	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


KSignAccess V5.0 Security Target V1.4



Ksign Co., Ltd.



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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Copyright © 2024 KSIGN Co., Ltd. All rights reserved.

KSignAccess V5.0 Security Target

KSIGN, KSignSecureDB, KSignAccess, WizSign, KSignCASE, KSignPKI, KSignCA, KSignRA, KAMOS is a program and registered trademark of KSign Co., Ltd. and protected by copyright law.

Therefore, the copyright of this document is provided by KSign Co., Ltd. without the permission of the head office, without any permission to reproduce or use this trademark partly or wholly

13th, 14th floor, 25th, Gwacheon-daero 7na-gil, Gwacheon-si, Gyeonggi-do (Galhyeon-dong K-Sign)

TEL : 02-564-0182 FAX : 02-564-1627

<http://www.ksign.com>

Ksign Co., LTD.



	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Table of Contents

1. ST INTRODUCTION.....	11
1.1 ST REFERENCE	11
1.2 TOE REFERENCE	11
1.3 TOE OVERVIEW	12
1.3.1 Single Sign On overview	12
1.3.2 TOE type and scope	13
1.3.3 TOE usage and major security features.....	13
1.4 TOE OPERATIONAL ENVIRONMENT	16
1.4.1 Non-TOE and TOE operational environment	16
1.4.2 Requirements for non-TOE software, hardware, firmware	17
1.5 TOE DESCRIPTION	20
1.5.1 Physical scope of the TOE.....	20
1.5.2 Logical scope of the TOE	23
1.6 CONVENTIONS.....	26
1.7 TERMS AND DEFINITIONS	28

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

2. CONFORMANCE CLAIM..... 35

2.1 CC CONFORMANCE CLAIM35

 2.1.1 CC, PP, and security requirement packages.....35

 2.1.2 Type of conformance35

 2.1.3 PP composite conformance claim.....36

 2.1.4 PP conformance claim.....36

 2.1.5 Package conformance claim36

 2.1.6 Conformance claim rationale36

2.2 CONFORMANCE CLAIM RATIONALE36

 2.2.1 Reference to evaluation methods/activities.....36

3. SECURITY PROBLEM DEFINITION..... 38


3.1 ASSETS.....38

3.2 THREATS.....38

 3.2.1 Unauthorized access.....38

 3.2.2 Information leakage.....39

 3.2.3 TOE functionality compromise.....39

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

3.3 ORGANIZATIONAL SECURITY POLICY (OSP).....39

3.4 ASSUMPTIONS40

4. SECURITY OBJECTIVES41

4.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT41

4.2 SECURITY OBJECTIVES RATIONALE42

 4.2.1 Operational environment security objectives rationale.....43

5. EXTENDED COMPONENT DEFINITION46

5.1 IDENTIFICATION AND AUTHENTICATION (FIA).....46

 5.1.1 TOE Internal mutual authentication.....46

 5.1.2 Specification of Secrets.....47

5.2 SECURITY MANAGEMENT (FMT).....48


 5.2.1 ID and password48

5.3 PROTECTION OF THE TSF.....49


 5.3.1 Protection of stored TSF data49

6. SECURITY REQUIREMENTS.....51


6.1 SECURITY FUNCTIONAL REQUIREMENTS.....51

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


Security audit (FAU).....	54
6.1.2 Cryptographic support (FCS).....	58
6.1.3 Identification and authentication (FIA).....	66
6.1.4 Security management (FMT).....	70
6.1.5 Protection of the TSF (FPT).....	73
6.1.6 TOE access (FTA).....	74
6.1.7 Trusted path/channels (FTP).....	75
6.2 SECURITY ASSURANCE REQUIREMENTS	76
6.2.1 Security target evaluation	77
6.2.2 Development.....	83
6.2.3 Guidance documents	84
6.2.4 Life-cycle support	87
6.2.5 Tests.....	88
6.2.6 Vulnerability assessment.....	89
6.3 SECURITY REQUIREMENTS RATIONALE.....	91
6.3.1 Security functional requirements rationale	91

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


6.3.2	Assurance requirements rationale.....	101
6.4	DEPENDENCIES RATIONALE	102
6.4.1	Dependencies of security functional requirements.....	102
6.4.2	Dependencies of assurance requirements.....	105
7.	TOE SUMMARY SPECIFICATIONS.....	105
7.1	SECURITY AUDIT	105
7.1.1	Security alerts.....	105
7.1.2	Audit data generation	106
7.1.3	Potential violation analysis	107
7.1.4	Audit data review.....	108
7.1.5	Audit data loss prevention	108
7.1.6	SFR Mapping.....	108
7.2	CRYPTOGRAPHIC SUPPORT	109
7.2.1	Cryptographic support.....	109
7.2.2	Random bit generation.....	111
7.2.3	SFR Mapping.....	111

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.3 IDENTIFICATION AND AUTHENTICATION.....	112
7.3.1 User authentication failure handling.....	112
7.3.2 Protection of authentication information	112
7.3.3 Password policy verification	113
7.3.4 Prevention of reuse of authentication information	113
7.3.5 Mutual authentication between components.....	114
7.3.6 Authentication token creation and disposal.....	115
7.3.7 SFR Mapping.....	116
7.4 SECURITY MANAGEMENT	116
7.4.1 Security function management	116
7.4.2 ID and password management	117
7.4.3 SFR Mapping.....	118
7.5 TSF PROTECTION.....	118
7.5.1 Maintaining safe state in case of failure	118
7.5.2 Internal transmission data protection between TSF components.....	118
7.5.3 Protection of stored TSF data	119

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.5.4	Self-test.....	119
7.5.5	Integrity check.....	120
7.5.6	SFR Mapping.....	122
7.6	TOE ACCESS.....	122
7.6.1	Administrator session limit.....	122
7.6.2	Security management interface session termination	122
7.6.3	SFR Mapping.....	123
7.7	TRUSTED PATH/CHANNELS(FTP).....	123
7.7.1	Trusted channel between TSFs	123
7.7.2	SFR Mapping.....	123

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

1. ST introduction

This document is the Security Target (ST) for KSignAccess V5.0 (hereinafter referred to as 'TOE'), aiming for the Common Criteria (CC) EAL1+ evaluation level.


1.1 ST reference

Title	KSignAccess V5.0 Security Target
Version	V1.4
Author	KSign Co., LTD.
Date	2025. 02. 26
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning Notification No. 2013-51)
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, 2022.11 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, 2024.07
Evaluation Assurance Level	EAL 1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Single Sign On V3.0
Keywords	Single Sign On, SSO

[Table 1-1] ST reference

1.2 TOE reference

Item		Specification
TOE		KSignAccess V5.0
Version		V5.0.3
Components	KSignAccess Server	KSignAccess Server V5.0.1

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

	KSignAccess Agent	KSignAccess Agent for Linux	KSignAccess Agent for Linux V5.0.1
		KSignAccess Agent for Windows	KSignAccess Agent for Windows V5.0.1
Manuals	Preparative Procedure	KSignAccess V5.0 Preparative Procedure	KSignAccess V5.0 Preparative Procedure V1.4
	Operation Manual	KSignAccess V5.0 Operational User Guidance	KSignAccess V5.0 Operational User Guidance V1.3
Developer			KSign Co., LTD.

[Table 1-2] TOE reference


1.3 TOE overview

1.3.1 Single Sign On overview

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

The TOE shall provide the user login capability using authentication methods (e.g., ID and password), issue a token during user login, and verify the issued token if accessing another business system after user login. Authentication functions based on ID and password for authorized administrators and authorized end users in the TOE are mandatorily required. For end users, however, authentication functions are only applied when the TOE, not external authentication system, provides them in the initial authentication phase of single sign on.

The primary security features provided by the TOE include user identification and authentication, token issue, storage, verification and destruction. During the generation of authentication token and user single sign on based on the authentication token, the TOE must use a validated cryptographic module

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP).

1.3.2 TOE type and scope

The TOE defined by this Security Target is SSO that enables the user to access various business systems through a single user login, and the TOE components are provided in the form of appliance or software.

The essential TOE components defined in this Security Target are KSignAccess Server and KSignAccess Agent. The TOE is composed of the KSignAccess Server that processes user login, manages the token, and sets the policy, etc; and the KSignAccess Agent that is installed in each business system performs the function of token issue and verification, etc. In addition, the KSignAccess Agent operates in the form of an 'API type' composed of the library file.


1.3.3 TOE usage and major security features

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

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

In addition, the token requires confidentiality and integrity protection, and the TOE executable code requires integrity protection.

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


	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

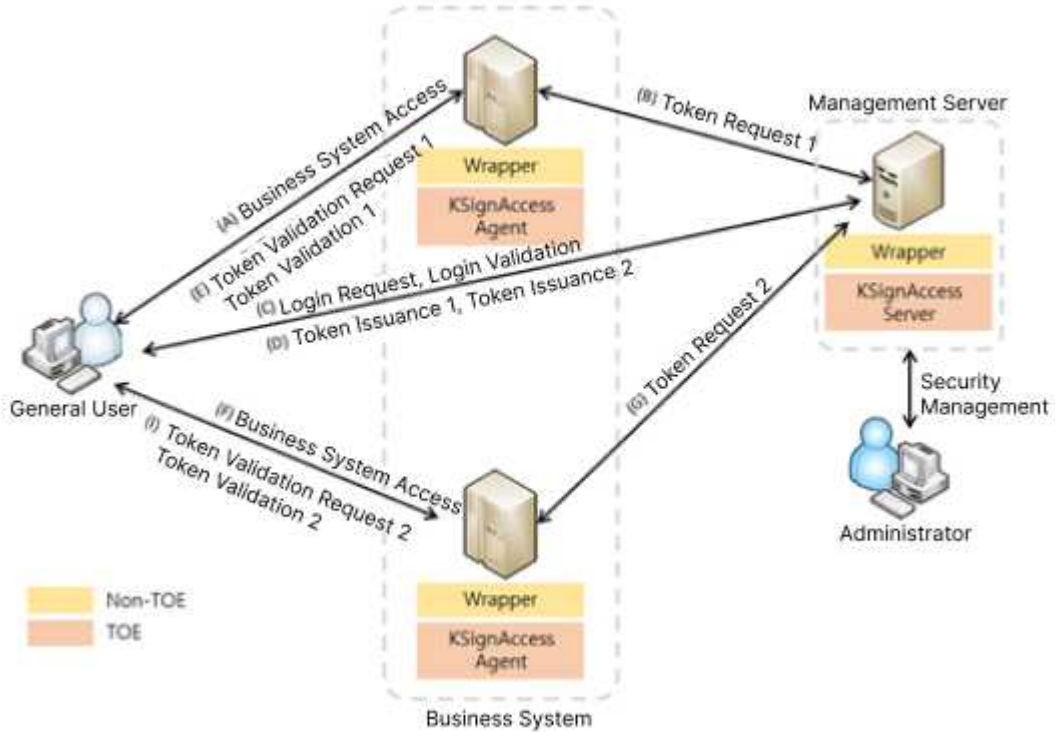
using the token issued during the initial authentication procedure. The detailed execution procedure for each authentication phase corresponds to the flow illustrated in Figure 1-1.

The execution procedure of the initial authentication phase is as follows. The user requests login by using ID/PW alone, and the KSignAccess Agent that receives the login request message sends a login verification request to the KSignAccess Server, which in turn checks the authorized user status. Upon receiving the login verification request, the KSignAccess Server performs login verification directly using the user information stored in the DBMS, or by interfacing with the authentication system. The KSignAccess server issues a token if the login verification result is valid. The KSignAccess agent transfers an issued token to the user

The token-based authentication phase is performed only when the token has been normally issued in the initial authentication phase.

When the user utilizes business system services, the issued token transferred to the SSO agent installed in the pertinent business system, and the SSO agent verifies the validity of the token by interfacing with the SSO server upon receiving the token.

 KSIGN <i>e-Security Leader</i>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		




[Figure 1-1] Product operation flow

authentication phase	operation procedure
initial authentication	(A) Business system Access – (B) Token issue request 1 – (C) Login request and Login verification – (D) Token issue 1 - (E) Token verification request 1 and Token verification 1
token-based authentication	(F) Business system Access – (G) Token issue request 2 – (H) Token issue 2 - (I) Token verification request 2 and Token verification 2

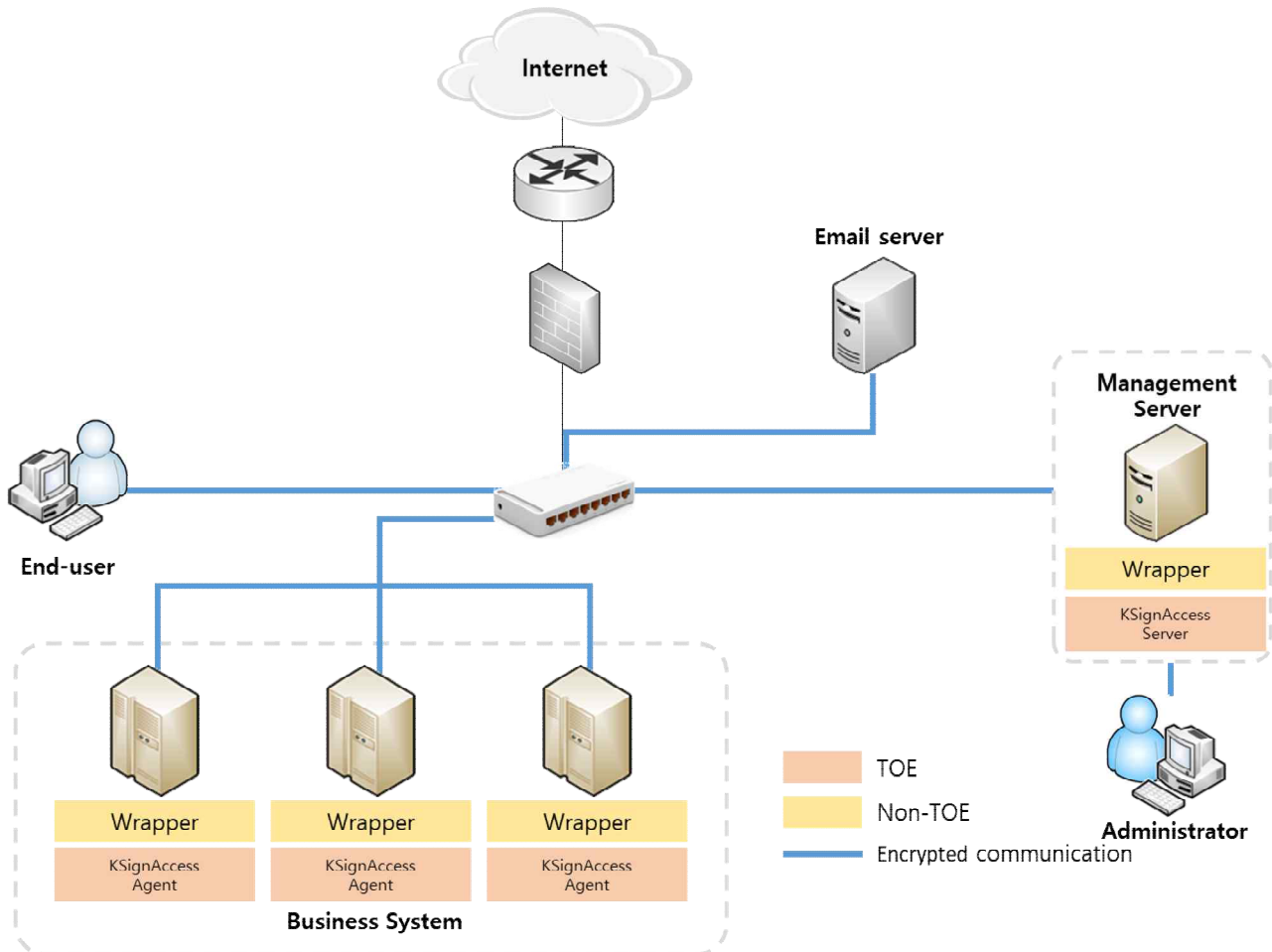
[Table 1-3] Product operation procedure

- Subject who issues the token: KSignAccess Server
- Token storage location: End user PC
- Subject who verifies the token: KSignAccess Server + KSignAccess Agent

 KSIGN <i>e-Security Leader</i>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


1.4 TOE operational environment

1.4.1 Non-TOE and TOE operational environment



[Figure 1-2] TOE operational environment

Figure 1–2 shows the general TOE operational environment. The operational environment is composed of the KSignAccess Server and KSignAccess Agent. The KSignAccess server verifies user login attempts directly using the user information stored in the DBMS, the token management, and the policy configuration. The KSignAccess agent is installed in each business system and requests user login verification to the KSignAccess server or issues the token. Additionally, the KSignAccess Agent operates as an 'API type' composed of the library file.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Authorized administrators can perform security management by accessing the KSignAccess Server through web browsers.


External IT entities required for operating the TOE include an email server. The email server is used to notify authorized administrators in case of anticipated audit data loss or integrity failures. Encrypted communication is performed between the email server and TOE components during communication.

1.4.2 Requirements for non-TOE software, hardware, firmware

The TOE components consist of KSignAccess Server and KSignAccess Agent, which are distributed in software form.

The minimum system requirements for systems where the TOE is installed and operated are as follows.

TOE		Item	Specification
KSignAccess Server		CPU	Intel Core i7 3.60 GHz or higher
		Memory	16 GB or higher
		HDD	Space required for installation of TOE 500 MB or higher
		NIC	100/1000 Mbps x 1EA or higher
KSignAccess Agent	KSignAccess Agent for Linux	CPU	Intel Core i5 3.30 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for installation of TOE 500 MB or higher
		NIC	100/1000 Mbps x 1EA or higher
	KSignAccess Agent for Windows	CPU	Intel Core i5 3.30 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for installation of TOE 500 MB or higher

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

	NIC	100/1000 Mbps x 1EA or higher
--	-----	-------------------------------

[Table 1-4] Requirement hardware for non-TOE

The operating system on which the TOE operates is as in the following

TOE		Operating System
KSignAccess Server		Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)
KSignAccess Agent	KSignAccess Agent for Linux	Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)
	KSignAccess Agent for Windows	Windows Server 2016 (64bit)

[Table 1-5] Operating system for TOE support


The requirements for security management are as in the following.

Item	Sub-Item	Specification
Software	Web Browser	Google Chrome 132 (64bit)

[Table 1-6] Requirement for management system

The following non-TOE software is required for proper operation, although it is not included in the TOE scope.

TOE	S/W	Purpose
KSignAccess Server	JRE 1.8.0_431	Operation and execution of KSignAccess Server based on Java Application, performing security management functions, and operating the web server
	Apache Tomcat 9.0.98	Web Application Server (WAS) operating on a Java Application basis for the normal operation of the TOE
	MySQL 8.0.41	Storage for TOE policy configuration and audit data
KSignAccess Agent	JRE 1.8.0_431	Operation and execution of KSignAccess Agent based on Java Application
	Apache Tomcat 9.0.98	Web Application Server (WAS) operating on a


	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		
		Java Application basis for the normal operation of the TOE			

[Table 1-7] Non-TOE software

To operate the TOE, the following additional systems are required in the IT environment.

Item	TOE Support Function
Mail Server (SMTP Server)	Server for sending alert emails to administrators

[Table 1-8] IT environment supporting TOE operation

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

1.5 TOE description

This section describes the physical and logical scope and boundaries of the TOE.

1.5.1 Physical scope of the TOE


The TOE consists of Server, Agent, Preparation Procedures and Operation Guide

Scope		Distribution Status	Type	Distribute
Name		KSignAccess V5.0		
Detailed Version		V5.0.3		
TOE Components	KSignAccess Server	KSignAccess Server V5.0.1 (KSignAccess_Server_V5.0.1.tar)	S/W	CD
	KSignAccess Agent	KSignAccess Agent for Linux V5.0.1 (KSignAccess_Agent_Linux_V5.0.1.tar)		
		KSignAccess Agent for Windows V5.0.1 (KSignAccess_Agent_Windows_V5.0.1.zip)		
Manuals	Preparative Procedure	KSignAccess V5.0 Preparative Procedure V1.4 (KSignAccess V5.0 Preparative Procedure V1.4.pdf)	Electronic Document (PDF)	
	Operation Manual	KSignAccess V5.0 Operational User Guidance V1.3 (KSignAccess V5.0 Operational User Guidance V1.3.pdf)		

[Table 1-12] Physical scope of the TOE

The information about the validated cryptographic modules used in the TOE is as follows.

TOE	Software	use
KSignAccess Server	KSignCASE64 v2.5.2.0	Validated cryptographic module for key generation, distribution, destruction, renewal, cryptographic operations, and encrypted communication between KSignAccess Server

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

		and KSignAccess Agent.
KSignAccess Agent	KSignCASE64 v2.5.2.0	Validated cryptographic module for key generation, distribution, destruction, renewal, cryptographic operations, and encrypted communication between KSignAccess Server and KSignAccess Agent.

[Table 1-9] Validated cryptographic module information

Detailed information about the validated cryptographic module included in the TOE is as follows.


Item	Details
Cryptographic Module Name	KSignCASE64 v2.5.2.0
Developer	Ksign Co., Ltd.
Validation Date	2023. 10. 16
Validation Level	VSL1
Validation Number	CM-237-2028.10
Expiration Date	2028. 10. 16.

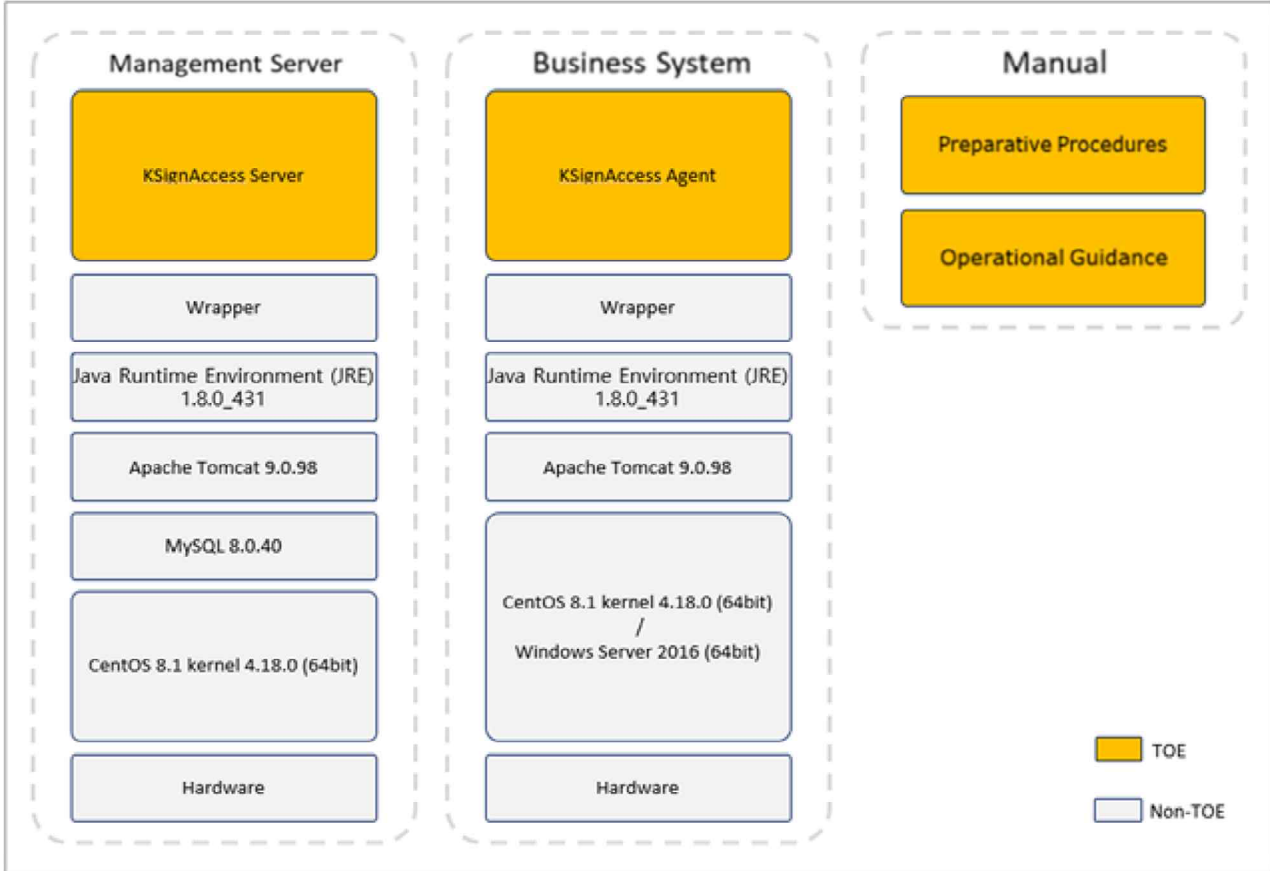
[Table 1-10] Detailed information of validated cryptographic module

The following third-party software is used to perform the TOE's security functions.


TOE	Software	Purpose
KSignAccess Server	log4j 2.24.3.jar	Evidence of product operation logs
	javax.mail 1.6.2.jar	Mail transmission
	spring security 5.8.16.jar	Perform Authentication and Authorization during Admin Page Login
KSignAccess Agent	log4j 2.24.3.jar	Evidence of product operation logs

[Table 1-11] Third-party software for performing security functions

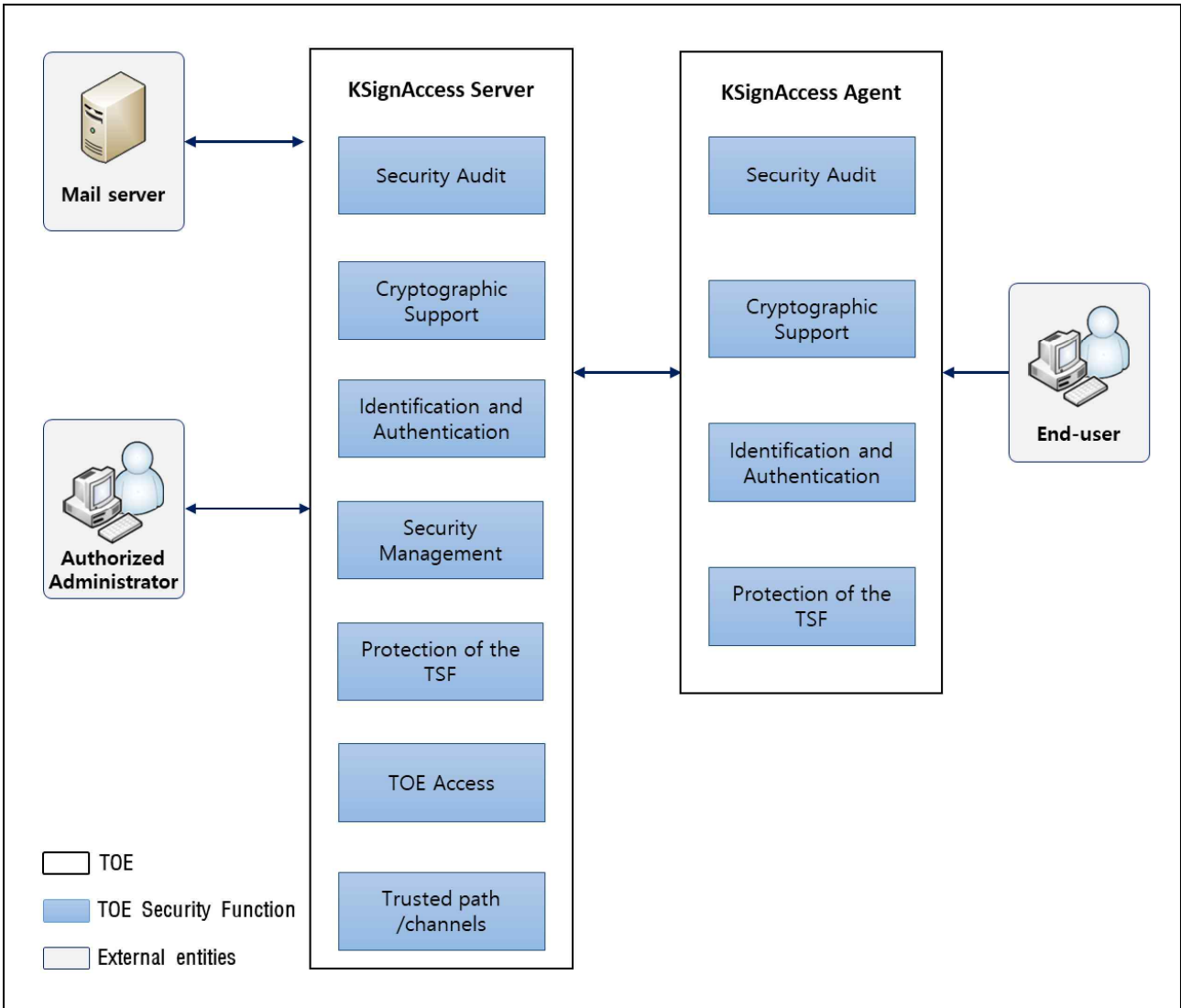
 KSIGN <i>e-Security Leader</i>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		



[Figure 1-3] Physical scope of the TOE

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


1.5.2 Logical scope of the TOE



[Figure 1-4] Logical scope of the TOE

- Security audit

KSignAccess Server provides authorized administrators with the means to access audit information and presents it in an understandable format. When an auditable event occurs, it generates audit data, detects potential violations, and sends alert emails to authorized administrators. Additionally, all generated audit data is securely stored in the audit evidence repository (DBMS) for safe management.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

The audit data prevents unauthorized deletion and includes functionality to protect the audit evidence repository by ignoring audited events when the repository reaches full capacity. In such cases, an email notification is sent to the registered administrator to indicate repository overflow or saturation.

- Cryptographic support

KSignAccess Server and KSignAccess Agent use the validated cryptographic module KSignCASE64 v2.5.2.0, which has been confirmed for safety and implementation compliance through the Cryptographic Module Validation Program (KCMVP). This module securely generates and destroys all cryptographic keys used in product operations (destroyed by overwriting with 0 three times) and performs cryptographic operations for authentication token generation and validation in accordance with the defined cryptographic policy. Additionally, for encrypted communication between the physically separated KSignAccess Server and KSignAccess Agent, cryptographic keys are securely generated and distributed using the validated cryptographic module KSignCASE64 v2.5.2.0.


- Identification and authentication

KSignAccess Server performs identification and authentication for administrators attempting to use security management functions before any actions are taken. It also provides functionality to protect authentication feedback during authentication data input. Additionally, it ensures secure identification and authentication by locking access in the event of consecutive authentication failures. Furthermore, it prevents attempts to reuse authentication information for administrators logging into KSignAccess Server.

KSignAccess Agent performs identification and authentication for general users attempting to utilize integrated authentication functions. It provides functionality to protect authentication feedback during authentication data input and ensures secure identification and authentication by locking access in the event of consecutive authentication failures. Additionally, it prevents attempts to reuse authentication information for general users logging into KSignAccess Agent.

Issues the Authentication Token: Authentication tokens are generated using the validated cryptographic module on KSignAccess Server.

Verifies the Authentication Token: Authentication tokens are validated using the validated cryptographic module on both KSignAccess Server and KSignAccess Agent.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

KSignAccess Server verifies administrator and general user passwords according to a secure password combination rule.

When generating authentication tokens for general users in integrated authentication, tokens are created using validated cryptographic modules based on token creation information. Tokens are securely destroyed by overwriting the data three times with 0 during the token destruction process.

TOE performs mutual authentication through a self-implemented protocol between the KSignAccess Server and the KSignAccess Agent.

- Security management

KSignAccess Server provides authorized administrators with security management functions, including access control policy management, administrator management, and KSignAccess Server environment configuration. Authorized administrators perform these management functions through the security management interface.


Authorized administrators include super administrators and audit administrators. The super administrator can perform all security management functions of the TOE through the security management interface, while the audit administrator can perform audit data query functions.

When an authorized administrator first accesses the security management interface, they are forced to change their password. In the case of an audit administrator, after the password is reset by an authorized administrator, they must change their password upon login.

General users are required to change their passwords during their initial login through the user login page. Additionally, after an authorized administrator resets their password through the security management interface, general users must change their password upon their next login.

- Protection of the TSF

KSignAccess Server ensures the confidentiality and integrity of TSF data transmitted between physically separated KSignAccess Agents through encrypted communication. Integrity checks on TSF data and TSF

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

executable code, which are subject to integrity verification, are performed during startup, periodically during normal operation, and upon request by an authorized administrator.

The KSignAccess Agent loads TSF data during startup to enable encrypted communication and mutual authentication with the KSignAccess Server. After successful mutual authentication, integrity checks on TSF data and components are performed during startup and periodically during normal operation.

The KSignAccess Server and KSignAccess Agent perform self-tests during startup and periodically during normal operation to ensure the system remains in a secure state and that security functions operate correctly, even in the event of a failure in the noise source integrity test. Additionally, to protect TSF data, general user and administrator authentication information, TOE integrity verification information, and KSignAccess Server and KSignAccess Agent information are securely stored and managed in files and the DBMS.

- TOE access


For the execution of KSignAccess Server's security management functions, the maximum number of simultaneous administrator management access sessions is limited to one. If the same administrator account logs in from another administrator PC after an authorized administrator has already logged in, the existing session will be terminated. For general user access sessions, the maximum number of simultaneous sessions is limited to one. Additionally, if the administrator session and general user session exceeds the configured inactivity timeout period (10 minutes), the session will be terminated.

All administrators are restricted based on allowed IP access rules, and audit data is generated for the results of session restrictions on the security management interface.

- Trusted path/channels

KSignAccess Server performs encrypted communication using secure cryptographic protocols through a secure path (HTTPS) when communicating with the mail server.

1.6 Conventions

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

This Protection Profile (PP) uses some abbreviations and mixes English for clarity of meaning. The notation, formatting, and conventions used are consistent with the Common Criteria for Information Technology Security Evaluation.

The Common Criteria allows operations such as iteration, assignment, selection, and refinement to be performed for functional requirements. Each operation is used in this PP.

Iteration

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

Assignment


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

Selection

Selection is used to choose one or more options provided by the Common Criteria when stating a requirement. The result of a selection is shown as underlined and italicized text.

Refinement

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

1.7 Terms and definitions

The terms used in this PP, which are the same as those in the CC, follow the definitions in the CC.

Agent Type1

Antivirus products, software-based security USB products, and Host Data Loss Prevention products, etc.

- The endpoint on which the agent is located is typically a PC with Windows® operating system accessible to employees within the organization, and if the agent is compromised, data present on the user's host can be compromised and leaked, requiring strict security requirements in terms of confidentiality, integrity, and availability.

Agent Type2

Network Access Control products, Patch Management Systems, etc.

- The endpoint on which the agent is located is typically a PC with Windows® operating system accessible to employees in the organization, and if the agent is compromised, it is unlikely that data present on the user's host will be corrupted or leaked, but it can cause problems in using the resources provided by the organization, requiring security requirements in terms of confidentiality, integrity.

Agent Type3

Database Access Control products, Access Control in Operating System(Server) products, Enterprise security management products, etc.


- Since the endpoint where the agent is located is generally a physically secure environment that can only be accessed by authorized employees of the organization, it corresponds to a product type with a relatively low threat occurrence

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,

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Client

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

Client Type

Vitual Private Network products, Wireless LAN Authentication Products, etc.

- The client is an entity installed on the user's host and serves to request communication with the server on behalf of the user.

Component

Smallest selectable set of elements on which requirements may be based

Critical Security Parameters (CSP)

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

Database Management System (DBMS)

A software system composed to configure and apply the database.

Decryption

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

Dependency


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

Element

Indivisible statement of a security need

Encryption

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Endpoint

The point where the TOE components such as agents, clients, etc. are installed and operated without any further sub-interacted entities

End-user

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

Evaluation Assurance Level (EAL)

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

External Entity

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

Family

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

Identity

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

Iteration

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

Korea Cryptographic Module Validation Program (KCMVP)


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

Local access

Connection established through the console port between the administrator and the TOE

Management access

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Management Console

Application program that provides GUI, CLI, etc. to the administrator and provides system management and configuration

Manual recovery

Recovery through an update server, etc. by user execution or user intervention

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 a unique entity(the subject using the public key), it can be disclosed

Public Key(asymmetric) cryptographic algorithm

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

Public Security Parameters (PSP)

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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

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.

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

Sensitive Security Parameters (SSP)

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

Session Key

Key generated from a validated cryptographic module, used for encryption communication for secure encryption communication between the KSignAccess Server and the KSignAccess Agent

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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

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

TSF Data


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

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.

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

2. Conformance claim


2.1 CC conformance claim

2.1.1 CC, PP, and security requirement packages

Common Criteria (CC)		Information Technology Security Evaluation Criteria CC:2022 Revision 1 <ul style="list-style-type: none"> - Part 1: Introduction and General Model, CC:2022 r1 (CCMB-2022-11-001, November 2022) - Part 2: Security Functional Components, CC:2022 r1 (CCMB-2022-11-002, November 2022) - Part 3: Security Assurance Components, CC:2022 r1 (CCMB-2022-11-003, November 2022) - Part 4: Framework for the Specification of Evaluation Methods and Activities, CC:2022 r1 (CCMB-2022-11-004, November 2022) - Part 5: Predefined Packages of Security Requirements, CC:2022 r1 (CCMB-2022-11-005, November 2022) Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, 2024.07
Protection Profile (PP)		Korean National Protection Profile for Single Sign On V3.0
Conformance Claim	Part 2 Security functional components	Extended : FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1
	Part 3 Security assurance components	Conformant
	Package	Augmented: EAL1 Augmented (ATE_FUN.1)

[Table 2-1] Conformance claim

2.1.2 Type of conformance

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

This Security Target follows "Strict Protection Profile Conformance."

2.1.3 PP composite conformance claim

The Protection Profile that this Security Target complies with is 'Korean National Protection Profile for Single Sign On V3.0,' and no other composite Protection Profiles are included.

2.1.4 PP conformance claim

The Protection Profile that this Security Target complies with is 'Korean National Protection Profile for Single Sign On V3.0'

Additionally, this Security Target only declares PP compliance. As it is based on CC:2022, it declares compliance exclusively with the directly referenced PP.

2.1.5 Package conformance claim

The Security assurance components package that this Security Target complies with is EAL1, and defines some additional Security assurance components

- assurance package: EAL1 Augmented (ATE_FUN.1)


2.1.6 Conformance claim rationale

Since this Security Target adopts the TOE type, security objectives, and security requirements of the 'Korean National Protection Profile for Single Sign On V3.0,' its conformance claim is classified as "strict Protection Profile conformance."


2.2 Conformance claim rationale

2.2.1 Reference to evaluation methods/activities

The Security assurance components package that this Security Target complies with requires the use of the evaluation methods and evaluation activities defined in <6.2 Security Assurance Requirements>. Additional evaluation methods and activities also include those specified in extended assurance components and supplementary documents based on CC v3.1 Protection Profiles.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

- ※ The evaluation methods and activities defined in <6.2 Security Assurance Requirements> are written to include newly added or modified task units from CEM:2022.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

3. Security problem definition

This section defines the threats, organizational security policies, and assumptions that the TOE and its operational environment are intended to address.

3.1 Assets

The primary assets protected by the TOE are as follows.

- Data transmitted through the TOE (e.g., authentication tokens for user integrated authentication).
- The TOE itself and critical data within the TOE (e.g., TSF data).

3.2 Threats

A threat agent is an IT entity and user that causes harm to the assets intended for protection through unauthorized access or abnormal methods, and can pose various types of threats. In this case, the threat agent against the TOE has basic levels of expertise, resources, and motivation.

3.2.1 Unauthorized access

T.SESSION_HIJACK

The threat agent can gain access to an abandoned user screen or use an unclosed session after logout to hijack the user's privileges.

T.RETRY_AUTH_ATTEMPT

The threat agent can repeatedly attempt authentication, use the acquired information to successfully authenticate, and impersonate an authorized user to access the TOE.


T.IMPERSONATION

The threat agent can impersonate an authorized user or TOE component to access the TOE.

T.REPLAY

The threat agent can capture authentication information, copy it, and reuse it to access the TOE.

T.WEAK_PASSWORD

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

The threat agent can obtain a poorly managed password, such as using default passwords, and impersonate an authorized user to access the TOE. If weak password policies are applied, the threat agent can also impersonate an authorized user to access the TOE.

3.2.2 Information leakage

T.STORED_DATA_LEAKAGE

The threat agent can leak critical data (e.g., cryptographic keys, TOE settings) stored inside the TOE or in external entities interacting with the TOE (e.g., DBMS) in an unauthorized manner.

T.TRANSMISSION_DATA_DAMAGE

The threat agent can expose or modify transmission data between TOE components or between the TOE and external IT entities in an unauthorized manner.

T.WEAK_CRYPTO_PROTOCOLS

The threat agent can analyze traffic using vulnerable cryptographic protocols or low cryptographic strength to infer cryptographic key information or determine the content of encrypted communication.

3.2.3 TOE functionality compromise

T.TSF_COMPROMISE

The threat agent can compromise the TSF through unauthorized access, causing malfunction of TOE functions or disabling TOE functionality.


3.3 Organizational security policy (OSP)

OSP refers to the security rules, procedures, and guidelines applied within the operational environment. OSP can be determined by the organization controlling the TOE's operational environment or by policy-making and regulatory bodies. OSP can be applied to the TOE and/or its operational environment.

The following security policies are described for the TOE and its operational environment, or for both.

P.AUDIT

Security-related actions must be recorded and maintained to track responsibility for security incidents, and the recorded data must be reviewed. In addition, the available space for audit data storage must be regularly checked to prevent audit data loss, and unauthorized changes and deletions of stored

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

audit data must be prevented.

P.SECURE_OPERATION

Administrators must be provided with the means to securely configure the TOE and operate it accurately according to the TOE operation manual to ensure compliance with the organization's security policy.

P.CRYPTO_STRENGTH

The organization must apply encryption measures for the storage and transmission of critical data, such as passwords used for user authentication, and must use secure cryptographic algorithms.

3.4 Assumptions

The following assumptions are required for the operational environment to provide the security functionality of the TOE. If the operational environment where the TOE is installed does not meet these assumptions, the TOE may not be able to provide all of its security functionality. These assumptions include physical, human, and connectivity aspects of the operational environment.

A.PHYSICAL_CONTROL

The location where the TOE is installed and operated must have access control and protective facilities to ensure that only authorized administrators can access it.

A.TRUSTED_ADMIN


The authorized administrator of the TOE is assumed to be non-malicious, adequately trained in TOE management functions, and expected to perform their duties accurately in accordance with the administrator guidelines.

A.LOG_BACKUP

The authorized administrators of the TOE must be non-malicious, appropriately trained in TOE management functions, and must perform their duties accurately according to the administrator guidelines.

A.OPERATION_SYSTEM_REINFORCEMENT

The operating system on which the TOE is installed must undergo reinforcement against the latest vulnerabilities, ensuring the trustworthiness and security of the operating system.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

A.SECURE_DEVELOPMENT

Developers integrating cryptographic functions into the Application or DBMS using the TOE must adhere to the requirements in the documentation provided with the TOE to ensure that the TOE's security features are applied securely.

A.SECURE_DBMS

The DBMS interacting with the TOE, which stores audit data, must be protected from unauthorized deletion or modification.

A.TRUSTED_TIMESTAMP

The TOE must use a trusted timestamp provided by the TOE's operational environment to accurately record security-related events.

A.SECURED_ADMIN_ACCESS

The web server in the management server's operational environment and the web browser on the administrator's PC must communicate using a secure path.

A. MANUAL_RECOVERY

The TOE must support manual recovery procedures, such as user-involved reinstallation, to restore tampered information after the TOE agent experiences a failure or service disruption.


4. Security objectives

This section categorizes and defines security objectives into TOE security objectives and security objectives for the operational environment. TOE security objectives are directly addressed by the TOE, while security objectives for the operational environment are handled by technical and procedural methods supported by the environment to ensure the TOE accurately provides its security functionality.

4.1 Security objectives for the operational environment

OE.PHYSICAL_CONTROL

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

OE.TRUSTED_ADMIN

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

OE.LOG_BACKUP

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

OE.OPERATION_SYSTEM_REINFORCEMENT

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

OE.SECURE_DEVELOPMENT

The developer who uses the TOE to interoperate with the 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.SECURE_DBMS

The DBMS interacting with the TOE, which stores audit data, must be protected from unauthorized deletion or modification.

OE.TRUSTED_TIMESTAMP

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

OE.SECURED_ADMIN_ACCESS


The web server in the management server's operational environment and the web browser on the administrator's PC must communicate using a secure path.

OE. MANUAL_RECOVERY

The TOE must support manual recovery procedures, such as user-involved reinstallation, to restore tampered information after the TOE agent experiences a failure or service disruption.

4.2 Security objectives rationale

The theoretical basis for security objectives demonstrates that the specified security objectives are

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

appropriate, sufficient to address security problems, not excessive, and strictly necessary. The theoretical basis for security objectives is presented as follows.


Security Objectives Security Problem Definition	Security Objectives for the Operational Environment								
	OE:PHYSICAL_CONTROL	OE:TRUSTED_ADMIN	OE:LOG_BACKUP	ORCEMENT OE:OPERATION_SYSTEM_REINF	OE:SECURE_DEVELOPMENT	OE:SECURE_DBMS	OE:TRUSTED_TIMESTAMP	OE:SECURED_ADMIN_ACCESS	OE:MANUAL_RECOVERY
P.Audit			X						
P.SECURE_OPERATION		X							
A.PHYSICAL_CONTROL	X								
A.TRUSTED_ADMIN		X	X						
A.LOG_BACKUP			X						
A.OPERATION_SYSTEM_REINFORCEMENT				X					
A.SECURE_DEVELOPMENT					X				
A.SECURE_DBMS						X			
A.TRUSTED_TIMESTAMP							X		
A.SECURED_ADMIN_ACCESS								X	
A. MANUAL_RECOVERY									X

[Table 4.1] Security problem definition and corresponding security objectives for the operating environment.

4.2.1 Operational environment security objectives rationale

The following describes the mapping and rationale for the TOE security objectives in the operational environment.

OE.PHYSICAL_CONTROL

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

By ensuring that access to the locations where the SSO agent and SSO server are installed is restricted to authorized administrators and equipped with access control and protective facilities, OE.PHYSICAL_CONTROL is necessary to support the assumption A.PHYSICAL_CONTROL.

OE.TRUSTED_ADMIN

The authorized administrators of the TOE must be non-malicious, properly trained in TOE management functions, and must perform their duties accurately according to the administrator guidelines. Therefore, OE.TRUSTED_ADMIN is necessary to implement the organizational security policy P.SECURE_OPERATION and supports the assumption A.TRUSTED_ADMIN.

OE.LOG_BACKUP

The authorized administrators of the TOE must regularly check the capacity of the audit data storage to ensure the backup process, thus ensuring that OE.LOG_BACKUP supports the organizational security policy P.AUDIT and the assumptions A.TRUSTED_ADMIN and A.LOG_BACKUP.

OE.OPERATION_SYSTEM_REINFORCEMENT


For the management server, operating system hardening involves removing unnecessary services and means from the operating system and performing remediation work for system vulnerabilities to ensure the operating system is safe and reliable. Similarly, for agents, it ensures that the underlying operating systems are safe and reliable. Therefore, OE.OPERATION_SYSTEM_REINFORCEMENT is necessary to support the assumption A.OPERATION_SYSTEM_REINFORCEMENT.

OE.SECURE_DEVELOPMENT

Developers who integrate user identification and authentication features for general users and authorized administrators into the business system's operational environment using TOE must follow the requirements provided with the TOE documentation to ensure the secure application of TOE's security functions. Therefore, OE.SECURE_DEVELOPMENT is necessary to support the assumption A.SECURE_DEVELOPMENT.

OE.SECURE_DBMS

By using a secure and reliable DBMS, TOE ensures protection against unauthorized deletion or modification of data. Therefore, OE.SECURE_DBMS is necessary to support the assumption A.SECURE_DBMS.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

OE.TRUSTED_TIMESTAMP


TOE ensures the accurate recording of security-related events by using a trusted timestamp provided by the TOE operational environment. Therefore, OE.TRUSTED_TIMESTAMP is necessary to support the assumption A.TRUSTED_TIMESTAMP.

OE.SECURED_ADMIN_ACCESS

TOE ensures that communication between the administrator PC's web browser and the management server's operational environment web server uses secure paths to ensure the confidentiality and integrity of transmitted data. Therefore, OE.SECURED_ADMIN_ACCESS is necessary to support the assumption A.SECURED_ADMIN_ACCESS.

OE.MANUAL_RECOVERY

TOE ensures that manual recovery procedures, such as reinstallation by user intervention, are supported to recover altered information after agent failure/service interruption. Therefore, OE.MANUAL_RECOVERY is necessary to support the assumption A.MANUAL_RECOVERY.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

5. Extended component definition

5.1 Identification and authentication (FIA)

5.1.1 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) Minimal: Success and failure of mutual authentication

5.1.1.1 FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.

Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: different

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

parts of TOE] using the [assignment: authentication protocol] that meets the following [assignment: list of standards].

5.1.2 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) Minimal : Success and failure of the activity

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

5.1.2.1 FIA_SOS.3 Destruction of Secrets

Hierarchical to No other components.
Dependencies FIA_SOS.2 Generation of Secrets

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

5.2 Security management (FMT)

5.2.1 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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

included in the PP/ST:

- a) Minimal: All changes of the password

5.2.1.1 FMT_PWD.1 Management of ID and password

Hierarchical to No other components
Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles


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

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

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

5.3 Protection of the TSF

5.3.1 Protection of stored TSF data

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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.

5.3.1.1 FPT_PST.1 Basic protection of stored TSF data

Hierarchical to No other components.

Dependencies No dependencies.

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6. Security requirements


This section describes the security functional requirements and assurance requirements that the TOE must satisfy.

6.1 Security functional requirements


The security functional requirements defined in this security target have been selected from the relevant security functional components in Part 2 of the Common Criteria to meet the security objectives identified in Chapter 4. For those security objectives that cannot be satisfied using the components selected from Part 2 of the Common Criteria, the requirements included in the extended component definitions in Chapter 5 are used to express them.

The following table summarizes the security functional components.

Security Function Class	Security Function Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Selectable audit review
	FAU_STG.4	Action in case of Possible Audit Data Loss
	FAU_STG.5	Prevention of Audit Data Loss
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.5	Cryptographic Key Derivation
	FCS_CKM.6	Timing and event of Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
	FCS_RBG.1	Random Bit Generation (RBG)
	FCS_RBG.3	Random Bit Generation (Internal Seeding - Single


	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

		Source)
	FCS_RBG.4	Random Bit Generation (Internal Seeding - Multiple Sources)
	FCS_RBG.5	Random Bit Generation (Entropy Source Combination)
Identification and Authentication (FIA)	FIA_AFL.1(1)	Authentication Failure Handling (General User)
	FIA_AFL.1(2)	Authentication Failure Handling (Authorized Administrator)
	FIA_IMA.1(Extended)	TOE Internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User Identification Before Any Action
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TSF Protection (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF Self-Testing
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1	TOE session establishment
Trusted	FTP_ITC.1	Inter-TSF trusted channel

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Path/Channel (FTP)		
-----------------------	--	--

[Table 6-1] Security functional requirements

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Security audit (FAU)


6.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to No other components.
Dependencies FAU_SAA.1 Potential Violation Analysis

FAU_ARP.1 The TSF shall take [assignment: actions specified in [Table 6-2] Potential Security Violation Response Actions] upon detection of a potential security violation.

Security Violation	Action
Validated Cryptographic Module Self-Test Failure	Process termination
KSignAccess Server Integrity Check Failure during Startup	Process termination / Send email to authorized administrator
KSignAccess Agent Integrity Check Failure during Startup	Send email to authorized administrator
KSignAccess Server Self-Test Failure during Startup	Process termination / Send email to authorized administrator
KSignAccess Agent Self-Test Failure during Startup	Send email to authorized administrator
KSignAccess Server Periodic Integrity Check Failure	Process termination / Send email to authorized administrator
KSignAccess Agent Periodic Integrity Check Failure	Send email to authorized administrator
KSignAccess Server Periodic Self-Test Failure	Process termination / Send email to authorized administrator
KSignAccess Agent Periodic Self-Test Failure	Send email to authorized administrator
KSignAccess Server Integrity Check Failure on Administrator Request	Send email to authorized administrator

[Table 6-2] Potential security breach actions

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.1.2 FAU_GEN.1 Audit data generation

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


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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the *not specified* level of audit; and
- c) [assignment: other specifically defined auditable events]

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

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

Sub-category	Audit events	Additional audit information
Identification and Authentication	User login and logout	
	User registration, change and deletion	
	The reaching of the threshold for the unsuccessful user authentication attempts and the actions taken	
	All changes of the password	
Security Management	IP registration, deletion and change of administrative terminals	
	Execution of security management function that the TOE must implement, and any changes and deletions of security attribute values.	Changed security attribute data
	Default account(ID)/Password change	

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

	Management terminal access IP blocking	
	Agent registration status change	
Trusted session management	User's session locking or termination	
	Response actions when duplicate login attempts of the same account are detected	
	Denial of new sessions based on the limit on the number of concurrent sessions	
Cryptographic Key Generation	Cryptographic key generation failure	
Cryptographic operation	Cryptographic operation failure (including cryptographic operation type)	
Audit record	Start-up and shutdown of the TOE audit functions in the form of H/W appliance	
	Execution of self-test	Failed security functions
	Execution of integrity verification of the TOE itself	Failed components
	Response actions when audit record fails to be stored	Response actions upon failure
	Agent startup	
Self-Protection	Integrity check execution and results	


[Table 6-3] Audit target events

6.1.1.3 FAU_SAA.1 Potential violation analysis

Hierarchical to Dependencies No other components.
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:

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

- a) Known events indicating potential security violations, such as: [
- Verified cryptographic module self-test failure
 - Integrity check failure during KSignAccess Server startup
 - Integrity check failure during KSignAccess Agent startup
 - Self-test failure during KSignAccess Server startup
 - Self-test failure during KSignAccess Agent startup
 - Periodic integrity check failure of KSignAccess Server
 - Periodic integrity check failure of KSignAccess Agent
 - Periodic self-test failure of KSignAccess Server
 - Periodic self-test failure of KSignAccess Agent
 - Integrity check failure on administrator request of KSignAccess Server]
- b) [None]

6.1.1.4 FAU_SAR.1 Audit Review

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


FAU_SAR.1.1 The TSF shall provide [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.

6.1.1.5 FAU_SAR.3 Selectable Audit Review

Hierarchical to No other components.
Dependencies FAU_SAR.1 Audit Review

FAU_SAR.3.1 The TSF shall provide the capability to apply [by default in descending order of date and time, and optionally by code, requester, requestip, result, detail, and sessionid] of audit data based on [Session ID, Detail, Subject Identity (user or

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

administrator ID, user or administrator IP, TOE components), event timestamp, event type, and success/failure of the event].

6.1.1.6 FAU_STG.4 Action in case of Possible Audit Data Loss

Hierarchical to No other components
Dependencies FAU_STG.2 Protection of Audit Data Storage

FAU_STG.4.1 The TSF shall [sending a warning email to the authorized administrator, [none]] if the audit data storage exceeds [80% of the threshold relative to the total audit record storage capacity].

6.1.1.7 FAU_STG.5 Prevention of Audit Data Loss


Hierarchical to FAU_STG.4 Action in case of Possible Audit Data Loss
Dependencies FAU_STG.2 Protection of Audit Data Storage

FAU_STG.5.1 The TSF shall *ignore the audited events* [send a warning email to the authorized administrator] if the audit data storage is full.

6.1.2 Cryptographic support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to None
Dependencies [FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Key Derivation or FCS_COP.1 Cryptographic Operations]
[FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of Cryptographic Key Destruction


	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [cryptographic key generation algorithm of Table 6-4] and specified cryptographic key sizes [cryptographic key sizes of Table 6-4] that meet the following: [list of standards of Table 6-4].

Standards	Cryptographic Operation	Cryptographic key generation Algorithm	Key Sizes	TOE Module	Function
KS X ISO/IEC 18033-2	Asymmetric Key Encryption	RSAES	2048	KSignAccessServer	Public key, private key generation
KS X ISO/IEC 18031	Random Number Generation	HASH-DRBG-SHA256	128	KSignAccessServer KSignAccessAgent	DEK
KS X ISO/IEC 18031	Random Number Generation	HASH-DRBG-SHA256	128	KSignAccessAgent	Session Key, Authentication Token key generation
KS X ISO/IEC 18031	Random Number Generation	HASH-DRBG-SHA256	264	KSignAccessServer	Transmission Data Integrity Key

[Table 6-4] TSF data encryption algorithms and key lengths

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.2.2 FCS_CKM.2 Cryptographic Key Distribution

Hierarchical to No other components.
Dependencies [FDP_ITC.1 User data input without security attributes or FDP_ITC.2 User data input with security attributes or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [as specified in [Table 6-5] Cryptographic Key Distribution Methods] that meets the following: [standards listed in [Table 6-5] Cryptographic Key Distribution Standards].


Standard List	Distribution Target	Distribution Method
KS X ISO/IEC 18033-2	FCS_CKM.1 session key FCS_CKM.1 authentication token encryption key	Use RSAES public key encryption provided by the validated cryptographic module to securely encrypt and transmit the session key.

[Table 6-5] Cryptographic key distribution methods

6.1.2.3 FCS_CKM.5 Cryptographic Key Derivation

Hierarchical to No other components.
Dependency [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys [KEK, private key KEK] from [password entered during installation] in accordance with a specified key derivation

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


algorithm [as specified in [Table 6-6] Cryptographic Key Derivation Algorithms] and specified cryptographic key sizes [as specified in [Table 6-6] Cryptographic Key Derivation Key Sizes] that meet the following: [standards listed in [Table 6-6] Cryptographic Key Derivation Standards].

Standard List	Cryptographic Operation	Cryptographic Algorithm	Key Length	TOE Module	Function
TTAK.KO-12.0334-Part2	Password -based Key Derivation	PBKDF2(HMAC-SHA256)	128	KSignAccessServer KSignAccessAgent	KEK generation
TTAK.KO-12.0334-Part2	Password -based Key Derivation	PBKDF2(HMAC-SHA256)	128	KSignAccessServer	Private Key KEK generation

[Table 6-6] Key derivation algorithms

6.1.2.4 FCS_CKM.6 Timing and event of Cryptographic Key Destruction

Hierarchical to Dependencies	No other components. [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, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6.1	The TSF shall destroy [DEK, KEK, private key, private key KEK, session key, transmission data integrity key, authentication token encryption key] <u>when no longer needed.</u>

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [overwriting data 3 times with 0] that meets the following: [None].

6.1.2.5 FCS_COP.1 Cryptographic Operations

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.6 Timing and events for cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [as specified in [Table 6-7] Cryptographic Operations for User Data and TSF Data Descriptions] in accordance with a specified cryptographic algorithm [as specified in [Table 6-7] Cryptographic Operations for User Data and TSF Data Cryptographic Algorithms] and cryptographic key sizes [as specified in [Table 6-7] Cryptographic Operations for User Data and TSF Data Cryptographic Key Sizes] that meet the following: [as specified in [Table 6-7] Standards for Cryptographic Operations for User Data and TSF Data].

Standard List	Cryptographic Operation	Algorithm	Key Length	TOE Module	Description
TTAS.KO-12.0004/R1	Symmetric Key	SEED-CBC	128	KSignAccessServer KSignAccessAgent	Encryption and decryption of authentication tokens, encryption/decryption of DEK (Data Encryption Key) using KEK (Key Encryption Key), encryption/decryption of sensitive information stored in

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


					configuration files using DEK, encryption/decryption of transmitted data, and use during mutual authentication
TTAS.KO-12.0004/R1	Symmetric Key	SEED-CBC	128	KSignAccessServer	Encryption and decryption of the private key using KEK
ISO/IEC 10118-3	Hash Function	SHA256	N/A	KSignAccessServer KSignAccessAgent	Generation of integrity verification data for TSF data.
ISO/IEC 10118-3	Hash Function	SHA256	N/A	KSignAccessServer	Storage of authentication data for administrators and general users
TTAK.KO-12.0330-Part2	Hash Function	HMAC-SHA256	128	KSignAccessServer KSignAccessAgent	Generation of integrity verification data for mutual authentication, authentication tokens, and transmitted data
KS X ISO/IEC 14888-2	Asymmetric Key	RSA-PSS	2048	KSignAccessServer KSignAccessAgent	Generation and verification of digital signatures during mutual authentication

[Table 6-7] Cryptographic operations for user data and TSF data

6.1.2.6 FCS_RBG.1 Random Bit Generation (RBG)

Hierarchical to No other components.
Dependencies [FCS_RBG.2 Random bit generation (external seeding), or
FCS_RBG.3 Random bit generation (internal seeding – single source)]
FPT_FLS.1 Failure with preservation of secure state
FPT_TST.1 TSF self-testing

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [HASH-DRBG-SHA256] in accordance with [KS X ISO/IEC 18031] after initialization with a seed.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FCS_RBG.1

.2


The TSF shall use a TSF entropy source [as specified in [Table 6-8] Entropy Source Names by Operating System] for initialization and seeding.

FCS_RBG.1.3

The TSF shall update the RBG state by reseeding using a TSF noise source [as specified in [Table 6-8] Entropy Source Names by Operating System] in accordance with [TTAS.KO-12.0235/R2] under the following condition: [reseed count limit reached].

Operating System	Entropy Source Name
Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)	gettimeofday()
	getDiskFreeInfo()
	GetMeminfo()
	GetTimerList()
	GetNetworkInfo()
	GetInterrupts()
	GetUptime_LINUX()
	sysinfo()
Windows Server 2016 (64bit)	GetCurrentProcessId()
	GetCurrentThreadId()
	QueryPerformanceCounter()
	GetForegroundWindow()
	GetIcmpStatistics()
	GetIppStatistics()
	GetPerformanceInfo()
	GetTcpStatistics()
	CloseHandle()
	GetDiskFreeSpaceA()
	GlobalMemoryStatusEx()
	GetTickCount()
	GetSystemTime()

[Table 6-8] Entropy sources by operating system

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.2.7 FCS_RBG.3 Random Bit Generation (Internal Seeding - Single Source)


Hierarchical to No other components.

Dependencies FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.3.1 The TSF shall be able to seed the RBG using a *TSF software-based noise source* [as specified in [Table 6-9] Entropy Source Names for Internal Seeding] with a minimum of $[2^{112}]$ bits of min-entropy.

Operating System	Entropy Source Name
Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)	gettimeofday()
	getDiskFreeInfo()
	GetMeminfo()
	GetTimerList()
	GetNetworkInfo()
	getentropy()
	GetInterrupts()
	GetUptime_LINUX()
Windows Server 2016 (64bit)	sysinfo()
	GetCurrentProcessId()
	GetCurrentThreadId()
	QueryPerformanceCounter()
	GetForegroundWindow()
	GetIcmpStatistics()
	GetIppStatistics()
	CloseHandle()
	GetDiskFreeSpaceA()
	GlobalMemoryStatusEx()
	GetTickCount()
GetSystemTime()	

[Table 6-9] List of entropy sources for internal seeding

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.2.1 FCS_RBG.4 Random Bit Generation (Internal Seeding – Multiple Sources)

Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)
FCS_RBG.5 Random bit generation (combining noise sources)

FCS_RBG.4.1 The TSF shall be able to seed the RBG using 9 of TSF software-based noise sources for **Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)**, 11 of TSF software-based noise sources for **Windows Server 2016 (64bit)**.

6.1.2.2 FCS_RBG.5 Random Bit Generation (Entropy Source Combination)


Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)
[FCS_RBG.2 Random bit generation (external seeding), or
FCS_RBG.3 Random bit generation (internal seeding – single source), or
FCS_RBG.4 Random bit generation (internal seeding – multiple sources)]

FCS_RBG.5.1 The TSF shall [concatenate] output from TSF noise source(s) to create the entropy input into the derivation function as defined in [KS X ISO/IEC 18031], resulting in a minimum of [2¹¹²] bits of min-entropy.

6.1.3 Identification and authentication (FIA)

6.1.3.1 FIA_AFL.1(1) Authentication Failure Handling (General User)

Hierarchical to No other components.
Dependencies FIA_UAU.1 Timing of Authentication

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FIA_AFL.1.1 The TSF shall detect when [5] unsuccessful authentication attempts occur related to [general user TOE authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [lock the account for 5 minutes].

6.1.3.2 FIA_AFL.1(2) Authentication Failure Handling (Authorized Administrator)

Hierarchical to No other components.
Dependencies FIA_UAU.1 Timing of Authentication

FIA_AFL.1.1 The TSF shall detect when [5] unsuccessful authentication attempts occur related to [administrator TOE authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [lock the account for 5 minutes].


6.1.3.3 FIA_IMA.1 TOE Internal Mutual Authentication (Extension)

Hierarchical to No other components.
Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [KSignAccess Server and KSignAccess Agent] in accordance with a specified [custom protocol] that meets the following: [None].

6.1.3.4 FIA_SOS.1 Verification of Secrets

Hierarchical to No other components.
Dependencies No dependencies.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the defined acceptable criteria below].

- Password length: minimum 9 characters, maximum 16 characters
- Allowed password characters: Uppercase and lowercase letters: a ~ Z (52)
Numbers: 0 ~ 9 (10) Special characters: .-/+=_~!@#%&^*()~{}|<>;& (27)
- Password rule validation: Must combine at least 4 of the following: uppercase, lowercase, numbers, special characters. The length must be between 9 and 16 characters.
- Password Restrictions: Prohibition of setting a password identical to the user account (ID), prohibition of continuous repetition of the same characters and numbers, prohibition of sequential input of characters or numbers on the keyboard, and prohibition of reusing the previously used password.

6.1.3.5 FIA_SOS.2 Generation of secrets

Hierarchical to No other components.
Dependencies No dependencies.


FIA_SOS.2.1 The TSF shall provide a mechanism to generate an **authentication token** that meets [timestamp, general user IP, authentication method, UID, extInfo (name, email), state (nonce), HMAC].

FIA_SOS.2.2 TSF shall be able to enforce the use of TSF-generated **authentication token** for [assignment: list of TSF functions].

6.1.3.6 FIA_SOS.3 Destruction of secrets (Extended)

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

FIA_SOS.3.1 The TSF shall destroy **authentication tokens** in accordance with a specified

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

authentication token destruction method [overwriting with '0' three times] that meets the following: [None].

6.1.3.7 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.

6.1.3.8 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 [general user's Nonce (nonce), authorized administrator's CSRF token].


6.1.3.9 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 [masking of password input (●)] to the **authorized general user** while the authentication is in progress.

6.1.3.10 FIA_UID.2 User Identification Before Any Action

Hierarchical to FIA_UID.1 Timing of Identification
Dependencies No dependencies.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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

6.1.4 Security management (FMT)


6.1.4.1 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 [as specified in [Table 6-10] Security Management Function List] to [authorized administrators].

Sub-category	Security Management
Identification and Authentication	User registration, deletion, modification, and authorization
Security Management	IP registration, deletion, and modification for management terminals
	Agent status, version, and applied security policy query
	Agent security policy management - policy setting, policy transmission
	TOE version information query
Self Protection	Performing an integrity verification of the TOE setting values and the TOE itself by the administrator's request
Audit Logs	Inquiry of audit records

[Table 6-10] Security management function list

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.4.2 FMT_MTD.1 Management of TSF data

Hierarchical to No other components.
Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to **manage** [other operations as specified in [Table 6-11] TSF Data List]] to [authorized administrators].


Security Function Component	TSF Data Management Actions
FIA_UAU.2 FIA_UID.2	Authorization of user account (ID)
FIA_UAU.2 FIA_UID.2	Add, delete, or modify user IDs
FMT_MTD.1 FMT_PWD.1	Add, delete, or modify user passwords
FTA_TSE.1	Register, delete, or modify management terminal IP addresses
FMT_MTD.1	Manage agent security policies
FMT_MTD.1	Query identification information for TOE and TOE components (e.g., server, agent, client, etc.)
FAU_SAR.1	Query audit records

[Table 6-11] TSF data list

6.1.4.3 FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to No other components.
Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [password changes in the security management interface] to [the authorized administrator] as follows:

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

1. [Password consisting of 9 to 16 characters, including at least 4 types: uppercase letters, lowercase letters, numbers, and special characters].
2. [Management of allowable special characters (.-/+=_~!@#\$\$%^*()~{}|<>;&), prohibition of setting a password identical to the user account (ID), prevention of repetitive input of the same character + number sequence, prohibition of sequential input of consecutive characters or numbers on the keyboard, and prohibition of reusing the previously used password].

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [account registration in the security management interface] to **[the authorized super administrator]** as follows:

1. [ID consisting of 4 to 20 characters, allowing uppercase letters, lowercase letters, numbers, and "_"].
2. [Prohibition of special characters other than "_"].

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

6.1.4.4 FMT_SMF.1 Specification of management functions


Hierarchical to No other components.
Dependencies No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [items specified in FMT_MOF.1 Security Function Management, items specified in FMT_MTD.1 TSF Data Management, items specified in FMT_PWD.1 ID and Password Management].

6.1.4.5 FMT_SMR.1 Security Role

Hierarchical to No other components.
Dependencies FIA_UID.1 Timing of Identification

FMT_SMR.1.1 The TSF shall maintain the roles [the following authorized administrators]:
- Super Administrator

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

- Audit Administrator

FMT_SMR.1.2 TSF must be able to associate users with the roles **defined in FMT_SMR.1.1.**

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to No other components

Dependencies No dependencies.

FPT_FLS.1 The TSF shall preserve a secure state when the following types of failures occur: [failure of noise source integrity test].

6.1.5.2 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to No other components

Dependencies No dependencies.


FPT_ITT.1 The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

6.1.5.3 FPT_PST.1 Basic Protection of Stored TSF Data (Extended)

Hierarchical to No other components

Dependencies No dependencies.

FPT_PST.1 The TSF shall protect [TSF data] stored in containers controlled by the TSF from unauthorized disclosure and modification.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.5.4 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 *at the initial start-up, periodically during normal operation*, and as specified in [Table 6-12] Self-Test Execution List] to demonstrate the correct operation of [the TSF].
- FPT_TST.1.2 The TSF shall provide authorized **administrators** with the capability to verify the integrity of *TSF data*.
- FPT_TST.1.3 The TSF shall provide authorized **administrators** with the capability to verify the integrity of *the TSF*.

TOE	Item
Server	Validated Cryptographic Module Self-Test
	License Check
	Process Check
	Integrity Check
	Authentication Token Issuance Test
Agent	Validated Cryptographic Module Self-Test
	License Check
	Process Check
	Integrity Check
	Authentication Token Verification Test

[Table 6-12] Self-test execution list

6.1.6 TOE access (FTA)

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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

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

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions belonging to the same user according to the rules [limiting the maximum number of concurrent sessions to 1 for administrator management access sessions and limiting the maximum number of concurrent sessions to 1 for general user access sessions].

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

6.1.6.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to No other components.
Dependencies FMT_SMR.1 Security Roles


FTA_SSL.3.1 The TSF shall terminate an interactive session after a [10-minute] interval of user inactivity.

6.1.6.3 FTA_TSE.1 TOE session establishment

Hierarchical to No other components.
Dependencies No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **session establishment** based on [connection IP, expiration (logout) of existing sessions for the same account during management access].

6.1.7 Trusted path/channels (FTP)

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.1.7.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to No other components.
Dependencies No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels, provides assured identification of its endpoints, and protects the channel data from modification or disclosure.


FTP_ITC.1.2 The TSF shall permit TSF to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [sending notification emails when a security alert occurs].

6.2 Security assurance requirements

The assurance requirements of this security target are composed of assurance components from Part 3 of the Common Criteria, and the Evaluation Assurance Level (EAL) is EAL1+. The following table summarizes the assurance components.

Assurance Class	Assurance Components	
Security Target Evaluation	ASE_INT.1	ST Introduction
	ASE_CCL.1	Compliance Declaration
	ASE_SPD.1	Definition of Security problems
	ASE_OBJ.1	Security Objectives for the Operational Environment
	ASE_ECD.1	Extended Component Definitions
	ASE_REQ.1	Direct rationale security requirements
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Documentation	AGD_OPE.1	User Operation Documentation
	AGD_PRE.1	Preparation Procedures
Lifecycle Support	ALC_CMC.1	TOE Labeling

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

	ALC_CMS.1	TOE CM Scope
Testing	ATE_FUN.1	Functional Testing
	ATE_IND.1	Independent Testing: Functional Verification
Vulnerability Assessment	AVA_VAN.1	Vulnerability Investigation

[Table 6-13] Assurance requirements

6.2.1 Security target evaluation

6.2.1.1 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 summarize the usage and major security features of the TOE.

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

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

ASE_INT.1.7C For a multi-assurance ST, the TOE overview shall describe the TSF organization in terms of the sub-TSFs defined in the PP-Configuration the ST claims conformance to.

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

ASE_INT.1.9C 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.

6.2.1.2 ASE_CCL.1 Conformance claims


- Dependencies
- ASE_INT.1 ST introduction
 - ASE_ECD.1 Extended components definition
 - ASE_REQ.1 Direct rationale 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 identify the edition of the CC to which the ST and the TOE claim conformance.
- ASE_CCL.1.2C The 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 conformance claim shall describe the conformance of the ST as either "CC Part 3 conformant" or "CC Part 3 extended".
- ASE_CCL.1.4C The conformance claim shall be consistent with the extended components definition.
- ASE_CCL.1.5C The conformance claim shall identify a PP-Configuration, or 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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim shall describe any conformance of the ST to a PP as PP-Conformant.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP-Configuration or PPs for which conformance is being claimed.

ASE_CCL.1.9C 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 PP-Configuration1, PPs and any functional packages for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PP-Configuration2, PPs, and any functional package 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.

6.2.1.3 ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements


ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements

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

6.2.1.4 ASE_OBJ.1 Security objectives for the operational environment

Dependencies ASE_SPD.1 Security problem definition

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives for the operational environment.

ASE_OBJ.1.2D The developer shall provide a security objectives rationale for the operational environment.

Content and presentation elements


ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

ASE_OBJ.1.2C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.1.3C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.2.1.5 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 may 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 may be clearly expressed using existing components.

6.2.1.6 ASE_REQ.1 Direct rationale security requirements

Dependencies ASE_ECD.1 Extended components definition
ASE_SPD.1 Security problem definition
ASE_OBJ.1 Security objectives for the operational environment


	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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 For a single-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE. The sets of SARs shall be consistent with the PPs or PP-Configuration to which the ST claims conformance.
- ASE_REQ.1.3C For a multi-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE and the sets of SARs that apply to each sub-TSF. The sets of SARs shall be consistent with the multi-assurance PP-Configuration to which the ST claims conformance.
- ASE_REQ.1.4C 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.1.5C The statement of security requirements shall identify all operations on the security requirements.
- ASE_REQ.1.6C All operations shall be performed correctly.
- ASE_REQ.1.7C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
- ASE_REQ.1.8C The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.
- ASE_REQ.1.9C The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs.
- ASE_REQ.1.10C The security requirements rationale shall explain why the SARs were chosen.
- ASE_REQ.1.11C The statement of security requirements shall be internally consistent.
- ASE_REQ.1.12C If the ST defines sets of SARs that expand the sets of SARs of the PPs or PP-Configuration it claims conformance to, the security requirements rationale

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

shall include an assurance rationale that justifies the consistency of the extension and provides a rationale for the disposition of any Evaluation methods and Evaluation activities identified in the conformance statement that are affected by the extension of the sets of SARs

Evaluator action elements

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

6.2.1.7 ASE_TSS.1 TOE summary specification

Dependencies ASE_INT.1 ST introduction
ASE_REQ.1 Direct rationale 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.

6.2.2 Development

6.2.2.1 ADV_FSP.1 Basic functional specification

Dependencies No dependencies.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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.

6.2.3 Guidance documents


6.2.3.1 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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that shall 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.


6.2.3.2 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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


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.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.2.4 Life-cycle support

6.2.4.1 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.

6.2.4.2 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 Requirements

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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.2.5 Tests

6.2.4.3 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 document must include a test plan, expected test results, and actual test results.

ATE_FUN.1.2C The test plan must identify the test items to be performed and describe the scenarios for each test. These scenarios must include order dependencies for other test results.

ATE_FUN.1.3C The expected test results must present the outcomes expected from successful execution of the test.

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

Evaluator action elements

ATE_FUN.1.1E The evaluator must verify that the provided information satisfies all evidence requirements.


6.2.4.4 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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

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.

6.2.6 Vulnerability assessment

6.2.6.1 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

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

performed by an attacker possessing Basic attack potential.

 KSIGN <i>e-Security Leader</i>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


6.3 Security requirements rationale

6.3.1 Security functional requirements rationale

The theoretical basis of the security functional requirements demonstrates the following:


- ▷ Each threat and the organization's security policy are addressed by at least one security functional requirement.
- ▷ Each security functional requirement is traced to at least one threat or the organization's security policy.

Threat and/or OSP SFR	Threat									OSP		
	T.S ESSI ON_ HIJA CK	T.R ETR Y_A UTH _AT TE MP T	T.I MP ERS ON ATI ON	T.R EPL AY	T. WE AK_ PAS SW ORD	T.S TOR ED_ DAT A_L EAK AGE	T.T RAN SMI SSI ON_ DAT A_D AM AGE	T. WE AK_ CRY PTO _PR OTO COL S	T.T SF_ CO MP RO MIS E	P.A UDI T	P.S ECU RE_ OPE RATI ON	P.C RYP TO_ STR ENG TH
FAU_ARP.1									X			
FAU_GEN.1										X		
FAU_SAA.1									X			
FAU_SAR.1										X		
FAU_SAR.3										X		
FAU_STG.4										X		
FAU_STG.5										X		
FCS_CKM.1						X	X	X				X
FCS_CKM.2						X	X	X				X
FCS_CKM.5						X	X	X				X
FCS_CKM.6						X	X	X				X
FCS_COP.1						X	X	X				X

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4				Dept.		Integrated Authentication Development		Author	Kim Dae- kyeom
					Edit Date		2025-02-26		Version	V1.4
					No.		KSignAccess V5.0 Security Target			

FCS_RBG.1						X	X	X				X
FCS_RBG.3						X	X	X				X
FCS_RBG.4						X	X	X				X
FCS_RBG.5						X	X	X				X
FIA_AFL.1(1)		X	X						X			
FIA_AFL.1(2)		X	X						X			
FIA_IMA.1(Extended)			X									
FIA_SOS.1					X							
FIA_SOS.2	X		X				X					
FIA_SOS.3(Extended)	X		X									
FIA_UAU.2			X						X			
FIA_UAU.4			X	X					X			
FIA_UAU.7			X		X				X			
FIA_UID.2			X						X			
FMT_MOF.1									X		X	
FMT_MTD.1									X		X	
FMT_PWD.1(Extended)					X				X		X	
FMT_SMF.1									X		X	
FMT_SMR.1									X		X	
FPT_FLS.1						X	X	X				X
FPT_ITT.1							X					
FPT_PST.1(Extended)						X						
FPT_TST.1						X	X	X	X			X
FTA_MCS.2	X											
FTA_SSL.3	X											
FTA_TSE.1	X											
FTP_ITC.1							X					

[Table 6-14] Mapping of security problem definitions to security functional requirements

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FAU_ARP.1 Security Alarm

FAU_ARP.1 ensures the ability to take responsive actions upon detecting security violations such as TOE integrity compromise, thus addressing T.TSF damage.

FAU_GEN.1 Audit Data Generation

FAU_GEN.1 ensures the generation of audit records for audit events such as the startup/shutdown of audit functions, and the success/failure of administrator identification and authentication, satisfying P.AUDIT.

FAU_SAA.1 Potential Violation Analysis

FAU_GEN.1 ensures the generation of audit records for audit events such as the startup/shutdown of audit functions, and the success/failure of administrator identification and authentication, thus satisfying P.AUDIT.

FAU_SAR.1 Audit Review

FAU_SAR.1 ensures the ability to allow authorized administrators to query audit records and provides the audit records in a format suitable for interpretation by administrators, thus satisfying P.AUDIT.

FAU_SAR.3 Selectable Audit Review

FAU_SAR.3 ensures the ability to conduct selective audit reviews of audit data based on logical relationship criteria, thus satisfying P.AUDIT.

FAU_STG.4 Audit Data Loss Prediction Response


FAU_STG.4 ensures that appropriate actions are taken when the audit evidence on the TOE server exceeds the storage capacity threshold, thus satisfying P.AUDIT.

FAU_STG.5 Prevention of Audit Data Loss

FAU_STG.5 ensures the ability to take appropriate actions when the audit evidence on the TOE server becomes saturated, thus satisfying P.AUDIT.

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1 ensures that keys are generated and distributed according to secure encryption algorithms

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

and key lengths for data storage encryption, thus addressing T.Stored Data Leakage.

FCS_CKM.1 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for communication encryption, thus addressing T.Transmission Data Tampering.

FCS_CKM.1 ensures that keys are generated and distributed according to standard encryption algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

FCS_CKM.1 ensures that keys are securely generated and distributed according to standard encryption algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.

FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for data storage encryption, thus addressing T.Stored Data Leakage.

FCS_CKM.2 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for communication encryption, thus addressing T.Transmission Data Tampering.

FCS_CKM.2 ensures that keys are generated and distributed according to standard encryption algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

FCS_CKM.2 ensures that keys are securely generated and distributed according to standard encryption algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.


FCS_CKM.5 Cryptographic Key Derivation

FCS_CKM.5 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for data storage encryption, thus addressing T.Stored Data Leakage.

FCS_CKM.5 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for communication encryption, thus addressing T.Transmission Data Tampering.

FCS_CKM.5 ensures that keys are generated and distributed according to standard encryption algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

FCS_CKM.5 ensures that keys are securely generated and distributed according to standard encryption algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FCS_CKM.6 Timing and event of Cryptographic Key Destruction

FCS_CKM.6 ensures that keys and related information are destroyed according to specified methods when data storage encryption ends, addressing T.Stored Data Leakage.

FCS_CKM.6 ensures that keys and related information are destroyed according to specified methods when communication encryption ends, addressing T.Transmission Data Tampering.

FCS_CKM.6 ensures that keys and related information are destroyed according to specified methods, addressing T.Weak Cryptographic Protocols.

FCS_CKM.6 ensures that keys required for data encryption using standard cryptographic algorithms with a security strength of 112 bits or more are securely generated and distributed, thus satisfying P.Crypto Strength.

FCS_COP.1 Cryptographic Operations

FCS_COP.1 ensures that cryptographic operations are performed according to specified secure algorithms and key lengths for data storage encryption, addressing T.Stored Data Leakage.

FCS_COP.1 ensures that cryptographic operations are performed according to specified secure algorithms and key lengths for communication encryption, addressing T.Transmission Data Tampering.

FCS_COP.1 ensures that cryptographic operations are performed using standard cryptographic algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

FCS_COP.1 ensures that cryptographic operations are performed according to standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.


FCS_COP.1 ensures that cryptographic operations are performed using standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, satisfying P.Crypto Strength.

FCS_RBG.1 Random Bit Generation (RBG)


FCS_RBG.1 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for data storage encryption, addressing T.Stored Data Leakage.

FCS_RBG.1 ensures that keys are generated and distributed according to secure encryption algorithms and key lengths for communication encryption, addressing T.Transmission Data Tampering.

FCS_RBG.1 ensures that keys are generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FCS_RBG.1 ensures that keys are securely generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FCS_RBG.3 Random Bit Generation (Internal Seeding - Single Source)

FCS_RBG.3 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for data storage encryption, addressing T.Stored Data Leakage.

FCS_RBG.3 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for communication encryption, addressing T.Transmission Data Tampering.

FCS_RBG.3 ensures that cryptographic keys are generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

FCS_RBG.3 ensures that cryptographic keys are securely generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.

FCS_RBG.4 Random Bit Generation (Internal Seeding - Multiple Sources)

FCS_RBG.4 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for data storage encryption, addressing T.Stored Data Leakage.

FCS_RBG.4 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for communication encryption, addressing T.Transmission Data Tampering.

FCS_RBG.4 ensures that cryptographic keys are generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.


FCS_RBG.4 ensures that cryptographic keys are securely generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.

FCS_RBG.5 Random Bit Generation (Entropy Source Combination)

FCS_RBG.5 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for data storage encryption, addressing T.Stored Data Leakage.

FCS_RBG.5 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for communication encryption, addressing T.Transmission Data Tampering.

FCS_RBG.5 ensures that cryptographic keys are generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for transmission data encryption,

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

addressing T.Weak Cryptographic Protocols.

FCS_RBG.5 ensures that cryptographic keys are securely generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, thus satisfying P.Crypto Strength.

FIA_AFL.1(1) Authentication Failure Handling (General User)

FIA_AFL.1(1) defines the number of failed authentication attempts for general users and ensures that actions are taken once the defined number is reached, addressing T.Repeated Authentication Attempts and T.Impersonation.

FIA_AFL.1(1) ensures that access to the TOE is only possible after the user's identification and authentication is successful, blocking bypass attempts by the threat source, thus addressing T.TSF Compromise.

FIA_AFL.1(2) Authentication Failure Handling (Authorized Administrator)

FIA_AFL.1(2) defines the number of failed authentication attempts for authorized administrators and ensures that actions are taken once the defined number is reached, addressing T.Repeated Authentication Attempts and T.Impersonation.

FIA_AFL.1(2) ensures that access to the TOE is only possible after the user's identification and authentication is successful, blocking bypass attempts by the threat source, thus addressing T.TSF Compromise.

FIA_IMA.1 (Extended) TOE Internal mutual authentication

FIA_IMA.1 ensures mutual authentication between TOE components, addressing T.Impersonation.


FIA_SOS.1 Verification of Secrets

FIA_SOS.1 ensures compliance with password complexity rules, addressing T.Weak Passwords.

FIA_SOS.2 Generation of Secrets

FIA_SOS.2 ensures that authentication tokens are created with guaranteed uniqueness based on the criteria of "encrypted timestamp, general user IP, authentication method, UID, extInfo (name, email), state (nonce), HMAC" and forces the use of the created authentication tokens for integrated authentication, addressing T.Session Hijacking and T.Impersonation.

FIA_SOS.2 ensures that critical information included in the authentication token is protected with confidentiality and integrity, addressing T.Transmission Data Tampering.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FIA_SOS.3 Destruction of Secrets (Extended)

FIA_SOS.3 ensures that authentication tokens are destroyed by invalidating the session storing them and zeroing out variables when the user session ends, addressing T.Session Hijacking and T.Impersonation.

FIA_UAU.2 User Authentication Before Any Actions

FIA_UAU.2 ensures that administrators and general users are successfully authenticated before accessing the TOE, addressing T.Impersonation.

FIA_UAU.2 ensures that access to the TOE is only possible after the user's identification and authentication is successful, blocking bypass attempts by the threat source, thus addressing T.TSF Compromise.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4 ensures that administrators and general users are successfully authenticated before accessing the TOE, addressing T.Impersonation.

FIA_UAU.4 ensures the prevention of reuse of authentication data, addressing T.Reuse.

FIA_UAU.4 ensures that access to the TOE is only possible after the user's identification and authentication is successful, blocking bypass attempts by the threat source, thus addressing T.TSF Compromise.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7 ensures that only masked values are displayed or not displayed during authentication and that no feedback is provided on authentication failure, addressing T.Impersonation.


FIA_UAU.7 ensures that only masked values are displayed or not displayed during authentication, addressing T.Weak Passwords.

FIA_UAU.7 ensures that access to the TOE is only possible after the user's identification and authentication is successful, blocking bypass attempts by the threat source, thus addressing T.TSF Compromise.

FIA_UID.2 User Identification Before Any Actions

FIA_UAU.7 ensures that only masked values are displayed or not displayed during authentication and that no feedback is provided on authentication failure, addressing T.Impersonation.

FIA_UID.2 ensures that access to the TOE is only possible after the user's identification and authentication is successful, blocking bypass attempts by the threat source, thus addressing T.TSF Compromise.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1 differentiates access and settings for management functions by roles (administrator and general user), ensuring security policies and functions are provided by role to block unauthorized access by threat sources, addressing T.TSF Compromise.

FMT_MOF.1 ensures the management capability of security functions is provided only to authorized users, thus satisfying P.SECURE_OPERATIONS.

FMT_MTD.1 Management of TSF data

FMT_MTD.1 differentiates access and settings for management functions by roles (administrator and general user), ensuring security policies and functions are provided by role to block unauthorized access by threat sources, addressing T.TSF Compromise.

FMT_MTD.1 ensures the management capability of security functions is provided only to authorized users, thus satisfying P.SECURE_OPERATIONS.

FMT_PWD.1 (Extended) Management of ID and password

FMT_PWD.1 ensures the ability to enforce a mandatory password change upon the first login for the authorized administrator for the default password, addressing T.Weak Passwords.

FMT_PWD.1 differentiates access and settings for management functions by roles (administrator and general user), ensuring security policies and functions are provided by role to block unauthorized access by threat sources, addressing T.TSF Compromise.

FMT_PWD.1 ensures the ability to manage ID and password combination rules and lengths only for authorized administrators and provides the ability to change passwords for first-time logins, thus satisfying P.SECURE_OPERATIONS.


FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 differentiates access and settings for management functions by roles (administrator and general user), ensuring security policies and functions are provided by role to block unauthorized access by threat sources, addressing T.TSF Compromise.

FMT_SMF.1 ensures the specification of security functions, security attributes, and TSF data, satisfying P.SECURE_OPERATIONS.

FMT_SMR.1 Security Roles

FMT_SMR.1 differentiates access and settings for management functions by roles (administrator and general user), ensuring security policies and functions are provided by role to block unauthorized access

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

by threat sources, addressing T.TSF Compromise.

FMT_SMR.1 ensures the specification of authorized roles for security management, satisfying P.SECURE_OPERATIONS.

FPT_FLS.1 Safe State on Failure

FPT_FLS.1 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for data storage encryption, addressing T.Stored Data Leakage.

FPT_FLS.1 ensures that cryptographic keys are generated and distributed according to secure algorithms and key lengths for communication encryption, addressing T.Transmission Data Tampering.

FPT_FLS.1 ensures that cryptographic keys are generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for transmission data encryption, addressing T.Weak Cryptographic Protocols.

FPT_FLS.1 ensures that cryptographic keys are securely generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or more for data encryption, satisfying P.Crypto Strength.

6.3.2 Assurance requirements rationale


The evaluation assurance level (EAL) selected for this security target is EAL1+ (ATE_FUN.1).

EAL1 applies when a moderate level of trust in the correct operation is required, but the security threats are not severe. EAL1 can be applied when the development methodology commonly used by the developer is followed, and it does not require additional effort from the developer to prepare the evaluation deliverables. In other words, it does not require more costs or time investment for evaluation preparation.

EAL1 provides a basic level of assurance by analyzing the security functional requirements included in the security target through limited specifications of functions and interfaces, and using documentation to understand security behavior.

This analysis is supported by independent testing of the TSF, searches for potential vulnerabilities in the public domain (functional testing and penetration testing).


EAL1 does not require evidence of tests performed by the developer based on functional specifications, but this security target includes ATE_FUN.1, which allows the developer to test whether the TSF has been correctly implemented and document the results of such tests, including the detection of defects.

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


6.4 Dependencies rationale

6.4.1 Dependencies of security functional requirements

Number	Security Functional Requirement	Dependency	Reference Number
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.Timestamp
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
7	FAU_STG.4	FAU_STG.2	OE. Secure DBMS
8	FAU_STG.5	FAU_STG.2	OE. Secure DBMS
9	FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1]	10, 13
		[FCS_RBG.1 or FCS_RNG.1]	14
		FCS_CKM.6	12
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	9
11	FCS_CKM.5	[FCS_CKM.2 or FCS_COP.1]	13
		FCS_CKM.6	12
12	FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	9, 11
13	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	9, 11
		FCS_CKM.6	12
14	FCS_RBG.1	[FCS_RBG.2 or FCS_RBG.3]	15
		FPT_FLS.1	33
		FPT_TST.1	36
15	FCS_RBG.3	FCS_RBG.1	14

 KSIGN e-Security Leader	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

16	FCS_RBG.4	FCS_RBG.1	14
		FCS_RBG.5	17
17	FCS_RBG.5	FCS_RBG.1	14
		[FCS_RBG.2 or FCS_RBG.3 or FCS_RBG.4]	15,16
18	FIA_AFL.1(1)	FIA_UAU.1	24
19	FIA_AFL.1(2)	FIA_UAU.1	24
20	FIA_IMA.1	-	-
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	31
		FMT_SMR.1	32
29	FMT_MTD.1	FMT_SMF.1	31
		FMT_SMR.1	32
30	FMT_PWD.1	FMT_SMF.1	31
		FMT_SMR.1	32
31	FMT_SMF.1	-	-
32	FMT_SMR.1	FIA_UID.1	27
33	FPT_FLS.1	-	-
34	FPT_ITT.1	-	-
35	FPT_PST.1	-	-
36	FPT_TST.1	-	-
37	FTA_MCS.2	FIA_UID.1	27
38	FTA_SSL.3	FMT_SMR.1	32
39	FTA_TSE.1	-	-

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

40	FTP_ITC.1	-	-
----	-----------	---	---


[Table 6 15] Theoretical basis for dependencies

FAU_GEN.1 depends on FPT_STM.1, which uses the trusted timestamp provided by the TOE's operating environment to record security-related tests, thus satisfying the security objective OE. Trusted Timestamp for the operating environment.

FAU_STG.4 and FAU_STG.5 depend on FAU_STG.2, which is satisfied by the OE. Secure DBMS of the operating environment.

FIA_AFL.1 and FIA_UAU.7 depend on FIA_UAU.1, which is satisfied by FIA_UAU.1 and its hierarchical relationship with FIA_UAU.2.

FIA_UAU.1, FMT_SMR.1, and FTA_MCS.2 depend on FIA_UID.1, which is satisfied by FIA_UID.1 and its hierarchical relationship with FIA_UID.2.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

6.4.2 Dependencies of assurance requirements

The dependencies of the EAL1 assurance package provided in the Common Criteria for Information Security Systems have already been satisfied, so the theoretical basis for this is omitted.

The added assurance requirement, ATE_FUN.1, includes ATE_COV.1 as a dependency. ATE_FUN.1 was added to ensure that the developer correctly performed tests on the test items and recorded them in the test report. However, since ATE_COV.1, which demonstrates the consistency between the test items and TSFI, is not strictly necessary, it has not been added to this security target.


7. TOE Summary specifications

7.1 Security audit

7.1.1 Security alerts

The TOE applies a set of rules to the audit logs to generate security alerts when potential security violations occur. Potential security violation events are as follows:

Security Violation	Action
Verification failed in cryptographic module self-test	Process termination
Integrity check failure at KSignAccess Server startup	Process termination / Email sent to authorized administrator
Integrity check failure at KSignAccess Agent startup	Email sent to authorized administrator
Self-test failure at KSignAccess Server startup	Process termination / Email sent to authorized administrator
Self-test failure at KSignAccess Agent startup	Email sent to authorized administrator
Periodic integrity check failure at KSignAccess Server	Process termination / Email sent to authorized administrator
Periodic integrity check failure at KSignAccess	Email sent to authorized administrator

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Agent	
Periodic self-test failure at KSignAccess Server	Process termination / Email sent to authorized administrator
Periodic self-test failure at KSignAccess Agent	Email sent to authorized administrator
Integrity check failure at KSignAccess Server upon administrator request	Email sent to authorized administrator

[Table 7.1] Potential security violation events


7.1.2 Audit data generation

Audit data is generated for security events of each TOE component. The generated audit data is stored in a repository provided by the operating environment. TOE uses a trusted timestamp provided by the environment in which the TOE operates to ensure that audit data is generated sequentially.

Audit target events are generated and stored by categorizing them into Session ID, Detail, the identity of the subject (user or administrator ID, user or administrator IP, TOE component), the event time, event type, and event success/failure.

The following audit target events are generated.

Subcategory	Audit Event	Additional Audit Information
Identification and Authentication	User login, logout	
	User registration, modification, deletion	
	Actions upon reaching the limit of user authentication attempts	
	Changes to passwords	
Security Management	Registration, deletion, modification of management terminal IPs	
	Performance of security management functions and all changes, deletions of security attribute values	Changed security attribute data
	Default account (ID) and password change	

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		


	Blocking of management terminal access IP	
	Agent registration status change	
Secure Session Management	User session lock or termination	
	Actions upon detecting repeated login attempts for the same account	
	Rejection of new sessions based on simultaneous session limit	
Cryptographic Key Generation	Failure of cryptographic key generation	
Cryptographic Usage	Failure of cryptographic operations (including cryptographic operation types)	
Audit Logs	Starting and ending of software-based TOE audit functions	
	Conducting self-tests	Failed security functions
	Verification of TOE's integrity	Failed components
	Saving audit logs	Actions on failure
	Starting agent	
Self-Protection	Performing integrity checks and results	

[Table 7-2] Audit events

7.1.3 Potential violation analysis

The TSF must be able to apply a set of rules when examining audited events, and based on these rules, it must be able to identify potential violations of the SFRs.

The TSF must apply rules, such as security violations from the [Table 7-1] Potential Security Violation Events, when examining the audited events.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.1.4 Audit data review

The TOE stores audit data in the audit evidence storage (DBMS) and provides authorized administrators with the ability to interpret all audit data from the audit records. The review can be based on Session ID, Detail, the identity of the subject (user or administrator ID, user or administrator IP, TOE component), the time of the event, event type, and success/failure conditions.

Authorized administrators (e.g., super administrators, audit administrators) can review and search the audit data via the KSignAccess Server's security management interface.

7.1.5 Audit data loss prevention


The audit records created by the TOE are stored in the storage provided by the TOE's operating environment (DBMS). Only authorized administrators have access to the audit record DB through the storage and can perform maintenance tasks.

The TOE periodically checks the storage of audit records and, when the remaining space exceeds the limit set by the authorized administrator, generates an audit record for the overflow event and sends an alert (warning email) to the authorized administrator. If the audit record storage reaches its capacity, the TOE will disregard the audit content for protection and send an alert (warning email) to the administrator.

- The threshold overflow ratio for the total capacity of the audit record storage is 80% by default. When the threshold is exceeded, an alert (warning email) is sent to the authorized administrator.
- The threshold saturation ratio for the total capacity of the audit record storage is 91% by default. Upon saturation of the threshold, audited events are ignored, and an alert (warning email) is sent to the authorized administrator.

7.1.6 SFR Mapping

The security audit function satisfies the TOE security functional requirements FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.4, FAU_STG.5.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.2 Cryptographic support

The TOE supports cryptography between TOE components by using the validated cryptographic module KSignCASE64 v2.5.2.0 in the policy transmission area. The detailed information of the validated cryptographic module included in the TOE is as follows.

Category	Details
Cryptographic Module Name	KSignCASE64 v2.5.2.0
Developer	Ksign Co., Ltd.
Verification Date	October 16, 2023
Verification Level	VSL1
Verification Number	CM-237-2028.10

[Table 7-3] Verified cryptographic module information

7.2.1 Cryptographic support


The encryption of TSF data shall be performed using symmetric key cryptographic operations, and the cryptographic keys shall be generated in compliance with ISO/IEC 18031(2011) and NIST SP 800-90 standards. The keys are derived using PBKDF2 from PKCS#5 with HMAC(SHA256) and the HASH_DRBG algorithm, producing cryptographic keys of 128 bit and 264 bit lengths.

To protect TSF data transmitted within the TOE, the communicating entities generate certificates (private and public keys) and complete mutual authentication through digital signatures.

The session key is generated by the KSignAccess Agent and is encrypted using the public key from the KSignAccess Server certificate with the RSAES standard. It is then distributed to the KSignAccess Server. The generated and distributed cryptographic keys are encrypted by the KSignAccess Server's certificate and securely stored.

During communication between TOE components, the cryptographic keys are loaded into memory by each module, decrypted using the private key, and used for encryption and decryption operations.

For symmetric-key cryptographic operations, an Initial Vector (128-bit) is generated using the HASH_DRBG algorithm, compliant with the NIST SP 800-90 standard.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

For asymmetric-key cryptographic operations, a 2048-bit cryptographic key is generated using the RSAES algorithm, compliant with the ISO/IEC 18033-2 (2006) standard.

For key distribution, a proprietary method is used for key distribution.


Cryptographic keys loaded into memory during key generation, distribution, and operations shall be destroyed immediately after use by overwriting the data three times with 0.

- Time when cryptographic key information is deleted:

Cryptographic Key Storage Location	Destruction Method	Destruction Target	Destruction Timing
Memory	"0x00" Overwrite 3 Times	Cryptographic keys (public key, private key, TSF DEK) in memory	When the product shutdown process is called
Memory	"0x00" Overwrite 3 Times	Session key	At the end of communication
Memory	"0x00" Overwrite 3 Times	Transmission data encryption key	Upon termination, the agent Server immediately after use
Memory	"0x00" Overwrite 3 Times	KEK, Private key KEK	Immediately after use
Memory	"0x00" Overwrite 3 Times	Authentication token encryption key	Upon user logout

The supported cryptographic algorithms use a validated cryptographic module, and the algorithm information for each purpose is as follows.

Category	Algorithm	Key length	Standard
Authentication token issuance /storage / verification	HASH-DRBG-SHA256	128 bit	KS X ISO/IEC 18031
	SEED (CBC)	128 bit	TTAS.KO-12.0004/R1

 KSIGN <i>e-Security Leader</i>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

		RSAES	2048 bit	KS X ISO/IEC 18033-2
		HMAC-SHA256	256 bit	TTAK.KO-12.0330-Part2
Mutual authentication	Transmission data encryption	SEED (CBC)	128 bit	TTAS.KO-12.0004/R1
	Key distribution	RSAES	2048 bit	KS X ISO/IEC 18033-2
	Integrity	HMAC-SHA256	N/A	TTAK.KO-12.0330-Part2
	Digital signature generation and verification	RSA-PSS	2048 bit	ISO/IEC 14888-2
Stored data encryption and decryption	Confidentiality	SEED (CBC)	128 bit	TTAS.KO-12.0004/R1
	Integrity	SHA256	N/A	ISO/IEC 10118-3
Transmitted data encryption and decryption	Confidentiality	SEED (CBC)	128 bit	TTAS.KO-12.0004/R1
	Integrity	HMAC-SHA256	N/A	TTAK.KO-12.0330-Part2


[Table 7-4] Algorithm information by purpose

7.2.2 Random bit generation

The TOE generates the random numbers necessary for cryptographic key generation through the validated cryptographic module KSignCASE64 v2.5.2.0, which uses the HASH DRBG algorithm. The TOE uses an entropy source that collects outputs from noise sources, forming a seed for DRBG input.

7.2.3 SFR Mapping

The cryptographic support functionality satisfies the TOE security functional requirements: FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.3 Identification and authentication

The TOE identifies all users (administrators and general users) attempting to access it. Before identification, administrators and IT entities attempting access cannot use any TOE functionality.

All users (administrators and general users) undergo identification and authentication simultaneously via an ID and password-based authentication process.

Authorized administrators access the TOE's security management interface through a web browser. Upon login, identification and authentication procedures are carried out, and only authorized administrators who successfully complete these procedures can use the security management functions provided by the TOE.

7.3.1 User authentication failure handling


The TOE provides a user account lock feature to protect against malicious user authentication attempts during user identification and authentication.

For administrators and users, in the event of authentication failure, the system ensures that the reason for the failure in the authentication mechanism is not disclosed by displaying "User cannot be found, or does not match user information." on the web browser. If the authentication failure count for the account reaches 5, the account will be locked for 5 minutes.

For general users, in case of authentication failure at KSignAccess Agent, the account will be locked after 5 failed attempts, and after 5 minutes, the 'auto-unlock after 5 minutes' feature will be provided.

7.3.2 Protection of authentication information

When a general user accesses the TOE, identification and authentication are based on an ID and password. During authentication, the entered password is displayed as '●' instead of the original characters to prevent leakage of authentication information. In case of authentication failure, only a failure message is shown without disclosing the reason for failure.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

For administrators accessing the TOE, a security management access control policy is enforced, allowing only administrators with IP addresses authorized by the top administrator to access the system. Identification and authentication follow the ID and password-based process, and the entered password is displayed as '●' to prevent information leakage. If authentication fails, only a failure message is shown without disclosing the failure reason.

7.3.3 Password policy verification

For both general users and authorized administrators, password creation and changes are verified against password policies, including allowed characters, combination rules, and minimum/maximum length validation, and these criteria are enforced.


For authorized administrators, the system forces a password change during the first identification and authentication via the security management interface. The password verification mechanism is the same for both creation and modification.

The TOE provides the following validation mechanism for password creation and changes.

- Password length: Minimum 9 characters, maximum 16 characters
- Allowed characters for passwords: Uppercase and lowercase letters: ~~az~~(52) ~~Digits: 09~~ (10) Special characters: `./+ =_!@# $%^*()~{}|<>;&` (27)
- Password validation: A combination of at least four of the above (uppercase/lowercase, digits, special characters), and the password must be 9 to 16 characters long.
- Prohibited password items: The password cannot be the same as the user account (ID), consecutive repetitions of the same character + number are not allowed, sequentially typed characters or numbers on the keyboard are prohibited, and the reuse of the last used password is forbidden.

7.3.4 Prevention of reuse of authentication information

To prevent the reuse of authentication information, the TOE provides the following.


	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

- Prevention of re-use of administrator authentication information: Authorized administrators can only access the security management interface through the login page. To prevent CSRF (Cross-Site Request Forgery) attacks, each page is assigned a CSRF token before administrator authentication. During authentication, the assigned CSRF token is transmitted along with the login credentials.
- Prevention of re-use of general user authentication information: To prevent CSRF attacks, each page is assigned a Nonce before user authentication. If the assigned Nonce is not included in the request, access is restricted. Users authenticate via the KSignAccess Agent using tokens issued by the server. These tokens, which include a timestamp and one-time authentication data such as Nonce and session ID, are not stored for reuse and are immediately discarded after use.

7.3.5 Mutual authentication between components

The TOE performs mutual authentication between the KSignAccess Server and KSignAccess Agent via a custom protocol, with the detailed mechanism as follows.

1. When registering the KSignAccess Agent in the security management interface, an Agent Identifier and Agent Secret value are generated for mutual authentication with the KSignAccess Server. The KSignAccess Agent generates an authentication message using HMAC SHA256 over HTTPS and transmits it to the KSignAccess Server to request mutual authentication.
 - request header -> AccessAgent_Authroization:base64(Agent Gid + Agent Identifier)
 - request Body -> { alg: HS256, signature: hmac(state, Agent Secret), state: state }
2. The KSignAccess Server verifies the received authentication message (HMAC) to authenticate the KSignAccess Agent's request.
 - request header verification (Agent Gid, Agent Identifier)
 - request body verification (signature verification)
3. The KSignAccess Server performs verification and generates a digital signature using the server's private key (RSAPSS), sending the response message to the KSignAccess Agent.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

- response body -> { alg: PS256, signature: RSAPSSwithSHA256(KSignAccess server_state + KSignAccess agent_state, server private key), state: KSignAccess server_state }
4. The KSignAccess Agent receives the server's response and verifies the digital signature (RSAPSS), completing mutual authentication with the KSignAccess Server.
- verify_signature((KSignAccess server_state + KSignAccess agent_state), KSignAccess Server Certificate)

7.3.6 Authentication token creation and disposal

The TOE generates authentication tokens using the validated cryptographic module KSignCASE64 v2.5.2.0 and enforces the use of the authentication token for general user logins.


Detailed information about the validated cryptographic module included in the TOE is as follows.

Category	Details
Cryptographic Module Name	KSignCASE64 v2.5.2.0
Developer	KSign Co., Ltd.
Validation Date	October 16, 2023
Validation Level	VSL1
Validation Number	CM-237-2028.10

[Table 7 5] Verified cryptographic module information

When requesting the generation of an authentication token from KSignAccess Agent, a nonce (state) is generated through the verified cryptographic module's random number generator and included in the request. The encryption operation is performed using SEED-CBC, and HMAC data is generated to verify the integrity of the authentication token.

The composition of the authentication token is as follows.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Timestamp	Client IP	AuthenMethod	Subject	Extend_information	state(nonce)	HMAC
-----------	-----------	--------------	---------	--------------------	--------------	------

After the authentication token has been used, it is destroyed by overwriting the data with '0x00' three times.

- When the cryptographic key-related information is deleted:
Upon calling the cryptographic key deletion function, Upon closing the trusted channel (logout), Upon completing the authentication token verification

7.3.7 SFR Mapping

The identification and authentication function satisfies the TOE security functional requirements FIA_AFL.1(1), FIA_AFL.1(2), FIA_IMA.1 (extended), FIA_SOS.1, FIA_SOS.2, FIA_SOS.3 (extended), FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, and FIA_UID.2.


7.4 Security Management

7.4.1 Security function management

The TOE's security management access control function is invoked only after the identification and authentication functions are successfully performed. Access to the security management interface is allowed only to authorized administrators through a secure channel (SSL). Authorized administrators are divided into "Super Administrator" and "Audit Administrator." In the case of an audit administrator, only verification of audit records is allowed. In the case of a super administrator, access to all security management interfaces is permitted.

Here is the translation of the text you provided.

Subcategory	Security Management
Identification and Authentication	User Registration, Deletion, Modification, Authorization

 KSIGN <small>e-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Security Management	Registration, Deletion, Modification of Management Device IP
	Agent Query - Status, Version, Applied Security Policy
	Agent Security Policy Management - Policy Configuration, Policy Transmission
	TOE Version Information Query
Self-Protection	Execution of TOE Security Function Self-Test at Administrator's Request
	Execution of TOE Configuration and TOE Integrity Check at Administrator's Request
Audit Records	Audit Record Query

"TOE provides the capability to manage the following TSF data."


Security Function Component	TSF Data Management Action
FIA_UAU.2 FIA_UID.2	Granting authority to user account (ID)
FIA_UAU.2 FIA_UID.2	Adding, deleting, or modifying user ID
FMT_MTD.1 FMT_PWD.1	Adding, deleting, or modifying user passwords
FTA_TSE.1	Registering, deleting, or modifying management terminal IP addresses
FMT_MTD.1	Managing agent security policies
FMT_MTD.1	Retrieving identification information of TOE and TOE components (e.g., server, agent, client, etc.)
FAU_SAR.1	Retrieving audit records

7.4.2 ID and password management

When the authorized administrator first accesses the security management interface, they are required to change the password. In the case of an audit administrator, the password must be changed after the password reset by the authorized administrator upon login.

The authorized administrator can change the password of either administrators or general users through the security management interface.

When generating or changing passwords for both general users and authorized administrators, the validity of the password value is verified according to the password policy.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

TOE provides the following verification mechanism for password creation:

- Password length: Minimum 9 characters, Maximum 16 characters
- Allowed password characters:

Uppercase and lowercase letters: a ~ Z (52)

Numbers: 0 ~ 9 (10)

Special characters: .-/+=_~:~!@#%\$%^*()~{}|<>;& (27)

- Password rule verification (validation):

Validates combinations of at least 4 types from uppercase, lowercase, numbers, and special characters, and the length should be between 9 to 16 characters.

- Prohibited password items: Cannot set the same password as the user account (ID), No continuous repetition of the same letter + number, No sequential entry of consecutive characters or numbers from the keyboard,, No reuse of the previous password.

7.4.3 SFR Mapping

Security management functionality satisfies the TOE security functional requirements FMT_MOF.1, FMT_MTD.1, FMT_PWD.1 (extended), FMT_SMF.1, and FMT_SMR.1.


7.5 TSF Protection

7.5.1 Maintaining safe state in case of failure

In the case of a failure in the entropy source, such as the noise source integrity test failure, the TOE transitions into a critical error state, preventing the operation of the validated cryptographic module and TOE, thus ensuring a safe state is maintained.

7.5.2 Internal transmission data protection between TSF components

The TOE provides a secure channel for protecting TSF data between TOE components by using the TLS V1.3 cryptographic communication protocol during transmission. TLS V1.3 ensures data integrity and confidentiality, protecting the data from eavesdropping and tampering that may occur during communication.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.5.3 Protection of stored TSF data

The TOE protects stored TSF data from unauthorized exposure and modification by encrypting and managing the data.

The list of TSF data subject to protection and the applied cryptographic algorithms are as follows:

TSF Data	Applied Algorithm and Data
Administrator Password	SHA256 + Salt
User Password	SHA256 + Salt
DEK	SEED-CBC(token)
private key	SEED-CBC(token)
private key KEK	SEED-CBC(token)
TOE settings	SEED-CBC(token)
Transmission data integrity key	SEED-CBC(token)
DBMS account information	SEED-CBC(token)
Integrity Value	SHA256(data)


[Table 7 6] Applied cryptographic algorithms.

7.5.4 Self-test

The TSF self-test provides the functionality to verify that the TSF operates correctly and that the integrity of the TSF data has not been compromised. The TOE provides this function so that authorized administrators can verify it through self-testing. To prove the correct operation of all TSF, the TOE performs a self-test periodically (every 12 hours) during normal operation, and upon initialization.

- The list of self-test items is as follows.

TOE	Items
Server	Self-Test of Verified Cryptographic Module

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

	License Check
	Process Check
	Integrity Check
	Authentication Token Issuance Test
Agent	Self-Test of Verified Cryptographic Module
	License Check
	Process Check
	Integrity Check
	Authentication Token Issuance Test


[Table 7 7] List of self-test performances

TOE performs a self-test at specified intervals, generating hash values for process checks and integrity checks. These hash values are compared with the initially stored hash values (baseline) when the system is first activated. If any integrity violations are detected, TOE notifies the authorized administrator and generates audit data through the security management interface. After the authorized administrator successfully completes identification and authentication, they can update the hash values of the integrity checks through the TOE security management interface. TOE performs integrity checks on all configuration files and executable files necessary for its operation, such as security policy files. TOE logs the results of self-tests, integrity checks, and actions taken by the authorized administrator.

7.5.5 Integrity check

The integrity check function determines whether TSF data and TSF executable files have been tampered with. The authorized administrator performs integrity checks on KSignAccess Server. The stored HMAC value is compared with the HMAC value generated during the integrity check to verify the validity of the data. Integrity verification uses the HMAC-SHA256 algorithm.

- The integrity check list performed by KSignAccess Server is as follows:

 KSIGN <small>ℓ-Security Leader</small>	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae-kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

Library Name	Description
/{KSignAccess Server Installation Path} /{Server binary Path } 예) /app/ksignaccessserver/serverhome	Configuration File Related Binary Path (All)
/{KSignAccess Server Installation Path} /{Security Management Interface binary Path} 예) /app/ksignaccessserver/adminhome	Security Management Interface Configuration File Related Binary Path (All)
/{WAS Installation Path}/webapps/ROOT /WEB-INF/lib/	Library of Deployed to WAS


- The integrity check list performed by the KSignAccess Agent is as follows.

Library Name	Description
/{KSignAccess Agent Installation Path } /{Agent binary Path} 예) /app/ksignaccessagent/agenthome	Entire Binary Path for Agent Configuration Files
/{WAS Installation Path}/webapps/ROOT /WEB-INF/lib/	Library of Deployed to WAS

Integrity Check Occurrence Conditions.

TOE Component	Integrity Check Occurrence Condition
KSignAccess Server	Perform integrity checks periodically (every 12 hours) during startup and regular operation.
KSignAccess Server	Perform integrity checks upon request by an authorized administrator.
KSignAccess Agent	Perform integrity checks periodically (every 12 hours) during startup and regular operation.

[Table 7-8] Integrity check occurrence conditions

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.5.6 SFR Mapping

The TSF protection features meet the TOE security functional requirements FPT_FLS.1, FPT_ITT.1, FPT_PST.1 (extended), and FPT_TST.1.

7.6 TOE Access


7.6.1 Administrator session limit

For the highest level administrators, TOE limits the maximum number of simultaneous sessions for the same administrator to one. If a session is active on one device and the same administrator attempts to log in from another device, the previous session will be terminated. Additionally, access is allowed only from IP addresses registered in the security management interface (by default, two or fewer IP addresses). Unauthorized IP addresses will be blocked.

For audit administrators, access is also restricted according to the access rules for allowed IP addresses, and audit data will be generated accordingly.

7.6.2 Security management interface session termination

Once the TOE is properly deployed and installed, authorized administrators access the TOE security management interface via a web browser on their administrator PC. TOE only allows access to the security management interface (HTTPS) if the administrator has successfully completed the identification and authentication process. After a successful login, TOE will terminate the session if the administrator remains inactive beyond the allowed time period, which is set by default to 10 minutes. This setting cannot be changed. If the session is terminated, all actions performed through that session are invalidated. If the administrator attempts to access the interface again, they must successfully re-authenticate to start a new session.

	KSignAccess V5.0 Security Target V1.4	Dept.	Integrated Authentication Development	Author	Kim Dae- kyeom
		Edit Date	2025-02-26	Version	V1.4
		No.	KSignAccess V5.0 Security Target		

7.6.3 SFR Mapping

The TOE access feature meets the TOE security functional requirements FTA_MCS.2, FTA_SSL.3, FTA_TSE.1

7.7 Trusted path/channels(FTP)

7.7.1 Trusted channel between TSFs

TOE provides a secure channel between TSFs using the TLS V1.2 cryptographic communication protocol. TLS V1.2 ensures the integrity and confidentiality of data, protecting it from eavesdropping and tampering during transmission. The TSF entities cooperate to establish a secure communication path when initiating communication.

In trusted IT products (SNMP servers), TLS V1.2 is also used to encrypt data, ensuring a secure network environment and preventing security threats during the transmission of management information.

7.7.2 SFR Mapping

The secure path/channel feature meets the TOE security functional requirement FTP_ITC.1.