KECS-CR-19-01

KSignAccess V4.0

Certification Report

Certification No.: KECS-CISS-0908-2019

2019. 1. 11.

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2019.01.02.	-	Certification report for KSignAccess V4.0 - First documentation

This document is the certification report for KSignAccess V4.0 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 V4.0 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, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on November 13, 2018.

The ST claims conformance to the Korean National PP for Single Sign On V1.0[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, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

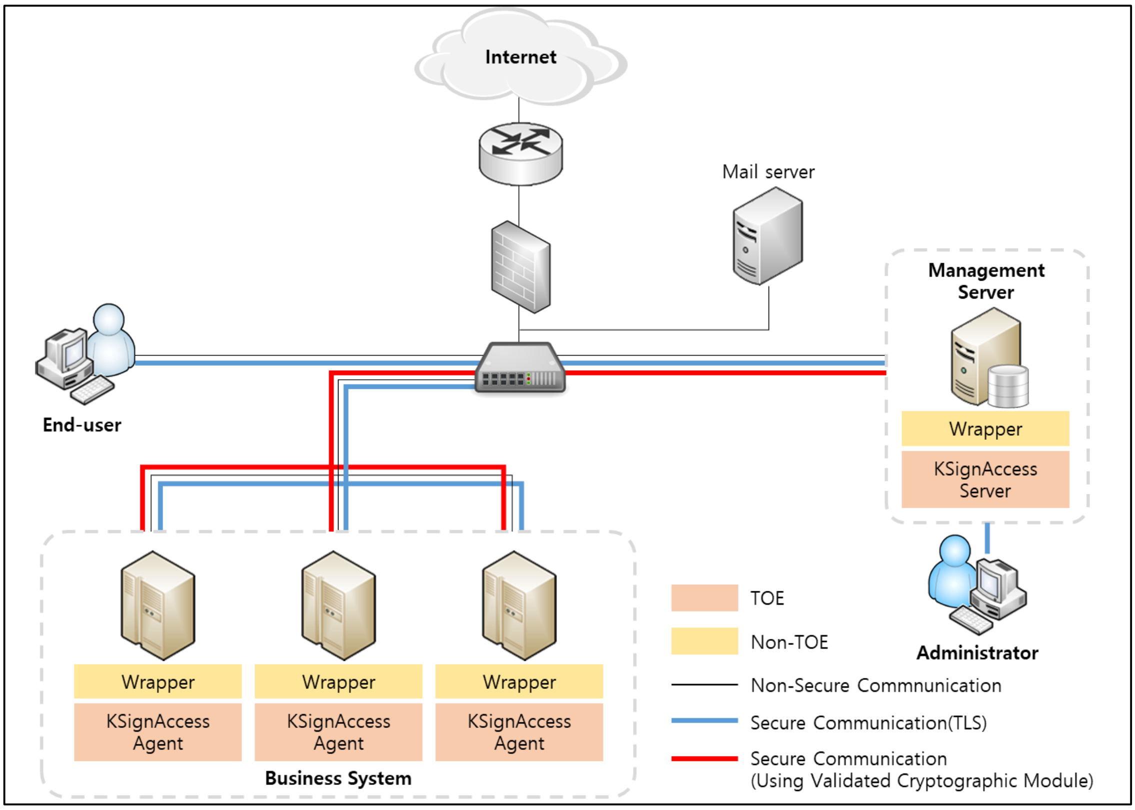
TOE is a 'Single-Sing-On' solution that allows access to various business systems through a single user login by end-user and it is offered in the form of software.

TOE is comprised of the KSignAccess Agent linked with the KSignAccess Server and business systems to carry out security management.

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

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

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



[Figure 1] Operational Environment of the TOE

The TOE operating environment consists of a management server and a business system.

The management server consists of the KSignAccess Server and performs security management. The business system is composed of the KSignAccess Agent in of the 'API type' composed of the library files. And performs an end-user login verification request and an authentication token manages function.

The KSignAccess Server conducts TOE security management through the web browser that supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer).

A wrapper is used for compatibility with various business systems, but it is excluded from the scope of the TOE.

When the TOE Administrator accesses the TOE security management interface by entering the management server web address on the browser, the browser forms an HTTPS security channel.

There are various external entities necessary for the operation of the TOE, including email server to notify the authorized administrator in case of audit data loss. The mail server, which is an external entity other than TOE, corresponds to the TOE operational environment.

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

Component				**Requirement**
KSignAccess Server		HW	CPU	Intel Xeon 3.5 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
		SW	OS	CentOS 6.8 kernel 2.6.32 (64 bit)
			DBMS	MySQL 5.6
			etc	Java(JDK) 1.8.0_191 Apache Tomcat 8.5.34
KSign Access Agent	KSignAccess Agent for Linux	HW	CPU	Intel Core i3 3.07 GHz or higher
			Memory	4 GB or higher
			HDD	Space required for installation of TOE : 500 MB or higher
			NIC	100/1000 Mbps x 1 EA or higher
		SW	OS	CentOS 6.8 kernel 2.6.32 (64 bit)
			etc	Java(JDK) 1.5.0_22 Apache Tomcat 5.5.36
	KSignAccess Agent for Solaris	HW	CPU	SUN SPARC 1.28 GHz or higher
			Memory	4 GB or higher
			HDD	Space required for installation of TOE : 500 MB or higher
			NIC	100/1000 Mbps x 1 EA or higher
		SW	OS	Solaris 5.10 (64 bit)

			etc	Java(JDK) 1.5.0_22 Apache Tomcat 5.5.36
	KSignAccess Agent for HP-UX	HW	CPU	Intel Itanium(IA64) 1.67 GHz or higher
			Memory	4 GB or higher
			HDD	Space required for installation of TOE : 500 MB or higher
			NIC	100/1000 Mbps x 1 EA or higher
		SW	OS	HP-UX 11.31 (64bit)
			etc	Java(JDK) 1.5.0_22 Apache Tomcat 5.5.36
	KSignAccess Agent for AIX	HW	CPU	PowerPC POWER5 2.1 GHz or higher
			Memory	4 GB or higher
			HDD	Space required for installation of TOE : 500 MB or higher
			NIC	100/1000 Mbps x 1 EA or higher
		SW	OS	AIX 7.1 (64 bit)
			etc	Java(JDK) 1.5.0_22 Apache Tomcat 5.5.36
	KSignAccess Agent for Windows	HW	CPU	Intel Core i3 3.30 GHz or higher
			Memory	4 GB or higher
			HDD	Space required for installation of TOE : 500 MB or higher
			NIC	100/1000 Mbps x 1 EA or higher
		SW	OS	Windows Server 2008 R2 (64bit) Windows Server 2012 R2 (64bit)
			etc	Java(JDK) 1.5.0_22 Apache Tomcat 5.5.36

[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
HW	CPU	Intel Core i3 2.30 GHz or higher

	Memory	4 GB or higher
	HDD	300 GB or higher
	NIC	100/1000 Mbps x 1 EA or higher
SW	OS	Windows 7 Professional Service Pack 1 (64 bit)
	Web Browser	Internet Explorer 11

[Table 2] The minimum requirements for the administrator's PC

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 is software libraries consisting of the following software components and related guidance documents.

TOE	KSignAccess V4.
Version	V4.0.2
TOE Components	KSignAccess Server V4.0.2 KSignAccess Agent for Linux V4.0.2 KSignAccess Agent for Solaris V4.0.2 KSignAccess Agent for HP-UX V4.0.2 KSignAccess Agent for AIX V4.0.2 KSignAccess Agent for Windows V4.0.2
Manuals	KSignAccess V4.0 Preparative Procedure V1.2 KSignAccess V4.0 Operation Guide V1.2

[Table 3] TOE identification

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security

	(September 12, 2017)
TOE	KSignAccess V4.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National PP for Single Sign On V1.0
Developer	KSign Co., LTD.
Sponsor	KSign Co., LTD.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	November 13, 2018

[Table 4] 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

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

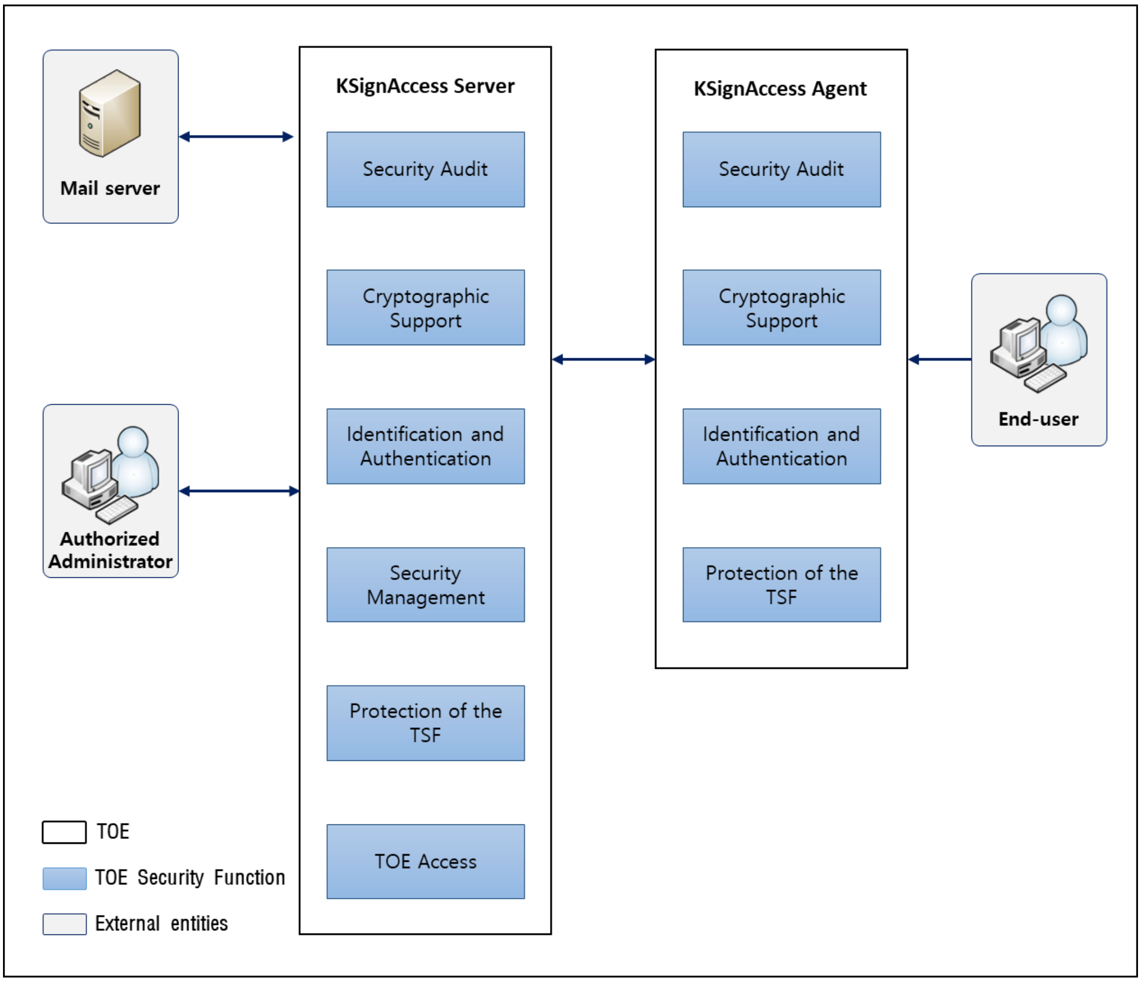
4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST. 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 3])

5. Architectural Information

The TOE consists of the KSignAccess Server, KSignAccess Agent and manuals(preparative procedure, operation guide). Verified Cryptographic Module(KSignCASE64 v2.5) is embedded in the TOE components The logical scope of the TOE is as in [Figure 2] below.



[Figure 2] TOE Logical scope

6. Documentation

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

Identification	Date

KSignAccess V4.0 Preparative Procedure V1.2 (KSignAccess V4.0 Preparative Procedure V1.2.pdf)	October 26, 2018
KSignAccess V4.0 Operation Guide V1.2 (KSignAccess V4.0 Operation Guide V1.2.pdf)	October 26, 2018

[Table 5] 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. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules 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 V4.0 (V4.0.2)

- KSignAccess Server V4.0.2
- KSignAccess Agent for Linux V4.0.2
- KSignAccess Agent for Solaris V4.0.2
- KSignAccess Agent for HP-UX V4.0.2
- KSignAccess Agent for AIX V4.0.2
- KSignAccess Agent for Windows V4.0.2

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 7 were evaluated with the TOE

9. Results of the Evaluation

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

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.

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 is 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 penetrating 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 Result 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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	ASE_CCL.1	ASE_CCL.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		
		AVA_VAN.1.3E	PASS		

[Table 6] Evaluation Result 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 shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default ID/password, etc., of the operating system and DBMS in the TOE operation.
- The administrator should periodically checks a spare space of audit data storage in case of the audit data loss, and carries 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 V4.0 Security Target V1.2 [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 system libraries existing between the application layer and the platform system, enables the easy development of the application running on the platform

Audit Administrator
An authorized administrator who can perform the audit record retrieval function in the security management interface

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 Document User
The TOE user who may, in accordance with the SFRs, perform an operation

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 cryptographic key

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

External Entity

An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE.

Top Administrator

The authorized administrator who has the highest authority to perform all security management functions in the security management interface

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 following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April, 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April, 2017

[3] Korean National Protection Profile for Single Sign On V1.0, August 18, 2017

[4] KSignAccess V4.0 Security Target V1.2, October 26, 2018

[5] KSignAccess V4.0 Independent Testing Report(ATE_IND.1) V2.00, December 17, 2018

[6] KSignAccess V4.0 Penetration Testing Report (AVA_VAN.1) V1.00, November 09, 2018