KECS-CR-20-73

KSignSecureDB V3.6

Certification Report

Certification No.: KECS-CISS-1059-2020

2020. 12. 3.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2020.12.03.	-	Certification report for KSignSecureDB V3.6 - First documentation

This document is the certification report for KSignSecureDB V3.6 for 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 certification result drawn by the evaluation facility on the results of the KSignSecureDB V3.6 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 database encryption software to prevent unauthorized exposure of the information from DBMS. 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, etc..

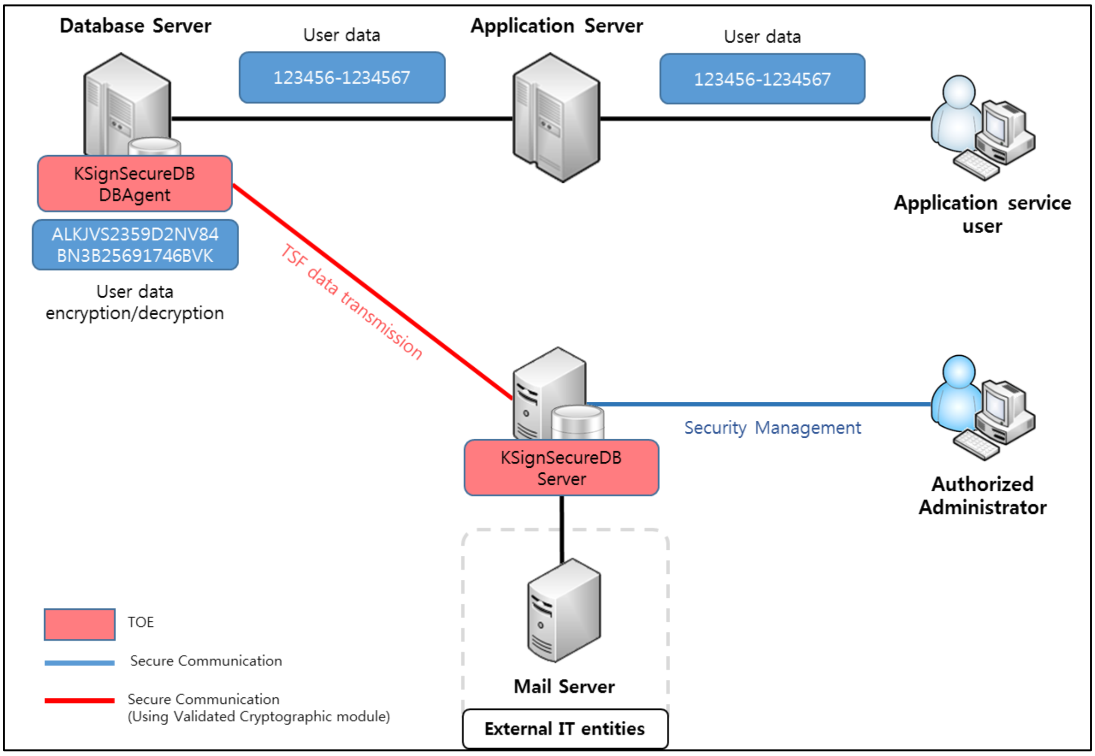
The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on October 29, 2020.

The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.1[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. 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.

The TOE is comprised of the KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent and can be installed 'Plug-in' and 'API' type. [Figure 1], [Figure 2] shows the operational environment of the TOE.

[Figure 1] shows a typical operational environment of the plug-in type.

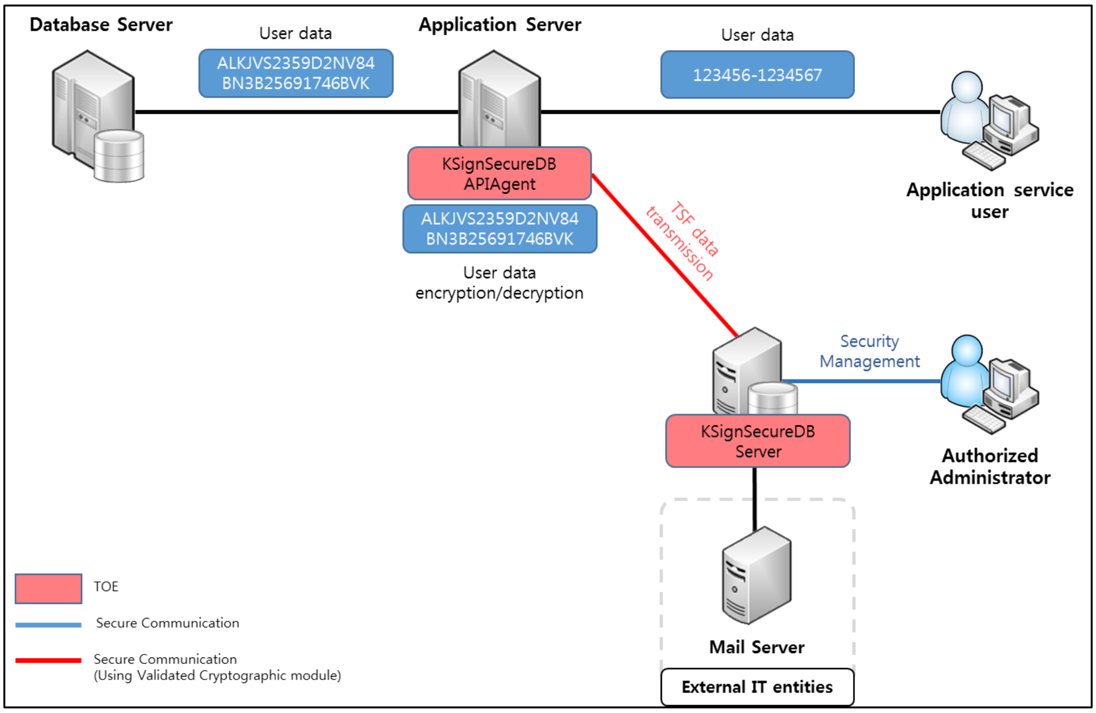
The plug-in operational environment is composed of the Management Server and DB Agent. First, the Management Server manages the information on policies established by the authorized administrator and manages the keys and the audit records. It also encrypts the information on a distributed key and loads it on the shared memory. Second, the DB Agent is installed inside the Database Server where the DB under the protection is located, and encrypts the user data received from the Application Server before they are stored in the DB. In addition, it decrypts the encrypted user data to be transmitted from the Database Server to the Application Server.



[Figure 1] Plug-in type operational environment of the TOE
(Agent, Management Server separate type)

The application service user requests the encryption or decryption of the user data through the Application Server in accordance with the scope of the encryption as required by the security policy. The requested data are encrypted by the DB Agent and stored in the DB. The authorized administrator accesses the Management Server to perform the security management of the encrypted data stored in the DB.

[Figure 2] shows the API type operational environment. The API type consists of the API Agent and the Management Server. The API Agent is installed and operated outside the DB under the protection, and performs the encryption and decryption of the important data in accordance with the policy established by the administrator. The authorized administrator can access the Management Server and perform the security management. The TOE components may be subject to change depending on the roles including the encryption and decryption of the important information, security management and cryptographic key management.



[Figure 2] API-type operational environment of the TOE

(API module, management server separate type)

The application service user performs the encryption and decryption of the user data through the API Agent on the Application Server in accordance with the scope of the encryption as required by the security policy. The authorized administrator accesses the Management Server to perform the security management of the encrypted data stored in the DB.

The cryptographic algorithm subject to the validation in the validated cryptographic module is used for the communication between the TOE components for the purpose of secure communication. In case the administrator accesses the Management Server through a web browser, a secure path (SSL/TLS V1.2) is generated to carry out the communication.

As other external entities necessary for the operation of the TOE, there is email server to send alerts by email to the authorized administrator.

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

Classification			Minimum Requirement
KSignSecureDB Server	HW	CPU	PowerPC POWER5 2.1 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for installation of TOE : 3 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	AIX 7.1 (64 bit)
		DBMS	Oracle 12c R2
		etc	Java(JRE) 1.8.0_261 (IBM-AIX pap6480sr6fp16-20200902_01) Apache Tomcat 8.5.59
KSignSecureDB DBAgent for Oracle_AIX	HW	CPU	PowerPC POWER5 2.1 GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE : 1 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	AIX 7.1 (64 bit)
		DBMS	Oracle 12c R2
		etc	Java(JRE) 1.8.0_261 (IBM-AIX pap6480sr6fp16-20200902_01)
KSignSecureDB DBAgent for Tibero_AIX	HW	CPU	PowerPC POWER5 2.1 GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE : 1 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	AIX 7.1 (64 bit)
		DBMS	Tibero 6
		etc	Java(JRE) 1.8.0_261 (IBM-AIX pap6480sr6fp16-20200902_01)
KSignSecureDB APIAgent for JAVA_AIX	HW	CPU	PowerPC POWER5 2.1 GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE : 1 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	AIX 7.1 (64 bit)

		etc	Java(JRE) 1.8.0_261 (IBM-AIX pap6480sr6fp16-20200902_01)

[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]

Classification		Minimum Requirement
SW	Web Browser	Google Chrome 86.0

[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 consisting of the following software components and related guidance documents.

TOE	KSignSecureDB V3.6	
Version	V3.6.1	
TOE Components	KSignSecureDB Server	KSignSecureDB Server V3.6.1 (KSDBV36-Server_V3.6.1.tar)
	KSignSecureDB DBAgent	KSignSecureDB DBAgent For Oracle_AIX V3.6.1 (KSDBV36-DBAgent_For_Oracle_AIX_V3.6.1.tar)
		KSignSecureDB DBAgent For Tibero_AIX V3.6.1 (KSDBV36-DBAgent_For_Tibero_AIX_V3.6.1.tar)
	KSignSecureDB APIAgent	KSignSecureDB APIAgent For JAVA_AIX V3.6.1 (KSDBV36-APIAgent_For_API_JAVA_AIX_V3.6.1.tar)
Guidance Document	KSignSecureDB V3.6 Preparative Procedure V1.6 (KSignSecureDB V3.6 Preparative Procedure V1.6.pdf) KSignSecureDB V3.6 Operation Guide V1.5 (KSignSecureDB V3.6 Operation Guide V1.5.pdf)	

[Table 3] TOE identification

Note that the TOE is delivered contained in a CD-ROM.

[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	KSignSecureDB V3.6
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017

Protection Profile	Korean National Protection Profile for Database Encryption V1.1
Developer	KSign Co., LTD.
Sponsor	KSign Co., LTD.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	October 29, 2020
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [4] for the TOE claims strict to the Korean National PP for Database Encryption V1.1 [3], and complies security policies defined in the PP by security requirements. Thus, the TOE provides security features defined in the PP as follows:

- Security audit: The TOE generates audit records of security relevant events such as the start-up/shutdown of the audit functions, integrity violation, self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic key management such as key generation, distribution, and destruction, and cryptographic operations such as encryption and decryption using the cryptographic modules (KSignCrypto for Java V1.0.1.0) validated under the KCMVP.
- User data protection: The TOE provides encryption and decryption for the user data in a column of a database.
- Identification and authentication: The TOE identifies and authenticates the administrators using their ID/password and mutually authenticates TOE components.
- Security management: The TOE allows only an authorized administrator to access the management interface provided by the TOE.
- Protection of the TSF: The TOE implements secure communications between the TOE components to protect the transmitted data. The TOE encrypts the stored TSF data to protect them from unauthorized exposure and modification. The TOE performs self-tests on the TOE components, which includes the self-test on the validated cryptographic module.

- TOE access: The TOE manages authorized administrators' sessions based on access IP addresses and administrator rights, and terminates the sessions after predefined time interval of inactivity.

4. Assumptions and Clarification of Scope

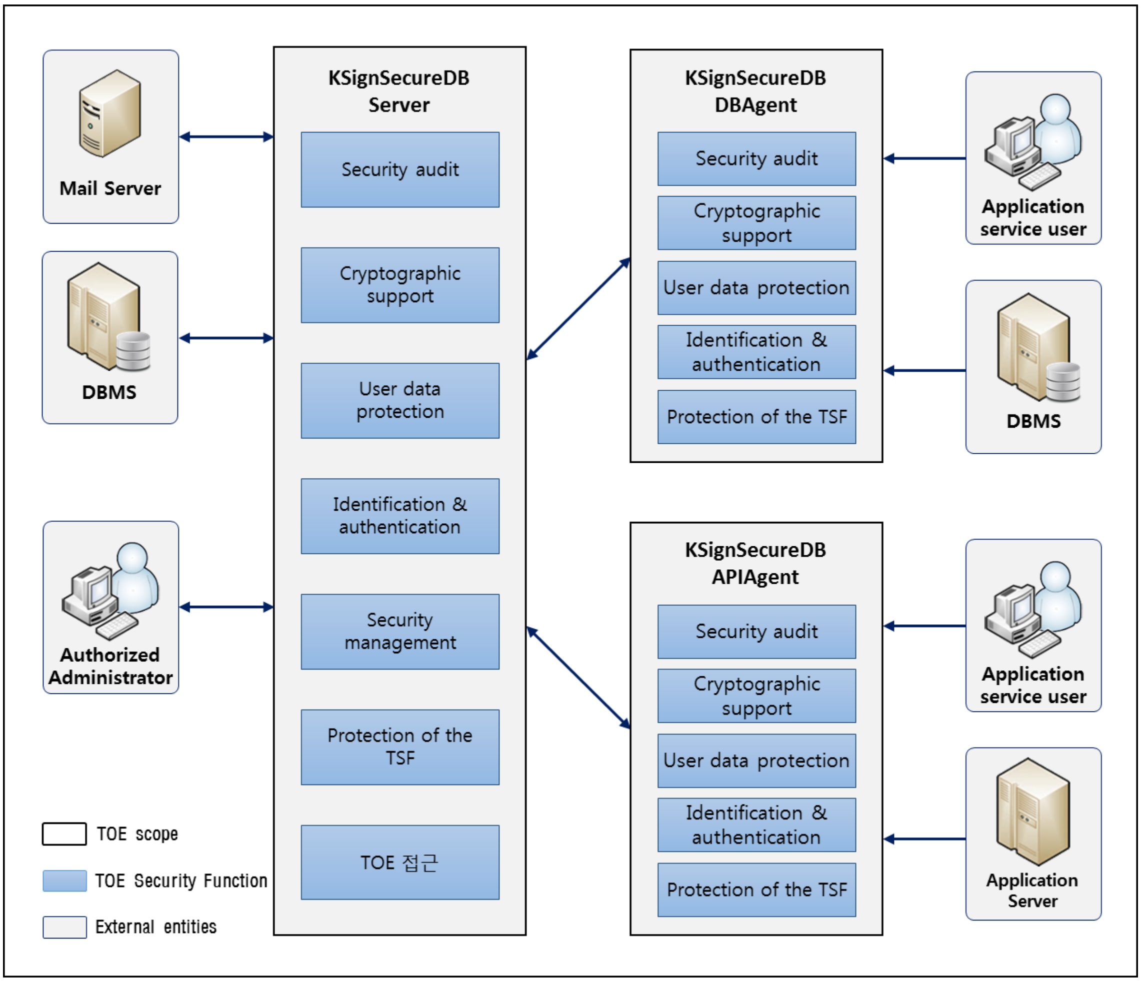
There is no explicit Security Problem Definition chapter, therefore no Assumptions secti on in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [3] in which the TOE will be used or is intended to be used (For the detailed and precise definition of the security objectives of the operational environment, refer to the ST [4], chapter 3.).

5. Architectural Information

The TOE is software consisting of the following components:

- KSignSecureDB Server
- KSignSecureDB DBAgent
- KSignSecureDB APIAgent

In [Figure 3], the three components are provided by the TOE Logical scope and boundary of TOE. For the detailed description on the architectural information, refer to the ST [4].



[Figure 3] Logical scope of the TOE

6. Documentation

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

Identification	Date
KSignSecureDB V3.6 Preparative Procedure V1.6 (KSignSecureDB V3.6 Preparative Procedure V1.6.pdf)	November 13, 2020
KSignSecureDB V3.6 Operation Guide V1.5 (KSignSecureDB V3.6 Operation Guide V1.5.pdf)	October 12, 2020

[Table 5] Documentations

7. TOE Testing

The developer 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 developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator installed and prepared the TOE in accordance to the preparative procedures, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities.

The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: KSignSecureDB V3.6 (V3.6.1)

- KSignSecureDB Server V3.6.1
- KSignSecureDB DBAgent For Oracle_AIX V3.6.1
- KSignSecureDB DBAgent For Tibero_AIX V3.6.1
- KSignSecureDB APIAgent For JAVA_AIX V3.6.1

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 6 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2].
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.
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 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.

9.3 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 Development Evaluation (ADV)

The functional specification specifies 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.

9.5 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 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		
	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		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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 5] 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 check 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

KSignSecureDB V3.6 Security Target V1.10 [4] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
Application Server	The application server defined in this PP refers to the server that installs and operates the application, which is developed to provide a certain application service by the organization that operates the TOE. The pertinent application reads the user data from the DB, which is located in the database server, by the request of the application service user, or sends the user data to be stored in the DB to the database server.
Critical Security Parameter (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).
Policy Key	Key generated from the validated cryptographic module. It is generated by the authorized administrator in the security management interface to be used for the encryption and decryption of the user data

Secret Key

Cryptographic key that is used along with a secret key cryptographic algorithm and can be uniquely combined with an entity or more / It shall not be made public.

Self-test

Pre-operational or conditional test executed by the cryptographic module

Validated Cryptographic Module

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

13. Bibliography

The certification body 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 Database Encryption V1.1, KECS-PP-0820a-2017, December 11, 2019.

[4] KSignSecureDB V3.6 Security Target V1.10, Nov 13, 2020.

[5] KSignSecureDB V3.6 Evaluation Technical Report(ETR) Lite V2.00, Nov 19, 2020.