Security Target
TouchEn wiseaccess v1.3

RaonSecure Co., Ltd.

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

Revision history

Configuration document no.	Detail	Data revised	Created by	Reviewed by
wiseaccess-D-ST v1.3.00	Initial version	2017-11-22	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.01	Updated	2018-01-08	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.02	Updated	2018-03-19	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.03	Updated	2018-03-21	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.04	Updated	2018-05-14	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.05	Updated	2018-06-21	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.06	Updated	2018-07-31	Kim Hye-won	Jo gyeong-min
wiseaccess-D-ST v1.3.07	Updated	2018-08-31	Kim Hye-won	Jo gyeong-min

Contents

1. ST Introduction

1.1 ST reference

Item	Specification
Title	TouchEn wiseaccess v1.3 Security Target
Document identification	wiseaccess-D-ST v1.3.07
Version	v1.3.07
Publication Date	2018.08.31
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	CC v3.1 R5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Protection Profile	Korean national protection profile for Single Sign On V1.0
Protection Profile Certification Number	KECS-PP-0822-2017
Author	RaonSecure Co., Ltd.
Keywords	Single Sign On, SSO

1.2 TOE reference

Item		Specification
TOE		TouchEn wiseaccess v1.3
Version		v1.3.3
Components	Policy Server	· TouchEn wiseaccess PolicyServer Version 1.3.1.107.6 : wiseaccess_policyserver_v1.3.1.107.6_aix.tar.gz : wiseaccess_policyserver_v1.3.1.107.6_hpux.tar.gz
	Session Server	· TouchEn wiseaccess SessionServer Version 1.3.2.7.7 : wiseaccess_sessionserver_v1.3.2.7.7_aix.tar.gz : wiseaccess_sessionserver_v1.3.2.7.7_hpux.tar.gz
	WPM	· TouchEn wiseaccess 1.3 PolicyManager version 1.3.26.2.8 : wiseaccess_WPM_v1.3.26.2.8_aix.war : wiseaccess_WPM_v1.3.26.2.8_hpux.war
	SSO Engine	· TouchEn wiseaccess ssoengine Version 1.3.2.19.6 : wiseaccess_ssoengine_v1.3.2.19.6_aix.tar.gz : wiseaccess_ssoengine_v1.3.2.19.6_hpux.tar.gz
	WAAPI	· TouchEn wiseaccess WAJavaAPI Version 1.3.1.46.5 : wiseaccess_WAJavaAPI_v1.3.1.46.5_aix.tar.gz : wiseaccess_WAJavaAPI_v1.3.1.46.5_hpux.tar.gz
	Guidelines	· TouchEn wiseaccess v1.3 Administrator Manual v1.3.04

		: TouhEn wiseaccess v1.3 Administrator Manual.pdf · TouhEn wiseaccess v1.3 API Manual v1.3.01 : TouhEn wiseaccess v1.3 API Manual.pdf · TouhEn wiseaccess v1.3 Install Guideline v1.3.05 : TouhEn wiseaccess v1.3 Install Guideline.pdf
Developer		RaonSecure Co., Ltd.

1.3 TOE overview

This security target prescribes the security function requirements and assurance requirements of TouchEn wiseaccess v1.3 that provides services without additional login for various business systems to end-users with a single sign-on.

TouchEn wiseaccess v1.3 (hereinafter "TOE") provides end-user login functions through an ID and password. During the initial end-user login attempt, the authentication token is issued and when a logged in end-user attempts to access another business system, it is verified through the issued authentication token to allow/block access.

The TOE sets the ID and password policy and login policies for end-user identification and authentication, and it manages various business systems through service registration. It offers authorities per business system to regulate the single authentication function. At this time, the authentication token that is issues/saved/verified/discarded must use a validated cryptographic module with proven safety and configurability through the cryptographic module validation program.

The TOE uses the following validated cryptographic module.

- Cryptographic module name : Key# Crypto v1.3
- Validation number: CM-110-2021.1
- Expiration date: Jan 27, 2021

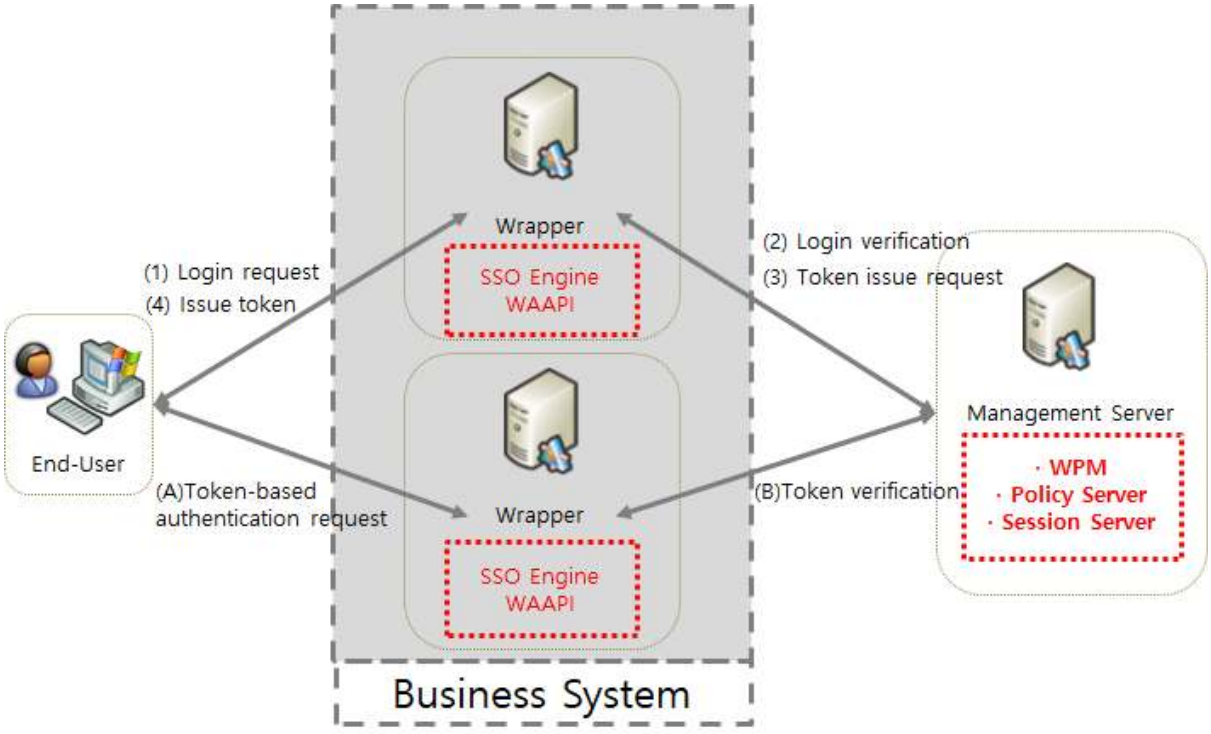
The TOE provides the security audit function that records and manages a critical events as audit data when activating the security functionality and management function, function of protecting the data that stored in the TSF controlled repository, and Protection of the TSF function such as TSF

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. Additionally, authentication tokens require confidentiality and integrity and the TOE execution codes require integrity.

The end-user identification and authentication process is divided into the initial authentication stage using the ID and password and the authentication token-based authentication stage that access to the business system using the authentication token issued through the initial authentication process.
The initial authentication process is as follows.
When the end-user requests login through the ID/password of the business system, the SSO Engine that received the login request message through the WAAPI that is linked to the business system sends a login verification request to confirm whether the end-user is appropriate to the Policy Server. The Policy Server that received the login verification request conducts login verification directly through the end-user information saved in DBMS. When the login verification results are successful, the Policy Server requests the success results and issuing of the authentication token.
The SSO Engine issues authentication tokens according to the verification token issue request.

The authentication token-based authentication stage is conducted only when normally issuing the authentication token through the initial authentication stage. When the end-user uses the service of the business system, the SSO engine verifies the validity of the authentication token to determine the use of services depending on the success/fail results.

- Authentication token issuer: SSO Engine
- Authentication token storage location: End-User PC
- Authentication token validator: SSO Engine



[Figure 1] end-user identification and authentication process

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

The TOE is an 'integrated authentication' solution that allows access to various business systems through a single log-in by end-user and it is offered in the form of software.

The TOE is comprised of the WAAPI and SSO Engine linked with the WPM and Policy Server, Session Server and work server to carry out security management.

▣ WPM

The WPM conducts integrity inspections when executed and during administrator login attempts, it carries out authentication failure handling functions for identification and authentication, and it restricts the number of simultaneous sessions of the security management screen access through web browsers to one.

The WPM manages organizations, groups, services, roles, policies, administrator groups and configurations for security function management.

Authorized administrators can set members per organization/group, roles, authorizations (service settings) and administrator settings and can set ID policies, password policies and login policies

applied to end-users within an organization.
Authorized administrators can add IP addresses that can access the security management screen through the web browser and the said administrators are in charge of managing administrator groups and delegated administrators.
Thresholds are set for protecting audit data repository, notifications are set for potential security violations, the capacity of the disk in which DBMS is installed is computed so that when it exceeds the threshold (alarm notification, delete past records) set by the administrator or when audit save fails, an event on this is generated and an audit log is generated.

▣ Policy Server
In the event that there is a request by end-user for identification or authentication attempts, the Policy Server identifies and authenticates end-users based on the end-user's authentication information (ID/password).
Once the end-user authentication information is normally processed, the Policy Server conducts channel encryption for secure communication with the SSO Engine. Also, session generation is requested to the Session Server to generate authentication tokens for the SSO Engine, and when necessary to generate authentication tokens, the necessary information (TokenID, user information, version, algorithm ID, expiration, etc.) are transmitted.

▣ Session Server
In the event that there is a session generation request from the Policy Server, the session for the end-user that requested authentication is generated and reduplication logins are checked.
TokenID issued during session generation is sent to the Policy Server.

▣ SSO Engine
The SSO engine verifies the authentication token when authenticating the end-user through the WAAPI that interfaces with the business system.
In the event that there is no authentication token information during the initial end-user login attempt, information for generating the authentication token (user info, version, algorithm ID, expiration, TokenID, etc.) is received from the Policy Server and Session Server to generate the authentication token. The generated authentication token is sent to the business system through the WAAPI.

▣ WAAPI
The WAAPI sends end-user generation information or token information when the WAAPI function is called from the business system to the SSO Engine or brings the authentication token generated from the SSO Engine or the authentication success/fail results.

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

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

1) Policy Server / Session Server / WPM

Item		Specification
Hardware	CPU/ Memory/ Hard Disk	· CPU : PowerPC 3.6GHz POWER6 or higher · Memory : 4GB or higher · Disk : Space required for installation of TOE 250MB or higher
	NIC	· 10/100/1000 Ethernet Port x 1EA
Software	OS	· AIX 5.3 (64bit)
	DBMS	· Oracle 11g 11.2.0.1.0
		· Tibero 6
	etc	· Apache Tomcat 7.0 (64bit)
		· JDK 1.6.0_45 (64bit)

Item		Specification
Hardware	CPU/ Memory/ Hard Disk	· CPU : Itanium 3.6GHz or higher · Memory : 4GB or higher · Disk : Space required for installation of TOE 250MB or higher
	NIC	· 10/100/1000 Ethernet Port x 1EA
Software	OS	· HP-UX(IA) 11.23 (64bit)
	DBMS	· Oracle 11g 11.2.0.1.0
		· Tibero 6
	etc	· Apache Tomcat 7.0 (64bit)
		· JDK 1.6.0_45 (64bit)

2) Administrator PC

Item		Specification
Hardware	CPU/ Memory/ Hard Disk	· CPU : Dual Core 2.8GHz or higher · Memory : 8GB or higher · Disk : 500GB x 1EA or higher
	NIC	· 10/100/1000 Ethernet Port x 1EA
Software	OS	· Windows 7 Professional (64bit)
		· Windows 10 Pro (64bit)

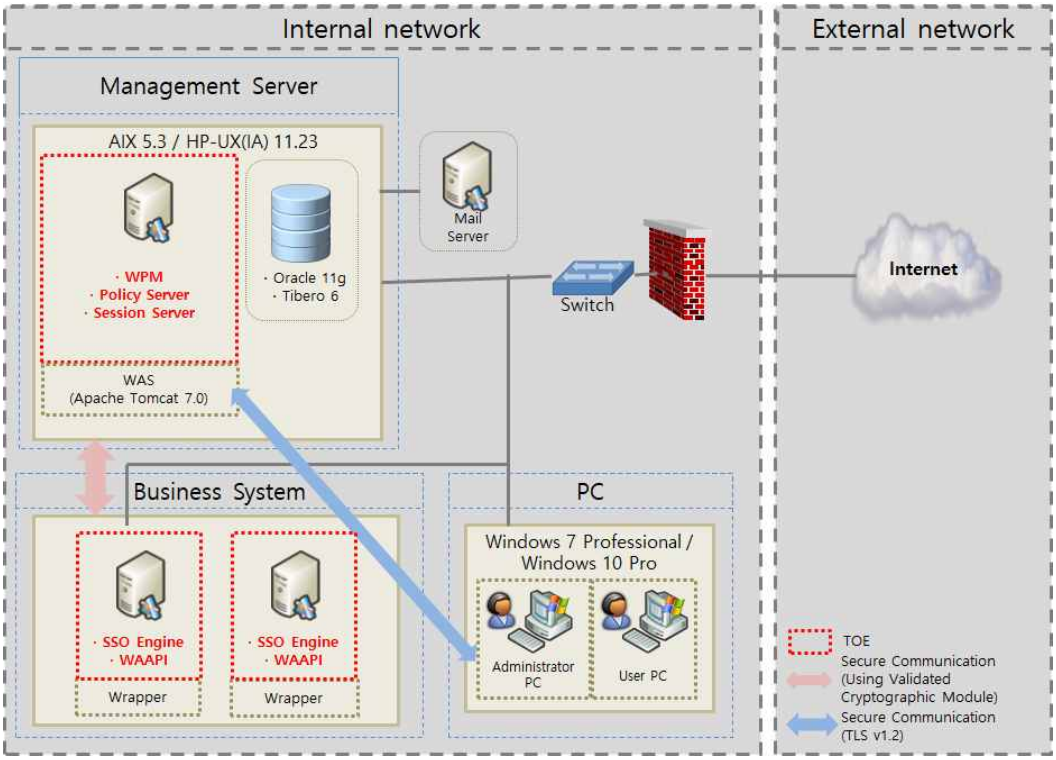
	Web Browser	・Internet Explorer 11
		・Chrome 66

3) SSO Engine / WAAPI

Item		Specification
Hardware	CPU/ Memory/ Hard Disk	・CPU : PowerPC 3.6GHz POWER6 or higher ・Memory : 4GB or higher ・Disk : Space required for installation of TOE 120MB or higher
	NIC	・10/100/1000 Ethernet Port x 1EA
Software	OS	・AIX 5.3 (64bit)
	etc	・Apache Tomcat 7.0 (64bit)
		・JDK 1.6.0_45 (64bit)

Item		Specification
Hardware	CPU/ Memory/ Hard Disk	・CPU : Itanium 3.6GHz or higher ・Memory : 4GB or higher ・Disk : Space required for installation of TOE 120MB or higher
	NIC	・10/100/1000 Ethernet Port x 1EA
Software	OS	・HP-UX(IA) 11.23 (64bit)
	Etc	・Apache Tomcat 7.0 (64bit)
		・JDK 1.6.0_45 (64bit)

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



[Figure 2] TOE operational environment

The TOE operating environment consists of a management server and a business system.
The management server consists of the WPM, Policy Server, and Session Server and performs security management. The business system is composed of the WAAPI and SSO Engine in combination of 'API type' composed of library files and 'Process type' composed of executable files. And performs a end-user login verification request and an authentication token issuance function.

The WPM conducts the TOE security management through the web browser that supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). A wrapper is used for compatibility with various business systems, but it is excluded from the scope of the TOE.

▣ DBMS(Oracle)

DBMS, which is linked together with the WPM and Policy Server in the AIX operating system or HP-UX operating system, is installed with Oracle, an open source relational database management system. When data query/change using random conditions from the WPM is requested, the DBMS Oracle (11g 11.2.0.1.0) searches, sorts, sequences and statistically processes the TSF data and audit data saved in the DBMS based on the entered conditions.

▣ DBMS(Tibero)

DBMS, which is linked together with the WPM and Policy Server in the AIX operating system or

HP-UX operating system, is installed with Tibero, an open source relational database management system. When data query/change using random conditions from the WPM is requested, the DBMS Tibero 6 searches, sorts, sequences and statistically processes the TSF data and audit data saved in the DBMS based on the entered conditions.

▣ Web Server (Apache Tomcat)

This is used to provide web-based management functions through the web browser.

▣ Tomcat Encryption Functions

The authorized administrator communicates using the WPM and browser activated in Apache Tomcat that supports HTTPS protocol.

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

▣ Mail Server

The mail server sends an e-mail to the authorized administrator who is the recipient designated by the WPM about the potential security violation.

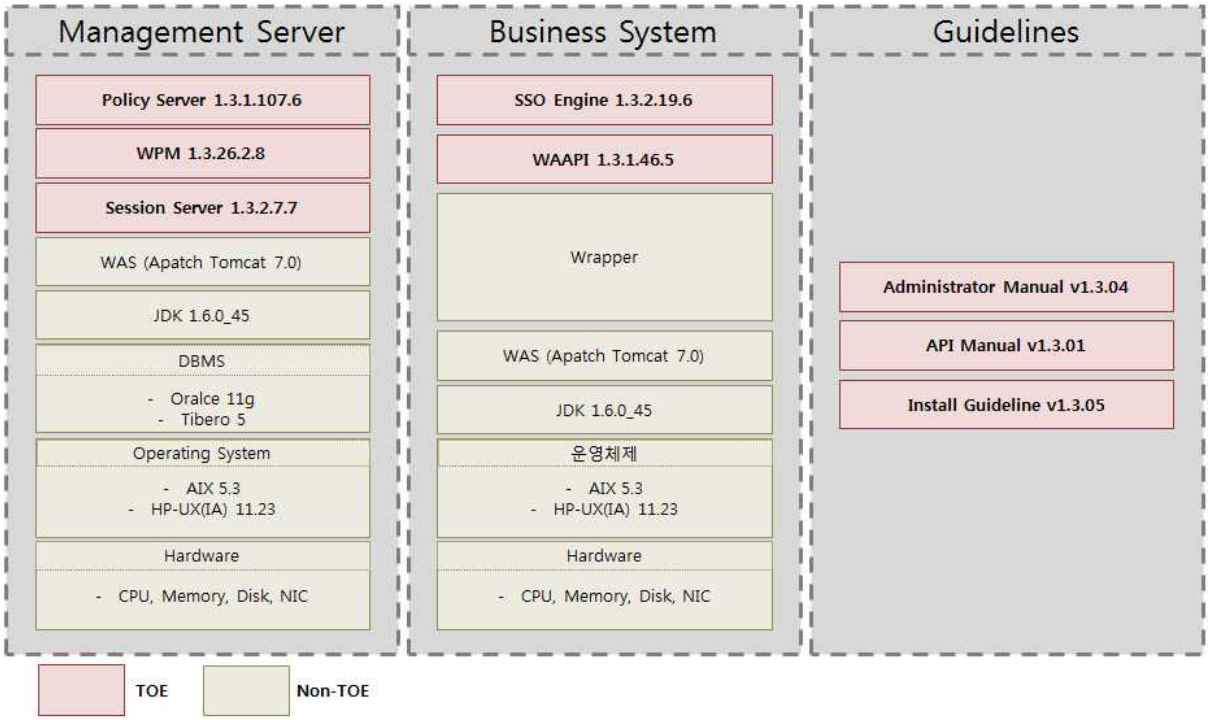
1.4 TOE description

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

1.4.1 Physical scope of the TOE

The physical scope that makes up the TOE is the WPM, Policy Server, Session Server, SSO Engine and WAAPI, and guidelines (administrator manual, API manual, installation guideline) as shown in the below [Figure 2]. Validated Cryptographic Module(Key # crypto v1.3) is embedded in the TOE components.

Hardware, operating system, DBMS, WAS, JDK, Wrapper which are operating environments of the TOE are excluded from the physical scope of the TOE.



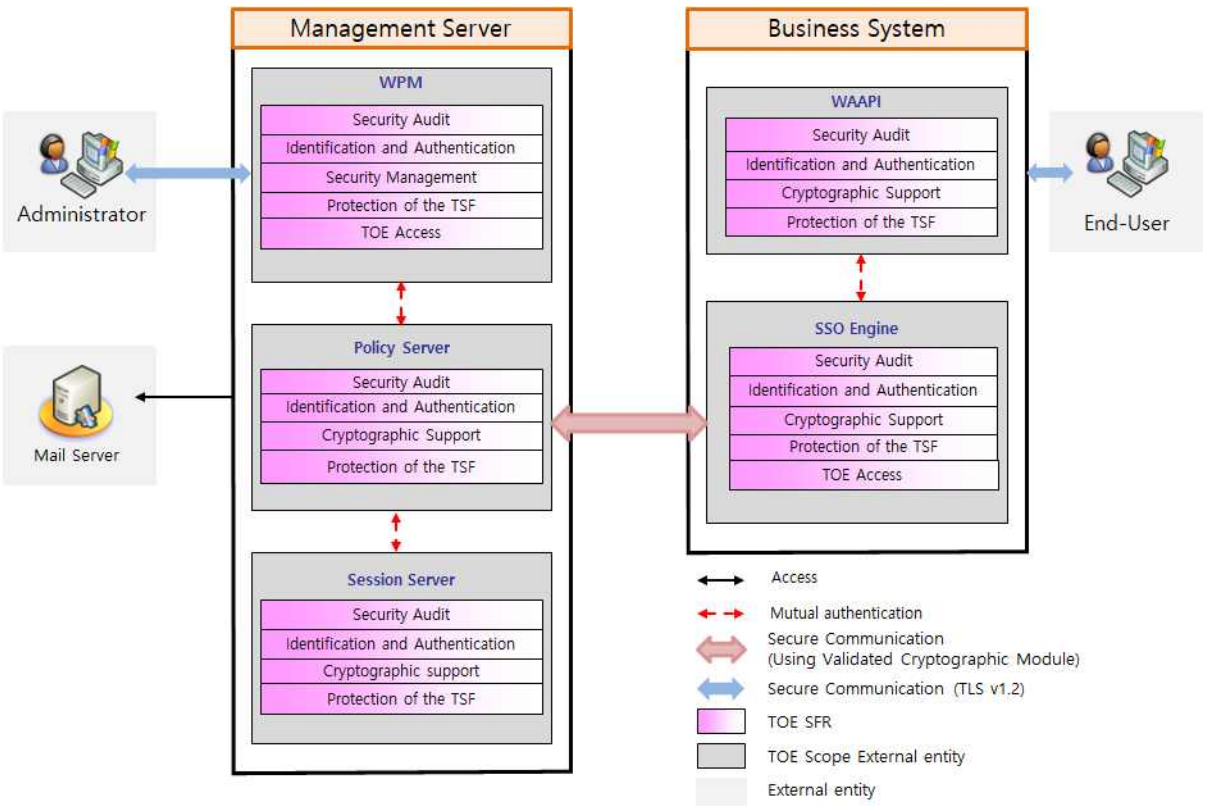
[Figure 3] Physical scope

Scope	Type	Distribution Status
WPM	Install S/W on management server (Distributed as a CD)	· TouchEn wiseaccess 1.3 PolicyManager version 1.3.26.2.8 : wiseaccess_WPM_v1.3.26.2.8_aix.war : wiseaccess_WPM_v1.3.26.2.8_hpux.war
Policy Server		· TouchEn wiseaccess PolicyServer Version 1.3.1.107.6 : wiseaccess_policyserver_v1.3.1.107.6_aix.tar.gz : wiseaccess_policyserver_v1.3.1.107.6_hpux.tar.gz
Session Server		· TouchEn wiseaccess SessionServer Version 1.3.2.7.7 : wiseaccess_sessionserver_v1.3.2.7.7_aix.tar.gz : wiseaccess_sessionserver_v1.3.2.7.7_hpux.tar.gz
SSO Engine	Install S/W on business system (Distribute as a CD)	· TouchEn wiseaccess ssoengine Version 1.3.2.19.6 : wiseaccess_ssoengine_v1.3.2.19.6_aix.tar.gz : wiseaccess_ssoengine_v1.3.2.19.6_hpux.tar.gz
WAAPI		· TouchEn wiseaccess WAJavaAPI Version 1.3.1.46.5 : wiseaccess_WAJavaAPI_v1.3.1.46.5_aix.tar.gz : wiseaccess_WAJavaAPI_v1.3.1.46.5_hpux.tar.gz
Guidelines	Administrator Manual, API Manual, Install Guideline	· TouchEn wiseaccess v1.3 Administrator Manual v1.3.04 : TouchEn wiseaccess v1.3 Administrator Manaul.pdf · TouchEn wiseaccess v1.3 API Manual v1.3.01 : TouchEn wiseaccess v1.3 API Manual.pdf

	(Distribute as a CD)	· TouchEn wiseaccess v1.3 Install Guideline v1.3.05 : TouchEn wiseaccess v1.3 Install Guideline.pdf

1.4.2 Logical scope of the TOE

The logical scope of the TOE is as in [Figure 3] below.



[Figure 4] Logical scope

Includes logical scopes in each module.

▣ WPM

[Security Audit]

The WPM generates audit data for TSF data management and security management provided through the web browser.

The WPM generates audit data for management and security settings, TSF data information change and identification and authentication, integrity inspections, start/end of audit functions, and on security violations.

The generated audit data includes log generation time, identity of the subject, case results (success or fail), items for case types, and audit data additionally generated.

Audit data is saved in the DBMS and information is provided in appropriate format to authorized administrators through the WPM.
In addition to the super administrator, delegated administrators with authority to view audits can also query audit data.

[Identification and authentication]
During identification and authentication attempts, the administrator is identified with the ID and administrator authentication is carried out prior to all actions. Passwords for authentication are indicated with '*' and only provides information on the cause for failed authentication to prevent exposure of passwords.
Administrator passwords must be created according to password rules and when identification and authentication is successful, the administrator maintains security management authorities.

When attempting to authenticate through the WPM, if it passes the number of authentication attempt failures (1-10 times) set by the administrator, the account is locked for the designated account lock time.

[Security management]
Security management is carried out through the WPM.
Set the security policy for single authentication functions through organization/group/service/role/policy, etc. and set the delegated administrator through the administrator group/management authority. Also set configurations such as audit data repository inspection cycles and Key# Crypto self-tests for potential security violations, checking DBMS disk capacity, the WPM/Policy Server/Session Server/SSO Engine/WAAPI self-testing and integrity test execution, check failed audit saves, and notification cycles according to the number of failures for administrator/end-users.

[Protection of the TSF]
The separated partial security communication of the TOE protects against exposure and change when sending TSF data, protects information saved in the repository from unauthorized exposure and change, and conducts regular integrity tests when starting the WPM.

[TOE Access]
When the WPM is not used for a specified period, the session is automatically terminated and the administrator must go through authentication processes again to resume use.
Furthermore, in the case of administrator sessions for security management, the max number of sessions connections are limited to one to prevent reduplication logins.

▣ **Policy Server**

[Security Audit]

The TOE generates audit data for response behavior against security violations, the Policy Server and Session Server, interaction between the Policy Server and SSO Engine, resulting cryptographic key management, integrity tests, and audit function start/end.

The generated audit data include log generation time, identity of subject, case results (success or fail), items for case types, and additionally generated audit data.

The TOE regularly examines the audit data repository according to the notification cycle set by the administrator and sends warning mails to the administrator when reaching the warning notification threshold and deletes past DBMS records when reaching the past records deletion threshold.

In addition, when security violations (Key# Crypto self-test failure, exceeding DBMS disk capacity, failures of the WPM, Policy Server, Session Server, SSO Engine, and WAAPI self-test and integrity test, non-operation of the WPM, Policy Server, Session Server, SSO Engine, and WAAPI, failure to save audits, or when exceeding the number of allowed administrator/end-user failures), or when warning messages occur, response behavior (send e-mail to administrator) is carried out.

[Identification and authentication]

The Policy Server conducts mutual-authentication the SSO Engine and Session Server.

[Cryptographic support]

The TOE generates random bits through the random bit generator for mutual-authentication and during mutual-authentication, the digital signature algorithm is used to conduct signature verification. Once mutual-authentication is complete, the symmetric key algorithm is used to distribute cryptographic keys to the SSO Engine. At this time, the algorithm used will use the validated cryptographic module, Key# Crypto v1.3.

[Protection of the TSF]

The separated partial security communication of the TOE protects against exposure and change when sending TSF data and conducts regular integrity tests when starting.

▣ **Session Server**

[Security Audit]

The TOE generates audit data for interaction between the Session Server and Policy Server, and its resulting cryptographic key management, integrity tests, and audit function start/end.

The generated audit data include log generation time, identity of subject, case results (success or fail), items for case types, and additionally generated audit data.

[Identification and authentication]

The TOE conducts mutual-authentication between the Session Server and Policy Server.

[Cryptographic support]

The TOE generates random bits through the random bit generator for mutual-authentication and during mutual-authentication, the digital signature algorithm is used to conduct signature verification. At this time, the random bit generator and digital signature algorithm will use the validated cryptographic module, Key# Crypto v1.3.

[Protection of the TSF]

The separated partial security communication of The TOE protects against exposure and change when sending TSF data and conducts regular integrity tests when starting The Session Server.

▣ SSO Engine

[Security Audit]

The TOE generates audit data for interaction between The SSO Engine and Policy Server, generates authentication token using cryptographic key, operation, destruction, cryptographic key management, integrity test, and audit data for audit function start/end.

The generated audit data include log generation time, identity of subject, case results (success or fail), items for case types, and additionally generated audit data.

[Identification and authentication]

During initial end-user identification and authentication attempts, the OE identifies end-users with the ID and end-user authentication is carried out prior to all actions. Passwords for authentication are indicated with '*' and only provides message for failed authentication to prevent exposure of passwords.

Once initial end-user identification and authentication is complete, authentication tokens are generated according to the authentication token configuration method and afterwards, identification and authentication is carried out through the authentication token. Onetime Token is used for the authentication token to prevent reuse.

The TOE conducts mutual-authentication between the SSO Engine and Policy Server.

If the administrator exceeds the number of authentication attempt failures (5-10 times) set by the administrator during end-user authentication attempts, the account is locked for the account lock time designated by the administrator.

[Cryptographic support]

The TOE generates random bits through the random bit generator for mutual-authentication with the Policy Server and during mutual-authentication, the digital signature algorithm is used to conduct signature verification. After mutual-authentication, authentication token is generated and managed using the symmetric key algorithm and MAC algorithm, and it will use the validated cryptographic module, Key# Crypto v1.3.
The generated authentication token is not saved and destroyed.

[Protection of the TSF]
The separated partial security communication of the TOE protects against exposure and change when sending TSF data and conducts regular integrity tests when starting.

[TOE Access]
After end-user identification and authentication, once the idle time of the authentication token passes, the session will be terminated and identification and authentication must be carried out again for reauthentication.

▣ WAAPI

[Security Audit]
The TOE generates audit data for interaction between the WAAPI and SSO Engine, and its resulting cryptographic key management, and integrity tests.
The generated audit data include log generation time, identity of subject, case results (success or fail), items for case types, and additionally generated audit data.

[Identification and authentication]
The TOE conducts mutual-authentication between the WAAPI and SSO Engine.

[Cryptographic support]
The TOE generates random bits through the random bit generator for mutual-authentication with the and during mutual-authentication, the digital signature algorithm is used to conduct signature verification. At this time, the random bit generator and digital signature algorithm uses the validated cryptographic module, Key# Crypto v1.3.

[Protection of the TSF]
The separated partial security communication of the TOE protects against exposure and change when sending TSF data.

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 PP.

Iteration

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

Assignment

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

Selection

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

Refinement

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

1.6 Terms and definitions

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

Term	Definitions
Application Programming Interface (API)	A set of software libraries that exist between the application layer and the platform system layer and facilitate the development of applications that run on the platform
Approved cryptographic algorithm	A cryptographic algorithm selected by Korean Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability
Approved mode of operation	The mode of cryptographic module using approved cryptographic algorithm

Assets	Entities that the owner of the TOE presumably places value upon
Assignment	The specification of an identified parameter in a component (of the CC) or requirement
Attack potential	Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation
Augmentation	Addition of one or more requirement(s) to a package
Authentication Data	Information used to verify a user's claimed identity
Authentication token	Authentication data that authorized end-users use to access the business system
Authorized Administrator	Authorized user to securely operate and manage the TOE
Authorized User	The TOE user who may, in accordance with the SFRs, perform an operation
Business System	An application server that authorized end-users access through 'SSO'
Can/could	The 'can' or 'could' presented in Application notes indicates optional requirements applied to the TOE by ST author's choice
Class	Set of CC families that share a common focus
Client	Application program that can access the services of SSO server or SSO agent through network
Component	Smallest selectable set of elements on which requirements may be based
Critical Security Parameters (CSP)	Information related to security that can erode the security of the encryption module if exposed or changed (e.g., verification data such as secret key/private key, password, or Personal Identification Number)
Database Management System (DBMS)	A software system composed to configure and apply the database
Decryption	The act that restoring the ciphertext into the plaintext using the decryption key
Dependency	Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package
Element	Indivisible statement of a security need
Encryption	The act that converting the plaintext into the ciphertext using the cryptographic key
end-user	Users of the TOE who want to use the business system, not the

	administrators of the TOE
Evaluation Assurance Level (EAL)	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
External Entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary
Family	Set of components that share a similar goal but differ in emphasis or rigour
Identity	Representation uniquely identifying entities (e.g. user, process or disk) within the context of the TOE
Iteration	Use of the same component to express two or more distinct requirements
Kerberos	A centralized authentication scheme, described in RFC 1510, that provides user authentication using symmetric cryptographic technique in a distributed computing environment
Korea Cryptographic Module Validation Program (KCMVP)	A system to validate the security and implementation conformance of cryptographic modules used for protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions
Management access	The access to the TOE by using the HTTPS, SSH, TLS, etc to manage the TOE by administrator, remotely
Management Console	Application program that provides GUI, CLI, etc. to the administrator and provides system management and configuration
Object	Passive entity in the TOE containing or receiving information and on which subjects perform operations
Operation(on a component of the CC)	Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection
Operation(on a subject)	Specific type of action performed by a subject on an object
Private Key	A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity(the subject using the private key), not to be disclosed
Protection Profile (PP)	Implementation-independent statement of security needs for a TOE type
Public Key	A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity(the subject using the public key), it can be disclosed
Public Key(asymmetric)	A cryptographic algorithm that uses a pair of public and private key

cryptographic algorithm	
Public Security Parameters (PSP)	security related public information whose modification can compromise the security of a cryptographic module
Random bit generator (RBG)	A device or algorithm that outputs a binary sequence that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the sequence can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a "seed key," and the non-deterministic type RBG produces output that depends on the unpredictable physical source
Recommend/be recommended	The 'recommend' or 'be recommended' presented in Application notes is not mandatorily recommended, but required to be applied for secure operations of the TOE
Refinement	Addition of details to a component
Remote Authentication Dial-In User Services (RADIUS)	Service to identify and authenticate users by sending information such as user ID, password and IP address to the authentication server when a remote user requests a connection
Role	Predefined set of rules on permissible interactions between a user and the TOE
Secret Key	The cryptographic key which is used in symmetric cryptographic algorithm and is associated with on or more entity, it is not allowed to release
Secure Sockets Layer (SSL)	This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network
Security Policy Document	Document uploaded to the list of the validated cryptographic module with the module's name and specifying the summary for the cryptographic algorithms and operational environments of the TOE
Security Target (ST)	Implementation-dependent statement of security needs for a specific identified TOE
Selection	Specification of one or more items from a list in a component
Self-test	Pre-operational or conditional test executed by the cryptographic module
Sensitive Security Parameters (SSP)	critical security parameters (CSP) and public security parameters (PSP)
Shall/must	The 'shall' or 'must' presented in Application notes indicates

	mandatory requirements applied to the TOE
Subject	Active entity in the TOE that performs operations on objects
Symmetric cryptographic technique	Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique
Target of Evaluation (TOE)	Set of software, firmware and/or hardware possibly accompanied by guidance
Terminal Access Controller Access Control System (TACACS)	Authentication protocol that is common for UNIX networks, described in RFC 1492, used by remote access server to send user login passwords to an authentication server
Threat Agent	Entity that can adversely act on assets
TOE Security Functionality (TSF)	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs
Transport Layer Security (TLS)	This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246
TSF Data	Data for the operation of the TOE upon which the enforcement of the SFR relies
User	Refer to "External entity", authorized administrator and authorized end-user in the TOE
Validated Cryptographic Module	A cryptographic module that is validated and given a validation number by validation authority
Wrapper	Interfaces for interconnection between the TOE and various types of business systems or authentication systems

2. Conformance claim

2.1 CC conformance claim

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

		Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) · Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
Conformance claim	Part 2 Security functional components	Extended : FCS_RBG.1, FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security assurance components	*Conformant*
	Package	Augmented : EAL1 augmented (ATE_FUN.1)

2.2 PP conformance claim

This ST claim conformance the following PP.

• Korean National Protection Profile for Single Sign On V1.0

2.3 Package conformance claim

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

2.4 Conformance claim rationale

This ST claims conformance to security objectives and security requirements by "strict PP onomance" adherence to 'Korean National Protection Profile for Single Sign On V1.0'.

2.4.1 Security Target

PP	ST
OE.PHYSICAL_CONTROL	OE.PHYSICAL_CONTROL
OE.TRUSTED_ADMIN	OE.TRUSTED_ADMIN
OE.LOG-BACKUP	OE.LOG-BACKUP
OE.OPERATION_SYSTEM_REINFORCEMENT	OE.OPERATION_SYSTEM_REINFORCEMENT
OE.SECURE_DEVELOPMENT	OE.SECURE_DEVELOPMENT
OE.AUTHENTICATION_SYSTEM_SECURITY	-
-	OE.TIME_STAMP
-	OE.DBMS
-	OE.MANAGEMENT_ACCESS

* In the initial authentication stage of the TOE, identification and authentication functions of end-users are not supported by external authentication systems and therefore, the security goal of 'OE. Reinforce operating system' does not correspond.

* OE.TIME_STAMP : Accurately records incidents related to security by receiving reliable time stamps provided by the TOE operating environment and so the security goal is additionally prescribed.

* OE.DBMS : DBMS that saves the TSF data and audit data is operated in a physically safe environment and so the security goal is additionally prescribed.

* OE.MANAGEMENT_ACCESS : All information sent when attempting administrator access with the TOE component WPM is safely protected so the security goal of management access is additionally prescribed.

2.5 PP conformance statement

By complying with the same security goal as for the operating environment of the protection profile that is complied with in this security target, it 'complies with strict protection profiles'.

3. Security objectives

3.1 Security objectives for the operational environment

OE.PHYSICAL_CONTROL

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

OE.TRUST_ADMIN

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

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_DEVELOPEMENT

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

OE.TIME_STAMP

The TOE accurately records incidents related to security by receiving reliable time stamps provided by the TOE operating environment.

OE.DBMS

DBMS that saves the TSF data and audit data is operated in a physically safe environment.

OE. MANAGEMENT_ACCESS

All information sent when attempting administrator access with the TOE component WPM is safely protected.

4. Extended components definition

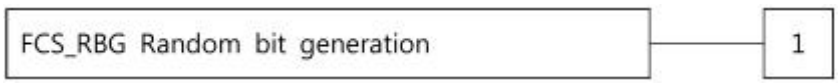
4.1 Cryptographic support

4.1.1 Random Bit Generation

Family Behaviour

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

Component leveling



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

Management: FCS_RBG.1

There are no management activities foreseen.

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

4.1.1.1. FCS_RBG.1 Random bit generation

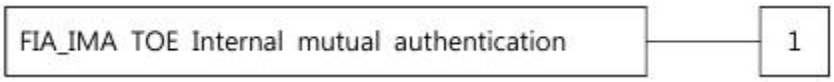
Hierarchical to No other components.
Dependencies No dependencies.
FCS_RBG.1.1The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [assignment: list of standards].

4.2 Identification and authentication

4.2.1 TOE Internal mutual authentication

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

Component leveling



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

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

Audit: FIA_IMA.1
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimum: Success and failure of mutual authentication

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

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

standards].

4.2.2 Specification of Secrets

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

Component leveling

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

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

Management: FIA_SOS.3
There are no management activities foreseen.

Audit: FIA_SOS.3
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimum : Success and failure of the activity

4.2.2.1. FIA_SOS.3 Destruction of Secrets

Hierarchical to No other components.
Dependencies FIA_SOS.2 TSF Generation of secrets
FIA_SOS.3.1The TSF shall destroy secrets in accordance with a specified secrets destruction method [assignment: secret destruction method] that meets the following: [assignment: list of standards].

4.3 Security Management

4.3.1 ID and password

Family Behaviour

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

Component leveling

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

Management: FMT_PWD.1

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

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

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

a) Minimum: All changes of the password

4.3.1.1 FMT_PWD.1 Management of ID and password

Hierarchical to No other components.

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

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

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

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

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

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

authorized administrator accesses for the first time].

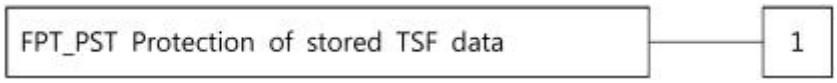
4.4 Protection of the TSF

4.4.1 Protection of stored TSF data

Family Behaviour

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

Component leveling



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

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

4.4.1.1. FPT_PST.1 basic protection of stored TSF data

Hierarchical to No other components.

Dependencies No dependencies.

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

4.5 TOE Access

4.5.1 Session locking and termination

Family Behaviour

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

Component leveling

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

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

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

Management: FTA_SSL.5
The following actions could be considered for the management functions in FMT:

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

Audit: FTA_SSL.5
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimum: Locking or termination of interactive session

4.5.1.1. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to No other components.
Dependencies FIA_UAU.1 authentication or No dependencies.
FTA_SSL.5.1The TSF shall [selection:

- *lock the session and re-authenticate the user before unlocking the session,*
- *terminate] an interactive session after a [assignment: time interval of user inactivity].*

5. Security requirements

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

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

5.1 Security functional requirements

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

[Table 1] Security functional component

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FUA_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation(1)
	FCS_CKM.1(2)	Cryptographic key generation(2)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation(1)
	FCS_COP.1(2)	Cryptographic operation(2)
	FCS_COP.1(3)	Cryptographic operation(3)
	FCS_COP.1(4)	Cryptographic operation(4)
	FCS_COP.1(5)	Cryptographic operation(5)
	FCS_RBG.1(Extended)	Random bit generation
FIA	FIA_AFL.1(1)	Authentication failure handling(1)
	FIA_AFL.1(2)	Authentication failure handling(2)
	FIA_IMA.1(Extended)	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action

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

5.1.1 Security audit (FAU)

FAU_ARP.1 Security alarms

Hierarchical to No other components.

Dependencies FAU_SAA.1 Potential violation analysis

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

Potential security violation list	Action list
Key# Crypto v1.3 self-test fail	Send e-mail to authorized administrator
DBMS disk capacity exceeded	
WPM/Policy Server/Session Server/SSO Engine/WAAPI Self-test and integrity test fail	
WPM/Policy Server/Session Server/SSO Engine/WAAPI not-operating	Send e-mail to authorized administrator
Audit save fails	
Administrator authorization fail exceeds allowed number (Default : 5 times or times set by authorized administrator)	Send e-mail to authorized administrator
End-user authorization fail exceeds allowed number (Default : 5 times)	Send e-mail to authorized administrator

FAU_GEN.1 Audit data generation

Hierarchical to No other components.

Dependencies FPT_STM.1 Reliable time stamps

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

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

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

c) [Refer to the "auditable events" in [Table 2] Audit events, [none]].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST [Refer to the contents of "additional audit record" in [Table 2] Audit events, [none]].

[Table 2] Audit 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	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_SOS.2	Rejection by the TSF of any tested secret	
FIA_SOS.3 (Extended)	Success and failure of the activity(applicable to the destruction of SSO token only)	
FIA_UAU.1	All use of the authentication mechanism	

FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the administrator identification mechanism, including the administrator identity provided	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1 (Extended)	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MSC.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5 (Extended)	Locking or termination of interactive session	-
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	-

FAU_SAA.1 Potential violation analysis

Hierarchical to No other components.

Dependencies FAU_GEN.1 Audit data generation

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

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

a) Accumulation or combination of [

self-test failure of the validated cryptographic module(Key# Crypto v1.3)

DBMS disk capacity exceeded

Not-operating of the WAS

Not-operating of the Policy Server

Not-operating of the Session Server

Not-operating of the SSO Engine

Not-operating of the WAAPI

Integrity test fail of the WPM
Integrity test fail of the Policy Server
Integrity test fail of the Session Server
Integrity test fail of the SSO Engine
Integrity test fail of the WAAPI
Audit save fails
Administrator authorization fail exceeds allowed number(Default : 5 times or times set by authorized administrator)
End-user authorization fail exceeds allowed number(Default : 5 times)
] known to indicate a potential security violation;
b) [none].

FAU_SAR.1 Audit review

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

FAU_SAR.3 Selectable audit review

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

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

		descending order based on the time of audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to No other components.

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Notification to the authorized administrator, [none] if the audit trail exceeds [the threshold set by the authorized administrator(default value 90%, the range of values that the authorized administrator is able to set 50% ~ 99%)].

FAU_STG.4 Prevention of audit data loss

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

Dependencies FAU_STG.1 Protected audit trail storage

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

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

5.1.2 Cryptographic support (FCS)

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

Hierarchical to No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [HASH_DRBG(SHA 256)] and specified cryptographic key sizes [128 Bit] that meet the following: [TTAK.KO-12.0190(2012)].

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

Hierarchical to No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSAES] and specified cryptographic key sizes [2048 Bit] that meet the following: [ISO/IEC 18033-2(2006)].

FCS_CKM.2 Cryptographic key distribution

Hierarchical to No other components.

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

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSAES 2048] that meets the following: [ISO/IEC 18033-2(2006)].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components.

Hierarchical to No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with random bit] that meets the following: [none].

FCS_COP.1(1) Cryptographic operation(Digital Signature)

Hierarchical to No other components.

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

FCS_COP.1.1 The TSF shall perform [Digital Signature and verification] in accordance with a specified cryptographic algorithm [RSA-PSS 2048] and cryptographic key sizes [2048 Bit] that meet the following: [ISO/IEC 14888-2(2008)].

FCS_COP.1(2) Cryptographic operation(Public key)

Hierarchical to No other components.

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

FCS_COP.1.1 The TSF shall perform [Key Distribution, Store Key in memory] in accordance with a specified cryptographic algorithm [RSAES] and cryptographic key sizes [2048 Bit] that meet the following: [ISO/IEC 18033-2(2006)].

FCS_COP.1(3) Cryptographic operation(MAC)

Hierarchical to No other components.

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

FCS_COP.1.1 The TSF shall perform [Generate message authentication code, Verification of authentication token] in accordance with a specified cryptographic algorithm [HMAC-SHA256] and cryptographic key sizes [256 Bit] that meet the following: [ISO/IEC 9797-2(2011)].

FCS_COP.1(4) Cryptographic operation(Symmetric key)

Hierarchical to No other components.

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

FCS_COP.1.1 The TSF shall perform [Encryption Between Components] in accordance with a specified cryptographic algorithm [SEED] and cryptographic key sizes [128 Bit] that meet the following: [KO-12.0004/R1(2005)].

FCS_COP.1(5) Cryptographic operation(HASH)

Hierarchical to No other components.

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

FCS_COP.1.1 The TSF shall perform [Generate authentication token] in accordance with a specified cryptographic algorithm [SHA-256/SHA-384/SHA-512] and cryptographic key sizes [256 Bit] that meet the following: [ISO/IEC 10118-3(2004)].

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 [the following list of standards].

list of standards	Random bit generation algorithm
TTAK.KO-12.0190	HASH_DRBG(SHA 256)

5.1.3 Identification and authentication (FIA)

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

Hierarchical to No other components.

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [1~10]* unsuccessful authentication attempts occur related to [authentication of administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*] the TSF shall [lock account for disabled time set by administrator (default value: 5 minutes)].

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

Hierarchical to No other components.

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within [5~10]*] unsuccessful authentication attempts occur related to [authentication of user].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed* the TSF shall [lock account for disabled time set by administrator (default value: 5 minutes)].

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 [Policy Server and SSO Engine, Policy Server and Session Server, and SSO Engine and WAAPI] using the [CHAP (Challenge Handshake Authentication Protocol)] that meets the following [RFC 1994(1996)].

FIA_SOS.1 Verification of secrets

Hierarchical to No other components.

Dependencies No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following permission criteria].

Acceptable characters	52 English letters (case sensitive)
	10 numbers (0~9)
	No special character limit
Password combination rules	Must include at least one English letter, number and special character each
	[Administrator password]

	- 9 – 20 characters [User password] - 9 – 63 characters - 3-4 upper/lower case letters, numbers and special characters - ID check - DOB check - Not case sensitive - Same characters cannot be used 3-5 times - Sequential characters cannot be used 3-5 times

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

FIA_SOS.2 TSF Generation of secrets

Hierarchical to No other components.

Dependencies No dependencies.

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

Prescribed allowance standards	Contents
Authentication token configuration method	Keys shared between servers, user IP, user info, version, algorithm ID, expiration, idle time, session slot, HMAC for Token ID
Composition field length	256 byte
Symmetric encryption algorithm	SEED 128

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

FIA_SOS.3 Destruction of secrets (Extended)

Hierarchical to No other components.

Dependencies FIA_SOS.2 TSF Generation of secrets

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

FIA_UAU.2 User authentication before any action

Hierarchical to FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components.

Dependencies No dependencies.

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

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components.

Dependencies FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*, Authentication failure message] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to FIA_UID.1 Timing of identification

Dependencies No dependencies.

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

5.1.4 Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to No other components.

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

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

[Table 3] List of functions

List of functions		Conduct management actions				The authorized role
		determine	Enable	modify	disable	
WPM	service	O	O	O	O	the

	EAM set	O	O	O	O	authorized administrator
	Manager set	O	O	O	O	
	Password policy	X	O	O	O	
	Login Policy	X	O	O	O	
	Delegation authority	O	O	O	O	
	Access ip	X	O	O	O	

FMT_MTD.1 Management of TSF data

Hierarchical to No other components.

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

The authorized role	manage / list of TSF data	Change_default	query	modify	delete	[create]
the authorized administrator	Organizaton	X	O	O	O	O
	User	X	O	O	O	O
	User Password regulation	O	O	O	X	X
	User ID regulation	O	O	O	X	X
	Role	X	O	O	O	O
	Group	X	O	O	O	O
	Policy	X	O	O	O	O
	Manager group	X	O	O	O	O
	Rule	X	O	O	O	O
	Manager	X	O	O	O	O
	Service	X	O	O	O	O
	Access IP	X	O	O	O	O
	Session time set	O	O	O	X	X
	Number of authentication attempts	O	O	O	X	X
	Authentication attempt blocking time	O	O	O	X	X
	DBMS threshold	O	O	O	X	X

	setting					
	Set administrator notification (cycle, reciver)	O	O	O	O	X
	Password	O	X	O	X	X
End-user	Password	X	X	O	X	X

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to No other components

Dependencies FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

1. [password combination rules and/or length]

List of function	password combination rules and/or length]
Password combination rules (admin)	[Administrator password] - 9 – 20 characters - Combination of 3 or more letters, numbers, or special characters
Password combination rules (user)	[User password] - 9 – 63 characters - 3-4 upper/lower case letters, numbers and special characters - ID check - DOB check - Not case sensitive - Same characters cannot be used 3-5 times - Sequential characters cannot be used 3-5 times

2. [none]

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

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

2. [An administrator-enrolled exclusion character]

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to No other components

Dependencies No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[

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

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

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

]

FMT_SMR.1 Security roles

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification

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

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

5.1.5 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF data transfer protection

Hierarchical to No other components.

Dependencies No dependencies.

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

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

Hierarchical to No other components.

Dependencies No dependencies.

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

FPT_TST.1 TSF testing

Hierarchical to No other components.

Dependencies No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of [*WPM, Policy Server, SSO Engine, Session Server*].

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

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

integrity of *TSF*.

5.1.6 TOE access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies FIA_UID.1 Timing of identification

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

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

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

Hierarchical to No other components.

Dependencies FIA_UAU.1 Authentication or No dependencies.

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

FTA_TSE.1 TOE session establishment

Hierarchical to No other components.

Dependencies No dependencies

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

5.2 Security assurance requirement

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

Security assurance class	Security assurance component	
Security Target 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 claims

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

ASE_OBJ.1 Security objectives for the operational environment

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

ASE_ECD.1 Extended components definition

Dependencies	No dependencies.
Developer action elements	
ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
Content and presentation elements	
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
Evaluator action elements	
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly

expressed using existing components.

ASE_REQ.1 Stated security requirements

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

ASE_TSS.1 TOE summary specification

Dependencies	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Developer action elements	
ASE_TSS.1.1D	The developer shall provide a TOE summary specification
Content and presentation elements	
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
Evaluator action elements	

ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2 Development

ADV_FSP.1 Basic functional specification

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

5.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies	ADV_FSP.1 Basic functional specification
Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Content and	

presentation elements	
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies	No dependencies.
Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
Content and presentation elements	
AGD_PRE1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE1.2C	The preparative procedures shall describe all the steps necessary for secure

	installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
Evaluator action elements	
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1 Labelling of the TOE

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

ALC_CMS.1 TOE CM coverage

Dependencies	No dependencies.
Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
Evaluator action elements	

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

5.2.5 Tests

ATE_FUN.1 Functional testing

Dependencies	ATE_COV.1 Evidence of coverage
Developer action elements	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
Content and presentation elements	
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
Evaluator action elements	
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1 Independent testing - conformance

Dependencies	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action	

elements

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

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

5.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

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

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

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

5.3 Security requirement rationale

5.3.1 Dependency rationale of security functional requirements

The following table shows dependency of security functional requirement.

[Table 4] Rationale for the dependency of the security functional requirement

NO.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3

2	FAU_GEN.1	FPT_STM.1	OE.TIME_STAMP
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FUA_STG.3	FAU_STG.1	OE.DBMS
7	FAU_STG.4	FAU_STG.1	OE.DBMS
8	FCS_CKM.1(1)	[FCS_CKM.2 또는 FCS_COP.1] FCS_CKM.4	10,14,15 11
9	FCS_CKM.1(2)	[FCS_CKM.2 또는 FCS_COP.1] FCS_CKM.4	12,13 11
10	FCS_CKM.2	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	8 11
11	FCS_CKM.4	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1]	8,9
12	FCS_COP.1(1)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	9 11
13	FCS_COP.1(2)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	9 11
14	FCS_COP.1(3)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	8 11
15	FCS_COP.1(4)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	8 11
16	FCS_COP.1(5)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	-
17	FCS_RBG.1	-	-
18	FIA_IMA.1	-	-

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

FAU_GEN.1 has a dependent relationship with FPT_STM.1 and this uses reliable time stamp provided by the TOE operating environment and records tests related to security. Therefore, it satisfies the security goal time stamp for operating environments.

FAU_STG.3 and FAU_STG.4 have dependent relationships with FAU_STG.1 and this is satisfied by the DBMS operating environment.

FIA_AFL.1(1), FIA_AFL.1(2), FIA_UAU.7 and FTA_SSL.5 have dependent relationships with FIA_UAU.1 and this is satisfied by FIA_UAU.2 that have hierarchal relationships with FIA_UAU.1.

FIA_UAU.2, FMT_SMR.1, and FTA_MCS.2 have dependent relationships with FIA_UID.1 and this is satisfied by FIA_UID.2 that have hierarchal relations with FIA_UID.1

FCS_COP.1 (5) has dependencies on FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.4, but this is satisfied because the Hash algorithm does not use cryptographic keys.

5.3.2 Dependency rationale of security assurance requirements

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

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

6. TOE summary specification

6.1 Security Audit(AUDIT)

6.1.1 Audit data generation(AUDIT.1)

▣ WPM/Policy Server/Session Server/SSO Engine/WAAPI

The TOE conducts security managements and generates results for potential security violations of TOE components and results according to identification and authentication, and audit data for events that occur in the system and saves it in DBMS.

Audit data generated in the TOE are as follows.

Audit data	Cases for audits	Remarks
User use history	- User identification and authentication - Generation of authentication token - Verification of authentication token	SSO Engine
Administrator use history	- Administrator identification and authentication - WPM management - Security settings - Change TSF data information - Terminate session	WPM
System use history	- Start/end - Self-test and integrity inspection - Non-operation - Exceeding allowed administrator fail count	WPM
	- Key# Crypto v1.3 self-test - Audit data repository capacity exceeded	Policy Server

	- Self-test and integrity inspection	
	- Start/end - Self-test and integrity inspection - Non-operation	Session Server
	- Start/end - Self-test and integrity inspection - Non-operation - Cryptographic key management (generation, operation)	SSO Engine
	- Start/end - Self-test and integrity inspection - Non-operation	WAAPI

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

Related SFRS : FAU_GEN.1

6.1.2 Audit data review(AUDIT.2)

▣ WPM

The TOE provides functions that can review audit data to authorized administrators.

The provided audit data saves authorized administrator and end-user identification and authentication history, TSF function change and data value, management history for threshold change, history of start/end of TOE components saved in the TOE operating environment DBMS, and queries DBMS to provide it as a suitable format to the authorized administrator.

In addition to the super administrator, delegated administrators with accounts having audit rights can also query audit data.

Related SFRS : FAU_SAR.1, FAU_SAR.3

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

▣ Policy Server

The TOE detects potential violation (validated cryptographic module (Key# Crypto v1.3) self-test, checks DBMS disk capacity, self-test and integrity test and non-operation of the WPM/Policy Server/Session Server/SSO Engine/WAAPI, failure to save audits, exceeding number of allowed administrator/end-user failure) according to the set notification cycle to notifies of the security threats to the authorized administrator via e-mail.

Also, in order to loss prevent of audit data, when the DBMS warning notification threshold (default: 80%) is exceeded, an e-mail is sent to the authorized admin. When exceeding the DBMS past records deletion threshold (default: 90%), the oldest audit records are deleted to prevent loss of audit data.

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

6.2 Cryptographic support(CKM)

6.2.1 Cryptographic Key Management & Cryptographic operation (CKM.1)

▣ Policy Server, Session Server, SSO Engine, WAAPI

The TOE uses the following validated cryptographic modules to generate authentication tokens and conduct mutual-authentication.

- Cryptographic module name: Key# Crypto v1.3
- Validation no.: CM-110-2021.1
- Expiration date: Jan 27, 2021
- User mode

AIX	libjavaCmvp.so , libKeySharpCryptoV1_3.so
HP-UX	libjavaCmvp.so , libKeySharpCryptoV1_3.sl

The TOE performs cryptographic support functions for each component as follows.
- Session Server and Policy Server
- Policy Server and SSO Engine
- SSO Engine and WAAPI

Each component generates a cryptographic key using a public key cryptographic algorithm (RSAES 2048) for mutual authentication and uses an electronic signature algorithm (RSA-PSS 2048) for cryptographic operation.
The cryptographic keys generated by the Policy Server, the Session Server, and the SSO Engine are periodically destroyed by overwriting random numbers, and the WAAPI is immediately destroyed by overwriting random numbers.

The TOE component generates a 128-bit cryptographic key using a random number generator (HASH_DRBG (SHA256) and distributes the key to the SSO Engine using public key algorithm (RSAES 2048).
Then, the communication interval is encrypted using the symmetric key algorithm (SEED (CBC) 128 bit), and the random number is periodically overwritten and destroyed.

The policy server generates a 128-bit cryptographic key (token key) using a random number

generator (HASH_DRBG (SHA256)) and the generated cryptographic key (token key) distributes the key to the SSO Engine using a public key algorithm (RSAES 2048).
The SSO Engine generates / verifies the message authentication code and the authentication token using the MAC algorithm (HMAC-SHA256) and the hash algorithm (SHA-256), and the generated cryptographic key (token key) is periodically destroyed by overwriting the random number .
Related SFRS : FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1) , FCS_COP.1(2) , FCS_COP.1(3) , FCS_COP.1(4) , FCS_COP.1(5), FCS_RBG.1

6.3 Identification and authentication (IA)

6.3.1 Authentication failure handling (IA.1)

▣ WPM

The TOE has restrictions to allow only authorized administrators to state the number of failed authentication attempts for administrators and the allowed administrator authentication failures are limited to 1-10 times.
The TOE locks the administrator's account by the blocking time when the number of authentication failure times is reached in the authentication attempt through the WPM.

▣ SSO Engine

The TOE has restrictions to allow only authorized administrators to state the number of failed authentication attempts for end-users and the allowed user end-user authentication failures are limited to 5-10 times.
The TOE locks the end-user's account by the blocking time when the number of authentication failure times is reached in the authentication attempt through initial authorization by ID/PW based.

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

6.3.2 Identification and authentication (IA.2)

▣ Policy Server, Session Server, SSO Engine, WAAPI

During communication between components (Policy Server and SSO Engine, Policy Server and Session Server, and SSO Engine and WAAPI), the TOE uses the random bit generator (HASH_DRBG (SHA 256)), public key algorithm (RSAES 2048) and digital signature algorithm (RSA-PSS 2048) to validate signatures of each module and complete mutual-authentication.

▣ WPM

The admin's authentication information are ID and password. Password for identification and authentication allow upper case letters (A~Z), lower case letters (a~z), numbers (1~0), special characters (no limit) and must be created according to the combination rules to be 9-20

characters long containing at least one English letter, number and special character each. Passwords for authentication are indicated with '*' and only provides information on the cause for failed authentication to prevent exposure of passwords and maintains security management authorizations when successfully identifying and authenticating.
Authentication data prevents reuse of authentication information through session ID encryption including random bits.

▣ **SSO Engine**

During initial identification and authentication of end-user through the business system, end-user identification and authentication must be carried out first before allowing all actions. While authentication is under way, the user is provided only with [*] and information on the cause for failed authentication
The end-user's initial identification and authentication information are ID and password and the password combination rules are applied according to the settings of the authorized administrator. The authorized administrator shall set the number of upper and lower-case letters, numbers and special characters and ID when creating password, whether to include date of birth, whether to set as case sensitive, whether to prohibit 3-5 of the same characters, whether to prohibit 3-5 characters in sequence, and the combination rules for the password.
The user's authentication data encrypts session ID including random bits to prohibit reuse.

Once the user's initial identification and authentication is complete, the authentication token is generated. The authentication token is generated using the symmetric algorithm (SEED 128(CBC)) and MAC algorithm (HMAC-SHA256), and reuse is prohibited with the Onetime Token method.

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

6.4 Security management(SM)

6.4.1 Security management(SM.1)

▣ **WPM**

The WPM conducts security management for the organization, group, service, role, policy, administrator group, audit, management rights, and configuration.
[Organization]
Manages the uppermost and lowermost organization and the end-user account.
ID policy, password policy and login policy can be applied to the organization end-user in the generated organization and roles per organization or user, service use authority with business system and administrators can be set.
End-user ID is set with an ID length of 1-31 depending on the administrator settings and it is

managed by registering the ID composition combination (letters/numbers/letters, numbers/letters, numbers, special characters), first character (letter/number/no restriction) settings, and letters excluded for IDs.

Furthermore, user password shall be created between 9-63 characters according to administrator settings and the combination rules are managed such as necessary combination of upper/lower-case letters, numbers and special characters, same ID, DOB inspection, case sensitive, prohibiting the use of the same letter 3-5 times, prohibiting use of letters in sequence 3-5 times, etc.

[Group]

Set the roles, end-user authority and administrator authority by tying specific users in an organization as members of the group.

[Service]

Link with business system to register services that end-users can access as tree format.

The linked services set the user authority and service usage period per role, organization or group.

[Roles]

Categorize specific users within an organization by role and set the time and IP address information or restriction/allowance policies according to restriction rules. Set administrators per role.

[Policy]

In order to generate policies applied in the role, register the time and IP address for generating policies to manage IP/time restriction policies, or set the restriction policies or allowance policies with restriction rules by computing contents of the user profile.

[Administrator Group]

Add end-users within an organization as members to carry out management authorities through administrator groups and set the management authority (query, edit, add/delete) for the management item (organization/group/service/role/policy/configuration/audit) per administrator group.

[Management Authority]

View the management authority of authorized administrators and view management authority list of administrators for delegated management authorities.

[Configuration]

Register user profile for restriction rules within policies to manage.

Register and manage user authority (e.g. add, query, edit, delete, etc.) for each service registered as services.

Manage the allowance time and allowance IP to set login allowance policies applied to users per organization.

It manages allowed number of failures for administrator authentication, lock time, session timeout time, etc. and it sets the DBMS warning threshold and past record deletion threshold to protect the audit repository.

Register administrator IP address for the WPM access and set use of notification for potentially harmful items (check DBMS disk capacity, activation of policy service, activation of engine, activation of session server, activation of WAS, audit save fail) and set the notification period. Manage the administrator to receive the notifications.
When changing the administrator password, it must be managed with combination rules to be between 9 and 20 characters including letters, numbers and special characters.

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

6.5 Protection of the TSF(PT)

6.5.1 Protection of the TSF(PT.1)

▣ WPM, Policy Server, Session Server, SSO Engine, WAAPI

Mutual authentication and interval encryption are performed to protect the data from exposure and modification during transmission between separate parts of the TOE.

TSF Protect	TSF Component		Algorithm
Mutual Authentication	Session Server	Policy Server	- Public Key Encryption : RSAES(2048) - Digital Signature Algorithm : RSA-PSS(2048)
	Policy Server	SSO Engine	
	SSO Engine	WAAPI	
Encryption Between Components	Session Server	Policy Server	- Random Bit Generator : HASH_DRBG(SHA256) - Public Key Encryption : RSAES(2048) - Symmetric Key Encryption : SEED(CBC) 128 bit
	Policy Server	SSO Engine	
	SSO Engine	WAAPI	

The cryptographic key stored in the memory is encrypted and stored with the key encryption key (KEK), and the KEK is encoded and stored.

Administrator and user passwords are securely stored in DBMS using hash algorithm (SHA-256 / SHA-384 / SHA-512). TOE components (WPM, Policy Server, Session Server, SSO Engine, WAAPI) performs integrity verification (SHA-256) periodically (1 hour) after its operation.

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

6.6 TOE access(TA)

6.6.1 Session management(TA.1)

▣ **WPM**

The TOE controls the admin's management access based on connection IP when attempting to access the WPM and when attempting to connect from an IP not allowed, administrator access session is denied.

Access authority of the WPM is limited to one simultaneous session and sessions are not allowed simultaneously with the super administrator and delegated administrator with policy setting authorities.

Session terminate by the TOE that interacts after the inactive time (default: 10 minutes) of the authorized administrator and after this time, reauthentication is needed.

▣ **SSO Engine**

When the idle time of the authentication token passes, session terminate by the TOE. Afterwards, authentication token verification will fail. Identification and authentication is needed through the end-user's ID and password for reauthentication.

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