

# KSignSecureDB V3.5

## Certification Report

Certification No.: KECS-CISS-0958-2019

2019. 8. 27.



IT Security Certification Center

## History of Creation and Revision

No.	Date	Revised Pages	Description
00	2019.8.27.	-	Certification report for KSignSecureDB V3.5 - First documentation

This document is the certification report for KSignSecureDB V3.5 of KSign Co., LTD.

The Certification Body  
IT Security Certification Center

The Evaluation Facility  
Korea System Assurance (KOSYAS)

# Table of Contents

- 1. Executive Summary ..... 5**
- 2. Identification .....11**
- 3. Security Policy..... 13**
- 4. Assumptions and Clarification of Scope ..... 13**
- 5. Architectural Information ..... 13**
- 6. Documentation ..... 14**
- 7. TOE Testing..... 15**
- 8. Evaluated Configuration ..... 15**
- 9. Results of the Evaluation ..... 16**
  - 9.1 Security Target Evaluation (ASE) ..... 16
  - 9.2 Life Cycle Support Evaluation (ALC)..... 17
  - 9.3 Guidance Documents Evaluation (AGD) ..... 17
  - 9.4 Development Evaluation (ADV)..... 18
  - 9.5 Test Evaluation (ATE)..... 18
  - 9.6 Vulnerability Assessment (AVA) ..... 18
  - 9.7 Evaluation Result Summary ..... 18
- 10. Recommendations ..... 19**
- 11. Security Target..... 20**
- 12. Acronyms and Glossary ..... 21**
- 13. Bibliography ..... 22**

# 1. Executive Summary

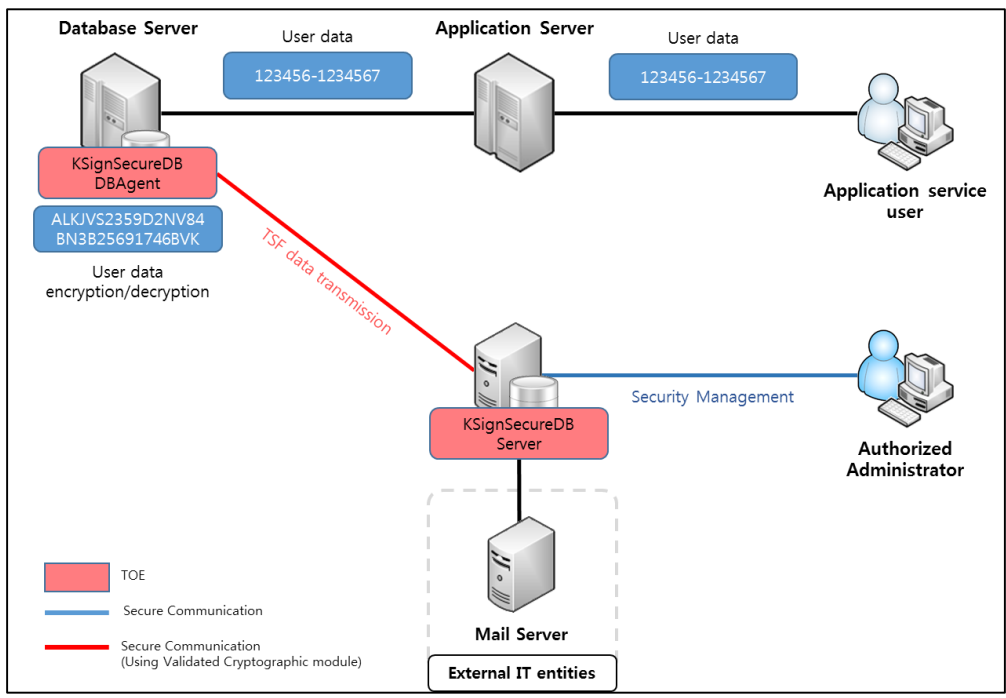
This report describes the certification result drawn by the certification body on the results of the KSignSecureDB V3.5 developed by KSign Co., LTD. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (“TOE” hereinafter) is database encryption software. The TOE provides a variety of security features: security audit, cryptographic operation using cryptographic module (KSignCASE64 v2.5) validated under the Korea Cryptographic Module Validation Program (KCMVP), identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function.

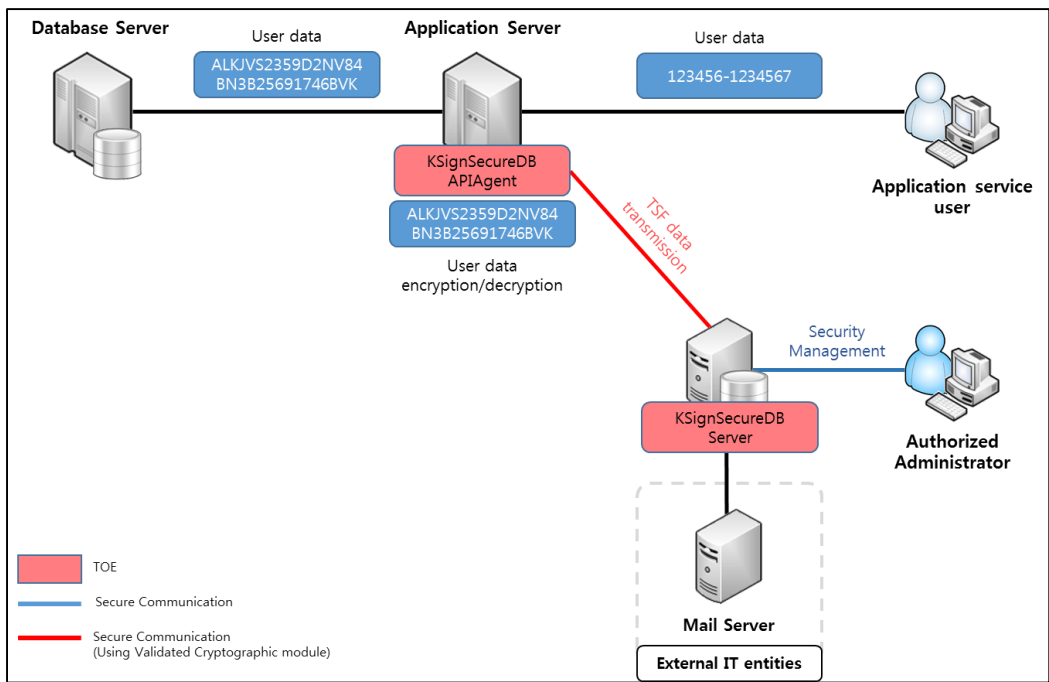
The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on July 29, 2019. This report grounds on the Evaluation Technical Report (ETR) [6] KOSYAS had submitted and the Security Target (ST) [7].

The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.0 [5]. 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 the PP [5]. 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.

[Figure 1] ~ [Figure 2] shows the operational environment of the TOE. The TOE is comprised of the KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent and can be installed 'Plug-in' and 'API' type. The KSignSecureDB 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. The KSignSecureDB DBAgent is installed inside the Database Server and encrypts the user data received from the Application Server before they are stored in the DB. It decrypts the encrypted user data to be transmitted from the Database Server to the Application Server. The KSignSecureDB APIAgent is installed and operated outside the DB, and performs the encryption and decryption of the important data in accordance with the policy established by the administrator.



[Figure 1] Plug-in type operational environment (Agent, management server separate type)



[Figure 2] API-type operational environment (API module, management server separate type)

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

necessary for installation and operation of the TOE are shown in [Table 1].

Component		Contents	
KSignSecureDB Server	HW	CPU	Intel Xeon 2.4 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	CentOS 6.8 kernel 2.6.32 (64 bit)
		DBMS	Oracle 11g R2
		etc	Java(JDK) 1.8.0_202 Apache Tomcat 8.5.41
KSignSecureDB DBAgent for Oracle_Solaris	HW	CPU	SUN SPARC 1.2 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	Solaris 5.10 (64 bit)
		DBMS	Oracle 12c R2
		etc	Java(JDK) 1.8.0_202
KSignSecureDB DBAgent for Oracle_HP-UX	HW	CPU	Intel Itanium(IA64) 1.4 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	HP-UX 11.31 (64bit)
		DBMS	Oracle 12c R2
		etc	Java(JDK) 1.8.0_202
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(JDK) 1.8.0_202
KSignSecureDB DBAgent for Tiberio_Linux	HW	CPU	Intel Core i3 3.07 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	CentOS 6.8 kernel 2.6.32 (64 bit)
		DBMS	Tiberio 6
		etc	Java(JDK) 1.8.0_202
KSignSecureDB DBAgent for Tiberio_Solaris	HW	CPU	SUN SPARC 1.2 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	Solaris 5.10 (64 bit)
		DBMS	Tibero 6
		etc	Java(JDK) 1.8.0_202
KSignSecureDB DBAgent for Tibero_HP-UX	HW	CPU	Intel Itanium(IA64) 1.4 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	HP-UX 11.31 (64bit)
		DBMS	Tibero 6
		etc	Java(JDK) 1.8.0_202
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(JDK) 1.8.0_202
KSignSecureDB DBAgent for MSSQL_Windows	HW	CPU	Intel Core i3 3.30 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	Windows Server 2012 R2 (64bit)
		DBMS	MSSQL 2016
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for JAVA_Linux	HW	CPU	Intel Core i3 3.07 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	CentOS 6.8 kernel 2.6.32 (64 bit)
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for JAVA_Solaris	HW	CPU	SUN SPARC 1.2 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	Solaris 5.10 (64 bit)
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for JAVA_HP-UX	HW	CPU	Intel Itanium(IA64) 1.4 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	HP-UX 11.31 (64bit)
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for	HW	CPU	PowerPC POWER5 2.1 GHz or higher
		Memory	4 GB or higher



JAVA_AIX		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(JDK) 1.8.0_202
KSignSecureDB APIAgent for C_Linux	HW	CPU	Intel Core i3 3.07 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	CentOS 6.8 kernel 2.6.32 (64 bit)
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for C_Solaris	HW	CPU	SUN SPARC 1.2 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	Solaris 5.10 (64 bit)
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for C_HP-UX	HW	CPU	Intel Itanium(IA64) 1.4 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	HP-UX 11.31 (64bit)
		etc	Java(JDK) 1.8.0_202
KSignSecureDB APIAgent for C_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(JDK) 1.8.0_202
KSignSecureDB APIAgent for C_Windows	HW	CPU	Intel Core i3 3.30 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	Windows Server 2012 R2 (64bit)
		etc	Java(JDK) 1.8.0_202

[Table 1] Hardware and Software required by TOE

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

Component		Contents
HW	CPU	Intel Core i5 2.30 GHz or higher
	Memory	4 GB or higher
	HDD	100 GB or higher

	NIC	100/1000 Mbps x 1 EA or higher
SW	OS	Windows 7 Professional Service Pack 1 (64 bit)
	Web Browser	Google Chrome 73.0

**[Table 2] Administrator PC Requirements.**

In addition, external IT entities linked to the TOE operation are as follows.

Mail Server: Send email to authorized administrator

**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	KSignSecureDB V3.5
Version	V3.5.2
TOE Components	<p>KSignSecureDB Server V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-Server_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Oracle_Solaris V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Oracle_Solaris_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Oracle_HP-UX V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Oracle_HP-UX_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Oracle_AIX V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Oracle_AIX_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Tibero_Linux V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Tibero_Linux_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Tibero_Solaris V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Tibero_Solaris_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Tibero_HP-UX V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Tibero_HP-UX_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For Tibero_AIX V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_Tibero_AIX_V3.5.2.tar)</li> </ul> <p>KSignSecureDB DBAgent For MSSQL_Windows V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-DBAgent_For_MSSQL_Windows_V3.5.2.zip)</li> </ul> <p>KSignSecureDB APIAgent For JAVA_Linux V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-APIAgent_For_API_JAVA_Linux_V3.5.2.tar)</li> </ul> <p>KSignSecureDB APIAgent For JAVA_Solaris V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-APIAgent_For_API_JAVA_Solaris_V3.5.2.tar)</li> </ul> <p>KSignSecureDB APIAgent For JAVA_HP-UX V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-APIAgent_For_API_JAVA_HP-UX_V3.5.2.tar)</li> </ul> <p>KSignSecureDB APIAgent For JAVA_AIX V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-APIAgent_For_API_JAVA_AIX_V3.5.2.tar)</li> </ul> <p>KSignSecureDB APIAgent For C_Linux V3.5.2</p> <ul style="list-style-type: none"> <li>- (KSDBV35-APIAgent_For_API_C_Linux_V3.5.2.tar)</li> </ul>

	KSignSecureDB APIAgent For C_Solaris V3.5.2 - (KSDBV35-APIAgent_For_API_C_Solaris_V3.5.2.tar) KSignSecureDB APIAgent For C_HP-UX V3.5.2 - (KSDBV35-APIAgent_For_API_C_HP-UX_V3.5.2.tar) KSignSecureDB APIAgent For C_AIX V3.5.2 - (KSDBV35-APIAgent_For_API_C_AIX_V3.5.2.tar) KSignSecureDB APIAgent For C_Windows V3.5.2 - (KSDBV35-APIAgent_For_API_C_Windows_V3.5.2.zip)
Guidance Documents	KSignSecureDB V3.5 Preparative Procedure V1.3 - (KSignSecureDB V3.5 Preparative Procedure V1.3.pdf) KSignSecureDB V3.5 Operation Guide V1.3 - (KSignSecureDB V3.5 Operation Guide V1.3.pdf)

**[Table 3] TOE identification**

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 V3.5
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 V1.0, KECS-PP-0820-2017, August 18, 2017
Developer	KSign Co., LTD.
Sponsor	KSign Co., LTD.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	July 29, 2019
Certification Body	IT Security Certification Center

**[Table 4] Additional identification information**

### 3. Security Policy

The TOE complies security policies defined in the ST [7] by security requirements. Thus the TOE provides following security features. For more details refer to the ST [7].

TSF	Explanation
Security Audit	The TOE generates audit records of security relevant events.
Cryptographic Support	The TOE performs cryptographic key management, cryptographic operation, and random bit generation using the cryptographic modules(KSignCASE 64 v2.5) validated under the KCMVP
User Data Protection	The TOE provides users with column-by-column encryption and decryption of user data.
Identification and Authentication	The TOE identifies and authenticates administrators with ID and PW.
Security Management	Only authorized administrators can perform security management functions.
Protection of the TSF	To protect TSF data transmitted between TOE components encryption communication is carried out. The TOE performs self-test on the main process at startup or periodically during operation.
TOE Access	The TOE manages management connection sessions based on access IP addresses and administrator rights

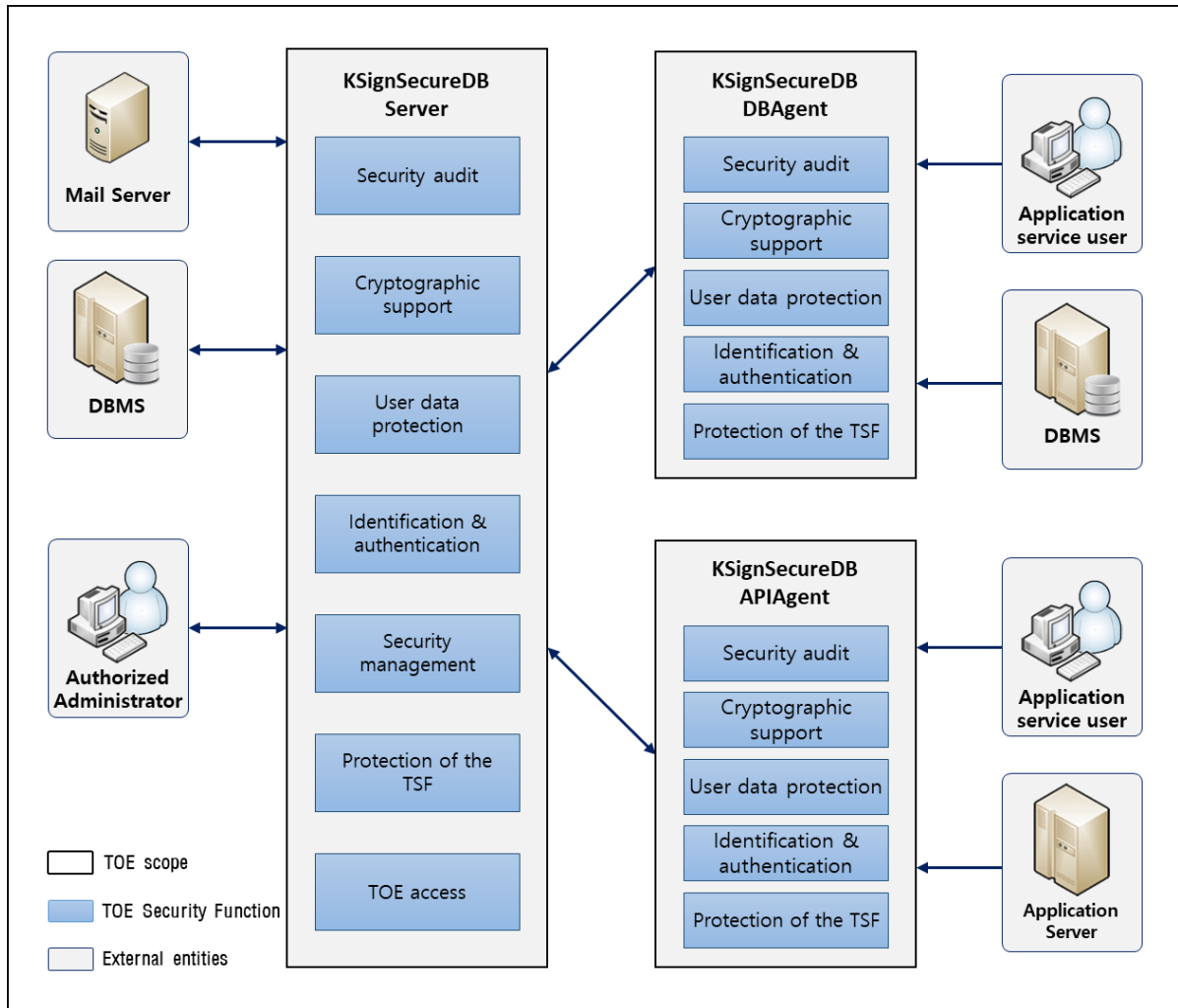
[Table 5] The TOE Security Functions

### 4. Assumptions and Clarification of Scope

There is no explicit security problem definition chapter, therefore, no assumptions section, in the low assurance ST. Some Security aspects of the operational environment are added to those of the PP 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, chapter 3)

### 5. Architectural Information

The physical scope of the TOE consists of the KSignSecureDB Server, KSignSecureDB DBAgent, KSignSecureDB APIAgent and guidance. The following security functions are provided by the TOE Logical scope and boundary of TOE is shown in [Figure 4]



[Figure 3] TOE Logical scope

## 6. Documentation

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

Identifier	Version	Date
KSignSecureDB V3.5 Preparative Procedure V1.3	V1.3	May 24, 2019
KSignSecureDB V3.5 Operation Guide V1.3	V1.3	May 24, 2019

[Table 6] Documentation

## 7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component 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 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 has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [6].

## 8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: KSignSecureDB V3.5 (V3.5.2)

- KSignSecureDB Server V3.5.2
- KSignSecureDB DBAgent For Oracle\_Solaris V3.5.2
- KSignSecureDB DBAgent For Oracle\_HP-UX V3.5.2
- KSignSecureDB DBAgent For Oracle\_AIX V3.5.2
- KSignSecureDB DBAgent For Tibero\_Linux V3.5.2
- KSignSecureDB DBAgent For Tibero\_Solaris V3.5.2
- KSignSecureDB DBAgent For Tibero\_HP-UX V3.5.2
- KSignSecureDB DBAgent For Tibero\_AIX V3.5.2

- KSignSecureDB DBAgent For MSSQL\_Windows V3.5.2
- KSignSecureDB APIAgent For JAVA\_Linux V3.5.2
- KSignSecureDB APIAgent For JAVA\_Solaris V3.5.2
- KSignSecureDB APIAgent For JAVA\_HP-UX V3.5.2
- KSignSecureDB APIAgent For JAVA\_AIX V3.5.2
- KSignSecureDB APIAgent For C\_Linux V3.5.2
- KSignSecureDB APIAgent For C\_Solaris V3.5.2
- KSignSecureDB APIAgent For C\_HP-UX V3.5.2
- KSignSecureDB APIAgent For C\_AIX V3.5.2
- KSignSecureDB APIAgent For C\_Windows V3.5.2

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 6, [Table 6] were evaluated with the TOE

## 9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [6] 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 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.

## 9.5 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		
	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	
		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 7] 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 with application server and DBMS fully understands the preparation procedure and user operation manual install and operate the security function.

- 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 V3.5 Security Target V1.7 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
Approved cryptographic algorithm	A cryptographic algorithm selected by Korea Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability
Column	A set of data values of a particular simple type, one for each row of the table in a relational database
Database	A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this PP, refers to the relational database.
DBMS (Database Management System)	A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this PP, refers to the database management system based on the relational database model.

Self-test

Pre-operational or conditional test executed by the cryptographic module

## 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
  - Part 1: Introduction and general model
  - Part 2: Security functional components
  - Part 3: Security assurance components
- [2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April, 2017
- [3] Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017)
- [4] Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)
- [5] Korean National Protection Profile for Database Encryption V1.0, August 18, 2017
- [6] KSignSecureDB V3.5 Evaluation Technical Report Lite V2.00, July 29, 2019
- [7] KSignSecureDB V3.5 Security Target V1.7, July 22, 2019