KECS-CR-24-43

KSignSecureDB V3.7

Certification Report

Certification No.: KECS-CISS-1321-2024

2024. 8. 2.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.08.02.	-	Certification report for KSignSecureDB V3.7 - First documentation

This document is the certification report for KSignSecureDB V3.7 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 KSignSecureDB V3.7 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.

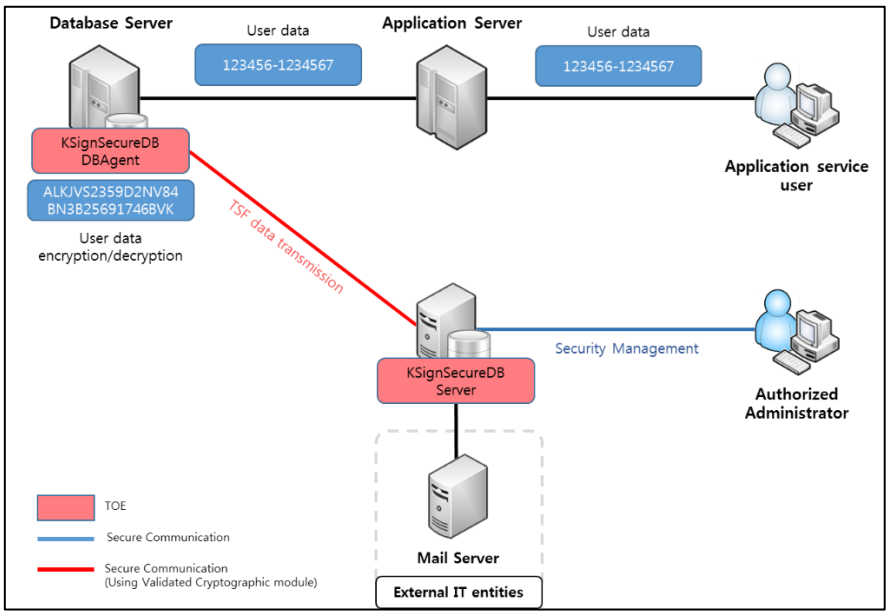
The Target of Evaluation (“TOE” hereinafter) is database encryption software to prevent unauthorized exposure of the information from DBMS. Also, the TOE shall provide a variety of security features: security audit, cryptographic operation using cryptographic module, the user identification and authentication 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 July 29, 2024.

The ST claims 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 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.

The TOE is comprised of the KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent.

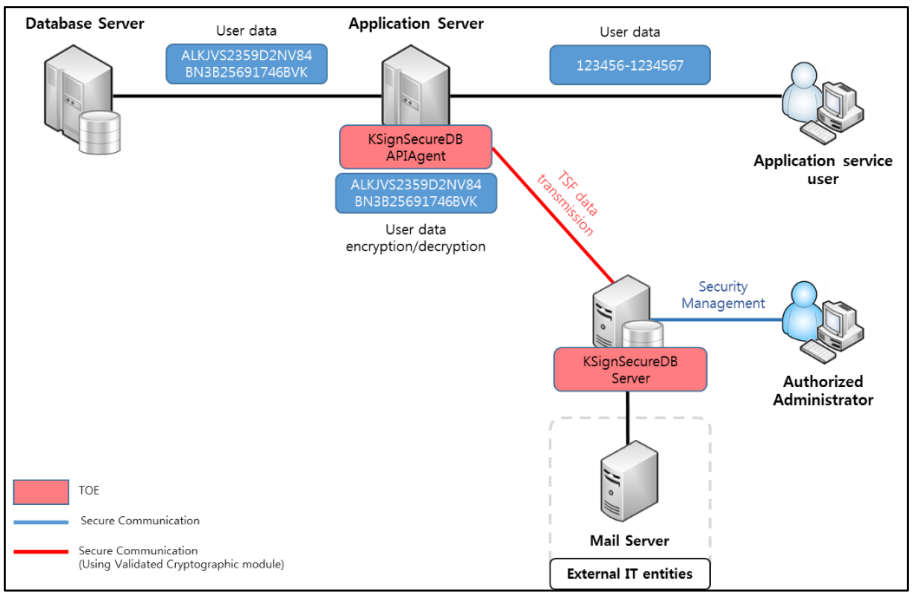
[Figure 1] shows an operational environment of the plug-in type. The plug-in operational environment is composed of KSignSecureDB Server and KSignSecureDB DBAgent. First, KSignSecureDB Server manages the information on policies established by the authorized administrator and manages the keys and the audit records. Second, KSignSecureDB DBAgent is installed inside the Database Server where the DB under the protection is located, and encrypts the user data receive from the Application Server before they are stored in the DB according to the policy configured by the authorized administrator. 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 KSignSecureDB DBAgent and stored in the DB.



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

(Agent, management server separate type)

[Figure 2] shows the API type operational environment.
The API type consists of KSignSecureDB APIAgent and KSignSecureDB Server. KSignSecureDB APIAgent is installed and operated in Application Server, 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 KSignSecureDB Server and perform the security management.
The application service user performs the encryption and decryption of the user data through KSignSecureDB APIAgent on the Application Server in accordance with the scope of the encryption as required by the security policy. The encrypted user data is transmitted to the Database Server, and the encrypted user data transmitted from the Database Server is decrypted by APIAgent installed in the Application Server and transmitted to the application service user.

The communication among the TOE components shall be based on the encrypted communication using the approved cryptographic algorithm of the validated cryptographic module. 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].

TOE	Item	Specification
KSignSecureDB Server	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 1EA or higher
	OS	AIX 7.2 (64 bit)
	S/W	Oracle 19c Java(JRE) 1.8.0_411 Apache tomcat 8.5.100

KSignSecureDB DBAgent For Oracle_AIX	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 1EA or higher
	OS	AIX 7.2 (64 bit)
	DBMS	Oracle 19c
	S/W	Java(JRE) 1.8.0_411
KSignSecureDB DBAgent For Tibero_AIX	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 1EA or higher
	OS	AIX 7.2 (64 bit)
	DBMS	Tibero 7
	S/W	Java(JRE) 1.8.0_411
KSignSecureDB APIAgent For JAVA_AIX	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 1EA or higher
	OS	AIX 7.2 (64 bit)
	S/W	Java(JRE) 1.8.0_411

[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 126.0

[Table 2] Administrator PC Requirements

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

Classification	Usage
Mail Server (SMTP Server)	Send the alert mail to an administrator

[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		KSignSecureDB V3.7
Version		V3.7.3
TOE Components	**KSignSecureDB Server**	KSignSecureDB Server V3.7.3
	KSignSecureDB DBAgent	KSignSecureDB DBAgent For Oracle_AIX V3.7.3
		KSignSecureDB DBAgent For Tibero_AIX V3.7.3
	KSignSecureDB APIAgent	KSignSecureDB APIAgent For JAVA_AIX V3.7.3
Manuals		KSignSecureDB V3.7 Preparative Procedure V1.3 KSignSecureDB V3.7 Operation Guide V1.3

[Table 4] TOE identification

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	KSignSecureDB V3.7
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 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	July 29, 2024

[Table 5] Additional identification information

3. Security Policy

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

- Security Audit
- Cryptographic Support
- User data protection
- 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 4])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the KSignSecureDB Server, KSignSecureDB DBAgent, KSignSecureDB APIAgent and manuals(preparative procedure, operation guide).

Scope	Identification		Type	Distribution Form
TOE	KSignSecureDB V3.7			
TOE Version	V3.7.3			
TOE Components	KSignSecure DB Server	KSignSecureDB Server V3.7.3 (KSDBV37-Server_V3.7.3.tar)	S/W	CD
	KSignSecure DB DBAgent	KSignSecureDB DBAgent For Oracle_AIX V3.7.3 (KSDBV37-DBAgent_For_Oracle_AIX_V3.7.3.tar)		
		KSignSecureDB DBAgent For Tibero_AIX V3.7.3 (KSDBV37-DBAgent_For_Tibero_AIX_V3.7.3.tar		
	KSignSecure DB APIAgent	KSignSecureDB APIAgent For JAVA_AIX V3.7.3 (KSDBV37-APIAgent_For_API_JAVA_AIX_V3.7.3.tar)		
Manual	Preparative procedure	KSignSecureDB V3.7 Preparative procedure V1.3 (KSignSecureDB V3.7 Preparative procedure V1.3.pdf)	File (PDF)	
	Operation Guide	KSignSecureDB V3.7 Operation Guide V1.3 (KSignSecureDB V3.7 Operation Guide V1.3.pdf)		

[Table 6] Physical scope of TOE

Validated cryptographic modules included the TOE are as follows.

Item	Description
Cryptographic module name	KSignCASE64 v2.5.2.0

Developer	KSign Co., Ltd
Validation date	2023. 10. 16.
Validation level	VSL1
Validation number	CM-237-2028.10
Expiration Date	2028. 10. 16.

[Table 7] Validated Cryptographic modules

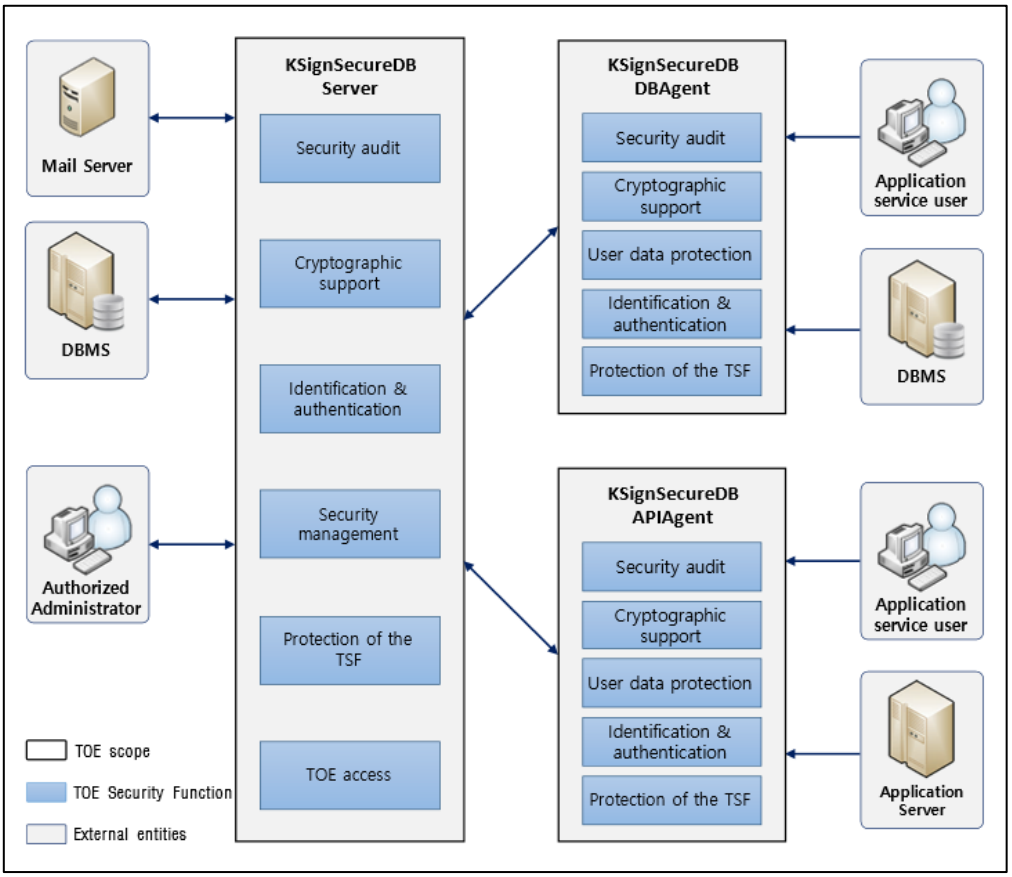
The 3rd Party libraries included in TOE is as follows.

TOE	Library	Usage
KSignSecureDB Server	ojdbc8.jar	Library for KSignSecureDB DBAgent For Oracle_AIX to access the protected DBMS
	tibero7-jdbc.jar	Library for KSignSecureDB DBAgent For Tibero_AIX to access the protected DBMS
	log4j-core-2.23.1.jar log4j-api-2.23.1.jar	Library used for generating temporary audit log files
KSignSecureDB DBAgent	log4j-core-2.23.1.jar log4j-api-2.23.1.jar	Library used for generating temporary audit log files
KSignSecureDB APIAgent	log4j-core-2.23.1.jar log4j-api-2.23.1.jar	Library used for generating temporary audit log files

[Table 8] 3rd party software required for TOE operation

2. Logical Scope of TOE

The logical scope of the TOE is as in [Figure 3] below.



[Figure 3] TOE Logical scope

▣ Security Audit

KSignSecureDB Server provides a means that enables only the authorized administrator to view the audit information and provides the audit information in an understandable form. If an auditable event occurs, it generates the audit data, detects a potential security violation and sends an alert mail to the authorized administrator. Furthermore, it provides the function of storing all audit data generated by KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent in the audit trail storage(DBMS) to manage them securely; preventing the audit data from unauthorized deletion; If the audit trail exceeds 80% of the audit storage capacity, an alert mail is sent to the authorized administrator, and when the audit trail is full, it provides a function to protect the audit trail storage by ignoring audited events.

▣ Cryptographic support

KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent generate and destroy all cryptographic keys used for the operation of the product in a secure manner through the validated cryptographic module KSignCASE64 v2.5.2.0 whose safety and suitability for the implementation have been confirmed by the cryptographic module validation scheme, and performs cryptographic operation in accordance with the user data cryptographic policy that defines the cryptographic algorithm, and performs cryptographic operation for confidentiality and integrity of the TSF data. It destroys cryptographic keys from memory after encryption and decryption. In addition, it generates and distribute cryptographic keys using the validated cryptographic module KSignCASE64 v2.5.2.0 for secure communication between KSignSecureDB Server and KSignSecureDB DBAgent/KSignSecureDB APIAgent that are physically separated.

- Cryptographic key generation:
  - HASH_DRBG (SHA256, 256bit): Cryptographic key generation for the encryption/decryption of the TSF data, the encryption/decryption of the user data and the encryption/decryption of the cryptographic key (policy key)
  - RSAES (2048bit): Asymmetric key generation for the encryption/decryption of the master key and KSign-implemented secure communication
  - PBKDF(HMAC(SHA256)): Key generation for the protection of the TSF data encryption key
- Cryptographic key distribution
  - RSAES (2048bit): Encryption/Decryption of the session key to transmit the data between KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent in case of the KSign-implemented secure communication
- Cryptographic operation
  - Encryption/Decryption of symmetric key (SEED-CBC, 128bit): Encryption/Decryption of the TSF data and the user data
  - Encryption/Decryption of symmetric key (ARIA-CBC, 128bit/192bit/256bit): Encryption/Decryption of the user data
  - One-way encryption (SHA256): Encryption of the user data, encryption of the TSF data and integrity verification
  - One-way encryption (SHA512): Encryption of the user data

- Encryption/Decryption of asymmetric key (RSAES, 2048bit): Encryption/Decryption of the master key

- Cryptographic key destruction
  - The cryptographic key information in the memory is deleted after the update with 0x00 if KSignSecureDB DBAgent and KSignSecureDB APIAgent are shut down.
  - The cryptographic key information is deleted by updating the temporarily stored cryptographic key information with 0x00 after sending the cryptographic key from KSignSecureDB Server to KSignSecureDB APIAgent and KSignSecureDB DBAgent.

▣ User data protection

KSignSecureDB DBAgent and KSignSecureDB APIAgent provide the function of encrypting/decrypting the data stored in the DBMS under the protection by the unit of column by using KSignKACE64 v2.5.2.0, a validated cryptographic module, and generates different ciphertext values for the same plaintexts. When performing encryption, the original data is deleted, and when decryption is performed, the encrypted data is deleted, so that the previous information content is not available.

▣ Identification and authentication

KSignSecureDB Server provides the function of performing the identification and authentication of the administrator who intends to use the security management function before the administrator initiates any behavior, masking with (●) when the authentication data are entered and protecting the authentication feedback. Furthermore. it provides the secure identification and authentication function by inactivating the authentication for 5 minutes and sending alert mail to administrator in case of 5 continuous failures in authentication attempts. It also prevents the reuse of authentication data of the administrator who logs on to KSignSecureDB Server.

KSignSecureDB Server provides the mechanisms to verify that the user password verification meets the following defined metrics. A password must have a combination of three or more among English alphabets, numbers and special characters.

KSignSecureDB Server and KSignSecureDB DBAgent/KSignSecureDB APIAgent perform the mutual authentication through a KSign-implemented protocol.

▣ Security Management

KSignSecureDB Server provides the security management function including the access control policy management, the administrator management and KSignSecureDB Server configuration for the authorized administrator. The authorized administrator carries out the management function through the security management interface.

The authorized administrator includes supervisor, policy administrator, system administrator, encryption administrator and audit record review administrator. The roles of the authorized administrator provided by KSignSecureDBServer are as follows.

- Supervisor: The top administrator has the privilege of system management, policy management, establishing and performing the table encryption/decryption and viewing audit record, and can create lower-level administrators other than supervisor.
- System administrator: The system administrator has the privilege of system management menu, generation, deletion and modification of the administrator and system configuration.
- Policy administrator: The policy administrator has the privileges of target DBMS management and key(policy) registration.
- Encryption administrator: The encryption administrator has the privilege of establishing and performing the table encryption.
- Audit record review administrator: The audit record review administrator has the privilege of reviewing the audit records.

It is enforced that the authorized administrator changes the password when the authorized administrator accesses to the security management interface. for the first time.

▣ Protection of the TSF

KSignSecureDB Server ensures the confidentiality and the integrity of the TSF data transmitted from/to KSignSecureDB DBAgent and KSignSecureDB APIAgent that are physically separated, through the encryption communication. KSignSecureDB Server runs a suite of self-tests to check the process status during initial start-up and periodically during normal operation to demonstrate that it remains in the safe condition and its security functions are in correct operation. It also verify the integrity of the TSF data and TSF executable codes, which are subject to the integrity verification during initial start-up, periodically during normal operation and when the authorized administrator request.

KSignSecureDB DBAgent and KSignSecureDB APIAgent loads TSF data for the encryption communication and mutual authentication upon the start-up. After the mutual authentication succeeds, the integrity information is sent to KSignSecureDB Server to verify the integrity against the integrity information registered inside the Server. Integrity verification is performed not only during initial start-up but also on request by authorized administrators. Furthermore, Self-tests is performed to check the process status during initial start-up and periodically during normal operation to ensure that it remains in the safe condition and its security functions are in correct operation.

KSignSecureDB Server, KSignSecureDB DBAgent and KSignSecureDB APIAgent manage the administrator authentication information, integrity verification information, KSignSecureDB Server and KSignSecureDB DBAgent/KSignSecureDB APIAgent information and so forth by storing them in the DBMS in secure manner or by storing with encryption to protect the TSF data.

▣ TOE access

In case of the management access session by administrator allowed to access perform the security management functions for KSignSecureDB Server, the maximum number of concurrent sessions is limited to one.
If the supervisor is log-in, a lower-level administrator is not allowed to access. If the supervisor accesses while a lower-level administrator is log-in, the access by a lower-level administrator is cancelled. Furthermore, if an access attempt is made with the account which is the same as the supervisor account, the preceding access is cancelled.
In case of log-in with the account or the privilege which is the same as that of a lower-level administrator, the preceding access is cancelled. In addition, the administrator session is terminated after a specified time interval of inactivity (10 minutes).
In this case, a lower-level administrator refers to the system administrator, the policy administrator, the encryption administrator and the audit record review administrator, except for the supervisor.
In case of all administrators, access sessions are restricted in accordance with the accessible IP rules, and the management access sessions are allowed only on the terminals (two or less) that have IPs designated as accessible. Audit data are generated regarding the execution result of the session restriction in the security management interface.

6. Documentation

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

Identification	Date
KSignSecureDB V3.7 Preparative Procedure V1.3 (KSignSecureDB V3.7 Preparative Procedure V1.3.pdf)	July 01, 2024
KSignSecureDB V3.7 Operation Guide V1.3 (KSignSecureDB V3.7 Operation Guide V1.3.pdf)	July 01, 2024

[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 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

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: KSignSecureDB V3.7 (V3.7.3)
- KSignSecureDB Server V3.7.3
- KSignSecureDB DBAgent For Oracle_AIX V3.7.3
- KSignSecureDB DBAgent For Tibero_AIX V3.7.3
- KSignSecureDB APIAgent For JAVA_AIX V3.7.3

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+).

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.

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.

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.

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.

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.

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.

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		
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 10] 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 authorized 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 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.
- In order to install and operate the TOE, it is recommended that developers of an application server should fully understand the guidance documents (the preparative procedures guidance and the operational user guidance).

11. Security Target

KSignSecureDB V3.7 Security Target V1.5 [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 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.

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.

Database Server
The database server defined in this PP refer to the server in which the DBMS managing the protected DB is installed in the organization that operates the TOE

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.

Data Encryption Key (DEK)
Key that encrypts and decrypts the data

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

Encryption

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

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Management access

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

Private Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm

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

Random bit generator

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic

and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a “seed key,” and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Secret Key

A cryptographic key which is used in an symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

Session Key

Key generated from the validated cryptographic module and used during secure communication between KSignSecureDB Server and KSignSecureDB DBAgent or APIAgent

Master Key

Key generated from the validated cryptographic module. It is generated on KSignSecureDB Server upon the initial start-up of the product. The generated Master

Key is encrypted with the public key, and then stored in the DBMS so that it is managed securely.

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.

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 Database Encryption V1.1, December 11, 2019

[4] KSignSecureDB V3.7 Security Target V1.5, July 25, 2024

[5] KSignSecureDB V3.7 Independent Testing Report(ATE_IND.1) V2.00, July 29, 2024

[6] KSignSecureDB V3.7 Penetration Testing Report(AVA_VAN.1) V2.00, July 29, 2024