INITECH

1st Financial & Security Service

CCP.C_NX43_SecurityTarget(ST)_Lite_V1.0

INITECH Co., Ltd.

This document is a translation of the Security Target written in Korean which has been evaluated

Revision History

Ver	Date	Author	Revision
1.0	Sep.22, 2023	Suyeon Mun	Sanitized version of the CCP.C_NX43_SecurityTarget(ST)_V1.1

Table of Contents

List of Figures

List of Tables

1. ST introduction

This document is the Security Target (ST) of INISAFE Nexess V4.3 of INITECH Co., Ltd. It is conformant to EAL 1+ of the Common Criteria for Information Technology Security Evaluation.

1.1. ST reference

[Table 1] ST reference

Document Title	CCP.C_NX43_SecurityTarget(ST)_Lite
Version	V1.0
Author	INITECH Co., Ltd.

1.2. TOE Reference

[Table 2] TOE reference

TOE Identification	INISAFE Nexess V4.3
TOE Detailed Version	V4.3.1.2
TOE Component	Nexess Server V4.3.1.2 (Nexess_Server_4.3.1.2.zip) Nexess Agent V4.3.1.2 (Nexess_Agent_4.3.1.2.zip)
Guidance Document	CCP.C_NX43_PrepatativeProcedure(PRE)_V1.1 (CCP.C_NX43_PreparativeProcedure(PRE)_V1.1.pdf) CCP.C_NX43_OperationalGuidance(OPE)_V1.1 (CCP.C_NX43_OperationalGuidance(OPE)_V1.1.pdf)
Developer	INITECH Co., Ltd.

1.3. TOE overview

1.3.1. Single Sign On overview

INISAFE Nexess V4.3 (hereinafter referred to as the TOE) is used to enable the user to access various business systems to use the service through a single user log-in (Single Sign On) without additional login actions. The TOE performs user identification and authentication, authentication token issue and validity verification according to the user authentication policy.

The TOE shall provide the user login function using ID/PW authentication method, issue a token during user login, and verify the issued token if accessing another business system after user

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

1.3.2. TOE type and scope

The TOE is Single Sign On (SSO) that enables the user to access various business systems through a single user login, and the TOE is provided as software. The TOE components are the agent and the server. The TOE is composed of the server that processes user login, issues and verifies an authentication token and sets the policy, and the agent that is installed in each business system performs the function of token issue and verification.

1.3.3. TOE usage and major security features

The TOE performs user identification and authentication to enable the user to access various business systems to use the service through a single user login (Single Sign On) without additional login actions.

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

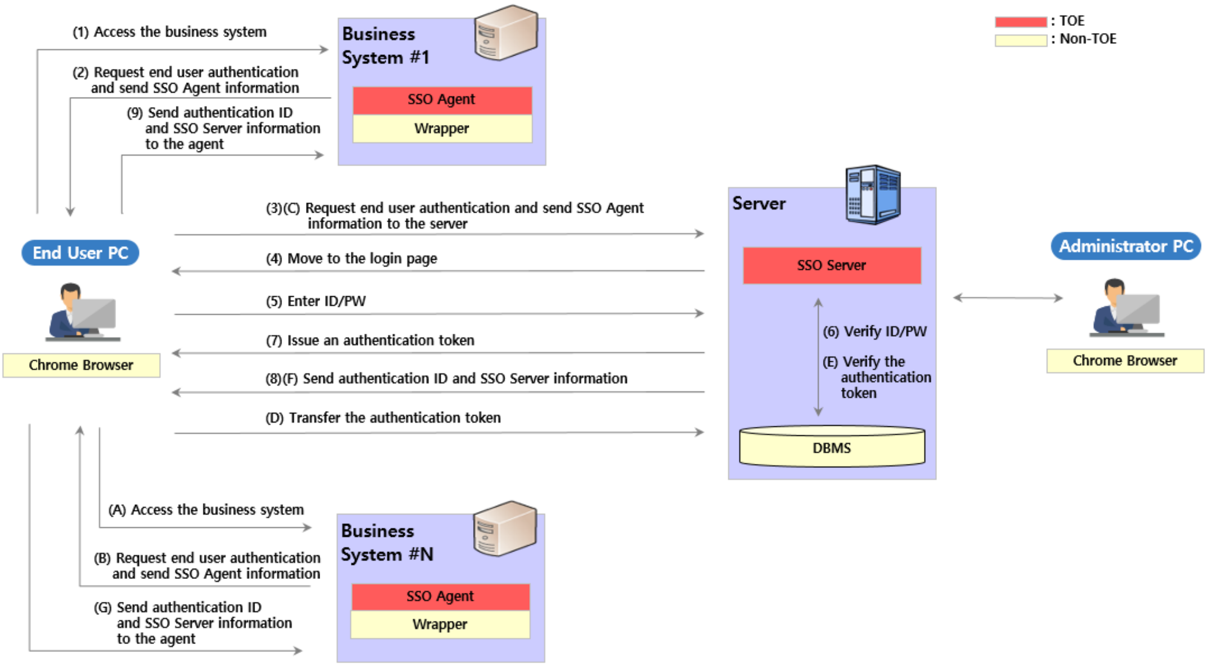
In addition, the TOE provides the function of testing the TOE's external entities.

(Figure 1) below shows the user identification and authentication procedure of the TOE.

The user identification and authentication procedure can be grouped into the initial authentication phase using the ID/password, and the token-based authentication phase that accesses the business system using the token issued during the initial authentication procedure.

The execution procedure of the initial authentication phase is as follows. The user requests login using the ID/password, and the SSO Agent that receives the login request message sends a login verification request to the SSO Server via a web browser on the user's personal computer, which in turn checks the authorized user status. Upon receiving the login verification request, the SSO Server performs login verification using the user information stored in the DBMS. The SSO Server issues an authentication token and transfers the issued token to the user if the login verification result is valid.

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


: TOE
: Non-TOE
(1) Access the business system
(2) Request end user authentication and send SSO Agent information
(9) Send authentication ID and SSO Server information to the agent
Business System #1
SSO Agent
Wrapper
(3)(C) Request end user authentication and send SSO Agent information to the server
(4) Move to the login page
(5) Enter ID/PW
(7) Issue an authentication token
(8)(F) Send authentication ID and SSO Server information
(D) Transfer the authentication token
End User PC
Chrome Browser
Server
SSO Server
(6) Verify ID/PW
(E) Verify the authentication token
DBMS
Administrator PC
Chrome Browser
(A) Access the business system
(B) Request end user authentication and send SSO Agent information
(G) Send authentication ID and SSO Server information to the agent
Business System #N
SSO Agent
Wrapper

(Figure 1) End user identification and authentication procedure

The table below describes the end user identification and authentication procedure.

[Table 3] Operation procedure by authentication phase

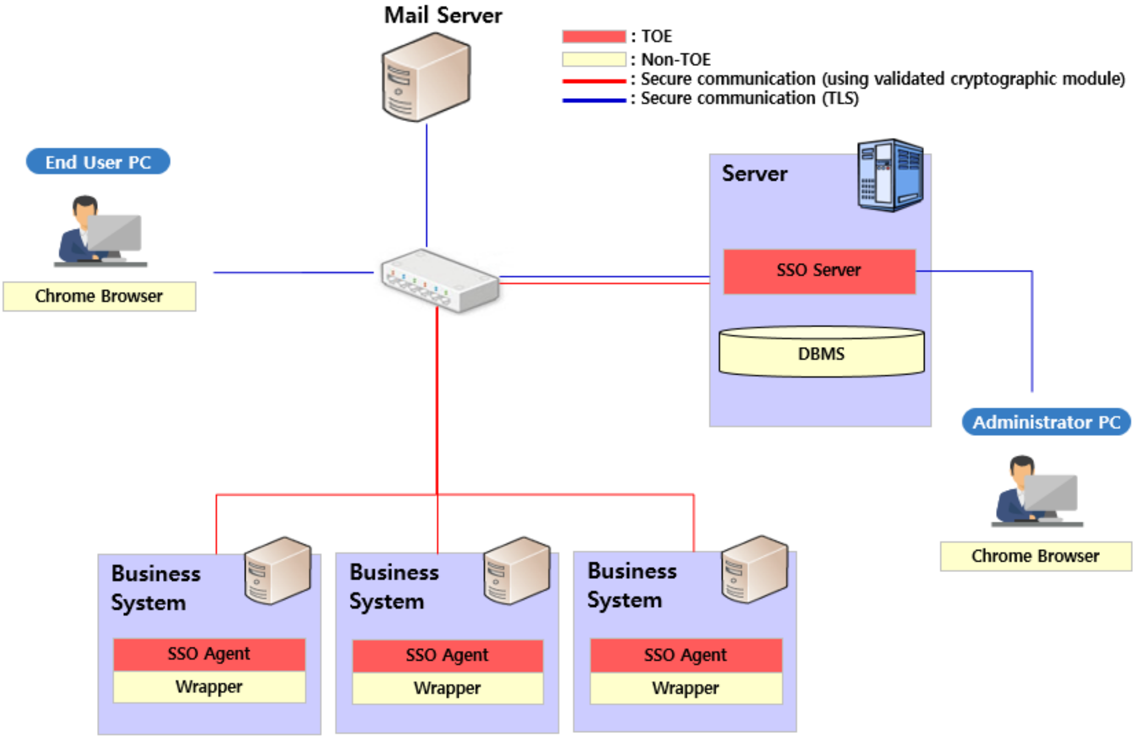
Authentication Phase	Operation Procedure
Initial authentication	(1) Access the business system ⟶ (2) Request end user authentication and send SSO Agent information ⟶ (3) Request end user authentication and send SSO Agent information to the server ⟶ (4) Move to the login page ⟶ (5) Enter ID/PW ⟶ (6) Verify ID/PW ⟶ (7) Issue an authentication token ⟶ (8) Send authentication ID and SSO Server

	information ⟶ (9) Send authentication ID and SSO Server information to the agent
Token-based authentication	(A) Access the business system ⟶ (B) Request end user authentication and send SSO Agent information ⟶ (C) Request end user authentication and send SSO Agent information to the server ⟶ (D) Transfer the authentication token ⟶ (E) Verify the authentication token ⟶ (F) Send authentication ID and SSO Server information ⟶ (G) Send authentication ID and SSO Server information to the agent

In addition, the subject who issues, stores, and verifies the token can be different, depending on the implementation. The subject who issues, stores, and verifies the token is as follows:

- Subject who issues the token: SSO Server
- Token storage location: SSO Server
- Subject who verifies the token: SSO Server

1.3.4. Non-TOE and TOE operational environment



(Figure 2) TOE operational environment

The TOE operational environment (Figure 2) is composed of the SSO Server and the SSO Agent. The SSO Server verifies user login attempts directly using the user information stored in the

DBMS. The SSO Agent is installed in each business system and requests end user login verification to the SSO Server. The authorized administrator performs the security management by accessing the SSO Server via a web browser. Wrappers which are used to support compatibility with business systems are out of the TOE scope. A mail server is used as an external entity necessary for the operation of the TOE.

[Table 4] Requirements for non-TOE operational environment

Category	Requirements for Operational Environment	
SSO Server	S/W	- JDK 1.8.0_202 - Apache Tomcat 9.0.80 - Oracle 19c(19.3)
	H/W	- Processor: intel(R) Core(TM) i7-1165G7 2.8Ghz or higher - Memory: 16GB or higher - Hard disk: 50GB or higher necessary for TOE installation - NIC: 10/100/1000 X 1Port or higher
	OS	- Windows 10 Pro 64bit
SSO Agent	S/W	- JDK 1.8.0_202 - Apache Tomcat 9.0.80
	H/W	- Processor: intel(R) Core(TM) i7-6500U 2.5GHz or higher - Memory: 8GB or higher - Hard disk: 50GB or higher necessary for TOE installation - NIC: 10/100/1000 X 1Port or higher
	OS	- Windows 10 Pro 64bit

The 3rd party S/W required for the TOE is as follows:

[Table 5] TOE 3rd-party S/W

Category	Role
JDK 1.8.0_202	- Protect the data transmitted between a web browser on the administrator PC and the SSO Server - Protect the data transmitted between a web browser on the end user PC and the SSO Agent

Apache Tomcat 9.0.80	- Provide the administrator security management function - Use Tomcat security - Set TLS for safe communication - Session timeout handling
Oracle 19c(19.3)	- Store user information - Store session and authentication token - Store audit logs

[Table 6] External entity

Category	Description and Role
Mail server	- Server that is interlinked with SSO Server to send a warning email to the administrator

The administrator requires the following operational environment in order to access the TOE. The administrator performs the roles of SSO Server configuration, status check, audit log search, etc. by using a web browser.

[Table 7] Requirements for operational environment for the administrator

Category	Item	Description
Administrator PC	S/W	- Web browser: Chrome 114

1.4. TOE description

1.4.1. Physical scope of the TOE

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

[Table 8] Physical scope of the TOE

Category		Identification	Form	Delivery Method
TOE identification		INISAFE Nexess V4.3		
TOE detailed version		V4.3.1.2		
TOE component	SSO Server	Nexess Server V4.3.1.2 (Nexess_Server_4.3.1.2.zip)	Installation program	CD-ROM (1EA)

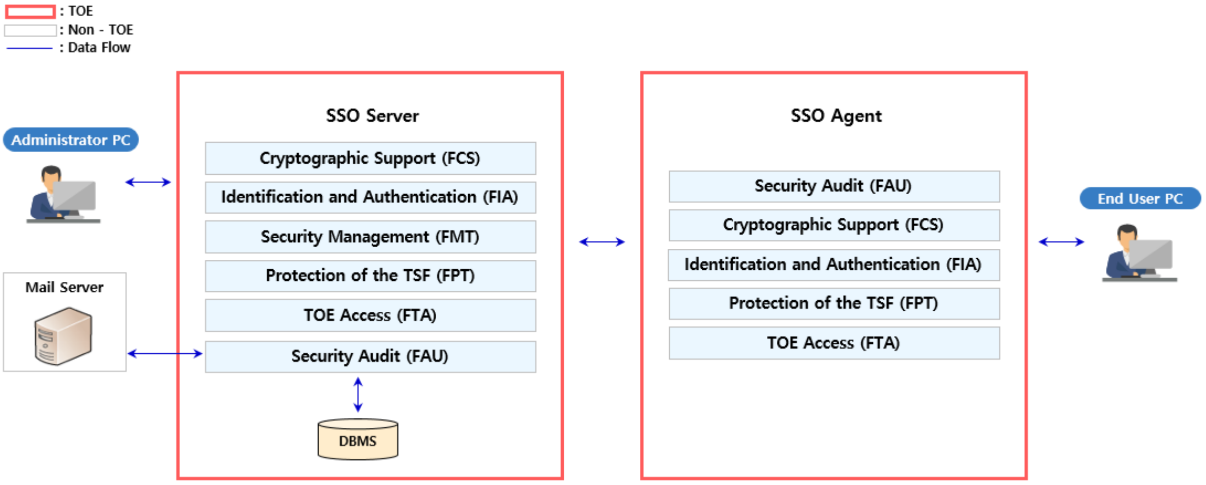
	SSO Agent	Nexess Agent V4.3.1.2 (Nexess_Agent_4.3.1.2.zip)	(S/W)	
Guidance document		CCP.C_NX43_PreparativeProcedure(PRE)_V1.1 (CCP.C_NX43_PreparativeProcedure(PRE)_V1.1.pdf)	Electronic document (PDF)	
		CCP.C_NX43_OperationalGuidance(OPE)_V1.1 (CCP.C_NX43_OperationalGuidance(OPE)_V1.1.pdf)		
Validated cryptographic module		INISAFE Crypto for Java V4.2.0 INISAFE Crypto for C v5.4		

The validated cryptographic module included in the TOE is as follows:

[Table 9] Validated cryptographic module

Cryptographic Module Name	Category	Detailed Category	Remarks
INISAFE Crypto for Java V4.2.0	Validation No.	CM-171-2025.10	Used for all cryptographic functions, except for KEK (Key Encryption Key) generation function
	Validation date	Oct. 15, 2020	
	Developer	INITECH Co., Ltd.	
INISAFE Crypto for C v5.4	Validation No.	CM-233-2028.6	Used for KEK (Key Encryption Key) generation function
	Validation date	June 19, 2023	
	Developer	INITECH Co., Ltd.	

1.4.2. Logical scope of the TOE


: TOE
: Non - TOE
: Data Flow
Administrator PC
Mail Server
SSO Server
Cryptographic Support (FCS)
Identification and Authentication (FIA)
Security Management (FMT)
Protection of the TSF (FPT)
TOE Access (FTA)
Security Audit (FAU)
DBMS
SSO Agent
Security Audit (FAU)
Cryptographic Support (FCS)
Identification and Authentication (FIA)
Protection of the TSF (FPT)
TOE Access (FTA)
End User PC

(Figure 3) Logical scope of the TOE

- Security Audit (FAU)

  The SSO Server provides the functions of detecting potential violations regarding security relevant actions and generating audit records. Records are generated for all actions made by users in a chronological order. Audit data related to authentication failures of the authorized administrator and end users generated in the SSO Server and the SSO Agent, and audit records such as successful and failed self tests are stored in the DBMS through the SSO Server. It provides the authorized administrator with the function of reviewing all audit data, and the function of selective viewing of audit data according to the logic relation criteria. In addition, in case the audit data reaches the threshold (90%), it is notified to the administrator via email, and in case the audit data exceeds the limit (95%), a warning email is sent to the authorized administrator, and audited events additionally generated are ignored. Regarding the time used in audit records, timestamps are provided by the reliable operating system.

- Cryptographic Support (FCS)

  The SSO Server and the SSO Agent performs cryptographic operations by using the validated cryptographic module (INISAFE Crypto for Java V4.2.0, INISAFE Crypto for C v5.4). The server information, the agent information, and authorized user ID, which are used for mutual authentication, are encrypted and decrypted with RSAES, and then transmitted. The server information and the agent information stored in the SSO Server and the SSO Agent are encrypted with SEED and then stored. The administrator password and the end user passwords are hashed using SHA256 and stored. A key used to encrypt the TSF data, excluding the administrator password and the end user passwords, is generated using HASH_DRBG(SHA-256), and the encryption and decryption are performed using SEED. In this case, the key (DEK) used for the encryption and decryption of the TSF data is encrypted and stored, using a key (KEK) generated using PBKDF. An authentication token used for the SSO authentication is protected with HMAC_SHA256.

- Identification and Authentication (FIA)

  The SSO Server performs the identification and authentication based on IDs and passwords in order to verify the authorized administrator and end users. In the process of the identification and authentication, a password being entered is masked (password masking with *) and the TOE does not provide feedback on authentication failure. In addition, if the limit of five unsuccessful authentication attempts for the authorized administrator and end users has been surpassed, the following actions are taken.

  - Authorized administrator: inactivate the identification and authentication function (10 minutes), and send a warning email
  - End user: lock the account until the authorized administrator allows unlocking

  The SSO Server prevents the reuse of authentication data related to password-based authentication mechanism and authentication token-based authentication mechanism, and performs the function of issuing, verifying and destroying an authentication token. The SSO Server and the SSO Agent perform mutual authentication by using "INI_NX protocol."

- Security Management (FMT)

  The SSO Server provides the security management function to enable the authorized administrator to set and manage the security function and the TSF data. Only one authorized administrator role has been defined.

- Protection of the TSF (FPT)

  The TSF data transmitted between the SSO Server and the SSO Agent are protected against disclosure or modification by using HTTPS communication. In addition, authorized administrator and end user account information, DB access account information, authentication tokens, cryptographic keys, security policies and configuration parameters stored in a container controlled by the TSF are protected against disclosure and modification by using SEED encryption.

  The SSO Server and the SSO Agent run TSF self tests and the integrity verification of the TSF and the TSF data during initial start-up, periodically during normal operation, and at the request of the authorized administrator. The SSO Server runs tests of external entities to ensure that abnormal conditions of external entities, such as mail server, DBMS (Oracle) and WAS (Tomcat), do not affect the major functions and the security functions of the TOE.

- TOE Access (FTA)

  The SSO Server denies the activation of management access session of the same account as the authorized administrator's management access session establishment, and restricts the number of connection IPs allowed for the authorized administrator to access to two. The maximum number of concurrent sessions accessible by the authorized administrator and an end user is limited to one, respectively, and an interacting session is terminated if it remains inactive for 10 minutes.

1.5. Conventions

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

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

Iteration

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

Assignment

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

Selection

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

Refinement

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

Security Target (ST) Author

This is used to represent the final decision of attributes being made by the ST author. The ST author's operation is denoted in braces, as in {decided by the ST author}. In addition, operations of SFR not completed in the Protection Profile must be completed by the ST author.

"Application notes" is provided to clarify the intent of requirements in this ST. The application notes is provided with corresponding requirements if necessary.

1.6. Terms and definitions

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

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

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

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

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

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

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

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

Random bit generator (RBG)

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

Security Target (ST)

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

Security Policy Document

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

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Decryption

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

Secret key

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

User

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

Selection

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

Identity

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

Encryption

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

Korea Cryptographic Module Validation Program (KCMVP)

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

Business system

An application server that authorized end users access through "SSO"

Element

Invisible statement of a security need

Role

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

Operation (on a component of the CC)

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

Operation (on an object)

Specific type of action performed by a subject on an object

External entity

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

Authorized administrator

Authorized user to securely operate and manage the TOE

End user

Users of the TOE who want to use the business system, not the administrator of the TOE

Authentication data

Information used to verify a user's claimed identify

Authentication token

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

Self-test

Pre-operational or conditional test executed by the cryptographic module

Refinement

Addition of details to a component

Dependency

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

Subject

Active entity in the TOE that performs operations on objects

Sensitive Security Parameters (SSP)

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

Augmentation

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

Component

Smallest selectable set of elements on which requirements may be based

Class

Set of CC families that share a common focus

Family

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

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

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

Assignment

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

Critical Security Parameters (CSP)

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

Database Management System (DBMS)

A software system composed to configure and apply the database

Secure Sockets Layer (SSL)

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

Transport Layer Security (TLS)

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

Wrapper

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

2. Conformance claim

2.1. CC conformance claim

[Table 10] CC conformance claim

Common Criteria		Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 - Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
Conformance Claim	**Part 2 Security Functional Components**	Extended: FCS_RBG.1, FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security Assurance Components	Conformant
	Package	Augmented: EAL1 augmented(ATE_FUN.1)

2.2. PP conformance claim

This ST conforms to the “Korean National Protection Profile for Single Sign On V1.1.”

2.3. Package conformance claim

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

- Assurance package: EAL1 augmented(ATE_FUN.1)

2.4. Conformance claim rationale

This ST “strictly conforms to the PP” in accordance with the PP conformance method described in the “Korean National Protection Profile for Single Sign On V1.1.” This ST adopts the TOE type, security objectives and security requirements in the same manner as the PP it conforms to.

3. Security objectives

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

3.1. Security objectives for the operational environment

[Table 11] Identification of security objectives for the operational environment

TOE Security Objective	Description
OE.PHYSIAL_CONTROL	The place where SSO Agent and SSO Server, among the TOE components, are installed and operated shall be equipped with access control and protection facilities so that only the authorized administrator can access.
OE.TRUSTED_ADMIN	The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidances.
OE.LOG_BACKUP	The authorized administrator shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.
OE.OPERATION_SYSTEM_ REINFORCEMENT	The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
OE.SECURE_DEVELOPMENT	The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.
OE.SECURE_DBMS	Security policies and audit records stored in the TOE are stored in the database. The database shall not be generated, modified or deleted without a request from the TOE.
OE.TIME_STAMP	The TOE shall accurately record security-relevant events by using reliable time stamps provided by the TOE operational environment.
OE.SECURE_CHANNEL	A secure communication shall be ensured between a web browser on a

	end user PC and the SSO Agent, and between a web browser on the authorized administrator PC and the SSO Server.

4. Extended components definition

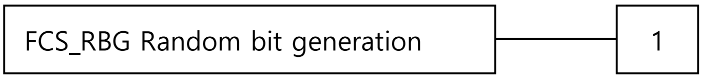
4.1. FCS, Cryptographic support

4.1.1. Random bit generation

Family Behaviour

This family (FCS_RBG, Random Bit Generation) defines requirements for 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.

FCS_RBG.1	**Random bit generation**	
	Hierarchical to	No other components
	Dependencies	No dependencies

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

4.2. FIA, Identification & authentication

4.2.1. TOE internal mutual authentication

Family Behaviour

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

Component Levelling

FIA_IMA TOE internal mutual authentication
1

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

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

Audit: FIA_IMA.1

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

a) Minimum: Success and failure of mutual authentication

4.2.1.1. FIA_IMA.1 TOE internal mutual authentication

Hierarchical to	No other components
Dependencies	No dependencies

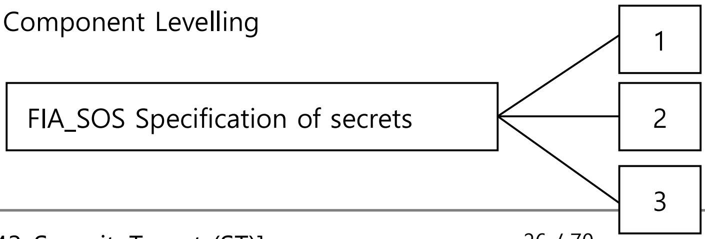
FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] using the [assignment: *authentication protocol*] that meets the following [assignment: *list of standards*].

4.2.2. Specification of secrets

Family Behaviour

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

Component Levelling



The specification of secrets family in CC Part 2 is composed of 2 components. It is now composed of three components, since the "Korean National Protection Profile for Single Sign On V1.1" adds one more component as below.
※ The description of 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 Generation of secrets

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

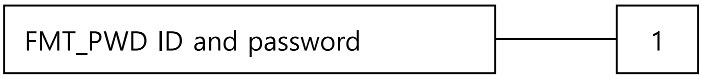
4.3. FMT, Security management

4.3.1. ID and password

Family Behaviour

This family (FMT_PWD, ID and password) 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 levelling



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

Management: FMT_PWD.1

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

a) Management of ID and password configuration rules

Audit: FMT_PWD.1

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

a) Minimum: All changes of the password

4.3.1.1 FMT_PWD.1 Management of ID and password

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

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

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

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

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

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

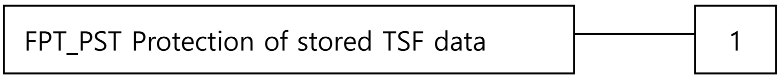
4.4. FPT, Protection of the TSF

4.4.1. Protection of stored TSF data

Family Behaviour

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

Component Levelling



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

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

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

4.4.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to	No other components
Dependencies	No dependencies

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

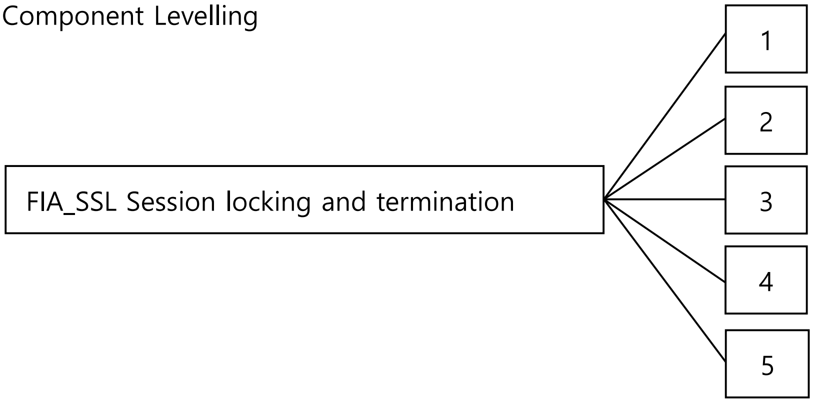
4.5. FTA, TOE access

4.5.1. Session locking and termination

Family Behaviour

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

Component Levelling



In CC Part 2, the session locking and termination family consists of four components. In the "Korean National Protection Profile for Single Sign On V1.1," it consists of five components by extending one additional component as follows.

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

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

Management: FTA_SSL.5

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

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

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

Audit: FTA_SSL.5

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

a) Minimum: Locking or termination of interactive session

4.5.1.1. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to	No other components
Dependencies	FIA_UAU.1 Authentication or no dependencies

FTA_SSL.5.1 The TSF shall [selection:

- *lock the session and/or 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 that adopts this ST.

5.1. Security functional requirements

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

[Table 12] Security functional requirements

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_RBG.1(Extended)	Random bit generation
Identification and authentication (FIA)	FIA_AFL.1(1)	Authentication failure handling (authorized administrator)
	FIA_AFL.1(2)	Authentication failure handling (end user)
	FIA_IMA.1(Extended)	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data

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

5.1.1. Security audit (FAU)

FAU_ARP.1 Security alarms

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [actions against security violations] upon detection of a potential security violation.

[Table 13] Actions against security violations

Security Violation	Action
Authentication failure audit events, among auditable events in FIA_UAU.2 and FIA_AFL.1(1)	· Inactivate the identification and authentication function for the authorized administrator (10 minutes) · Send a warning email to the authorized administrator
Authentication failure audit events, among auditable events in FIA_UAU.2 and FIA_AFL.1(2)	· lock the account for end users until the authorized administrator allows unlocking
Self-testing failure and integrity verification failure events specified in FPT_TST.1	· Send a warning email to the authorized administrator

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 shut-down of the audit functions;

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

c) [Refer to “auditable event” in **오류! 참조 원본을 찾을 수 없습니다.**, [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 identify (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Refer to the contents of “additional audit record” in [Table 14] Auditable events, [None]]

[Table 14] Auditable events

Security Functional Component	Auditable Event	Additional Audit Record
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (only applying to key distribution related to the TSF data encryption/decryption)	
FCS_CKM.4	Success and failure of the activity (only applying to key destruction related to the TSF data encryption/decryption)	
FCS_COP.1	Success and failure, and the type of cryptographic operation(only applying to items related to the issue, storing, verification, and destruction of a token)	
FIA_AFL.1(1)(2)	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	
FIA_SOS.2	Rejection by the TSF of any tested secret	
FIA_SOS.3(Extended)	Success and failure of the activity (applicable to the destruction of SSO token only)	
FIA_UAU.2	User authentication before any action	

FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.2	User identification before any action	
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	Modification to the user group of rules divided	
FPT_TEE.1	Successful or failed testing of external entities	
FPT_TST.1	Execution of the TSF self-tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5(Extended)	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

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

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

a) Accumulation or combination of [authentication failure audit event among auditable events in FIA_UAU.2, FIA_AFL.1(1) and FIA_AFL.1(2), failure of self-tests and integrity violation event in FPT_TST.1] known to indicate a potential security violation;

b) [None]

FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

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

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

FAU_SAR.3 Selectable audit review

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

FAU_SAR.3.1 The TSF shall provide the ability to apply ["selection method" and "ordering method" in [Table 15]] of audit data based on [criteria with logical relations in [Table 15]].

[Table 15] Criteria with logical relations by log type

Log Type	Criteria with Logical Relations	Selection Method	Ordering Method
System test history	System test name, search word, date and time of event (start date, end date)	AND	-
	System name, search word, date and time of event (start date, end date)	AND	-
	Registration time	-	Descending order
User history	ID, search word, date and time of event (start date, end date)	AND	-
	Name, search word, date and time of event (start date, end date)	AND	-
	Audit time	-	Descending order
Administrator history	ID, search word, date and time of event (start date, end date)	AND	-
	Name, search word, date and time of event (start date, end date)	AND	-
	Audit time	-	Descending order
Security policy change	System name, search word, date	AND	-

history	and time of event (start date, end date)		
	Policy name, search word, date and time of event (start date, end date)	AND	-
	Registration time	-	Descending order
Service start-up history	Service name, search word, date and time of event (start date, end date)	AND	-
	Operation, search word, date and time of event (start date, end date)	AND	-
	Operation time	-	Descending order

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 [90%].

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 *ignore audited events* and [notify the authorized administrator via email] if the audit trail is full.

5.1.2. Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ["Cryptographic key generation algorithm" in [Table 16]] and specified cryptographic key sizes in ["Cryptographic key size" in [Table 16]] **오류! 참조 원본을 찾을 수 없습니다.**that meet the following ["list of standards" in [Table 16]].

[Table 16] List of standards for cryptographic key generation

List of Standards	Cryptographic Key Generation Algorithm	Cryptographic Key Size
ISO/IEC 18033-2(2016) IETF RFC 8017(2016)	RSAES (SHA-256)	2048
KS X ISO/IEC 18031(2018) TTAK.KO-12.0331- Part1(2018) TTAK.KO-12.0331- Part2(2018)	HASH-DRBG (SHA-256)	256

TTAK.KO-12.0334-Part1(2018)
TTAK.KO-12.0334-Part2(2018)
	PBKDF (SHA 256)	256

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 [offline distribution of Private Key Value for Agent Private Key generation, Public Key Value for Server Public Key generation, and DEK encrypted with KEK] that meets the following [None].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ["cryptographic key destruction method" in [Table 17] Destruction method by cryptographic key type] that meets the following [None].

[Table 17] Destruction method by cryptographic key type

Cryptographic Key	Cryptographic Key Destruction Method

Cryptographic key for server and agent information used for mutual authentication	Overwrite with ‘00’
Cryptographic key for authenticated user ID	Overwrite with ‘00’
Cryptographic key for TSF data	Overwrite with ‘00’
KEK for the encryption of cryptographic key for TSF data	Overwrite with ‘00’

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

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

FCS_COP.1.1 The TSF shall perform [“list of cryptographic operations” in [Table 18] Cryptographic operation] in accordance with a specified cryptographic algorithm [“cryptographic algorithm” in [Table 18] Cryptographic operation] and cryptographic key sizes [“cryptographic key sizes” in [Table 18] Cryptographic operation] that meet the following [“list of standards” in [Table 18] Cryptographic operation].

[Table 18] Cryptographic operation

List of Standards	Cryptographic Algorithm	Cryptographic Key Sizes	List of Cryptographic Operations
ISO/IEC 18033-2(2016) IETF RFC 8017(2016)	RSAES	2048 bits	Encryption/decryption of mutual authentication information and authenticated user ID
KS X ISO/IEC 18033-3(2018) TTAS.KO-12.0004/R1(2005) TTAK.KO-12.0271- Part1/R1(2016) TTAK.KO-12.0274-Part4(2017)	SEED (CBC Mode)	128 bits	Encryption/decryption of TSF data
KS X ISO/IEC 18033-3(2018) TTAS.KO-12.0004/R1(2005) TTAK.KO-12.0271- Part1/R1(2016) TTAK.KO-12.0274-Part4(2017)	SEED (CBC Mode)	128 bits	Encryption/decryption of cryptographic key for TSF data
KS X ISO/IEC 9797-2(2018) TTAK.KO-12.0330-Part2(2018)	HMAC_SHA256	256 bits	Authentication token generation and verification

ISO/IEC 10118-3(2018)	SHA-256	256 bits	User secret information encryption

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 [KS X ISO/IEC 18031(2018), TTAK.KO-12.0331-Part1(2018), TTAK.KO-12.0331-Part2(2018)].

5.1.3. Identification and authentication (FIA)

FIA_AFL.1(1) Authentication failure handling (authorized administrator)
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall [the following list of actions].

[

- Inactivating the identification and authentication function (10 minutes)
- Sending a warning email

]

FIA_AFL.1(2) Authentication failure handling (end user)
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *[5]* unsuccessful authentication attempts occur related to [the end user authentication attempt].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall [lock the account until the authorized administrator allows unlocking].

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 [the SSO Server and the SSO Agent] using the [INI_NX protocol] that meets the following [None].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components
Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined quality metric].

[

a) Allowable characters

- At least one English alphabet, one number and one special character must be included.

b) Min/Max length

- 9 ~ 16 digits

c) Change interval (the period during which password is used)

- 30 days

]

FIA_SOS.2 Generation of secrets

Hierarchical to: No other components
Dependencies: No dependencies

FIA_SOS.2.1 The TSF shall provide a mechanism to generate **authentication tokens** that meet [the following defined quality metric].

[

a) Mechanism to generate authentication tokens

- Authentication information components
  - User ID, user IP, authentication time (timestamp), integrity value
- Implementation method of authentication information: HMAC
- Field length: 256
- Subject that generates authentication information
  - SSO Server

]

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

FIA_SOS.3 **Destruction of secrets (Extended)**

Hierarchical to: No other components

Dependencies: FIA_SOS.2 Generation of secrets

FIA_SOS.3.1 The TSF shall destroy authentication tokens in accordance with a specified authentication tokens destruction method [overwriting 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 [password-based authentication mechanism, authentication token-based authentication mechanism].

FIA_ UAU.7 **Protected authentication feedback**

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

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

[

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

]

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 19] list of security functions behaviour of the administrator] to [the authorized administrator].

[Table 19] List of security functions behaviour of the administrator

Administrator Type	Classification	Security Function	Ability			
			Determine the behaviour	Disable	Enable	Modify the behaviour
	Log out		-	-	O	-
	SYSTEM	Business system management > Config File	-	-	O	-
		Business system management > Meta Data XML	-	-	O	-
		System test	-	-	O	-

(※ Legend: - not supported, ○ supported)

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 [[Table 20] List of TSF data and management ability] to [the authorized administrator].

[Table 20] List of TSF data and management ability

Administrator	TSF Data	Ability

Type		Query	Modify	Delete	Generate
Authorized administrator	User management	○	○	○	○
	User session view	○	-	-	-
	Administrator management	○	○	-	-
	Business system management	○	○	○	○
	System test	○	-	-	-
	System policy management	○	○	-	-
	System test history	○	-	-	-
	User history	○	-	-	-
	Administrator history	○	-	-	-
	Security policy change history	○	-	-	-
	Service startup history	○	-	-	-

(※ Legend : - not supported, ○ supported)

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 [None] to [None].

1. [None]
2. [None]

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

1. [None]
2. [None]

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

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

[

- Management functions of TSF: Management functions specified in FMT_MOF.1
- Management of TSF data: Management functions 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].

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)

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

Hierarchical to: No other components

Dependencies: No dependencies

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

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

Hierarchical to: No other components

Dependencies: No dependencies

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

[

- User account information (administrator, end user)
- DB access account information
- Mail server access account information
- Authentication token
- Cryptographic key
- TOE set value (security policy, configuration parameter)

]

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TEE.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation, at the request of the authorized **administrator*** to check the fulfillment of [list of properties of the external entities in [Table 21]].

[Table 21] List of testing of external entities and action

List of Properties of the External Entities	Action	Interval
Mail server availability	Warning pop-up in the administrator login screen	During initial start-up, at the request of the authorized administrator
DBMS (Oracle) availability of SSO Server	Send an email	During initial start-up, periodically during normal operation, at the request of the authorized administrator
WAS (Tomcat) availability of SSO Server	Send an email	
WAS (Tomcat) availability of SSO Agent	Send an email	

FPT_TEE.1.2 If the test fails, the TSF shall perform [actions in [Table 21]].

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 in [Table 22]]*.

[Table 22] Items subject to TSF self test

Classification	TSF
SSO Server	IDP, ADMIN, validated cryptographic module
SSO Agent	SP

FPT_TST.1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of *[TSF data in [Table 23]]*

[Table 23] Items subject to TSF data integrity test

Classification	TSF Data
SSO Server	TSF data (configuration)
SSO Agent	Files subject to integrity verification (checksum.list) ssoAgentPrivateKey.key ssoAgentPublicKey.key ssoServerPublicKey.key encryptDEK.key salt.key

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity of *[[TSF in [Table 24]]*.

[Table 24] Items subject to TSF integrity test

Classification	TSF
SSO Server	TSF, validated cryptographic module
SSO Agent	sso.saml.jar INICrypto_v4.2.0.jar INICommonCrypto.jar INISAFECore-v2.2.40.jar INISAFEPKI-v1.1.42.jar CryptoC.dll inicrypto_v5.4.0_64.dll

5.1.6. TOE access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

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

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [the number of maximum concurrent sessions as 1 for the administrator management access sessions, the number of maximum concurrent sessions as 1 for end user access, rules for the number of maximum concurrent sessions {None}].

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

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

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication or No dependencies

FTA_SSL.5.1 The TSF shall *terminate* an interactive session after [10 minutes].

Application notes: User means the authorized administrator and end user.

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components

Dependencies: No dependencies

FTA_TSE.1.1 The TSF shall be able to deny the **administrator's management access session** establishment based on [connection IP].

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

5.2. Security assurance requirements

Security assurance requirements of this ST are composed of assurance components in Common Criteria Part 3 and the evaluation assurance level is EAL1+. The table below summarizes assurance component.

[Table 25] Security assurance requirements

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

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 claim

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_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

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

Evaluator action elements

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

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

5.2.4. Life-cycle support

ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements

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

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies

Developer action elements

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

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

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

Evaluator action elements

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

5.2.5. Tests

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

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

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

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

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

Evaluator action elements

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

ATE_IND.1 Independent testing: conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.6. Vulnerability assessment

AVA_VAN.1 Vulnerability survey

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker processing Basic attack potential.

5.3. Security requirements rationale

5.3.1. Dependency rationale of security functional requirements

The following table shows dependency of security functional requirements.

[Table 26] Rationale for the dependency of the security functional requirements

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

28	FPT_PST.1	-
29	FPT_STM.1	-
30	FPT_TST.1	-
31	FTA_MCS.2	FIA_UID.1
32	FTA_SSL.5	FIA_UAU.1 or No dependencies
33	FTA_TSE.1	-

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

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

Rationale (3): FIA_AFL.1, FIA_UAU.7 and FTA_SSL.5 have the dependency on FIA_UAU.1. However, it is satisfied by FIA_UAU.2 hierarchical to FIA_UAU.1.

Rationale (4): FIA_UAU.2, FMT_SMR.1 and FTA_MCS.2 have the dependency on FIA_UID.1. However, it is satisfied by FIA_UID.2 hierarchical to FIA_UID.1.

5.3.2. Dependency rationale of security assurance requirements

As the dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.
The augmented SAR ATE_FUN.1 has the dependency on ATE_COV.1. However, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation. ATE_COV.1 is not included in this ST since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

6.1. Security audit (FAU)

Security audit function of the TOE consists of audit data generation and collection, audit data view and review, potential violation analysis and action, and management of audit storage.

6.1.1. Audit data generation and collection

Audit data on start-up and shut-down of the TOE, and audit data generated from each TOE component (SSO Server and SSO Agent) related to auditable events in "[Table 14] Auditable events" are stored in the DBMS (Oracle), an audit trail storage.
Information recorded when audit records are generated is date and time of the event, type of event, subject identity (if applicable) and the outcome (success or failure) of the event. In the case of audit records on certain auditable events, additional audit records in "[Table 14] Auditable events" are included.

SFR to be satisfied: FAU_GEN.1

6.1.2. Potential violation analysis and action

The TSF takes actions in "[Table 13] Actions against security violations" if a potential security violation is detected, based on the generated audit records (refer to 6.1.1). If audit events on the authorized administrator's authentication failure are accumulated, the identification and authentication function for the authorized administrator is inactivated for 10 minutes, and a warning email is sent to the authorized administrator. In addition, if audit events on an end user's authentication failure are accumulated, the end user's account is locked until the authorized administrator allows unlocking. If an event of failed self test of the TOE or failed integrity verification occurs, a warning email is sent to the authorized administrator.

SFR to be satisfied: FAU_ARP.1, FAU_SAA.1

6.1.3. Management of audit storage

Audit data of the TOE are stored in the DBMS (Oracle) of the SSO Server. The SSO Server checks the utilization rate (%) of the audit trail storage every 60 minutes, and if the utilization rate exceeds 90%, it sends a warning email to the authorized administrator. Furthermore, if the utilization rate of the audit trail storage exceeds 95% (audit trail storage is full), a warning email is sent to the authorized administrator, and additionally generated audit events are ignored.

The utilization rate of the audit trail storage means the percentage (%) used compared to the total capacity of the storage where the SSO Server and the DBMS are installed.

SFR to be satisfied: FAU_STG.3, FAU_STG.4

6.1.4. Audit data view and review

Once the authorized administrator succeeds in the identification and authentication in the SSO Server, he/she can view all audit data stored in the DBMS (Oracle), which is an audit trail storage, by using menus on the security management screen. The authorized administrator can select and view audit data according to criteria with logical relations, selection methods and ordering methods described in "[Table 15] Criteria with logical relations by log type."

SFR to be satisfied: FAU_SAR.1, FAU_SAR.3

6.2. Cryptographic support (FCS)

The TOE performs the function of cryptographic key generation, distribution, operation and destruction by using a validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP). The followings are the information on the validated cryptographic module.

[Table 27] Validated cryptographic module

Cryptographic Module Name	Validation Date	Validation No.
INISAFE Crypto for Java V4.2.0	October 15, 2020	CM-171-2025.10
INISAFE Crypto for C v5.4	June 19, 2023	CM-233-2028.6

6.2.1. Cryptographic key generation and random bit generation

The table below shows the list of standards, cryptographic key generation algorithms, cryptographic key sizes and usage for the generation of cryptographic key used in the TOE.

[Table 28] Cryptographic key and random bit generation algorithms

List of Standards	Algorithm	Cryptographic Key Size	Usage	Validated Cryptographic Module
ISO/IEC 18033-2(2016) IETF RFC 8017(2016)	RSAES (SHA-256)	2048	Communication section (mutual authentication)	INISAFE Crypto for Java V4.2.0

			- Encryption/decryption of server and agent information within the transmitted data	
ISO/IEC 18033-2(2016) IETF RFC 8017(2016)	RSAES (SHA-256)	2048	Encryption/decryption of authenticated user ID	INISAFE Crypto for Java V4.2.0

KS X ISO/IEC 18031(2018)
TTAK.KO-12.0331-Part1(2018)
TTAK.KO-12.0331-Part2(2018)
	HASH-DRBG (SHA-256)	256	Encryption/decryption of TSF data (DEK)
			- Security setting
			- Server information
			- Agent information
			- Agent Private Key Value
			- Agent Public Key Value
			- Agent to Server Public Key Value
			- Server Private Key Value
			- Server Public Key Value
			- Server to Agent Public Key Value
			- DB password
				INISAFE Crypto for Java V4.2.0

TTAK.KO-12.0334-Part1(2018)
TTAK.KO-12.0334-Part2(2018)
	PBKDF (SHA 256)	256	Encryption/decryption of TSF data cryptographic key (KEK)	INISAFE Crypto for C v5.4

SFR to be satisfied: FCS_CKM.1, FCS_RBG.1(Extended)

6.2.2. Cryptographic key distribution

The process of cryptographic key distribution in the TOE is set manually. The authorized administrator uses the security management screen to generate Private Key Value for generating the Agent Private Key, Public Key Value for generating the Server Public Key, DEK encrypted with the KEK, and the encrypted server information. The file generated in the SSO Server is sent to the SSO Agent offline, and the distributed key and the encrypted server information are used for mutual authentication.

SFR to be satisfied: FCS_CKM.2

6.2.3. Cryptographic key destruction

The TOE uses the cryptographic key destruction method directly implemented by INITECH Co., Ltd. The timing and method of destruction for each cryptographic key are as described in the table below.

[Table 29] Timing and method of destruction for each cryptographic key

Cryptographic Key	Cryptographic Key Storage Area	Destruction Method	Timing of Destruction
Cryptographic key for server and agent information used for mutual authentication	Memory	Overwrite with '0'	Destruction immediately after mutual authentication is completed
Cryptographic key for authenticated user ID	Memory	Overwrite with '0'	Destruction immediately after mutual authentication is completed
Cryptographic key for TSF data	Memory	Overwrite with '0'	Destruction upon the shut-down of the SSO Server Destruction upon the shut-down of the SSO Agent
KEK for the encryption of cryptographic key for TSF data	Memory	Overwrite with '0'	Destruction immediately after encryption/ decryption of TSF data

SFR to be satisfied: FCS_CKM.4

6.2.4. Cryptographic operation

The table below shows the list of standards, cryptographic algorithms, cryptographic key sizes and usage for cryptographic operation used in the TOE.

[Table 30] Cryptographic operation algorithms

List of Standards	Algorithm	Cryptographic Key Size	Usage	Validated Cryptographic Module
ISO/IEC 18033-2(2016) IETF RFC 8017(2016)	RSAES	2048 bits	Communication section (mutual authentication) - Encryption/decryption of server and agent information within the transmitted data	INISAFE Crypto for Java V4.2.0
ISO/IEC 18033-2(2016) IETF RFC 8017(2016)	RSAES	2048 bits	Encryption/decryption of authenticated user ID	INISAFE Crypto for Java V4.2.0
KS X ISO/IEC 18033-3(2018) TTAS.KO-12.0004/R1(2005) TTAK.KO-12.0271-Part1/R1(2016) TTAK.KO-12.0274-Part4(2017)	SEED (CBC Mode)	128 bits	Encryption/decryption of TSF data (DEK) - Security setting - Agent information - Server information - Agent Private Key Value - Agent Public Key Value - Agent to Server Public Key Value - Server Private Key Value - Server Public Key Value - Server to Agent Public Key Value - DB password	INISAFE Crypto for Java V4.2.0
KS X ISO/IEC 18033-3(2018) TTAS.KO-12.0004/R1(2005)	SEED (CBC Mode)	128 bits	Encryption/decryption of TSF data cryptographic key (KEK)	INISAFE Crypto for Java V4.2.0

TTAK.KO-12.0271-Part1/R1(2016) TTAK.KO-12.0274-Part4(2017)				
KS X ISO/IEC 9797-2(2018) TTAK.KO-12.0330-Part2(2018)	HMAC_SHA256	256 bits	Generation and verification of authentication token	INISAFE Crypto for Java V4.2.0
ISO/IEC 10118-3(2018)	SHA-256	256 bits	Encryption of user secrets	INISAFE Crypto for Java V4.2.0

SFR to be satisfied: FCS_COP.1

6.3. Identification and authentication (FIA)

The security function of Identification and Authentication of the TOE consists of administrator identification and authentication, end user identification and authentication, TOE internal mutual authentication, generation, verification and destruction of authentication tokens and so forth for the purpose of performing security management through SSO.

6.3.1. TOE internal mutual authentication

The TOE performs the mutual authentication in case of communication between the SSO Server and the SSO Agent that exist separately. The mutual authentication uses "INI_NX protocol" directly implemented by INTECH Co., Ltd.

A cryptographic key used for mutual authentication is distributed offline.

The authorized administrator of the SSO Server, by using the security management screen, generates Private Key Value for generating the Agent Private Key, Public Key Value for generating Server Public Key, DEK encrypted with KEK, and encrypted server information. The file generated in the SSO Server is sent to the SSO Agent offline, and the distributed key and encrypted server information are used for mutual authentication.

The SSO Agent decrypts SEED-encrypted SSO Agent information sent from the SSO Server. It generates the Server Public Key by using Public Key Value, and encrypts SEED-decrypted SSO Agent information by using RSAES and send it to the SSO Server.

The SSO Server generates the Server Public Key, and decrypts RSAES-encrypted SSO Agent information.

On the authorized administrator's security management screen, SEED-encrypted SSO Agent information stored in the DB upon the generation of the SSO Agent is decrypted and compared to verify the SSO Agent.

The SSO Server generates the Agent Public Key, and decrypts the SSO Server information that was SEED-encrypted and stored in the DB. It encrypts SEED-decrypted SSO Server information by using RSAES, and sends it to the SSO Agent.

The SSO Agent generates the Agent Private Key, and decrypts the encrypted SSO Server information. It compares SEED-encrypted SSO Server information sent offline with the decrypted value to verify the SSO Server. The data transmitted between the SSO Server and the SSO Agent are protected by using HTTPS communication.

SFR to be satisfied: FIA_IMA.1(Extended), FPT_ITT.1

6.3.2. Identification and authentication

An end user performs ID and password-based user identification and authentication to the SSO Server through the SSO Agent using a web browser. The authorized administrator performs ID and password-based user identification and authentication in order to access the security management screen. The identification and authentication of an end user and the authorized administrator must be successfully performed before any TSF-mediated action is allowed (satisfying FIA_UAU.2 and FIA_UID.2).

In case of unsuccessful five times authentication attempts has been surpassed to authenticate the authorized administrator, the identification and authentication function for the authorized administrator is inactivated for 10 minutes, and a warning email is sent to the authorized administrator. Also, in case of unsuccessful five times authentication attempts has been surpassed to authenticate an end user, the identification and authentication function is inactivated and the account is locked until the authorized administrator allows unlocking. (satisfying FIA_AFL.1(1) and FIA_AFL.1(2))

The TOE provides a mechanism that verifies that the defined metric for password below is satisfied upon registering and changing passwords of the authorized administrator and end users. (FIA_SOS.1)

- Allowable characters
  - At least one English alphabet, one number and one special character must be included
- Min/max length
  - 9 ~ 16 digits
- Change interval (the period during which the password is used)
  - 30 days

In password-based authentication of the authorized administrator, the reuse of authentication information is prevented by using CSRF token. In password-based authentication of end users and authentication token-based authentication, the reuse of authentication information is prevented by generating and verifying nonce value for each request when generating authentication information (FIA_UAU.4)

In the process of authentication by the authorized administrator and end users, passwords being entered are masked (masking with *) to prevent them from being disclosed on the screen. If identification and authentication fail, feedback on a reason for failure is not provided. (satisfying FIA_UAU.7)

SFR to be satisfied: FIA_UAU.2, FIA_UID.2, FIA_AFL.1(1), FIA_AFL.1(2), FIA_SOS.1, FIA_UAU.4, FIA_UAU.7

6.3.3. Generation/verification/destruction of end user SSO authentication token

The end user identification and authentication procedure can be grouped into the initial authentication phase using the ID/password, and the token-based authentication phase that accesses the business system using the token issued during the initial authentication procedure. "1.3.3 TOE usage and major security features" provides detailed description. An authentication token is generated in the SSO Server, and the authentication information includes user ID, user IP, authentication time (time stamp) and integrity value (web browser fingerprint). Authentication information is generated and verified by using HMAC cryptographic algorithms of the validated cryptographic module (INISAFE Crypto for Java V4.2.0). In the token-based authentication phase of end users, it is enforced to use authentication tokens generated by the TSF for identification and authentication at all times. (satisfying FIA_SOS.2)
An authentication token used for the token-based authentication of an end user is destroyed if the end user logs out, if a session is terminated after a specified time of user inactivity (10 minutes), or if the existing access session is deleted in case of the concurrent access by the same user. An authentication token that has been used is destroyed by being overwritten with "0." (satisfying FIA_SOS.3)

SFR to be satisfied: FIA_SOS.2, FIA_SOS.3

6.4. Security management (FMT)

6.4.1. Management of security functions behaviour

The administrator role provided by the TOE is the authorized administrator only. Accounts of the authorized administrator may be added during the operation of the TOE. The authorized administrator can perform management behaviors (enable) for security functions specified in "[Table 19] List of security functions behaviour of the administrator" after going through the identification and authentication process in the SSO sever.

SFR to be satisfied: FMT_MOF.1, FMT_SMF.1, FMT_SMR.1

6.4.2. Management of TSF data

The administrator role provided by the TOE is the authorized administrator only. Accounts of the authorized administrator may be added during the operation of the TOE. The authorized administrator can perform management behaviors (query, modify, delete and generate) for TSF data specified in "[Table 20] List of TSF data and management ability" after going through the identification and authentication process in the SSO sever.

SFR to be satisfied: FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.4.3. Management of TSF data

Upon the initial installation of the TOE, the authorized administrator's default ID and password are set in the DB. After the installation process is completed, the authorized administrator is enforced to change the password upon the initial access.
It is not allowed to modify the rules for ID and password creation/change and combination for the authorized administrator and end users' IDs and passwords. The same combination rules for passwords apply to both the authorized administrator and end users. The combination rule enforces that a password is at least nine digits long and include at least one English alphabet, one number and one special character, respectively.

SFR to be satisfied: FMT_PWD.1(Extended)

6.5. Protection of the TSF (FPT)

6.5.1. Basic protection of stored TSF data

TSF data, necessary for the operation of the SSO Server, are stored in the DBMS (Oracle) which is the operating environment. Critical TSF data are encrypted by using the validated cryptographic module so that they are protected against disclosure and modification.

[Table 31] Protection of TSF data

TSF Data	Protection Mechanism
User account information (authorized administrator, end user)	Hash values generated with SHA256 are stored in the DB of the SSO Server.
TSF data encryption key (DEK)	Encrypted with KEK (SEED 128bit CBC) and stored in the file system of the SSO Server

	and SSO Agent. *※ KEK is generated by using PBKDF (SHA-256) of the validated cryptographic module (INISAFE Crypto for C v5.4).*
Agent Public Key Value Server Private Key Value Server Public Key Value DB access account information Mail server account information	Encrypted with DEK (SEED 128bit CBC) and stored in the file system of the SSO Server
Server Public Key Value Agent Private Key Value Agent Public Key Value	Encrypted with DEK (SEED 128bit CBC) and stored in the file system of the SSO Agent
TOE Configuration value (security policy, configuration parameter)	Encrypted with DEK (SEED 128bit CBC) and stored in the DB of the SSO Server
Server and agent information for mutual authentication	· SSO Server: Encrypted with DEK (SEED 128bit CBC) and stored in the DB · SSO Agent: Encrypted with DEK (SEED 128bit CBC) and stored in the file system
Authentication token	Hash values generated with HMAC_SHA256 are stored in the DB of the SSO Server.
File that is in the SSO Agent and subject to the integrity verification (checksum.list)	Encrypted with DEK (SEED 128bit CBC) and stored in the file system of the SSO Agent.

SFR to be satisfied: FPT_PST.1(Extended)

6.5.2. TSF self tests and integrity test

The TOE runs a suite of self tests on the SSO Server and the SSO Agent and also performs integrity monitoring of TSF and TSF data during initial start-up, periodically during normal operation and at the request of the authorized administrator. The TOE generates audit data on the results of self tests or integrity monitoring. If a self test or integrity monitoring fails, it sends an email to the authorized administrator. Details on self tests and integrity monitoring, including frequency, targets and methods, for each TOE component are described in the table below.

[Table 32] TSF self tests and integrity monitoring

	TOE Component	Frequency	Target	Method

Self tests	SSO Server	· During start-up · Self test by IDP on ADMIN periodically during normal operation (every 60 minutes after the SSO Server is activated) · Self test by ADMIN on IDP periodically during normal operation (00 minutes every hour)	· IDP · ADMIN · Validated cryptographic module	· IDP runs self tests on ADMIN process, and ADMIN runs self tests on IDP process · For self tests on the cryptographic module, the SSO Server calls the self test function of the validated cryptographic module and obtains the result value
	SSO Agent	· During start-up · Periodically during normal operation (00 minutes every hour) · At the request of the authorized administrator	· SP	ADMIN of the SSO Server performs self tests on major processes (SP) in the SSO Agent.
Integrity monitoring (TSF data)	SSO Server	· During start-up · Periodically during normal operation (00 minutes every hour) · At the request of the authorized administrator	· TSF data (configuration)	Generate hash value (SHA256) for the folder where the SSO Server is installed, and check the presence of manipulation
	SSO Agent	· During start-up · Periodically during normal operation (every 60 minutes after it is activated)	· Files subject to integrity monitoring (checksum.list) · ssoAgent PrivateKey.key · ssoAgent	Generate hash values (SHA256) for files subject to the integrity verification of the SSO Agent (files included in checksum.list), as well

			PublicKey.key · ssoServer PublicKey.key · encryptDEK .key · salt.key	as checksum.list file itself, and check the presence of manipulation
Integrity monitoring (TSF)	SSO Server	· During start-up · Periodically during normal operation (00 minutes every hour) · At the request of the authorized administrator	· TSF · Validated cryptographic module	Generate hash value (SHA256) for the folder where the SSO Server is installed, and check the presence of manipulation
	SSO Agent	· During start-up · Periodically during normal operation (every 60 minutes after it is activated)	· sso.saml.jar · INICrypto_ v4.2.0.jar · INICommon Crypto.jar · INISAFECore-v2.2.40.jar · INISAFEPKI-v1.1.42.jar · CryptoC.dll · inicrypto_ v5.4.0_64.dll	Generate hash values (SHA256) for files subject to the integrity verification of the SSO Agent (files included in checksum.list) and check the presence of manipulation

** checksum.list: File that contains hash values and a list of files subject to integrity monitoring of the SSO Agent (TSF data and TSF)*

SFR to be satisfied: FPT_TST.1

6.5.3. Testing of external entities

The SSO Server sends a test email to the mail server to check the availability of the mail server during initial start-up and at the request of the authorized administrator. If the test fails, a warning pop-up will be generated in the authorized administrator login screen.

The SSO Server checks whether or not the service port of the DBMS (Oracle) is operated normally to test the availability of the DBMS during initial start-up, periodically (60 minutes) during normal operation and at the request of the authorized administrator. If the test fails, it sends a warning email to the authorized administrator.

The SSO Server and the SSO Agent checks whether or not the service port of WAS (Tomcat) is operated normally to check the availability of WAS during initial start-up, periodically (60 minutes) during normal operation and at the request of the authorized administrator. If the test fails, it sends a warning email to the authorized administrator.

SFR to be satisfied: FPT_TEE.1

6.6. TOE access (FTA)

6.6.1. TOE access

The SSO Server restricts the maximum number of concurrent sessions accessible by the authorized administrator and an end user to one. In case the authorized administrator is logged in to the SSO Server and a login attempt in is made, either by the same or a different authorized administrator, the existing access session will be blocked and new access will be permitted. In case an end user is logged in to the SSO Agent and a login attempt is made by the same user, the existing access session will be blocked and new access will be permitted.

The SSO Server allows an attempt for identification and authentication only if access is made by an allowed IP address. It provides only two allowed IP address for connection by default, which may be added during the operation of the TOE.

After the authorized administrator and an end user successfully logs in, the SSO Server forcibly terminates the session after 10 minutes of user inactivity.

SFR to be satisfied: FTA_MCS.2, FTA_SSL.5(Extended), FTA_TSE.1