KECS-CR-25-05

KSignAccess V5.0

Certification Report

Certification No.: KECS-CISS-1342-2025

2025. 3. 7.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025. 3. 7.	-	Certification report for KSignAccess V5.0 - First documentation

This document is the certification report for KSignAccess V5.0 of KSign Co., LTD.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the KSignAccess V5.0 developed by KSign Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

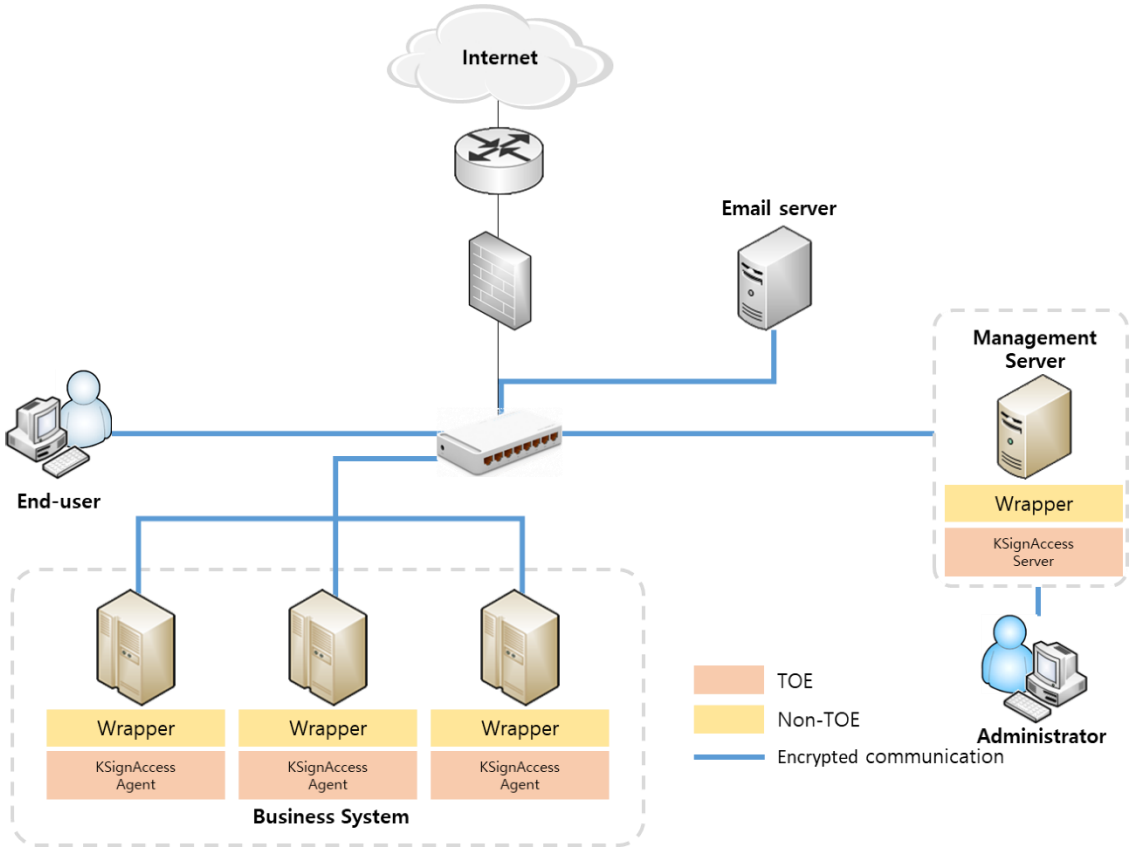
The Target of Evaluation (“TOE” hereinafter) is used to enable the user to access various business systems and use the service through a single user login without additional login action. Also, the TOE shall provide a variety of security features: security audit, cryptographic operation using cryptographic module, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, and trusted path and channels, etc.

The evaluation of the TOE has been carried out by Korea System Assurance (KoSyAs) and completed on February 26, 2025.

The ST claims conformance to the Korean National PP for Single Sign On V3.0[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the PP, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

The TOE consists of the KSignAccess Server and KSignAccess Agent.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational Environment of the TOE

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.

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.

The requirements for hardware, software and operating system to install the TOE are shown in [Table 1].

Component			Requirement
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 1 EA or higher
		OS	Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)
		DBMS	MySQL 8.0.41
		SW	Java Runtime Environment(JRE) 1.8.0_431 Apache Tomcat 9.0.98
KSign Access 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 1 EA or higher
		OS	Ubuntu 20.04 LTS kernel 5.15.0 (64 bit)
		SW	Java Runtime Environment(JRE) 1.8.0_431 Apache Tomcat 9.0.98
	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
		NIC	100/1000 Mbps x 1 EA or higher
		OS	Windows Server 2016 (64 bit)
		SW	Java Runtime Environment(JRE) 1.8.0_431 Apache Tomcat 9.0.98

[Table 1] TOE Hardware and Software specifications

Administrator uses the pc that can operate web browser to use the security management. Administrator pc minimum requirements are shown in [Table 2].

Component	Requirement

SW	Web Browser	Chrome 132.0

[Table 2] Administrator PC Requirements

Operating the TOE requires the following additional systems in the IT environment is shown in [Table 3].

Component	Requirement
Mail Server (SMTP Server)	Server for sending alert emails to administrators

[Table 3] External IT entity required for TOE operation

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

TOE	KSignAccess V5.0
Version	V5.0.3
TOE Components	KSignAccess Server V5.0.1 KSignAccess Agent for Linux V5.0.1 KSignAccess Agent for Windows V5.0.1
Manuals	KSignAccess V5.0 Preparative Procedure V1.4 KSignAccess V5.0 Operational User Guidance V1.3

[Table 4] TOE Identification

[Table 5] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)
TOE	KSignAccess V5.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ 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, July, 2024
EAL	EAL1+ (augmented by ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Single Sign On V3.0, KECS-PP-1230-2023, April. 27, 2023
Developer	KSign Co., LTD.
Sponsor	KSign Co., LTD.

Evaluation Facility	Korea System Assurance (KoSyAs)
Completion Date of Evaluation	February 26, 2025
Certification Body	IT Security Certification Center

[Table 5] Additional Identification Information

3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [4].

4. Assumptions and Clarification of Scope

The scope of this evaluation is limited to the functionality and assurance covered in the Security Target.

This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (For the detailed information of TOE version and TOE Components version refer to the [Table 1].)

5. Architectural Information

The physical scope of the TOE of the KSignAccess Server, KSignAccess Agent and manuals(Preparative Procedure, Operational User Guidance).

Category		Identification	Type
TOE Name		KSignAccess V5.0	
TOE Version		V5.0.3	
TOE component	KSignAccess Server	KSignAccess Server V5.0.1 (KSignAccess_Server_V5.0.1.tar)	Software (Distributed as a 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)	
Manual	Preparative Procedure	KSignAccess V5.0 Preparative Procedure V1.4 (KSignAccess V5.0 Preparative Procedure V1.4.pdf)	PDF (Distributed as a CD)
	Operational User Guidance	KSignAccess V5.0 Operational User Guidance V1.3 (KSignAccess V5.0 Operational User Guidance V1.3.pdf)	

[Table 6] Physical scope of TOE

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

Category	Description
Cryptographic module name	KSignCASE64 v2.5.2.0
Developer	KSign Co., Ltd
Validation date	2023. 10. 16.
Validation number	CM-237-2028.10
Expiration Date	2028. 10. 16.

[Table 7] Validated Cryptographic Modules

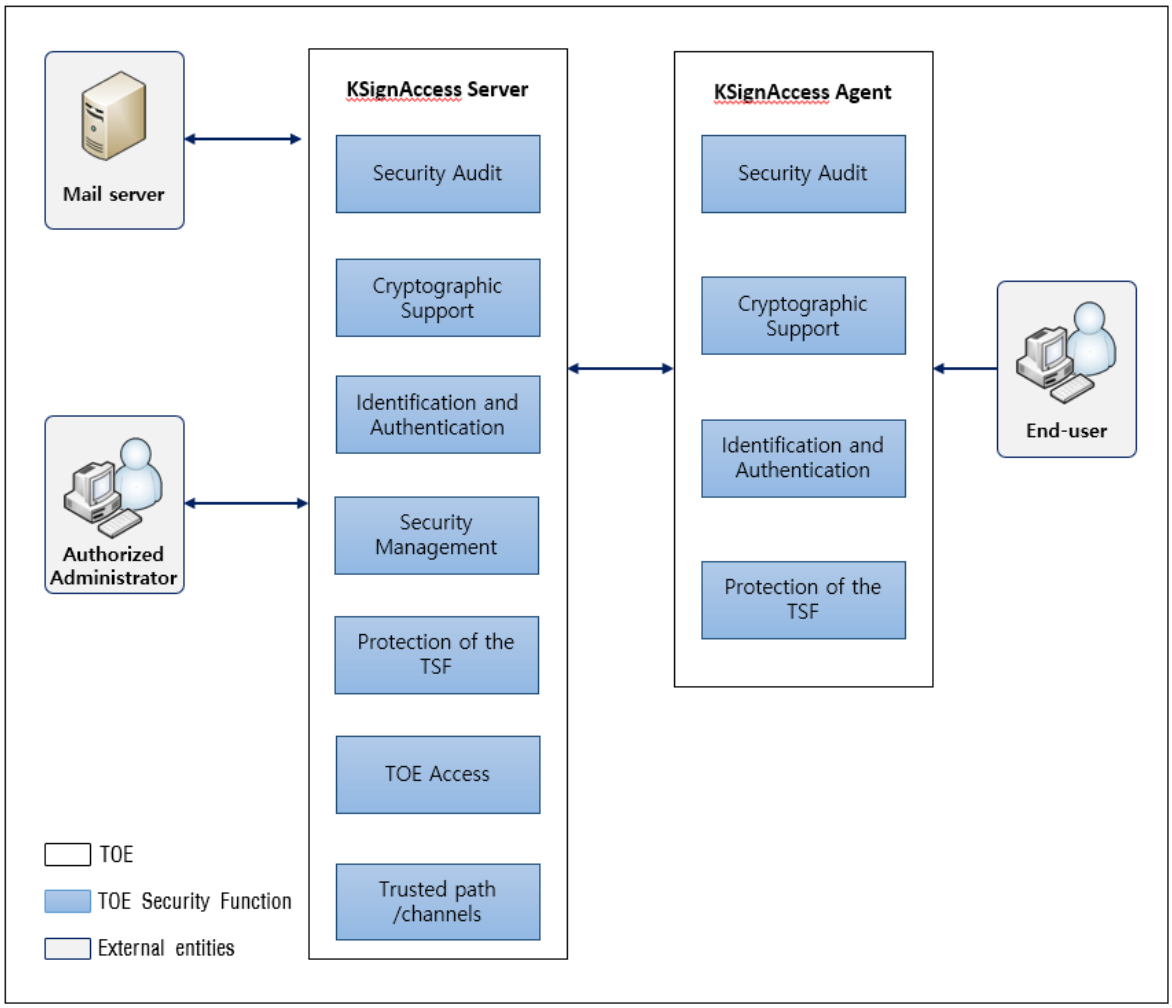
The 3rd Party libraries included in TOE is as follows.

TOE	Library	Usage
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 8] 3rd party software required for TOE operation

The logical scope of the TOE is as in [Figure 2] below.



[Figure 2] TOE logical scope

▣ Security Audit (FAU)

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. 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 (FCS)

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 (FIA)

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 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 (FMT)

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 (FPT)

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 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 (FTA)

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 (FTP)

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

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Date
KSignAccess V5.0 Preparative Procedure V1.4 (KSignAccess V5.0 Preparative Procedure V1.4.pdf)	February 7, 2025
KSignAccess V5.0 Operational User Guidance V1.3 (KSignAccess V5.0 Operational User Guidance V1.3.pdf)	January 8, 2025

[Table 9] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [5], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test case
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [4]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort,

the testing approach, configuration, depth, and results are summarized in the Penetration Testing Report [6].

8. Evaluated Configuration

The TOE is software consisting of the following components:

- TOE: KSignAccess V5.0 (V5.0.3)
- KSignAccess Server V5.0.1
- KSignAccess Agent for Linux V5.0.1
- KSignAccess Agent for Windows V5.0.1

The Administrator can identify the complete TOE reference after installation. And the guidance documents listed in chapter 6 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation results in the ETR [7] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation results were based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation(EAL1+).

As a result of the evaluation, the verdict **PASS** is assigned to all assurance components.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

Security Problem Definition clearly defines the security problems that the TOE and TOE operational environment are intended to address. Therefore, the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements are defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict **PASS** is assigned to the assurance class ASE.

9.2 Development Evaluation (ADV)

The functional specifications specify a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

The verdict **PASS** is assigned to the assurance class ADV.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict **PASS** is assigned to the assurance class AGD.

9.4 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

The verdict **PASS** is assigned to the assurance class ALC.

9.5 Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore, the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation.

Therefore, the verdict PASS is assigned to ATE_IND.1. Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict **PASS** is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t allow attackers possessing basic attack potential to violate the SFRs.

The verdict **PASS** is assigned to the assurance class AVA.

9.7 Evaluation Results Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		AVA_VAN.1.3E	PASS		

[Table 5] Evaluation Results Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.
- The administrator of the TOE shall preserve a secure state of the TOE by various methods such as keeping the OS and the DBMS up to date with the latest patch, eliminating unnecessary services, and changing the default ID and password.
- The administrator should periodically check a spare space of audit data, and carry out the audit data backup to prevent audit data loss.
- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

11. Security Target

KSignAccess V5.0 Security Target V1.4 [4] is included in this report for reference.

12. Acronyms and Glossary

(1) Acronyms

CC Common Criteria

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

SAR Security Assurance Requirement

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

(2) Glossary

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

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

Decryption

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

Encryption

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

end-user

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

External Entity

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

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

13. Bibliography

The evaluation facility has used the following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ 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, July, 2024

[2] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, CCMB-2022-11-006, November, 2022

Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, July, 2024

[3] Korean National Protection Profile for Single Sign On V3.0, KECS-PP-1230-2023, April 27, 2023

[4] KSignAccess V5.0 Security Target V1.4, February 26, 2025

[5] KSignAccess V5.0 Independent Testing Report(ATE_IND.1) V2.00, February 13, 2025

[6] KSignAccess V5.0 Penetration Testing Report (AVA_VAN.1) V2.00, February 13, 2025

[7] KSignAccess V5.0 Evaluation Technical Report (ETR) V3.00, February 26, 2025