KECS-CR-24-55

D’Guard v5.0

Certification Report

Certification No.: KECS-CISS-1333-2024

2024. 10. 25.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024. 10. 25.	-	Certification report for D'Guard v5.0 - First documentation

This document is the certification report for D'Guard v5.0 of INEB 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 D'Guard v5.0 developed by INEB 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.

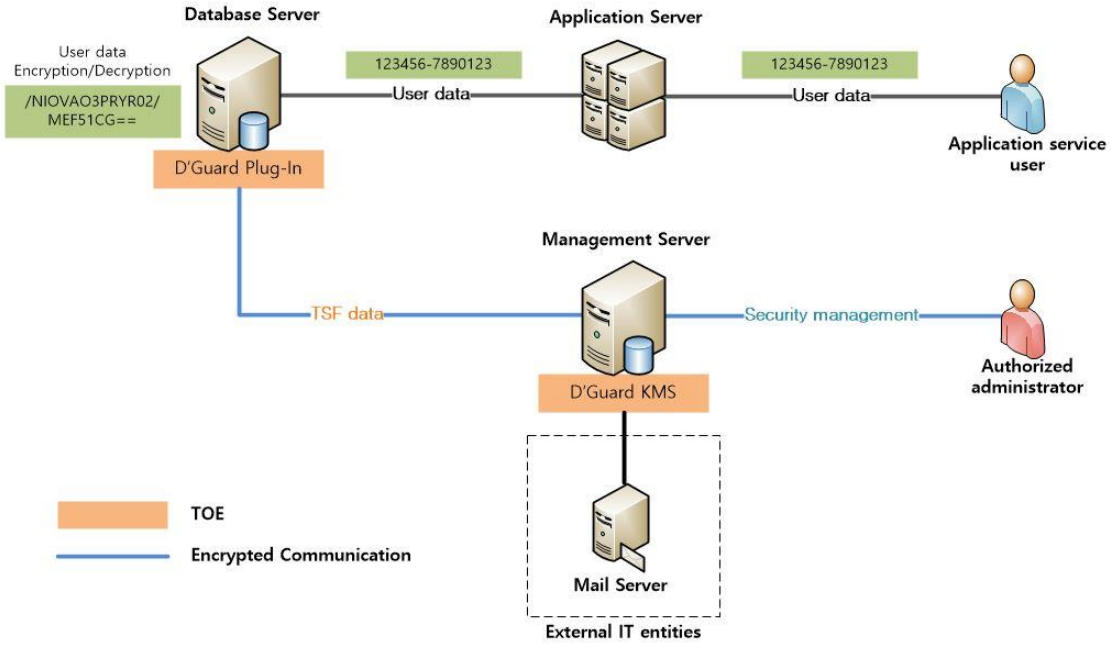
The Target of Evaluation (hereinafter referred to as "TOE") is database encryption software to prevent unauthorized exposure of the information from DBMS. Also, the TOE shall provide a variety of security features: security audit, cryptographic operation using cryptographic module, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on October 21, 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 operational environment defined in ST can be classified into two: plug-in type and API type.

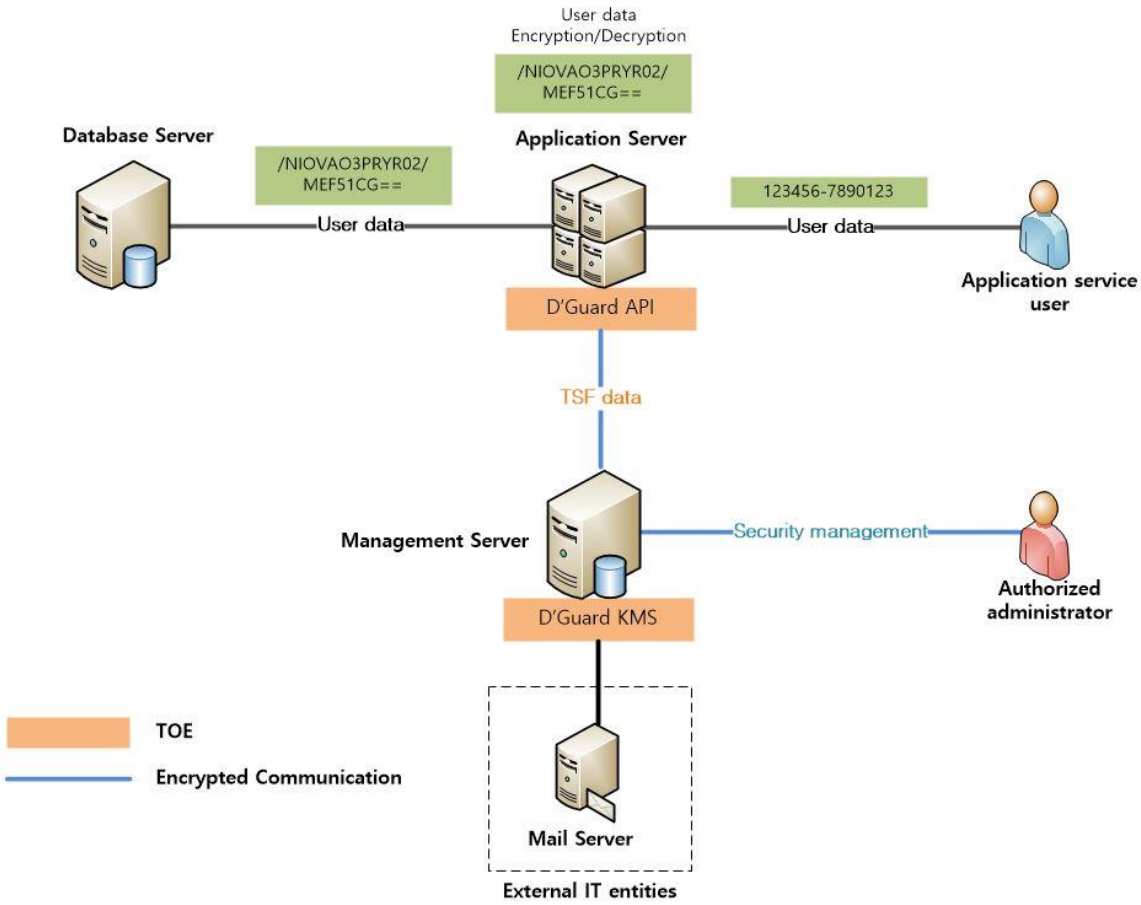
[Figure 1] shows the general operational environment of the plug-in type. The agent (D'Guard Plug-In), which is installed in the protected database server of the DB, encrypts the user data received from the application server before storing it in the DB according to the policy configured by the authorized administration, and decrypts the encrypted user data sent form the database server to the application server. Since the plug-in type is installed in the protected database to perform encryption/ decryption, the DBMS that can be installed and operated by the TOE is limited to Oracle 19.3 and Tibero 7.



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

The authorized administrator performs policy management distributed to D'Guard Plug-In according to the scope required by the organizations security policy through D'Guard KMS. In addition, the authorized administrator can perform security management through access to the management server.

[Figure 2] shows the general operational environment of the API type. The application, which is installed in the application server and provides application services, is developed using the D'Guard API provided by API module in order to use the cryptographic function of the TOE. The D'Guard API module is installed in the application server and performs encryption/decryption of the user data in accordance with the policies configured by authorized administrator. The user data entered by the application service user is encrypted by D'Guard API module, which is installed in the application server, and sent to the database server. The encrypted user data received from the database server is decrypted by the D'Guard API module, which is installed in the application server, and sent to the application service user.



[Figure 2] API type operational environment of the TOE
(API, Management Server separate type)

The authorized administrator performs policy management through the D'Guard KMS as an D'Guard API module according to the scope of the organization's security policy. In addition, the authorized administrator can perform security management through access to the management server.

The communication among the TOE components performs encrypted communication using the approved cryptographic algorithm of the validated cryptographic module, and the transmitted the TSF data includes security policy data and audit data transmitted from the agent. The self-implemented mutual authentication is performed when communicating among the TOE components.

The administrator accesses the management server through a web browser to perform security management functions. HTTPS (TLS 1.2), which implements a secure security protocol, is used for the communication section of the web environment-based

administrator. The communication section for management access is excluded from the evaluation scope

As an external IT entity required to operate TOE, there is a Mail server for administrator notifications authorized when predicting audit data loss. TOE works with an external Mail server to send security alerts to administrators according to security policies defined by the 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	D'Guard v5.0
Version	v5.0.3
TOE Components	D'Guard KMS v5.0.1 D'Guard Plug-In v5.0.1 D'Guard API v5.0.1
Guidance Documents	D'Guard v5.0 KMS Preparatory document and user operation manual v1.2 D'Guard v5.0 Plug-In Preparatory document and user operation manual v1.2 D'Guard v5.0 API Preparatory document and user operation manual v1.2

[Table 1] TOE Identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)
TOE	D'Guard v5.0
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+ (augmented by ATE_FUN.1)
Protection Profile	Korea National Protection Profile for Database Encryption V1.1,

	KECS-PP-0820a-2017, Dec. 11, 2019 [3]
Developer	INEB Inc.
Sponsor	INEB Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	October 21, 2024
Certification Body	IT Security Certification Center

[Table 2] 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 1].)

5. Architectural Information

The physical scope of the TOE consists of D'Guard KMS, D'Guard Plug-In, D'Guard API and guidance documents. Verified Cryptographic Module (MagicJCrypto V3.0.0, INISAFE Crypto for C v5.4) is embedded in the TOE components.

The logical scope of the TOE is as follows:

- Security Audit (FAU)

The security audit function consists of generating audit data, inquiring audit data, analyzing and responding to potential security violations, and protecting audit data. The generation of audit data is generated by including the start and end of the TOE, the result of performing security management for the TOE of the authorized administrator, and audit data collected by the Plug-In agent and API module, and is generated including the date and time of the event, the type of the event, the identity of the subject, and the event result information.

The authorized administrator may selectively check the generated audit data by distinguishing the driving and termination of the TOE and user data encryption according to the optional AND condition, and the generated audit data is protected from unauthorized deletion.

The D'Guard KMS analyzes potential security violations, such as failure of administrator authentication sequence, sends alarm mail to authorized administrator and generates audit data. In addition, by analyzing violations of the threshold of the audit repository, when the primary threshold of 80% is exceeded, an alarm mail is sent to the authorized administrator, and when the secondary threshold of 90% is exceeded, an alarm mail is sent to the authorized administrator, and after deleting some of the oldest audit data, audit data is generated.

- 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.

The generated user data encryption key is encrypted and stored using ARIA256(KCMVP) in the policy DB and integrity verification information is stored together using HMAC-SHA256. For TSF data protection, ARIA256 and HMAC-SHA256 are used to store encryption and integrity verification information.

The management server receives a policy distribution request from the agent, encrypts the security policy including the user data encryption key with the RSAES 2048-bit algorithm of the verified encryption module, and safely distributes it.

TOE destroys the memory in the area in three zeroing procedures according to the encryption key destruction procedure used internally, including the user data encryption key.

- User data protection (FDP)

The TOE protects against unauthorized attacks by initializing all information used inside the TOE for cryptographic key generation, cryptographic key distribution, cryptographic operation, and random bit generation after use.

In order to protect user data stored in the DBMS to be protected, block encryption algorithms (ARIA-128/256, SEED-128, and LEA-128/256) are encrypted and decrypted according to the security policy set by the administrator authorized through the verified encryption module. In addition, one-way encryption is supported through hash algorithms (SHA-256/512). Once the encryption/decryption is completed, it performs initialization to prevent the restoration of the previous value of the original user data.

D'Guard Plug-In, D'Guard 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)

The D'Guard KMS 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 protects against exposure by displaying only blank or masking characters and does not provide reason for failure when authentication fails. It also protects against authentication reuse attacks by receiving one-time captcha during authentication. In case of continuous authentication failure, time delay is disabled

and account lockout is performed according to the set value to protect against unauthorized attack. It also sends alert mails to authorized administrators.

The password combination rule for authentication must be 10 or more and 20 or less digits, and must use three combinations of English characters/number and special characters. The character must not be more than 3 consecutive digits, and cannot be used even if the same character is more than 3 times. Account information should not be included, and the same password as the password used before 3 times cannot be used.

In order to secure the communication interval between TOE components, the management server and the agent exchange each communication encryption key after mutual authentication using the RSA 2048-bit public key pair, and then encrypt and transmit the security policy using ARIA256. Mutual authentication uses a self-implemented method based on public key cryptography.

- Security Management (FMT)

The TOE user is divided into super manager who manages all the security functions of the TOE and security user who can only perform the inquiry function of audit data and security policy. The security management function can be performed by authorized administrator only.

The D'Guard KMS provides a management function of a console CLI environment and a management function of a web GUI environment. The management function of the console CLI environment is used at the time of initial installation, and after that, it provides encryption and integrity verification data update functions for major information in the configuration file (TSF data). The management function of the web GUI environment provides a security management function including generation of a user data encryption key and inquiry of audit data.

The use of D'Guard KMS's security management function is limited to authorized administrators who have performed authentication. It also forces the authorized administrator's password to be initialized during the TOE installation process.

- Protection of the TSF (FPT)

The TOE encrypts using ARIA256, which is a verification algorithm of validated cryptographic module, in order to prevent exposure and modification of data stored in the

storage controlled by TSF. The TOE generates and stores integrity verification information using HMAC-SHA256 algorithm. In addition, the TOE encrypts using ARIA256, which is a verification algorithm of validated cryptographic module, to prevent the exposure and modification of transmission data between physically separated TOE components, and performs integrity verification using HMAC-SHA256 algorithm.

The TOE monitors whether the main processes of the TOE operate normally through the TSF's own tests. The TOE performs self-test periodically during startup and operation to send an alarm mail and generate audit data to the authorized administrator when the integrity verification of the configuration file and execution module fails during startup or after normal operation.

- TOE access (FTA)

The D'Guard KMS limits the maximum number of simultaneous sessions to one by using the administrative access sessions that attempted access from the terminal designated as accessible IP and limiting the simultaneous access of the same user.

Also, D'Guard KMS provides the function to terminate the session when the authorized administrator has not been active for a certain period of time after logging in.

6. Documentation

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

Identifier	Date
D'Guard v5.0 KMS Preparatory document and user operation manual v1.2 (D'Guard v5.0 KMS Preparatory documents and user operation manual v1.2.pdf)	September 17, 2024
D'Guard v5.0 Plug-In Preparatory document and user operation manual v1.2 (D'Guard v5.0 Plug-In Preparatory document and user operation manual v1.2.pdf)	September 17, 2024

Identifier	Date
D'Guard v5.0 API Preparatory document and user operation manual v1.2 (D'Guard v5.0 API Preparatory document and user operation manual v1.2.pdf)	September 17, 2024

[Table 4] 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 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 [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: D'Guard v5.0 (v5.0.3)

- D'Guard KMS v5.0.1
- D'Guard Plug-In v5.0.1
- D'Guard API v5.0.1

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 6 [Table 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation results in the ETR [7] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation results were 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 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 penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

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

The verdict **PASS** is assigned to the assurance class AVA.

9.7 Evaluation Results 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 5] Evaluation Results 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 carry out the audit data backup to prevent audit data loss.
- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

11. Security Target

D'Guard v5.0 Security Target v1.2 [4] is included in this report by reference.

12. Acronyms and Glossary

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

13. Bibliography

The evaluation facility has used the following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April, 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April, 2017

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

[4] D'Guard v5.0 Security Target v1.2, September 17, 2024

[5] D'Guard v5.0 Independent Testing Report(ATE_IND.1) V1.00, September 27, 2024

[6] D'Guard v5.0 Penetration Testing Report (AVA_VAN.1) V1.00, September 27, 2024

[7] D'Guard v5.0 Evaluation Technical Report (ETR) V2.00, October 21, 2024