (FAU)

FAU_ARP.1 Security alarms

FAU_ARP.1 Security alarms

Hierarchical to No other components.

Dependencies FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1The TSF shall take [the following list of actions] upon detection of a potential security violation.

Potential security violation list	Action list
Key# Crypto V1.5 self-test fail	Send e-mail to authorized

DBMS disk capacity exceeded	administrator
Audit save fails	
SSO Server/SSO Agent not-operating	
End-user authorization fail exceeds allowed number (5 times)	

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 2] Audit events, [none]].

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 ST, [Refer to the contents of "additional audit record" in [Table 2] Audit events, [none]].

Security functional component	Auditable event	Additional audit record
FAU_ARP.1	Responses taken as a result of a potential security violation	
FAU_SAA.1	Initiation and deactivation of the analysis mechanism, Automatic response by tool	-
FAU_STG.3	Response in case of DBMS disk capacity exceeded	
FAU_STG.4	Responding Actions in Case of Audit Save Fail	
FCS_CKM.1	action successes and failures	
FCS_CKM.2	action successes and failures (applies only to key distribution related to TSF data encryption/decryption)	
FCS_CKM.4	action successes and failures (Applicable only to key destruction related to TSF data encryption/decryption)	
FCS_COP.1	Success and failure of cryptographic operation, type of cryptographic operation (applies only to matters related	

	to issuance, storage, verification, and destruction of authentication tokens)	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_SOS.2	Rejection by the TSF of any tested secret	
FIA_SOS.3 (Extended)	Success and failure of the activity(applicable to the destruction of SSO token only)	
FIA_UAU.1	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the administrator identification mechanism, including the administrator identity provided	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1 (Extended)	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MSC.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5 (Extended)	Locking or termination of interactive session	-
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	-

[Table 2] Audit events

FAU_SAA.1 Potential violation analysis

Hierarchical to No other components.

Dependencies FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and

based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events.
a) Accumulation or combination of [
Self-test failure of the validated cryptographic module (Key# Crypto V1.5)
Audit storage is full
Integrity test failure of the SSO Server
Integrity test failure of the SSO Agent
Audit storage failure
Exceed the allowed number of administrator/end-user authentication failures (5 times)
] known to indicate a potential security violation;
b) [none].

FAU_SAR.1 Audit review

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

FAU_SAR.3 Selectable audit review

Hierarchical to No other components.
Dependencies FAU_SAR.1 Audit review
FAU_SAR.3.1 The TSF shall provide the ability to apply [the following method of search] of audit data based on [the following criteria with logical relations].

Criteria with logical relations		Method of search
User use history	Time, type, search condition AND operation	User ID, name, organization name, time, engine info, user IP, target ID, command, result value, additional info, details : ordering in the descending order based on the time of audit data generation
Administrator use history		User ID, name, organization name, time, user IP, target ID, command, result value, details : ordering in the descending order based on the time of audit data generation
System user history	Time and type AND operation	Time, IP, product info, command, result value, additional info, details : : ordering in the

		descending order based on the time of audit data generation

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, [none]] if the audit trail exceeds [the threshold set by the authorized administrator(80%)].

FAU_STG.4 Prevention of audit data loss

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

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [none] if the audit trail is full.

Application notes : When exceeding past record deletion threshold (90%), loss damage is carried out.

5.1.2 Cryptographic support (FCS)

FCS_CKM.1(1) Cryptographic key generation(1)

Hierarchical to No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [HASH_DRBG(SHA 256)] and specified cryptographic key sizes [128 Bit] that meet the following: [TTAK.KO-12.0331-Part2 (2018)].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

FCS_CKM.1(2) Cryptographic key generation(2)

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 [RSAES] and specified cryptographic key sizes [2048 Bit] that meet the following: [ISO/IEC 18033-2(2006)].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

FCS_CKM.1(3) Cryptographic key generation(3)

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 [Password-based key derivation(PBKDF2)] and specified cryptographic key sizes [256 Bit] that meet the following: [ISO/IEC 18033-2(2006) TTAK.KO-12.0334-Part1/2 (2018)].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

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 [RSAES 2048] that meets the following: [ISO/IEC 18033-2(2006)].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components.

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 [Overwrite 3 times with 0] that meets the following: [none].

FCS_COP.1(1) 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 [Digital Signature and verification] in accordance with a

specified cryptographic algorithm [RSA-PSS 2048] and cryptographic key sizes [2048 Bit] that meet the following: [ISO/IEC 14888-2(2008)].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

FCS_COP.1(2) 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 [public key cryptographic operation] in accordance with a specified cryptographic algorithm [RSAES] and cryptographic key sizes [2048 Bit] that meet the following: [ISO/IEC 18033-2(2006)].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

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 [Generate message authentication code, Verification of authentication token] in accordance with a specified cryptographic algorithm [HMAC-SHA256] and cryptographic key sizes [256 Bit] that meet the following: [TTAK.KO-12.0330].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

FCS_COP.1(4) 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 [Symmetric key encryption] in accordance with a specified cryptographic algorithm [SEED] and cryptographic key sizes [128 Bit] that meet the following: [KO-12.0004/R1(2005)].

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

FCS_COP.1(5) Cryptographic operation(HASH)

Hierarchical to No other components.

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

FCS_COP.1.1 The TSF shall perform [the following list of cryptographic operations] in accordance with a specified cryptographic algorithm [cryptographic algorithm] and cryptographic key sizes [none] that meet the following: [ISO/IEC 10118-3:2001(2018)].

cryptographic algorithm	list of cryptographic operations
SHA 256	User password / integrity verification
SHA 512	Admin password

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

FCS_RBG.1 Random bit generation(Extended)

Hierarchical to No other components.

Dependencies No dependencies.

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

list of standards	Random bit generation algorithm
[TTAK.KO-12.0331-Part2 (2018)]	HASH_DRBG(SHA 256)

Application notes : It is implemented through Key# Crypto V1.5, a verified cryptographic module.

5.1.3 Identification and authentication (FIA)

FIA_AFL.1(1) Authentication failure handing(Admin)

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 of administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed* the TSF shall [lock account for disabled time set by administrator (10 minutes)].

FIA_AFL.1(2) Authentication failure handling(User)

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 of user].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed* the TSF shall [lock account for disabled time set by administrator (10 minutes)].

FIA_IMA.1 TOE Internal mutual authentication(Extended)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [TOE components] using the [own protocol] that meets the following [none].

Application notes : Perform mutual authentication between SSO Server and SSO Agent.

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 permission criteria].

Acceptable characters	52 English letters (case sensitive)
	10 numbers (0~9)
	~!@#$%^&*()_+`-={}|[]₩:";'<>?,./
Password combination rules	Must include at least one English letter, number and special character each
	[Administrator password] - 9 – 63 characters [User password] - 9 – 63 characters - 3-4 upper/lower case letters, numbers and special characters - ID check - DOB check - Not case sensitive - Same characters cannot be used 3-5 times - Sequential characters cannot be used 3-5 times

Application notes : Combination rules are conducted according to the settings of the authorized admin.

FIA_SOS.2 TSF Generation of secrets

Hierarchical to No other components.

Dependencies No dependencies.

FIA_SOS.2.1 TSF shall provide a mechanism to generate an **authentication token** that meet [the following a defined acceptable standard].

Prescribed allowance	Contents

standards	
Authentication token configuration method	Keys shared between servers, user ID, user ID, token generation time, valid time, idle time, session Slot and Token ID - valid time: valid time for accessing to the business system. Update after verification. - idle time: valid for the set time (8 hours) since the initial log-in and authentication token generation. - session slot: session index generated during log-in.
Composition field length	256 byte
Symmetric encryption algorithm	SEED 128

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

FIA_SOS.3 Destruction of secrets (Extended)

Hierarchical to No other components.

Dependencies FIA_SOS.2 TSF Generation of secrets

FIA_SOS.3.1 The TSF shall destroy **authentication tokens** in accordance with a specified **authentication token** destruction method [Overwrite 3 times with 0] that meets the following: [none].

FIA_UAU.2 User authentication before any action

Hierarchical to FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [identified authentication mechanism(s)].

Type	identified authentication mechanism(s)
Administrator/User password authentication	SessionID encryption with random bits
Authentication token	Use Onetime Token

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 [•, Authentication failure message] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to FIA_UID.1 Timing of identification

Dependencies No dependencies.

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

5.1.4 Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to ***conduct management actions of*** the functions [list of functions in [Table 3]] to [the authorized administrator].

List of functions		Conduct management actions				The authorized role
		determine	Enable	modify	disable	
WPM	service structure	O	O	O	O	the authorized administrator
	Service	O	O	O	O	
	Permission	O	O	O	O	
	Password policy	X	O	O	O	
	User login policy	X	O	O	O	
	Admin ip	X	X	O	X	

[Table 3] List of functions

FMT_MTD.1 Management of TSF data

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** the [the following list of TSF data] to [the authorized administrator].

The authorized role	manage	Change_default	query	modify	delete	[create]

	list of TSF data					
the authorized administrator	Organizaton	X	O	O	O	O
	User	X	O	O	O	O
	Password combination rules	O	O	O	X	X
	ID creation rules	O	O	O	X	X
	User profile	X	O	O	O	O
	Permission	X	O	O	O	O
	Allowed IP	X	O	O	O	O
	Password	O	X	O	X	X
user	password	X	X	O	X	X

[Table 4] list of TSF data

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to No other components

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

1. [password combination rules and/or length]

List of function	password combination rules and/or length]
Password combination rules (admin)	[Administrator password] - 9 – 63 characters characters - Combination of 3 or more English letters, numbers, or special characters(~!@#$%^&*()_+`-={}|[]₩:";'<>?,./)
Password combination rules (user)	[User password] - 9 – 63 characters characters - Combination of 3 or more English letters, numbers, or special characters(~!@#$%^&*()_+`-={}|[]₩:";'<>?,./) - ID check - DOB check - Not case sensitive - Same characters cannot be used 3-5 times - Sequential characters cannot be used 3-5 times

2. [none]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [ID combination rules] to [the

authorized administrator].

1. [user ID : 1~31 characters, IE Type(letters / numbers / letters and numbers / letters, numbers and special characters), First character(letters / numbers / none)]

2. [none]

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

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:

[

a) TSF function management: items specified in FMT_MOF.1

b) TSF security attributes management: items specified in FMT_MSA.1

c) TSF data management: items specified in FMT_MTD.1

]

FMT_SMR.1 Security roles

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator/delegated administrator].

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

5.1.5 Protection of the TSF

FPT_ITT.1 Basic Internal TSF data transfer protection

Hierarchical to No other components.

Dependencies No dependencies.

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

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

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PST.1.1 The TSF should protect the [TSF data] stored in the repository, which is controlled by the TSF, from unauthorized *exposure and modification*.

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 *TSF*.

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

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

5.1.6 TOE access

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [restriction to one for the maximum number of concurrent sessions for administrator management access session]

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

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

Hierarchical to No other components.

Dependencies FIA_UAU.1 Authentication or No dependencies.

FTA_SSL.5.1 The TSF shall *terminate* an interactive session after a [time interval of administrator inactivity(10 minute), Authenticated token idle time].

FTA_TSE.1 TOE session establishment

Hierarchical to No other components.

Dependencies No dependencies

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

5.2 Security assurance requirement

This section defines the assurance requirements for the TOE. Assurance requirements are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+(ATE_FUN.1). The following table summarizes assurance components.

Security assurance class	Security assurance component	
Security Target	ASE_INT.1	ST introduction

evaluation	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

5.2.1 Security Target evaluation

ASE_INT.1 ST introduction

Dependencies No dependencies.

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action

elements	
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements
Developer action elements	
ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
Content and presentation elements	
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of

	security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
Evaluator action elements	
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

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

ASE_ECD.1 Extended components definition

Dependencies	No dependencies.
Developer action elements	
ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
Content and presentation elements	
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements

	such that conformance or nonconformance to these elements can be demonstrated.
Evaluator action elements	
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

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

ASE_TSS.1 TOE summary specification

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

ASE_TSS.1.1D	The developer shall provide a TOE summary specification
Content and presentation elements	
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
Evaluator action elements	
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies	No dependencies.
Developer action elements	
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements	
ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance documents

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_PRE1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
Evaluator action elements	
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1 Labelling of the TOE

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

ALC_CMS.1 TOE CM coverage

Dependencies	No dependencies.
Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and	

presentation elements

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements

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

5.2.5 Tests

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 presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Security requirement rationale

5.3.1 Dependency rationale of security functional requirements

The following table shows dependency of security functional requirement.

NO.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	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	FUA_STG.3	FAU_STG.1	OE.DBMS
7	FAU_STG.4	FAU_STG.1	OE.DBMS
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	11, 15, 16 12
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	11, 13, 14 12
10	FCS_CKM.1(3)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	11, 16 12
11	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	8, 9 12
12	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8, 9, 10
13	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	9 12
14	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	9 12
15	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	8 12
16	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	8 12

17	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	-
18	FCS_RBG.1	-	-
19	FIA_AFL.1(1)	FIA_UAU.1	25
20	FIA_AFL.1(2)	FIA_UAU.1	25
21	FIA_IMA.1	-	-
22	FIA_SOS.1	-	-
23	FIA_SOS.2	-	-
24	FIA_SOS.3	FIA_SOS.2	23
25	FIA_UAU.2	FIA_UID.1	28
26	FIA_UAU.4	-	-
27	FIA_UAU.7	FIA_UAU.1	25
28	FIA_UID.2	-	-
29	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	32 33
30	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	32 33
31	FMT_PWD.1	FMT_SMF.1 FMT_SMR.1	32 33
32	FMT_SMF.1	-	-
33	FMT_SMR.1	FIA_UID.1	28
34	FPT_ITT.1	-	-
35	FPT_PST.1	-	-
36	FPT_STM.1	-	-
37	FPT_TST.1	-	-
38	FTA_MCS.2	FIA_UID.1	28
39	FTA_SSL.5	FIA_UAU.1 또는 없음	25
40	FTA_TSE.1	-	-

[Table 5] Rationale for the dependency of the security functional requirement

FAU_GEN.1 has the dependency on FPT_STM.1. It records security related tests using the reliable time stamp provided by the operational environment of TOE. It is satisfied by the operational environment of security objective OE. time stamp

FAU_STG.3 and FAU_STG.4 have the dependency on FAU_STG.1. It is satisfied by the operational

environment of OE.DBMS.

FIA_AFL.1(1), FIA_AFL.1(2), FIA_UAU.7, FTA_SSL.5 have the dependency on FIA_UAU.1. It is satisfied by FIA_UAU.2 which is in a hierarchical relationship with FIA_UAU.1.

FIA_UAU.2, FMT_SMR.1, FTA_MCS.2have the dependency on FIA_UID.1. It is satisfied by FIA_UID.2 which is in a hierarchical relationship with FIA_UID.1.

FCS_COP.1(5) has dependency on FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1, and FCS_CKM.4. It is satisfied by the Hash algorithm does not use the cryptographic key.

5.3.2 Dependency rationale of security assurance requirements

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

The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. but, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

6.1 Security Audit(AUDIT)

6.1.1 Audit data generation(AUDIT.1)

▣ SSO Server/SSO Agent

The TOE performs the security management function and generates the result of potential security violation of the TOE components, the result of identification and authentication, and the audit data of events from the system.

The TOE stores the audit data in the DBMS.

Audit data	Cases for audits	Remarks
User history	- User identification and authentication - Authentication token issue - Authentication token verification	SSO Agent
Admin history	- Administrator identification and authentication - Security setting - TSF data information change	SSO Server

	- Session termination	
System history	- Start/Terminate - Self-test and integrity test - Exceed the administrator allowed number of failures - Key# Crypto V1.5 self-test - Audit storage is full - Self-test and integrity test	SSO Server
	- Start/Terminate - Self-test and integrity test - Cryptographic key management (generation, operation)	SSO Agent

For each audit data, audit data is generated by including the log generation time, case type, identify of subject (if available), case results (success or fail) and selective audit review for case type is possible.

Related SFRS : FAU_GEN.1

6.1.2 Audit data review(AUDIT.2)

The TOE stores the audit data in the DBMS and provide the audit records in a manner suitable for the authorized administrator to interpret the information. It is possible to review Detail, the identity of the subject (end-user or administrator ID, end-user or administrator IP, TOE components), date of the event, type of the event and failure/success of the event with the AND condition.

▣ SSO Server

The TOE provides the ability to review the audit data to the authorized administrator.
The provided audit data that is stored in the DBMS, an operational environment of the TOE, includes the identification and authentication history of the authorized administrator and the user, TSF function change, data value, management history of threshold change and history of TOE component start/termination. Query the DBMS to provide the data in a manner suitable for the authorized administrator.
Only the top-level administrator can search the audit data.

Related SFRS : FAU_SAR.1, FAU_SAR.3

6.1.3 Audit repository inspection and security violation response (AUDIT.3)

▣ **SSO Server**

The TOE shall periodically detect self-test of potential security threats (validated cryptographic module (Key# Crypto V1.5), DBMS DISK capacity check, self-test of the SSO Server/SSO Agent, integrity test, audit storage failure, exceed the allowed number of failures for administrator/user) and send a warning email about security threats to the authorized administrator

In addition, send the emails to the administrator to prevent audit data loss when the DBMS exceeds the threshold (80%). When reaching the threshold for deleting past records in the DBMS, delete the oldest audit records to prevent audit data loss, and send the emails to the administrator.

The audit records generated by the TOE is stored in the DBMS that the TOE operational environment provides. Only authorized administrator can access to the audit record DB and organize the audit records.

Related SFRS : FAU_ARP.1, FAU_SAA.1, FAU_STG.3, FAU_STG.4

6.2 Cryptographic support(CKM)

6.2.1 Cryptographic Key Management and Cryptographic Operation(CKM.1)

The TOE uses the following verified cryptographic modules to perform cryptographic support functions.

구분	내용
cryptographic module name	Key# Crypto V1.5
Developer	RAONSECURE Co., Ltd.
verification date	2022-11-02
expiration date	2027-11-02
verification number	CM-220-2027.11
User mode	Linux (libjavaCmvp.so ,libKeySharpCryptoV1_5.so)

▣ **SSO Server/SSO Agent**

The TOE performs the password support function for each SSO Server/SSO Agent component as follows.

- SSO Server와 SSO Agent

6.2.2 Generate an encryption key

Cryptographic key classification	usage	Encryption key type	algorithm	Standard list	Encryption key length
DEK Encrypting TSF	Token key (authentication token data encryption)	random number generator	HASH_DRBG (SHA 256)	[TTAK.KO-12.0331-Part2 (2018)]	128
DEK Encrypting TSF	set encryption key	random number generator	HASH_DRBG (SHA 256)	[TTAK.KO-12.0331-Part2 (2018)]	128
KEK Encrypting DEK	public/private key	public key cryptographic algorithm	RSAES (SHA 256)	ISO/IEC 18033-2(2006)	2048
KEK Encrypting DEK	Encryption key (token key encryption)	random number generator	HASH_DRBG (SHA 256)	[TTAK.KO-12.0331-Part2 (2018)]	128
KEK Encrypting DEK	judo key	Password-based key derivation function	Pbkdf2	[TTAK.KO-12.0334-Part1/2 (2018)]	128
DEK to encrypt data in transit	section encryption key	random number generator	HASH_DRBG (SHA 256)	[TTAK.KO-12.0331-Part2 (2018)]	128

6.2.3 Cryptographic key distribution

Cryptographic key classification	usage	Encryption key type	algorithm	Standard list	Encryption key length
DEK to encrypt data in transit	Section encryption key distribution	public key cryptographic algorithm	RSAES (SHA 256)	ISO/IEC 18033-2(2006)	2048

6.2.4 Destroy the encryption key

Cryptographic key classification	usage	destruction cycle	Destruction method

DEK Encrypting TSF	Encryption key (token key)	Destroy immediately after use	Overwrite 3 times with 0
DEK Encrypting TSF	set encryption key	Destroy immediately after use	
KEK Encrypting DEK	encryption key	Destroy immediately after use	
DEK to encrypt data in transit	section encryption key	Destroy immediately after use	
-	private key	Destroy immediately after use	

6.2.5 Cryptographic operation

Cryptographic key classification	usage	Encryption key type	algorithm	Encryption key length	Standard list
Authentication Token Encryption	Token key (authentication token encryption)	block cipher	SEED-CBC	128	[TTAS-KO-12.0004/R1 (2005)]
	Encryption key (token key encryption)	block cipher	SEED-CBC	128	[TTAS-KO-12.0004/R1 (2005)]
	Authentication Token Integrity Verification (Token Message Authentication)	message authentication	HMAC (SHA-2)	256	[TTAK.KO-12.0330]
TSF data encryption	mutual authentication	public key cryptographic algorithm	RSAES (SHA 256)	2048	ISO/IEC 18033-2(2006)
		Digital Signature Algorithm	RSA-PSS	2048	ISO/IEC 14888-2(2008)
	Communication section encryption	public key cryptographic algorithm	RSAES (SHA 256)	2048	ISO/IEC 18033-2(2006)
		Digital Signature	RSA-PSS	2048	ISO/IEC 14888-

		Algorithm			2(2008)
	TFS Important Information	block cipher	SEED-CBC	128	[TTAS-KO-12.0004/R1 (2005)]
	TOE integrity	hash function	SHA-256		[KS X ISO/IEC 10118-3:2001 (2018)]
	Administrator/User Password	hash function	SHA-512		[KS X ISO/IEC 10118-3:2001 (2018)]

Each component generates an encryption key using the public key cryptographic algorithm (RSAES2048) and uses the digital signature algorithm (RSA-PSS2048) for cryptographic operation. Periodically overwrite the encryption key generated by the SSO Server and SSO Agent with 0 three times to destroy it.

The components of the SSO Server generate the interval cryptographic key of 128bit using the RBG (HASH_DRBG(SHA256). The interval cryptographic key uses the public key algorithm (RSAES 2048) to distribute the SSO Agent and the interval cryptographic key, and encrypt the communication interval. Overwrite the interval cryptographic key with 0 three times to destroy right after the use.

The components of the SSO Server generate the cryptographic key of 128bit using the RBG (HASH_DRBG(SHA256) and use the symmetric key algorithm (SEED(CBC) 128bit) to encrypt/decrypt the token key. Overwrite the encryption key with 0 three times to destroy it immediately right after the use.

The SSO Agent generates the token key of 128bit using the RBG (HASH_DRBG(SHA256). Encrypt the important components of the authentication token using the symmetric key algorithm (SEED(CBC) 128bit)

The SSO Agent generates and verifies the message authentication code and the authentication token using the MAC algorithm (HMAC-SHA256) and the hash algorithm (SHA-256). Overwrite the

authentication token with 0 three times to destroy it immediately right after the use.

Related SFRS : FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_RBG.1

6.3 Identification and authentication (FIA)

The TOE uses the following verified cryptographic modules to perform cryptographic support functions.

구분	내용
cryptographic module name	Key# Crypto V1.5
Developer	RAONSECURE Co., Ltd.
verification date	2022-11-02
expiration date	2027-11-02
verification number	CM-220-2027.11
User mode	Linux (libjavaCmvp.so ,libKeySharpCryptoV1_5.so)

6.3.1 Authentication failure handling

▣ SSO Server

The TOE requests the authorized administrator to set the specification of the unsuccessful authentication attempts for the administrator. The allowed number of authentication failures is set to 5.

If the administrator reaches the allowed number of authentication failures for the management console, lock the administrator's account for 10 minutes as the authorized administrator sets.

▣ SSO Agent

The TOE requests the authorized administrator to set the specification of the unsuccessful authentication attempts for the user. The allowed number of authentication failures is set to 5.

When the user initially attempts to authenticate with the business system, the SSO Agent that is installed in the business system gets the identification and authentication requests of the user. If reaching the allowed number of authentication failures, lock the user's account for 10 minutes as the authorized administrator sets.

Related SFRS : FIA_AFL.1(1), FIA_AFL.1(2)

6.3.2 Mutual authentication between TOE components

The TOE performs mutual authentication between the SSO Server and SSO Agent using the protocol. The detailed mechanism for mutual authentication between the SSO Server and SSO Agent is as follows.

1) During the SSO Server activation, generate the cryptographic key pairs (public key and private key) using the validated cryptographic module.
2) During the SSO Agent activation, generate the cryptographic key pairs (public key and private key) using the validated cryptographic module.
3) SSO Agent authentication request.
4) Generate the PChallenge value (HASH_DRBG(SHA 256)) from the SSO Server and send the SSO Server public key.
5) Sign the PChallenge value from the SSO Agent digitally (RSA-PSS 2048) with the private key of the SSO Agent
6) Generate the EChallenge value (HASH_DRBG(SHA 256)) from the SSO Agent and send the SSO Agent public key.
7) Verify (RSA-PSS 2048) the value which is signed in the SSO Server with the SSO Agent public key and the PChallenge.
8) Digitally sign (RSA-PSS 2048) the EChallenge value from 6) with the SSO Server private key
9) Verify (RSA-PSS 2048) the EChallenge value in the SSO Agent with the SSO Server public key.
10) Success of mutual authentication

Related SFRS : FIA_IMA.1

6.3.3 Verification of Confidential Information

▣ SSO Server

The TOE identifies an administrator who tries to access. Any administrator and IT entity without completing identification can utilize any function of the TOE.

The administrator's authentication information is ID and password. Uppercases (A~Z), lowercases (a~z), numbers (1~0) and special characters (~!@#$%^&*()_+`-={}|[]₩:";'<>?,./) are allowed for the password for identification and authentication. The password shall be able to be composed of combinations of English letters, numbers and special characters, and support passwords of from 9 characters to 63 characters in length. Present the password in '•' and send the failure message to prevent the information of authentication failure reason and the password from being exposed. If identification and authentication succeed, keep the authority for security management.

Prevent reuse of authentication data by encrypting the session ID including the random value.

▣ **SSO Agent**

For the initial user identification and authentication via the business system, perform the user identification and authentication before allowing all the actions. During authentication, send [•] and the failure message to hide the information of authentication failure reason to the user.

User's initial identification and authentication information is ID and password. The password combination rule is applied as the authorized administrator sets. The authorized authenticator sets the password combination rule which is able to be composed of three different characters among Uppercases, lowercases, numbers and special characters; inclusion of ID and DOB for password; case-sensitivity; repetition of the same letters (3~5 times); continuation letters (3~5times).
According to the combination rule, password can be generated from 9 characters to 63 characters in length.

Prevent reuse of end user's authentication data by encrypting the session ID including the random value.

Related SFRS : FIA_SOS.1, FIA_SOS.2, FIA_SOS.3, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

6.3.4 Creation and destruction of confidential information

▣ **SSO Agent**

After completing user's initial identification and authentication, the authentication token in generated. Use the validated cryptographic module when generating the authentication token.

The authentication token is composed of the shared key between the servers, user ID, user ID, token generation time, valid time, idle time, session Slot and Token ID.

Use the validated cryptographic module to generate the token key via the RBG ((HASH_DRBG(SHA 256)). Encrypt the components of the authentication token with the token key using the symmetric algorithm (SEED 128(CBC)).
Encrypt the token key, a cryptographic key from the SSO Server, using the symmetric algorithm (SEED 128(CBC))
Use the MAC algorithm (HMAC-SHA256) to generate the authentication token and verify integrity.

Do not save the authentication token. Overwrite the token with 0 three times to destroy it after sending it to the business system.

Onetime Token prevents the authentication token from being reused.

Related SFRS : FIA_SOS.1, FIA_SOS.2, FIA_SOS.3, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

6.4 Security management(SM)

6.4.1 Security management(SM.1)

▣ SSO Server

The SSO Server sets organization, service, audit and configuration.

[Organization]

There is only the top-level administrator for the authorized administrator.

Change the password when the authorized administrator accesses to the security management interface for the first time.

Manage the top-level organization and sub organization and the account of administrator and user.

Allocate the ID and password policy to users in the organization and set the service authority of the business system by organization and user.

User's ID can be generated from 1 character to 31 characters in length according to the administrator's setting. Register and manage the ID combination (English letters/numbers/English letters, numbers/ English letters, numbers, English letters), initial letter setting (English letters/numbers/no limit) and exception letters for ID.

Verify the validity of password value according to the password policy when generating and changing user's and authorized administrator's password.

The TOE provides the verification mechanism when creating and changing the password.

List of function	password combination rules and/or length]
Password combination rules (admin)	[Password Length] - 9 – 63 characters [Password Combination Rules] - Combination of 3 or more English letters, numbers, or special characters - English upper case : A - Z - English lower case : a – z - number : 0 – 9 - special characters : ~!@#$%^&*()_+`-={}|[]₩:";'<>?,./ (32)
Password combination rules (user)	[Password Length] - 9 – 63 characters

	[Password Combination Rules] - Combination of 3 or more English letters, numbers, or special characters - English upper case : A - Z - English lower case : a – z - number : 0 – 9 - special characters : ~!@#$%^&*()_+`-={}|[]₩:";'<>?,./ (32) - ID check - DOB check - Not case sensitive - Same characters cannot be used 3-5 times - Sequential characters cannot be used 3-5 times

[Service]
Linked with the business system, register services where the user accesses to as tree type.
Set authority for service use by organization and period of service use.

[Configuration]
Register and manage the user profile for the constraint rule in the policy.
Register and manage authority (e.g. add, search, edit, delete) for registered service use.

Manage the combination rule which is composed of length setting (from 9 characters to 63 characters) and mixing rule setting involving English letters, numbers and special characters.

Security function component	management function	management type
FAU_ARP.1	Manage corresponding actions (add, delete, edit).	Manager
FAU_SAA.1	Maintain the rule (add, edit or delete a rule from the rule set).	Manager
FAU_SAR.1	Review the audit record.	Manager
FAU_STG.3	Maintain the threshold.	fixed value
	Maintain corresponding actions (add, edit, delete) if audit storage failure is expected.	
FAU_STG.4	Maintain corresponding actions (add, edit, delete) if audit storage fails.	fixed value
FIA_AFL.1	Manage the threshold for unsuccessful authentication attempts.	fixed value

	Manage corresponding actions if authentication fails.	
FIA_SOS.1	Manage corresponding actions if authentication fails.	Manager
FIA_UAU.2	Manage the authentication data by the administrator.	Manager
FIA_UID.2	Manage the identity of the administrator.	Manager
FMT_MOF.1	Manage the security function which is interactable with the TSF function.	Manager
FMT_MTD.1	Manage the TSF data which is interactable with the TSF data.	Manager
FMT_PWD.1(Extended)	Manage the password setting rule.	Manager
FMT_SMR.1	Manage the security role.	Manager
FPT_ITT.1	Manage the mechanism that is used to protect the data transferred between the different parts of the TSF.	Manager
FPT_TST.1	Manage the time interval under which TSF self-test occurs, such as 'during initial start-up', 'regular interval', or 'under specified conditions'.	Manager
FTA_MCS.2	Manage the rule for managing the maximum number of concurrent user sessions by the administrator.	fixed value

[표 1] 보안기능요구사항

Related SFRS : FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1

6.5 Protection of the TSF(PT)

6.5.1 Protection of the TSF(PT.1)

▣ SSO Server, SSO Agent

The TOE performs mutual authentication and interval encryption by component to protect TSF data from disclosure and modification when transmitting the data between separate parts of the TOE.

TSF Protect	TSF Component		Algorithm
Mutual Authentication	SSO Server	SSO Agent	- Public Key Encryption : RSAES(2048) - Digital Signature Algorithm : RSA-PSS(2048)
Encryption Between Components	SSO Server	SSO Agent	- Random Bit Generator : HASH_DRBG(SHA256) - Public Key Encryption

			: RSAES(2048) - Symmetric Key Encryption : SEED(CBC) 128 bit

The TSF self-test verifies the accurate operation of the TSF and provides the function that is used by the authorized administrator to verify the integrity of the TSF data.
The TOE shall run its own tests to ensure that all TSFs are operating correctly every hour during the TOE run and during normal operation.
For self-test, the SSO Server sends an email to the administrator when the port goes inactivated. Generate the audit log to search in case of SSO Agent abnormal termination.

The TOE performs DB password encryption and decryption for protecting important information and connects to the DBMS. Use the hash algorithm (SHA-512) to safely store the administrator and user password in the DBMS.

The SSO Server and SSO Agent shall run self-test for major security function processes during running The SSO Server and SSO Agent shall perform integrity verification (SHA-256) hourly during running and normal operation. Manage the list of integrity verification as the Appendix [integrity verification]. the TOE shall run self-test for major processes periodically during initial start-up and operation, and ensure the integrity of the TOE configuration files

The TOE protects the TSF data from unauthorized disclosure and modification by encrypting it. And then store and manage it.
The TSF data list and the applied cryptographic algorithm is as follows.

TSF Protect	TSF Component		Algorithm
DB password encryption/decryption	SSO Server	DBMS	- block cipher : SEED-CBC
Encryption of encrypted DB password			- random number generator : HASH_DRBG(SHA256) - Password-based key derivation function : PBKDF2
Encryption of important setting values (administrator ip, stmp email address, password)	SSO Server		- block cipher : SEED-CBC

authentication token	SSO Agent	- block cipher : SEED-CBC
TOE integrity	SSO Server SSO Agent	- hash function : SHA-256
Administrator/User Password	-	- hash function : SHA-512 / SHA-256

Related SFRS : FPT_ITT.1, FPT_PST.1, FPT_TST.1

6.6 TOE access(TA)

6.6.1 Session management(TA.1)

▣ SSO Server

The TOE controls the management access of the administrator based on the access IP when the administrator attempts to access to the SSO Server, and blocks the management access session from the un-allowed IP.

Limit the number of concurrent sessions for the SSO Server to 1 so that the top-level administrator owns the rights. Concurrent session is not allowed.

The TOE terminates the interacting session after a specified time interval of authorized administrator inactivity (10 minutes), after that reauthentication is required.

▣ SSO Agent

The TOE terminates the session after the idle time of authentication token, after that authentication token verification will be failed. For reauthentication, identification and authentication with end user's ID/password is required.

Related SFRS : FTA_MCS.2, FTA_SSL.5, FTA_TSE.1

[Appendix]

1. Integrity verification target

1.1 SSO Server

1.1.1 sessionserver folder

path	File name
/home/cctest/wiseaccess_v1.4/server/sessionserver/integrity/	gson-2.2.4.jar
	jcl-over-slf4j-1.7.32.jar
	libjavaCmvp.so
	libKeySharpCryptoV1_5.so
	libsigar-amd64-linux.so
	logback-classic-1.2.9.jar
	logback-core-1.2.9.jar
	mysql-connector-java-8.0.21.jar
	sensor-1.4.4.3-linux-x8664.jar
	sensor.conf
	sessionserver.conf
	sigar-1.6.6.jar
	slf4j-api-1.7.32.jar
	solutionintegrity-1.5.0.2.jar
	xenv
	xinfo
	xstart
	xstop
	xversion

1.1.2 policyserver folder

path	File name
/home/cctest/wiseaccess_v1.4/server/policyserver/integrity	jcl-over-slf4j-1.7.32.jar
	libjavaCmvp.so
	libKeySharpCryptoV1_5.so
	libsigar-amd64-linux.so
	logback-classic-1.2.9.jar
	logback-core-1.2.9.jar
	mysql-connector-java-8.0.21.jar

	ojdbc6-11.2.0.4.jar
	policyserver.conf
	policyserver.jar
	ps.mysql.conf
	sensor-1.4.4.3-linux-x8664.jar
	sensor.conf
	sigar-1.6.6.jar
	slf4j-api-1.7.32.jar
	solutionintegrity-1.5.0.2.jar
	xenv
	xinfo
	xinfo_ps
	xstart
	xstart_ps
	xstop
	xstop_ps
	xversion
	xversion_ps

1.1.3 wpm folder

path	File name
/home/cctest/wiseaccess_v1.4/server/policy server/integrity	accessDenied.jsp
	acecommon.jar
	addAlarmRecipients.jsp
	addService.jsp
	addUacl.jsp
	addUaclOfService.jsp
	admin.gif
	adminAlarm.jsp
	adminIndex.jsp
	adminIP.jsp
	adminLog.jsp
	adminLogGridList.jsp
	adminSearchHeader.jsp
	admin_on.gif
	admin_password.jsp

	ajax-loader.gif
	animated-overlay.gif
	application-security.xml
	audit.props
	AuditLeftMenu.jsp
	base.css
	base64js.min.js
	batchjob_import.gif
	batchjob_import_on.gif
	batchjob_lumpprocess.gif
	batchjob_lumpprocess_on.gif
	bcprov-jdk14-128.jar
	bg_gnb.gif
	bg_header.gif
	bg_line.gif
	bg_list_over.gif
	bg_list_over.png
	bg_list_th.gif
	bg_list_th_over.gif
	bg_lnb.gif
	bg_login.gif
	bg_pop.png
	bg_pop_container.gif
	bg_pop_original.png
	bg_tab1.gif
	bi.gif
	bi.png
	blank.jsp
	bodySample.jsp
	bootstrap-datepicker.css
	bootstrap-datepicker.js
	bower.json
	btn.gif
	btn_black.gif
	btn_black_icon.gif
	btn_close.gif
	btn_excel2.gif

	btn_icon.gif
	btn_login.gif
	btn_logout.gif
	btn_orange.gif
	btn_search.gif
	btn_search_b.gif
	btn_search_small.gif
	btn_tab.gif
	bu_orange.gif
	calender.js
	chgPwd.jsp
	com.springsource.javax.mail-1.4.5.jar
	com.springsource.javax.servlet.jsp.jstl-1.1.2.jar
	com.springsource.org.aopalliance-1.0.0.jar
	com.springsource.org.apache.commons.beanutils-1.8.0.jar
	com.springsource.org.apache.commons.collections-3.2.1.jar
	com.springsource.org.apache.commons.dbcp-1.2.2.osgi.jar
	com.springsource.org.apache.commons.digester-1.8.1.jar
	com.springsource.org.apache.commons.fileupload-1.2.0.jar
	com.springsource.org.apache.commons.io-1.4.0.jar
	com.springsource.org.apache.commons.logging-1.1.1.jar
	com.springsource.org.apache.commons.pool-1.5.3.jar
	com.springsource.org.apache.taglibs.standard-1.1.2.jar
	com.springsource.org.apache.tiles-2.1.2.osgi.jar
	com.springsource.org.apache.tiles.core-2.1.2.osgi.jar
	com.springsource.org.apache.tiles.jsp-2.1.2.jar
	com.springsource.org.apache.tiles.servlet-2.1.2.jar

	com.springsource.org.aspectj.tools-1.6.6.RELEASE.jar
	com.springsource.org.codehaus.jackson-1.4.2.jar
	com.springsource.org.codehaus.jackson.mapper-1.4.2.jar
	com.springsource.org.joda.time-1.6.0.jar
	common.css
	common.js
	commonService.xml
	config.properties
	cos.jar
	daowired.xml
	dataSource.xml
	delegate.gif
	delegate_on.gif
	delimg.jpg
	dom4j-1.6.1.jar
	error.jsp
	error.props
	errorPage.jsp
	excelimg.jpg
	fileimg.jpg
	Footer.jsp
	forwardLogin.jsp
	frameSpringcommon.js
	frameSpringcommonOptions.js
	GeneralTiles.xml
	glyphicons-halflings.png
	gnb1.gif
	gnb10.gif
	gnb10_on.gif
	gnb11.gif
	gnb1_on.gif
	gnb2.gif
	gnb2_on.gif
	gnb3.gif
	gnb3_on.gif

	gnb4.gif
	gnb4_on.gif
	gnb5.gif
	gnb5_on.gif
	gnb6.gif
	gnb6_on.gif
	gnb7.gif
	gnb7_on.gif
	gnb8.gif
	gnb8_on.gif
	gnb9.gif
	gnb9_on.gif
	gnb_help.gif
	gnb_help_on.gif
	grid.addons.js
	grid.locale-ar.js
	grid.locale-bg.js
	grid.locale-bg1251.js
	grid.locale-cat.js
	grid.locale-cn.js
	grid.locale-cs.js
	grid.locale-da.js
	grid.locale-de.js
	grid.locale-dk.js
	grid.locale-el.js
	grid.locale-en.js
	grid.locale-es.js
	grid.locale-fa.js
	grid.locale-fi.js
	grid.locale-fr.js
	grid.locale-gl.js
	grid.locale-he.js
	grid.locale-hr.js
	grid.locale-hr1250.js
	grid.locale-hu.js
	grid.locale-id.js
	grid.locale-is.js

	grid.locale-it.js
	grid.locale-ja.js
	grid.locale-kr.js
	grid.locale-lt.js
	grid.locale-mne.js
	grid.locale-nl.js
	grid.locale-no.js
	grid.locale-pl.js
	grid.locale-pt-br.js
	grid.locale-pt.js
	grid.locale-ro.js
	grid.locale-ru.js
	grid.locale-sk.js
	grid.locale-sr-latin.js
	grid.locale-sr.js
	grid.locale-sv.js
	grid.locale-th.js
	grid.locale-tr.js
	grid.locale-tw.js
	grid.locale-ua.js
	grid.locale-vi.js
	grid.postext.js
	grid.setcolumns.js
	GruntFile.js
	gson-2.2.4.jar
	handleradap.xml
	hwpimg.jpg
	icons.gif
	icon_cal.GIF
	ic_calendar.gif
	index.html
	index.jsp
	jasper-el.jar
	jcl-over-slf4j-1.7.32.jar
	jquery-ui-custom.css
	jquery-ui.css
	jquery-ui.js

	jquery-ui.structure.css
	jquery-ui.theme.css
	jquery.contextmenu.js
	jquery.cookie.js
	jquery.dynatree.js
	jquery.dynatree.min.js
	jquery.jqGrid.min.js
	jquery.js
	jquery.searchFilter.js
	jquery.selectbox-0.6.1.js
	jquery.selectbox.css
	jquery.tablednd.js
	jquery.timepicker.css
	jquery.timepicker.d.ts
	jquery.timepicker.js
	jquery.timepicker.min.js
	json-simple-1.1.1.jar
	json2.js
	jt.timepicker.jquery.json
	jxl.jar
	last.gif
	lay-selectMoreButton.gif
	layer.jsp
	layer2.jsp
	left.gif
	leftMenu.jsp
	libjavaCmvp.so
	libKeySharpCryptoV1_5.so
	libsigar-amd64-linux.so
	line_lnb.gif
	lnb_1.gif
	lnb_1_on.gif
	lnb_2.gif
	lnb_2_on.gif
	lnb_3.gif
	lnb_3_on.gif
	lnb_4.gif

	lnb_4_on.gif
	lnb_5.gif
	lnb_5_on.gif
	loading.gif
	logback-classic-1.2.9.jar
	logback-core-1.2.9.jar
	logback-ext-spring-0.1.5.jar
	logback.xml
	login.jsp
	login_bg.gif
	login_bottom.gif
	login_fail.jsp
	login_ok.jsp
	login_top.gif
	logoutLayer.jsp
	MainFrame.jsp
	manager.gif
	manager_over.gif
	MANIFEST.MF
	mappingXml.prpertes
	modUserBasic.jsp
	mswimg.jpg
	mybatis-3.4.1.jar
	mybatis-spring-1.3.2.jar
	mysql-connector-java-8.0.21.jar
	my_macl.gif
	my_macl_on.gif
	next.gif
	odtimg.jpg
	org.jsp
	orgAddPopup.jsp
	orgBasicInfo.jsp
	orgBody.jsp
	orgDivAddPopup.jsp
	orgDivAdvanceInfo.jsp
	orgDivBasicInfo.jsp
	orgDivIndex.jsp

	orgIndex.jsp
	orgTree.jsp
	orgTreeOnActivate.jsp
	orgUserList.jsp
	package.json
	pdfimg.jpg
	pptimg.jpg
	prec.gif
	protobuf-java-3.11.4.jar
	pwdChange.jsp
	pwdChangePopup.jsp
	README.md
	resize.js
	root-context.xml
	scheduler.xml
	screenshot.png
	searchFilter.css
	searchResult.jsp
	securityAuth.js
	sensor-1.4.4.3-linux-x8664.jar
	sensor.conf
	service.jsp
	service.xml
	serviceAddPopup.jsp
	serviceBasicInfo.jsp
	serviceIndex.jsp
	serviceList.jsp
	serviceStructBody.jsp
	serviceStructureAddPopup.jsp
	serviceStructureBasicInfo.jsp
	serviceStructureIndex.jsp
	serviceTree.jsp
	servlet-context.xml
	sigar-1.6.6.jar
	site.css
	site.js
	sjxlsx-1.0.1.jar

	slf4j-api-1.7.32.jar
	solutionintegrity-1.5.0.2.jar
	spring-aop-3.2.18.RELEASE.jar
	spring-beans-3.2.18.RELEASE.jar
	spring-context-3.2.18.RELEASE.jar
	spring-core-3.2.18.RELEASE.jar
	spring-expression-3.2.18.RELEASE.jar
	spring-jdbc-3.2.18.RELEASE.jar
	spring-orm-3.2.18.RELEASE.jar
	spring-oxm-3.2.18.RELEASE.jar
	spring-security-acl-3.2.10.RELEASE.jar
	spring-security-config-3.2.10.RELEASE.jar
	spring-security-core-3.2.10.RELEASE.jar
	spring-security-taglibs-3.2.10.RELEASE.jar
	spring-security-web-3.2.10.RELEASE.jar
	spring-tx-3.2.18.RELEASE.jar
	spring-web-3.2.18.RELEASE.jar
	spring-webmvc-3.2.18.RELEASE.jar
	sqlMapConfig.xml
	SSL.crt
	SSL.csr
	SSL.jks
	SSL.key
	SSL.p12
	sub_manager.gif
	sub_manager_over.gif
	system.gif
	system.jsp
	systemLog.jsp
	systemLogGridList.jsp
	systemSearchHeader.jsp
	system_on.gif
	system_profile.jsp
	time.js
	ti_delegate_macl.gif
	ti_detail.gif
	ti_dsd.gif

	ti_group.gif
	ti_gro_detail.gif
	ti_importexport.gif
	ti_login.gif
	ti_loginincert.gif
	ti_logininPolicy_detail.gif
	ti_lumpprocess.gif
	ti_maclGroup.gif
	ti_maclGroup_detail.gif
	ti_my_macl.gif
	ti_org.gif
	ti_org_detail.gif
	ti_policy.gif
	ti_policy1.gif
	ti_policy2.gif
	ti_policy3.gif
	ti_policy_detail.gif
	ti_policy_detail2.gif
	ti_policy_detail3.gif
	ti_role.gif
	ti_role_detail.gif
	ti_role_detail2.gif
	ti_role_detail3.gif
	ti_sert_detail.gif
	ti_service.gif
	ti_ser_detail.gif
	ti_ser_tree.gif
	ti_set_detail.gif
	ti_set_detail2.gif
	ti_set_detail3.gif
	ti_set_detail4.gif
	ti_set_detail_admin.gif
	ti_ssd.gif
	ti_user.gif
	ti_user_view.gif
	topMenu.jsp
	transaction.xml

	uaclItem.jsp
	uaclList.jsp
	uaclListOfService.jsp
	uacl_config.jsp
	ui-bg_diagonals-thick_18_b81900_40x40.png
	ui-bg_diagonals-thick_20_666666_40x40.png
	ui-bg_flat_0_888888_40x100.png
	ui-bg_flat_0_aaaaaa_40x100.png
	ui-bg_flat_10_000000_40x100.png
	ui-bg_flat_55_fbec88_40x100.png
	ui-bg_flat_75_ffffff_40x100.png
	ui-bg_glass_100_f6f6f6_1x400.png
	ui-bg_glass_100_fdf5ce_1x400.png
	ui-bg_glass_25_e1f0f5_1x400.png
	ui-bg_glass_55_444444_1x400.png
	ui-bg_glass_55_fbf9ee_1x400.png
	ui-bg_glass_65_ffffff_1x400.png
	ui-bg_glass_75_dadada_1x400.png
	ui-bg_glass_75_e6e6e6_1x400.png
	ui-bg_glass_95_fef1ec_1x400.png
	ui-bg_gloss-wave_35_f6a828_500x100.png
	ui-bg_highlight-soft_100_eeeeee_1x100.png
	ui-bg_highlight-soft_75_cccccc_1x100.png
	ui-bg_highlight-soft_75_ffe45c_1x100.png
	ui-bg_inset-hard_100_fcfdfd_1x100.png
	ui-bg_inset-soft_95_fef1ec_1x100.png
	ui-icons_222222_256x240.png
	ui-icons_228ef1_256x240.png
	ui-icons_256x240.png
	ui-icons_2e83ff_256x240.png
	ui-icons_309bbf_256x240.png
	ui-icons_444444_256x240.png
	ui-icons_454545_256x240.png
	ui-icons_555555_256x240.png
	ui-icons_777620_256x240.png
	ui-icons_777777_256x240.png
	ui-icons_888888_256x240.png

	ui-icons_bf3030_256x240.png
	ui-icons_cc0000_256x240.png
	ui-icons_cd0a0a_256x240.png
	ui-icons_ef8c08_256x240.png
	ui-icons_ffd27a_256x240.png
	ui-icons_ffffff_256x240.png
	ui.dynatree.css
	ui.jqgrid.css
	ui.multiselect.css
	ui.multiselect.js
	user.gif
	userAddPopup.jsp
	userAdvanceInfo.jsp
	userBasicInfo.jsp
	userIndex.jsp
	userList.jsp
	userLog.jsp
	userLogGridList.jsp
	userSearchHeader.jsp
	user_on.gif
	viewdefines.xml
	virtualware_logo.gif
	virtualware_logo_small.gif
	VWIbatis.2.3.7.264base.vw.0.0.1.jar
	web.xml
	wpm-1.4.4.3.jar
	xmlbeans-2.3.0.jar
	Xstart
	Xstop

1.2 SSO Agent

1.2.1 api folder

path	File name
/home/cctest/wiseaccess_v1.4/demo/webapps/demo/integrity	jcl-over-slf4j-1.7.32.jar
	libjavaCmvp.so
	libKeySharpCryptoV1_5.so

	logback-classic-1.2.9.jar
	logback-core-1.2.9.jar
	logback.xml
	slf4j-api-1.7.32.jar
	sso.conf

1.2.2 ssoengine folder

path	File name
/home/cctest/wiseaccess_v1.4/demo/webapps/demo/integrity	gson-2.2.4.jar
	jcl-over-slf4j-1.7.32.jar
	libjavaCmvp.so
	libKeySharpCryptoV1_5.so
	libsigar-amd64-linux.so
	logback-classic-1.2.9.jar
	logback-core-1.2.9.jar
	mysql-connector-java-8.0.21.jar
	ojdbc6-11.2.0.4.jar
	sensor-1.4.4.3-linux-x8664.jar
	sensor.conf
	sigar-1.6.6.jar
	slf4j-api-1.7.32.jar
	solutionintegrity-1.5.0.2.jar
	sso_engine.conf
	sso_engined
	xenv
	xinfo
	xinfo_engine
	xstart
	xstart_engine
	xstop
	xstop_engine
	xversion
	xversion_engine