KECS-CR-23-04

PrivacyDB V2.1

Certification Report

Certification No.: KECS-CISS-1210-2023

2023. 1. 10.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.01.10.	-	Certification report for PrivacyDB V2.1 - First documentation

This document is the certification report for PrivacyDB V2.1 of OWL Systems Inc.

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 certification body on the results of the evaluation of PrivacyDB V2.1 of OWL Systems Inc. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

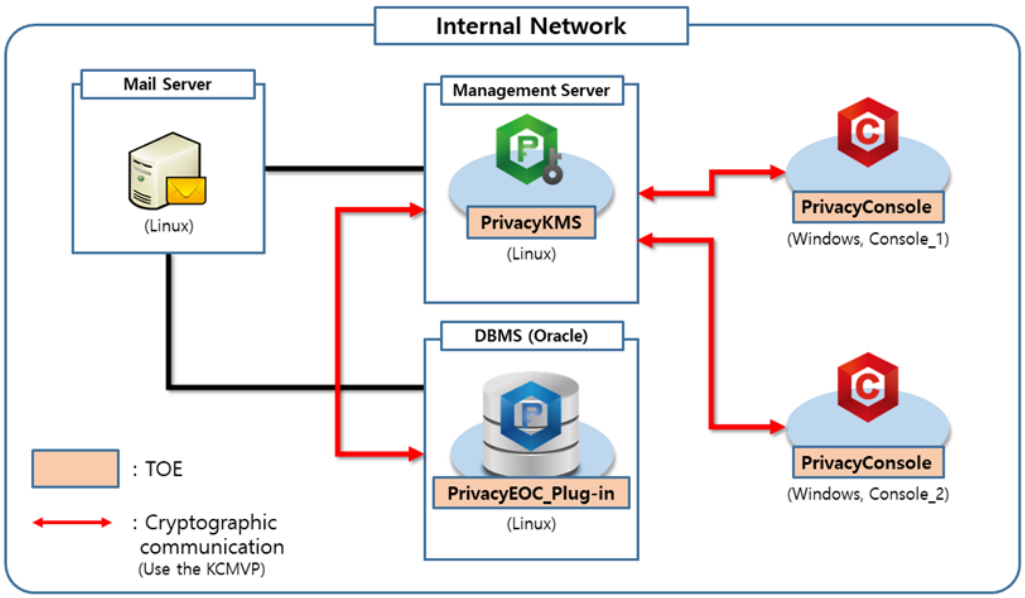
The Target of Evaluation (TOE) is database encryption software to prevent the unauthorized disclosure of confidential information by encrypting the database. The TOE consists of four components that are PrivacyKMS, PrivacyEOC_API, PrivacyEOC_Plug-in, and PrivacyConsole. PrivacyKMS and PrivacyConsole allow authorized administrators to manage security functions and TSF data such as cryptographic operation policies and keys. PrivacyEOC_API and PrivacyEOC_Plug-in are agents that encrypt and decrypt the user data based on the policies. The TOE includes cryptographic module (Key# Crypto v1.4) validated under the Korea Cryptographic Module Validation Program (KCMVP).

There are four types of the TOE operational environments: plug-in (EOC and KMS separated/integrated) and API(EOC and KMS separated/integrated) types. In the plug-in type, PrivacyEOC_Plug-in is installed in a database server, while the component PrivacyEOC_API is installed in an application server in the API type. Regardless of the types, PrivacyKMS and PrivacyConsole are installed on the physically separated systems. Note that PrivacyKMS is installed in the same server where PrivacyEOC is installed in the ‘EOC and KMS integrated type’.

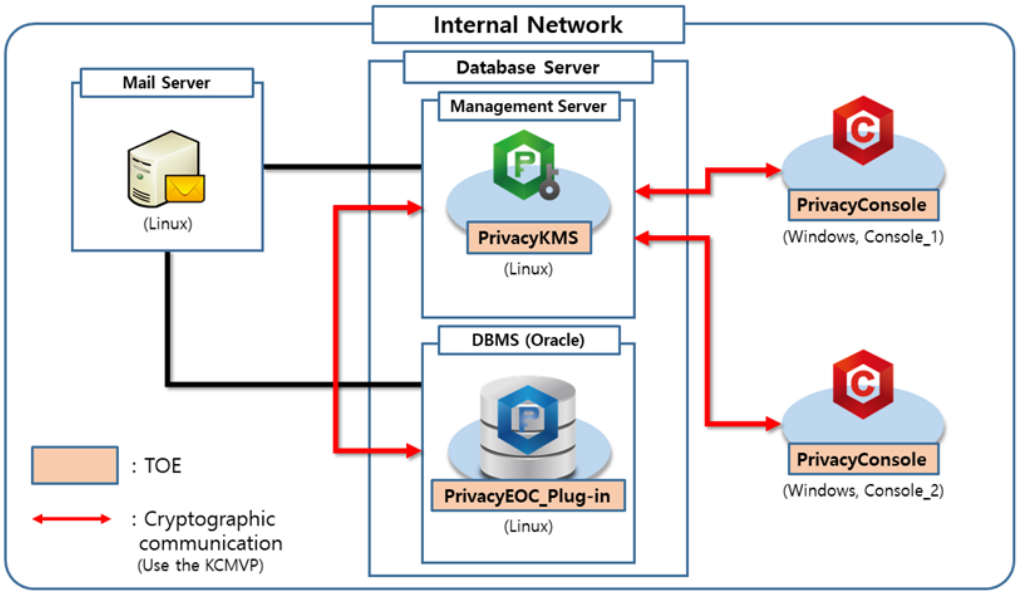
The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on 10 January 2023. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [5] and the Security Target (ST) [6].

The ST claims strict conformance to Korean National Protection Profile for Database Encryption V1.1 [7]. 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 [7]. 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 newly defined components in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

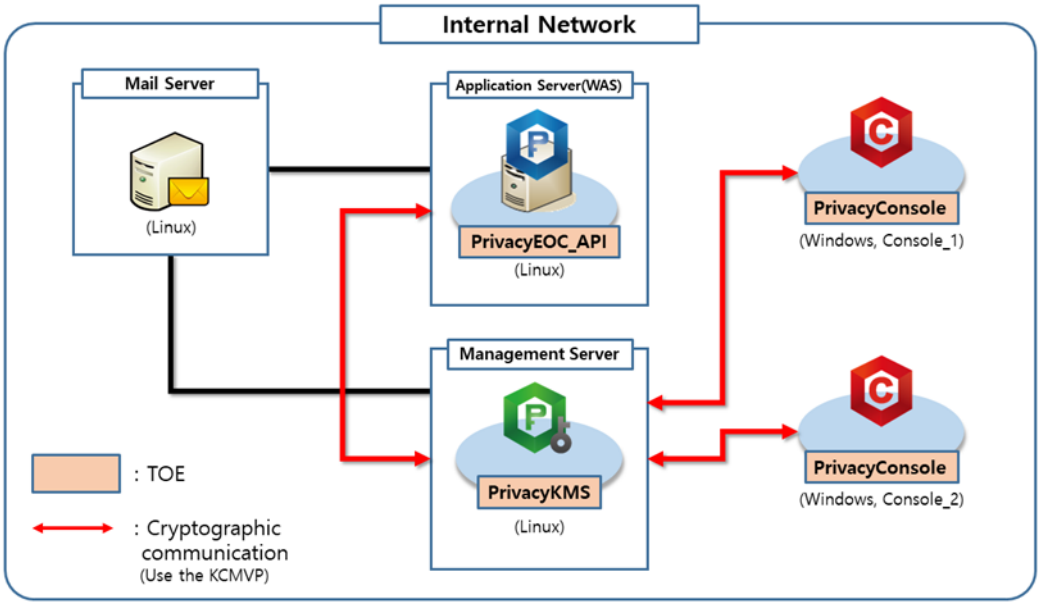
[Figure 1] to [Figure 4] show the operational environment of the TOE.



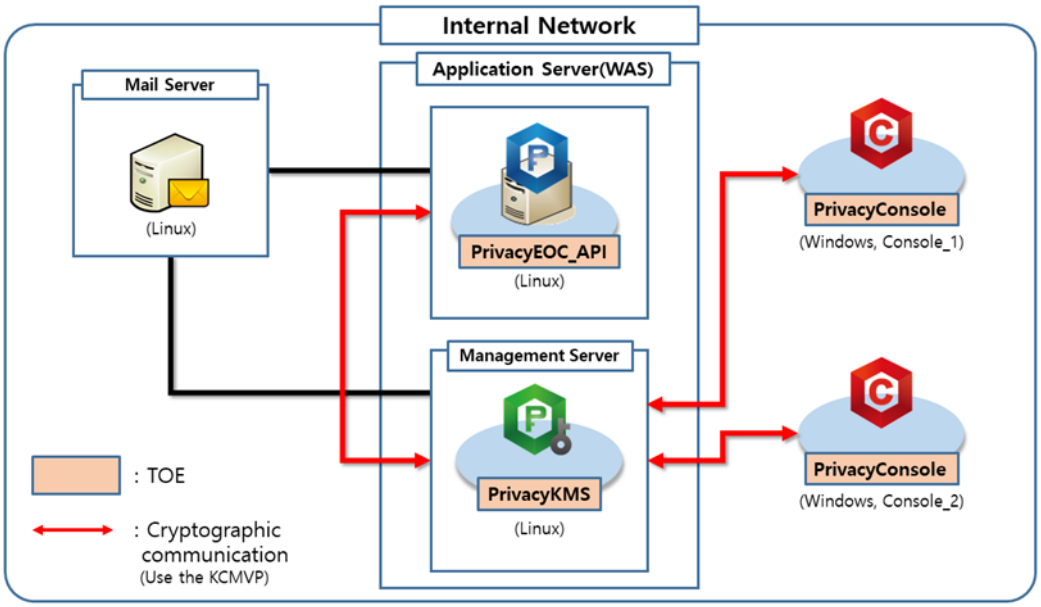
[Figure 1] Plug-in type operational environment of the TOE (EOC and KMS separated type)



[Figure 2] Plug-in type operational environment of the TOE (EOC and KMS integrated type)



[Figure 3] API type operational environment of the TOE (EOC and KMS separated type)



[Figure 4] API type operational environment of the TOE (EOC and KMS integrated type)

[Table 1] shows minimum hardware and software requirements necessary for installation and operation of the TOE.

Category		Contents
PrivacyKMS	CPU	Intel Dual core 2.4 GHz or higher
	Memory	8 GB or higher
	HDD	30GB or higher space for installation of PrivacyKMS
	NIC	10/100/1000 Mbps * 1 Port or more
	OS	Ubuntu 16.04.6 LTS 64 bit (GNU/Linux 4.4.0-142-generic x86_64)
	Required S/W	PostgreSQL 12.13
PrivacyEOC_API	CPU	Intel Dual core 2.4 GHz or higher
	Memory	8 GB or higher
	HDD	30GB or higher space for installation of PrivacyEOC_API
	NIC	10/100/1000 Mbps * 1 Port or more
	OS	Ubuntu 16.04.6 LTS 64 bit (GNU/Linux 4.4.0-142-generic x86_64)
PrivacyEOC_Plug-in	CPU	Intel Dual core 2.4 GHz or higher
	Memory	8 GB or higher
	HDD	30GB or higher space for installation of PrivacyEOC_Plug-in
	NIC	10/100/1000 Mbps * 1 Port or more
	OS	Ubuntu 16.04.6 LTS 64 bit (GNU/Linux 4.4.0-142-generic x86_64)
	Required S/W	Oracle Database 11g Release 2 (11.2)
PrivacyConsole	CPU	Intel Dual core 2.4 GHz or higher
	Memory	8 GB or higher
	HDD	30GB or higher space for installation of PrivacyConsole
	NIC	10/100/1000 Mbps * 1 Port or more
	OS	Windows 10 Pro 64 bit
	Required S/W	Java JRE 8u351

[Table 1] Hardware and software requirements for the TOE

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	PrivacyDB V2.1	
Version	PrivacyDB V2.1.0.44	
TOE Components	PrivacyKMS	PrivacyKMS V2.1.0.11 (PrivacyKMS_linux_64bit_V2.1.0.11.tar)
	PrivacyConsole	PrivacyConsole V2.1.1.11 (PrivacyConsole_x64_V2.1.1.11.zip)
	PrivacyEOC_API	PrivacyEOC_API V2.1.0.11 (PrivacyEOC_API_linux_64bit_V2.1.0.11.tar)
	PrivacyEOC_Plug-in	PrivacyEOC_Plug-in V2.1.0.11 (PrivacyEOC_Plug-in_linux_64bit_V2.1.0.11.tar)
Guidance Document	PrivacyDB V2.1 Preparative Procedures V1.7 (PrivacyDB V2.1 Preparative Procedures V1.7.pdf) PrivacyDB V2.1 User Operational Guidance V1.7 (PrivacyDB V2.1 User Operational Guidance V1.7.pdf)	

[Table 2] 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 Scheme for IT Security (May 17, 2021)

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, KECS-PP-0820a-2017, 11 December 2019
Developer	OWL Systems Inc.
Sponsor	OWL Systems Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	January 10, 2023
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The ST [6] for the TOE claims strict conformance to Korean National Protection Profile for Database Encryption V1.1 [7], and complies security policies defined in the PP [7] by security requirements. Thus, the TOE provides security features defined in the PP [7] as follows:

- Security audit: The TOE generates audit records of security relevant events including the start-up/shutdown of the audit functions, integrity violation and self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic operations such as encryption/decryption and hash, and cryptographic key managements such as key generation/distribution/destruction using cryptographic module (Key# Crypto v1.4) 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 perform password-based identification and authentication for PrivacyConsole. The TOE also mutually authenticates TOE components when they communicate each other.
- Security management: Security management of the TOE is restricted to only

the authorized administrator who can access the management interface provided by TOE.

- Protection of the TSF: The TOE provides secure communications between 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. The TOE 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 section in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [7] 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 [6], chapter 3.):

5. Architectural Information

The TOE is software consisting of the following four components:

- PrivacyKMS provides security features of identification and authentication of an administrator, cryptographic key generation for user data encryption.
- PrivacyConsole provides security features of identification and authentication of administrators. PrivacyConsole also provides management interface to an authorized administrator,
- PrivacyEOC_API and PrivacyEOC_Plug-in encrypt and decrypt the user data in a column of a database.

Note that all the three components perform the functionalities of audit data generation, cryptographic key management, cryptographic operations, protection of TSF data, and mutual authentication between the components. For the detailed description on the architectural information, refer to the ST [6], Chapter 1.4.2.

6. Documentation

The following documentations are evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
PrivacyDB V2.1 Preparative Procedures V1.7	V1.7	December 4, 2022
PrivacyDB V2.1 User Operational Guidance V1.7	V1.7	December 4, 2022

[Table 4] Documentation

7. TOE Testing

The developer took a testing approach based on the SFRs defined in the ST [6]. Each test case includes the following information:

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

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, performed all tests provided by developer, 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 PrivacyDB V2.1 (version PrivacyDB V2.1.1.44). See table 3 for detailed information on the TOE components.
The TOE is installed from the CD-ROM distributed by OWL Systems Inc. After installing the TOE, the customer can check the TOE version using GUI interface to view each TOE component version. And the guidance documents listed in this report chapter 6, [Table 4] 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 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 it is 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 uniquely identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.
The configuration list includes the TOE and the evaluation evidence required by the SARs in the ST. Therefore, the verdict PASS is assigned to ALC_CMS.1.
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 developer has provided a high-level description of at least 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 TSF, 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, 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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.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		
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 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 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.

- Developers who make the encryption/decryption functions of the TOE interact with other applications or DBMSs should ensure that the functions are securely applied according to the guidance document provided with the TOE.

11. Security Target

PrivacyDB V2.1 Security Target V1.7 [6] 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
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
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
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 (24 August 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (17 May 2021)

[5] KOSYAS-2021-14 PrivacyDB V2.1 Evaluation Technical Report V1.00, 10 January 2022

[6] PrivacyDB V2.1 Security Target V1.7, 12 December 2022

[7] Korean National Protection Profile for Database Encryption V1.1 (KECS-PP-0820a-2017, 11 December 2019)