KECS-CR-25-08

PrivacyDB V3.0

Certification Report

Certification No.: KECS-CISS-1345-2025

2025. 5. 26.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025.5.26.	-	Certification report for PrivacyDB V3.0 - First documentation

This document is the certification report for PrivacyDB V3.0 of OWL Systems Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance Co., Ltd. (KOSYAS)

Table of Contents

1. Executive Summary

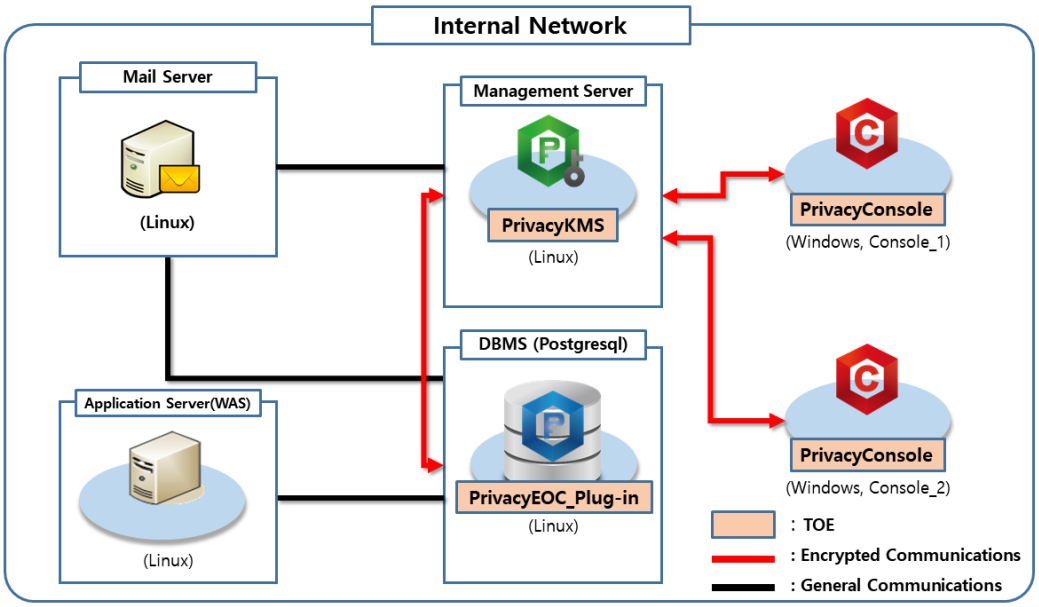
This report describes the certification result drawn by the certification body on the results of the EAL1+ evaluation of PrivacyDB V3.0 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is database encryption to prevent DBMS from unauthorized exposure of the information. The TOE also provides security features such as security audit, cryptographic key management and cryptographic operation using validated cryptographic module, user identification and authentication and mutual authentication between TOE components, security management, TSF data protection and self-protection, TOE access control.

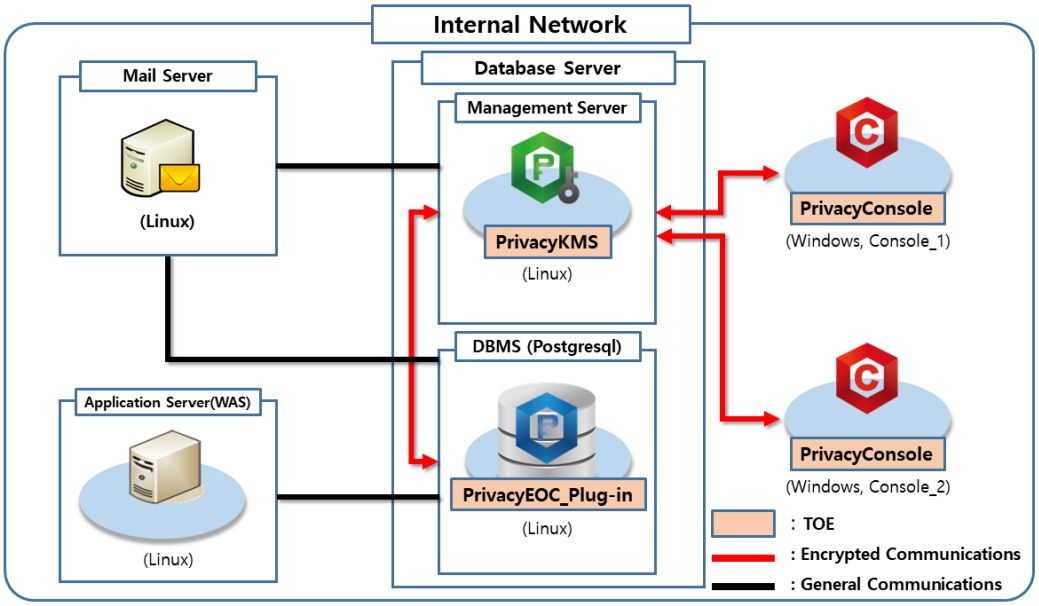
The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on 18 April 2024. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [6] and the security target (ST) [7][8].

The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V3.0 [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 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, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

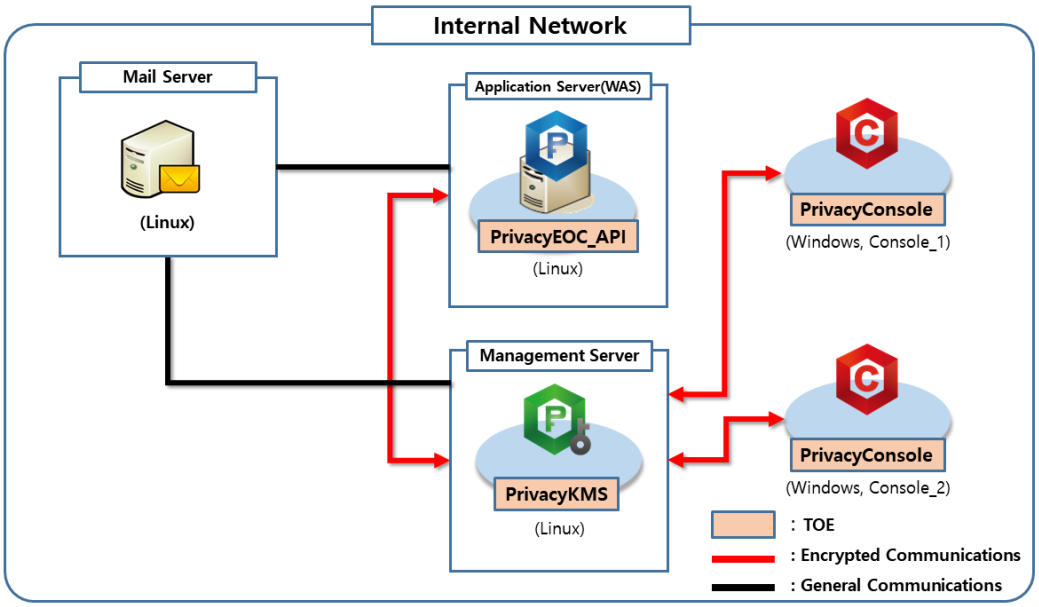
[Figure 1] and [Figure 2] show Plug-in type operational environments and [Figure 3] and [Figure 4] show API type operational environments, respectively. In each type of operational environment, PrivacyKMS can be installed on a server physically separate from PrivacyEOC_Plug-in or PrivacyEOC_API as shown in [Figure 1] or [Figure 3]. Alternatively, PrivacyKMS can be installed with PrivacyEOC_Plug-in on the DB server as shown in [Figure 2] or installed with PrivacyEOC_API on the Application server as shown in [Figure 4]. PrivacyConsole is installed in a user’s PC.



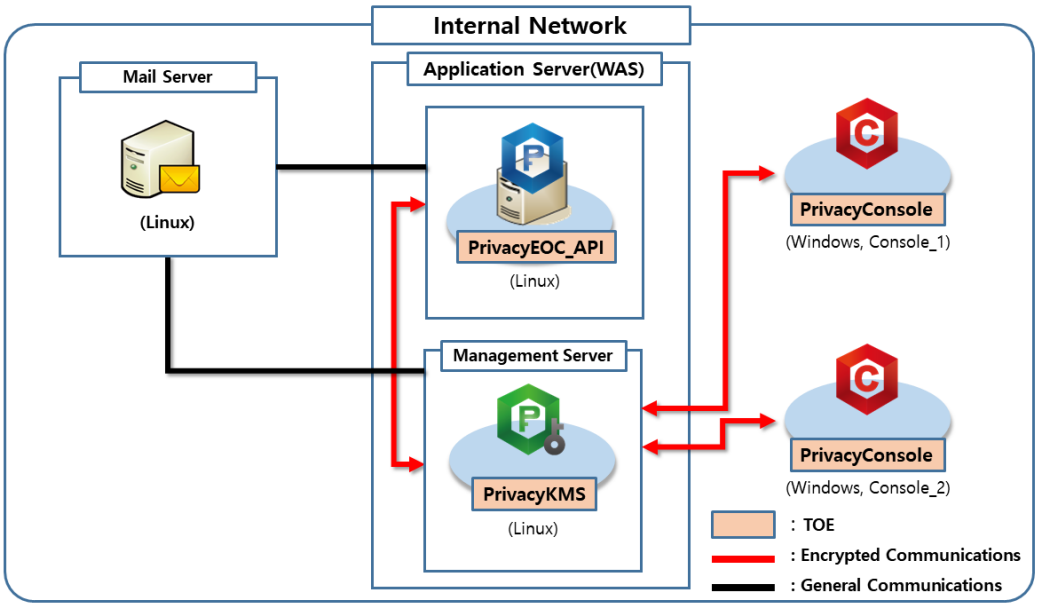
[Figure 1] Plug-in type operational environment (separate installation of PrivacyKMS)



[Figure 2] Plug-in type operational environment (collocated installation of PrivacyKMS)



[Figure 3] API type operational environment (separate installation of PrivacyKMS)



[Figure 4] API type operational environment (collocated installation of PrivacyKMS)

[Table 1] shows the hardware and software requirements to install and operate the TOE.

TOE Component		Requirement	
PrivacyKMS	HW	CPU	Intel Dual core 2.4 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for TOE installation is 30 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	Ubuntu Pro 16.04.6 LTS (kernel 4.4.0, 64 bit)
		DBMS	PostgreSQL 14.17
PrivacyEOC_Plug-in	HW	CPU	Intel Dual core 2.4 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for TOE installation is 30 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	Ubuntu Pro 16.04.6 LTS (kernel 4.4.0, 64 bit)
		DBMS to be protected	PostgreSQL 14.17
PrivacyEOC_API	HW	CPU	Intel Dual core 2.4 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for TOE installation is 30 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	Ubuntu Pro 16.04.6 LTS (kernel 4.4.0, 64 bit)
PrivacyConsole	HW	CPU	Intel Dual core 2.4 GHz or higher
		Memory	8 GB or higher
		HDD	Space required for TOE installation is 30 GB or higher
		NIC	100/1000 Mbps x 1 EA or higher
	SW	OS	Windows 10 Pro (64 bit)
		JRE	Java JRE 8u421

[Table 1] TOE Hardware and Software requirements

The 3rd party software included in the TOE are shown in [Table 2].

Component	3rd party S/W	Description
PrivacyKMS V3.0.0.1	OpenSSL V3.4.1	TSF Data Transfer
PrivacyEOC_API V3.0.0.1	OpenSSL V3.4.1	TSF Data Transfer
PrivacyEOC_Plug-in V3.0.0.1	OpenSSL V3.4.1	TSF Data Transfer
PrivacyConsole V3.0.0.1	OpenSSL V3.4.1	TSF Data Transfer
	zlib1 V1.3.1	Certificate Generator Compression Library

[Table 2] The 3rd party software included in 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 identified as follows.

TOE	PrivacyDB V3.0
TOE Version	V3.0.0.4
TOE Components	PrivacyKMS V3.0.0.1 - PrivacyKMS_linux_64bit_V3.0.0.1.tar
	PrivacyEOC_Plug-in V3.0.0.1 - PrivacyEOC_Plug-in_linux_64bit_V3.0.0.1.tar
	PrivacyEOC_API V3.0.0.1 - PrivacyEOC_API_linux_64bit_V3.0.0.1.tar
	PrivacyConsole V3.0.0.1 - PrivacyConsole_x64_V3.0.0.1.zip
Guidance	PrivacyDB V3.0 Preparative Procedures V1.1

Document	- PrivacyDB V3.0 Preparative Procedures V1.1.pdf
	PrivacyDB V3.0 User Operational Guidance V1.1 - PrivacyDB V3.0 User Operational Guidance V1.1.pdf

[Table 3] TOE identification

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, July, 2024
EAL	EAL1+ (augmented by ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Database Encryption V3.0, KECS-PP-1232-2023, April 27, 2023
Developer	OWL Systems Inc.
Sponsor	OWL Systems Inc.
Evaluation Facility	Korea System Assurance Co., Ltd. (KOSYAS)
Completion Date of Evaluation	April 18, 2025
Certification Body	IT Security Certification Center

[Table 4] 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 ST [7][8].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the chapter 3.1 of ST [7][8]):

- The TOE must be in a physically safe environment, and protected from unauthorized physical accesses.
- The authorized administrators of the TOE should not be malicious, and should be properly trained and perform their duties accurately according to administrator guidelines.
- Developers integrating the encryption function of the TOE into an application or DBMS should comply with the requirements specified in the guidance documents to ensure that the security function of the TOE is applied properly.
- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement work on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

Furthermore, some aspects of threats, and organizational security policies are not fulfilled by the TOE itself, thus these aspects are addressed by the TOE environment. Details can be found in the chapter 3.1 and 3.2 of ST [7][8].

The scope of this evaluation is limited to the functionality and assurance covered in ST [7][8]. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

5. Architectural Information

The TOE consists of PrivacyKMS, PrivacyConsole, PrivacyEOC_API, PrivacyEOC_Plug-in

and Guidance document. In the TOE components, the validated cryptographic module (OWLCrypto V1.0) is embedded for protection of user data and TSF data. The physical scope of the TOE and the information of validated cryptographic module are presented in [Table 5] and [Table 6], respectively.

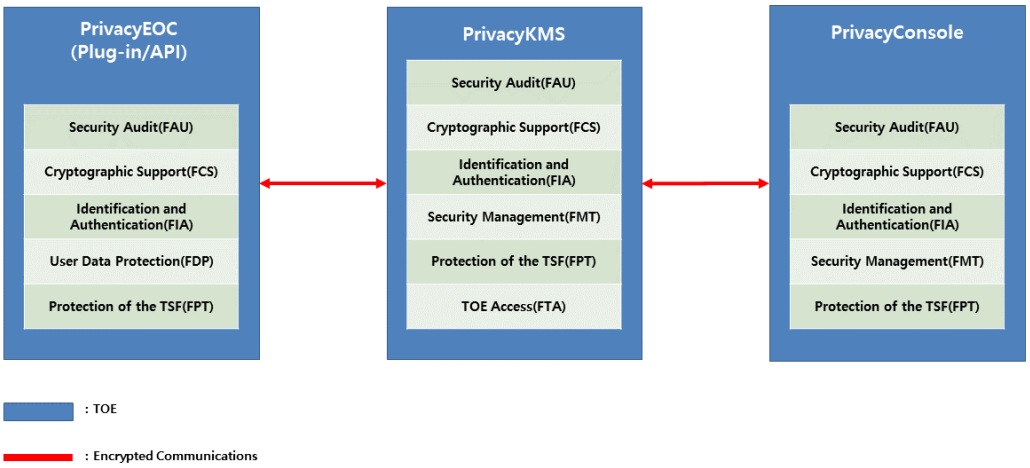
Category	Name	Type	Delivery
TOE	PrivacyDB V3.0	-	-
TOE version	V3.0.0.4	-	-
TOE Component	PrivacyKMS V3.0.0.1 - PrivacyKMS_linux_64bit_V3.0.0.1.tar	SW	CD
	PrivacyConsole V3.0.0.1 - PrivacyConsole_x64_V3.0.0.1.zip	SW	
	PrivacyEOC_API V3.0.0.1 - PrivacyEOC_API_linux_64bit_V3.0.0.1.tar	SW	
	PrivacyEOC_Plug-in V3.0.0.1 - PrivacyEOC_Plug-in_linux_64bit_V3.0.0.1.tar	SW	
Guidance Document	PrivacyDB V3.0 Preparative Procedures V1.1 - PrivacyDB V3.0 Preparative Procedures V1.1.pdf	PDF	
	PrivacyDB V3.0 User Operational Guidance V1.1 - PrivacyDB V3.0 User Operational Guidance V1.1.pdf	PDF	

[Table 5] Physical Scope of TOE

Category	Description
Cryptographic module name	OWLCrypto V1.0
Validation No.	CM-241-2028.12
Developer	OWL Systems Inc.
Module type	S/W(library)
Validation date	22 Dec 2023
Expiration Date	22 Dec 2028

[Table 6] Validated Cryptographic Module

The logical scope of the TOE is depicted in [Figure 5].



[Figure 5] Logical Scope of TOE

- Security Audit (FAU)

Each TOE component (PrivacyConsole, PrivacyKMS, PrivacyEOC_Pluig-in, Privacy EOC_API) generates audit data and transmits it to PrivacyKMS, and then PrivacyKMS stores the transmitted audit data in the DBMS. The audit data includes the date and time of the event, the type of the event, the identity of the subject, and the event result.

PrivacyKMS sends an alert mail to the email address registered by the administrator when audit data is generated indicating potential security violations such as administrator continuous authentication failure, integrity violation, and KCMVP self-test failure.

The stored audit data can be viewed only by an authorized administrator through the PrivacyConsole.

PrivacyKMS periodically monitors the audit data storage, and when the number of audit logs reaches 90% of the specified threshold, it generates an audit log indicating the threshold has been exceeded and sends an alert email to the authorized administrator. When the audit data storage reaches 100% capacity, PrivacyKMS generates an audit log indicating storage saturation and sends an alert email to the authorized administrator. PrivacyKMS also overwrite the oldest audit data to ensure that the latest audit data is stored.

- Cryptographic support (FCS)

The TOE supports cryptographic key management, cryptographic operation, and

random bit generation. The encryption key generation for encryption of user data and TSF data is generated using HASH_DRBG(SHA256), which is a random bit generator of the validated cryptographic module.

KEK with key legnth of 256 bit is generated through Password-Based Encryption Key Derivation (PBKDF) in accordance with the PKCS#5 standard.

When encrypting and decrypting user data stored in the DBMS that TOE wants to protect, the encryption and decryption operation is performed using ARIA-256 of the the validated cryptographic module (KCMVP). In addition, it protects user data using a one-way hash algorithm such as SHA-256, 512.

Algorithm	Key Length
ARIA (CBC)	256
SHA-256	N/A
SHA-512	N/A

[Table 7] User Data Encryption Algorithm

Additionally, To protect TSF Data, the algorithms in [Table 8] of the validated cryptographic module are used.

Algorithm	Key Length	Operation List
ARIA	256	TSF data Encryption
		TSF Data Encryption Key Encryption
		User Data Encryption Key Encryption
RSAES	2048	Distribution CipherKey
SHA256	N/A	Administrator password encryption
		Policy File intergrity Verification
RSA-PSS	2048	Mutual Authentication, Module and Configuration Integirty verification

[Table 8] TSF Data Encryption algorithm

To desctruct the encryption key, the TOE sanitizes the memory by zerorizing three times according to the encryption key destruction procedure used internally.

Details of the The validated cryptographic module (KCMVP) that provides the random number generator used by TOE are as follows.

When using a random number generator, noise output from entropy sources is collected and composed through /dev/urandom and time jitter. Each noise source

undergoes health tests using the Repetition Count Test (RCT) and the Adaptive Proportion Test (APT). Since the final collection of seed contains sufficient entropy, the conditioning process is omitted.
After each entropy source is validated through health-tests, the output from entropy sources are just concatenated to contruct the final entropy.

- User data protection (FDP)

In order to protect user data stored in the DBMS, block encryption algorithms (ARIA-256) are encrypted and decrypted according to the security policy set by the authorized administrator through the validated cryptographic module. In addition, one-way hash algorithms (SHA-256/512) are also supported. After the encryption/decryption process, the TOE performs sanitization to ensure that plaintext user data cannot be restored.
PrivacyEOC_Plug-in, PrivacyEOC_API provides a function of encrypting and decrypting user data by column, and prevents the same ciphertext from being generated for the same plaintext when encrypting user data.

- Identification and authentication (FIA)

PrivacyKMS performs the identification and authentication based on user ID and password. All TOE management functions cannot be used before user authentication is performed.
When authenticating a user, password input is protected against exposure by displaying only blank or masking characters. When authentication fails, the TOE does not provide reason for failure. It also protects against authentication data reuse attacks by using sequence number during authentication. In case of continuous authentication failure, account is locked out for 5 minutes. It also sends alert mails to authorized administrators.
The password composition rules are as follows: passwords shall be between 10 and 40 characters in length, and shall include uppercase and lowercase English letters, numbers, and special characters. Passwords shall not contain more than four consecutive letters or numbers, and the same character shall not appear more than twice in a row. Passwords must not include the user account ID, and the previously used password shall not be reused for the next password.
The TOE performs mutual authentication among its components PrivacyKMS, PrivacyEOC_Plug-in, PrivacyEOC_API and PrivacyConsole using a certificate-based proprietary authentication protocol.

- Security Management (FMT)

The TOE defines a single administrative role and account for the administrator. The authorized administrator is the only user permitted to perform the management of TOE's security functionalities.

PrivacyConsole provides the GUI based management interface. PrivacyConsole provides a security management function including generation of a user data encryption key and inquiry of audit data.

The use of PrivacyConsole security management function is limited to the authorized administrator. It also enforces modification of the authorized administrator's password during the TOE installation process.

- Protection of the TSF (FPT)

The TOE encrypts data stored in the storage controlled by TSF using ARIA-256, provided by validated cryptographic module, in order to prevent its disclosure and modification. The TOE generates and stores integrity verification information using RSA-PSS and SHA-256 algorithms.

The TOE components (PrivacyKMS, PrivacyEOC_Plug-in, PrivacyEOC_API, Privacy Console) use TLS 1.3 standard protocol to protect data in transit.

The TOE monitors whether the main processes of the TOE operate normally through the TSF self-test. The TOE performs self-test at startup and periodically during normal operation (at every midnight), and send an alarm mail and generate audit data to the authorized administrator when the integrity verification of the configuration file and execution module fails at startup and periodically during normal operation(at every midnight).

The failure of the health tests of noise source during self-tests of the validated cryptographic module is probable to occur due to a transient fault in the noise source. In such cases, therefore, the random number generator maintains a secure state by retrying the test after a certain period of time.

- TOE access (FTA)

PrivacyConsole limits maximum number of simultaneous sessions to one by permitting administrative access only from terminals with IP addresses designated for connection and restricting concurrent logins by the same user.

Additionally, the TOE provides a session timeout mechanism that terminates the session if no activity is detected from an authorized administrator for a defined period (10 minutes) after successful login.

6. Documentation

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

Identifier	Release	Date
PrivacyDB V3.0 Preparative Procedures V1.1	V1.1	March 17, 2025
PrivacyDB V3.0 User Operational Guidance V1.1	V1.1	March 17, 2025

[Table 9] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [9], 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 to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [7]. 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 [10].

8. Evaluated Configuration

The TOE is PrivacyDB V3.0 (V3.0.0.4). See [Table 3] for details 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 display thev version of each TOE component. The guidance documents listed in [Table 9] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote 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 of EAL1+.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problems that the TOE and operational environment are intended to address. Therefore, the verdict PASS is assigned to ASE_SPD.1

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to

ASE_TSS.1.
Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.
The verdict PASS is assigned to the assurance class ASE.

9.2 Development Evaluation (ADV)

The functional specifications specify a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.
The verdict PASS is assigned to the assurance class ADV.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.
The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g., those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.
The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.
Also, the evaluator confirmed that the correct version of the software is installed in device.
The verdict PASS is assigned to the assurance class ALC.

9.5 Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore, the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore, the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g., by flaw hypotheses), don't allow attackers possessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
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 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 developers integrating the encryption function of the TOE into an application or DBMS should comply with the requirements specified in the guidance documents to ensure that the security function of the TOE is applied properly.

11. Security Target

PrivacyDB V3.0 Security Target V1.1[7] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [8] according to the CCRA supporting document ST sanitizing for publication [11].

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

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November, 2022
Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, July, 2024

[2] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, CCMB-2022-11-006, November, 2022
Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, July, 2024

[3] Korea Evaluation and Certification Guidelines for IT Security (31 October 2022)

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

[5] Korean National Protection Profile for Database Encryption V3.0, KECS-PP-1232-2023, April 27, 2023

[6] PrivacyDB V3.0 Evaluation Technical Report V1.00, 18 April 2025

[7] PrivacyDB V3.0 Security Target V1.1, 17 March 2025 (Confidential Version)

[8] PrivacyDB V3.0 Security Target V1.1, 17 March 2025 (Sanitized Version)

[9] PrivacyDB V3.0 Independent Testing Report(ATE_IND.1) V1.00, 17 April 2025

[10] PrivacyDB V3.0 Penetration Testing Report (AVA_VAN.1) V1.00, 17 April 2025

[11] ST sanitizing for publication, CCDB-2006-04-004, April 2006