KECS-CR-26-27

MagicDBPlus v2.1

Certification Report

Certification No.: KECS-CISS-1409-2026

2026. 7. 8.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2026. 7. 8.	-	Certification report for MagicDBPlus v2.1 - First documentation

This document is the certification report

for MagicDBPlus v2.1 of Dreamsecurity Co., Ltd.

The Certification Body

IT Security Certification Center (ITSCC)

The Evaluation Facility

Korea System Assurance, Inc. (KOSYAS)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the MagicDBPlus v2.1 developed by Dreamsecurity 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(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 June 26, 2026.

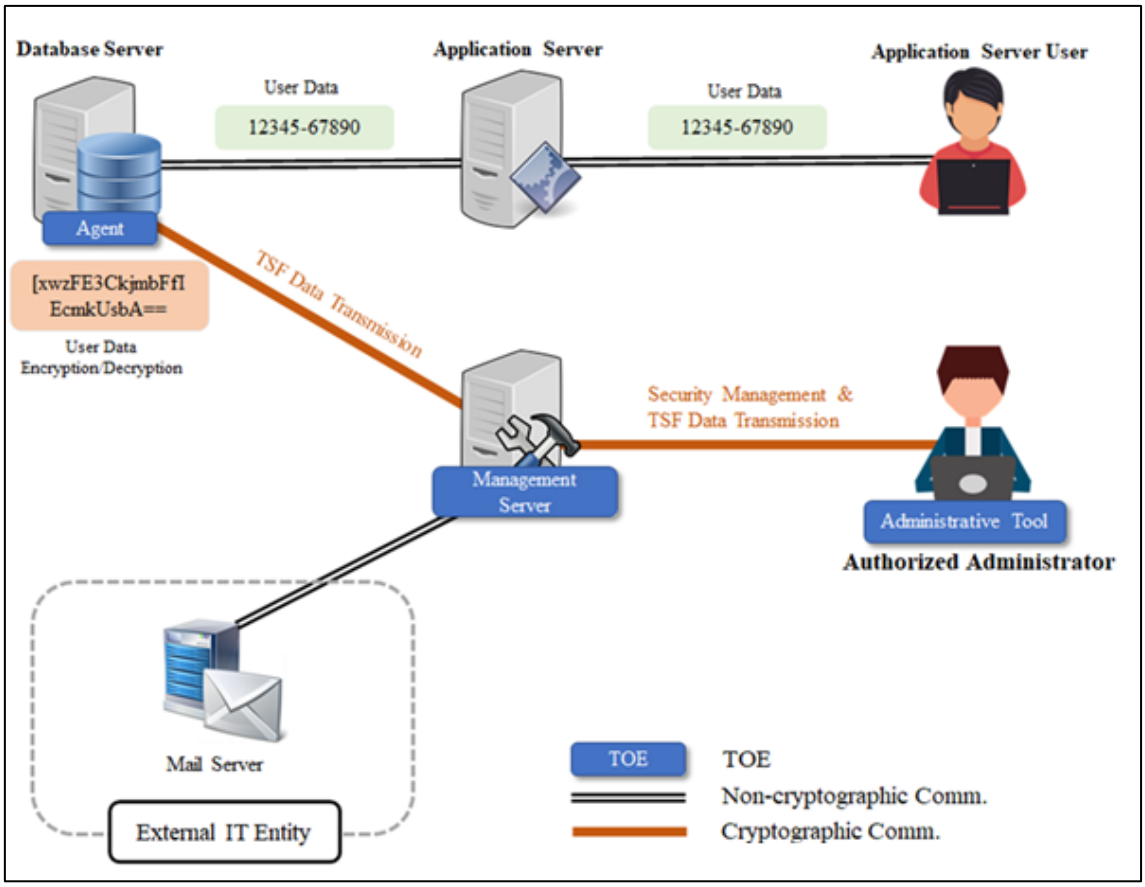
The ST claims conformance to the Korean National Database Encryption Protection V3.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the ST and the resulting TOE 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.

As shown in [Figure 1], the operational environment is consisted of MagicDBPlus v2.1 Server(“Management Server”), MagicDBPlus v2.1 Admin(“Administrative Tool”), MagicDBPlus v2.1 Agent(“Agent”).

Installed as a plug-in to the DBMS which has to be protected, the Agent receives TSF data from the Management Server and performs encryption/decryption of user data upon the request from the Application Server. In addition, the authorized administrator manages the scope and policies of encryption befitting security policy required in the organization via the Management Server, using the Administrative Tool. Upon the request of Application Service Users, the Application Server makes a request to the Database

Server while the Agent encrypts/decrypts user data, if necessary, and deliver them to Application Service Users.

Moreover, if a critical event(e.g., reaching to audit data threshold, etc.) arises in the Management Server, a mail is sent to a user designated by the authorized administrator via a mail server.



[Figure 1] Plug-in type operational environment of the TOE

Communications among TOE components, which rely on a self-implemented protocol, carry out cryptographic communication, using an approved algorithm of the validated cryptographic module(MagicCrypto V2.3.0).

The requirements for hardware, software and operating system to install the TOE are shown in [Table 1].

Component			Requirement
Management Server	HW	CPU	Intel Core i5 CPU 2.20 GHz or higher
		Memory	4 GB or higher
		HDD	100 GB or more of space required for TOE installation
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	Rocky 9.6(Linux Kernel 5.14.0, 64 bit)
Agent	HW	CPU	Intel Core i5 CPU 2.20 GHz or higher
		Memory	4GB or higher
		HDD	500 MB or more of space required for TOE installation
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	Rocky 9.6(Linux Kernel 5.14.0, 64 bit)
		DBMS to be protected	Db2 11.5.8.0, 64 bit
			Oracle 19.3.0.0.0, 64 bit
Administrative Tool	HW	CPU	Intel Core i5 CPU 2.50 GHz or higher
		Memory	4 GB or higher
		HDD	500 MB or more of space required for TOE installation
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	Windows 11 Pro 64 bit

[Table 1] TOE Hardware and Software specifications

External IT Entity	Description
Mail Server	It is used to send information mail to administrator in case of potential security threat of the TOE

[Table 2] External IT Entity

Validated cryptographic modules included the TOE are as follows.

Category	Description
Cryptographic Module	MagicCrypto V2.3.0
Validation No.	CM-263-2030.1
Developer	DreamSecurity Co., Ltd.
Module type	S/W(library)
Validation Date	January 24, 2025
Effective Expiration Date	January 24, 2030

[Table 3] Validated Cryptographic Module

The 3rd party S/W Included in TOE is as follows.

Component	3rd party S/W	Description
Management Server	SQLite v3.53.2	Used as file DB storage for TSF data (DEK for user data, TOE configuration, audit data, etc.) on Management Server
	OpenSSL 3.6.3	Used for TLS v1.3 encrypted communication
Agent	OpenSSL 3.6.3	Used for TLS v1.3 encrypted communication
Administrative Tool	OpenSSL 3.6.3	Used for TLS v1.3 encrypted communication

[Table 4] The 3rd party S/W 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 reference is identified as follows.

Category	Contents
TOE	MagicDBPlus v2.1
TOE Version	v2.1.0.1
TOE Component	MagicDBPlus v2.1 Server v2.1.0.1 : MagicDBPlus_v2.1_Server_v2.1.0.1sh
	MagicDBPlus v2.1 Agent v2.1.0.1 : MagicDBPlus_v2.1_Agent_v2.1.0.1sh
	MagicDBPlus v2.1 Admin v2.1.0.1 : MagicDBPlus v2.1_Admin_v2.1.0.1.exe
Manual	MagicDBPlus v2.1 Installation Guide v1.1 : MagicDBPlus_v2.1_PRE_v1.1.pdf
	MagicDBPlus v2.1 Operational Guidance v1.1 : MagicDBPlus_v2.1_OPE_v1.1.pdf

[Table 5] TOE identification

[Table 6] 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, October 31, 2022) Korea IT Security Evaluation and Certification Regulation(Ministry of Science and ICT · ITSCC, April 07, 2026)
TOE	MagicDBPlus v2.1
Common Criteria	Common Criteria for Information Technology Security Evaluation (CC:2022 Revision 1) Part 1: Introduction and general model, CC:2022 R1(CCMB-2022-11-001, 2022.11.) Part 2: Security functional components, CC:2022 R1(CCMB-2022-11-

	002, 2022.11.) Part 3: Security assurance components, CC:2022 R1(CCMB-2022-11-003, 2022.11.) Part 4: Framework for the specification of evaluation methods and activities, CC:2022 R1(CCMB-2022-11-004, 2022.11.) Part 5: Pre-defined packages of security requirements, CC:2022 R1(CCMB-2022-11-005, 2022.11.) Evaluation methodology, CEM:2022 R1(CCMB-2022-11-006, 2022.11.) Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Database Encryption Protection V3.1
Developer	DreamSecurity Co., Ltd.
Sponsor	DreamSecurity Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	June 26, 2026

[Table 6] Additional identification information

3. Security Policy

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

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Prtoection of the TSF
- User Data Protection
- 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 5])

5. Architectural Information

5.1 Physical Scope of TOE

The physical scope of the TOE consists of the MagicDBPlus v2.1 Server, MagicDBPlus v2.1 Agent, MagicDBPlus v2.1 Admin and Manual. Verified Cryptographic Module(MagicCrypto V2.3.0) is embedded in the TOE components.

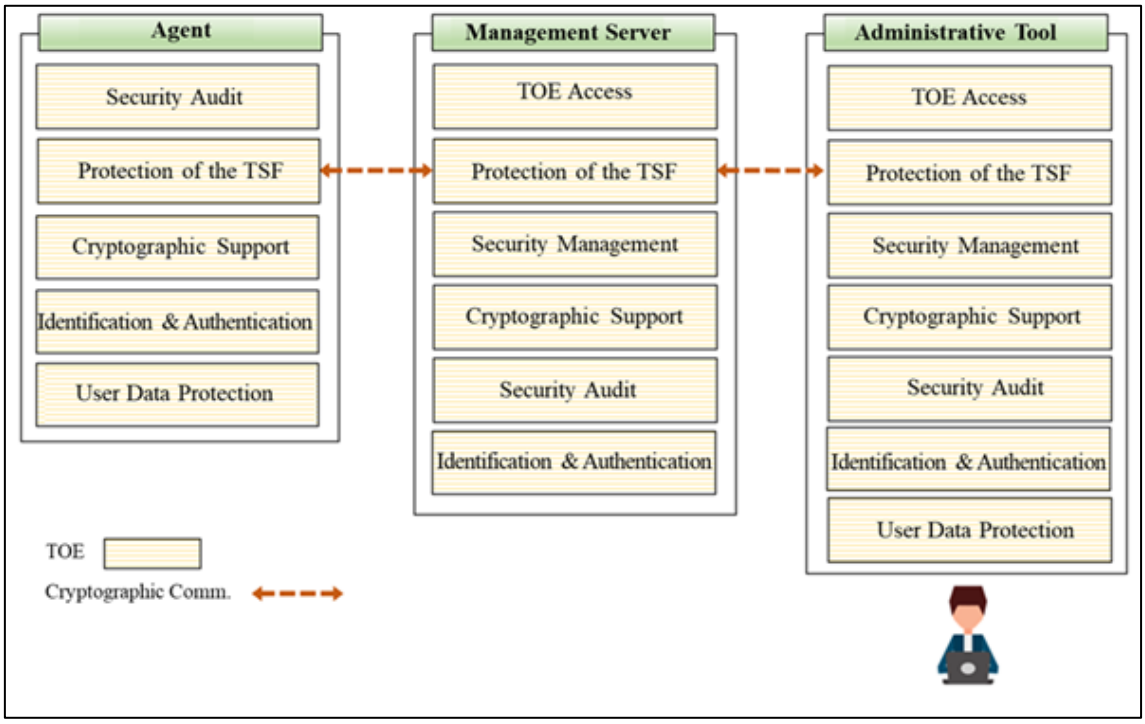
Hardware and OS where the TOE is installed are not included in the scope of the TOE.

Category		Type	Delivery
TOE	MagicDBPlus v2.1	-	-
TOE Version	v2.1.0.1	-	-
TOE Component	MagicDBPlus v2.1 Server v2.1.0.1 : MagicDBPlus_v2.1_Server_v2.1.0.1.sh	S/W	CD
	MagicDBPlus v2.1 Agent v2.1.0.1 : MagicDBPlus_v2.1_Agent_v.2.1.0.1.sh		
	MagicDBPlus v2.1 Admin v2.1.0.1 : MagicDBPlus_v2.1_Admin v2.1.0.1.exe		
Manual	MagicDBPlus v2.1 Installation Guide v1.1 : MagicDBPlus_v2.1_PRE_v1.1.pdf	PDF	
	MagicDBPlus v2.1 Operational Guidance v1.1 : MagicDBPlus_v2.1_OPE_v1.1.pdf		

[Table 7] Physical scope of TOE

5.2 Logical Scope of TOE

The logical scope of the TOE is as in [Figure 2] below.



[Figure 2] TOE Logical Scope

▣ Security Audit (FAU)

The TOE records and manages audit data including event date/time, event type, subject's ID (identity) and privileges, event result, and event detail in the Management Server. The generated audit data can be queried by the administrator through the Administrative Tool MagicDBPlus v2.1 Admin, and there is only one authorized administrator who can perform security management and view audit records.

Security audit records can be selectively queried in descending order by event occurrence date/time based on event date, access IP, access ID, event type, and event result.

The results of self-tests performed by each TOE component are stored and managed in the Management Server. If a self-test fails, an alert is sent to the email address set by the authorized administrator.

When the space for storing audit data exceeds the capacity designated by the administrator, a warning message is sent to the administrator's email. When the audit data storage is full, old audited event data is overwritten and a warning message is sent to the administrator's email.

All audit data is encrypted and stored in a local file DB on the Management Server, and access is managed to allow only authorized Management Server processes.

▣ Cryptographic support (FCS)

The validated cryptographic module (KCMVP) MagicCrypto V2.3.0 used by the TOE supports random number generator algorithms and constructs entropy input with noise sources satisfying entropy of 128 bits or more that have passed the entropy test (TTAK.KO-12.0341/R1 randomness test). It performs health tests (RCT, APT) on collected entropy noise sources when the RNG entropy is first collected or reseeded.

After passing the noise source health test, input/output data uses hexadecimal binary data by default to input/output messages and hash values. When input is received through the console, it is converted to hexadecimal, and additional seed values (QRNG output, etc.) from users are input using algorithm parameters.

The TOE uses the validated cryptographic module (KCMVP) MagicCrypto V2.3.0 to perform cryptographic key generation, distribution, destruction, operations, and random number generation. The cryptographic module is also used for cryptographic key generation and exchange during encrypted communication between physically separated TOE components.

The TOE generates TSF data encryption keys and user data encryption keys using the random number generator (HASH_DRBG 256) of the validated cryptographic module. It encrypts user data of the target DBMS using symmetric key encryption algorithms (ARIA-CBC 128/192/256-bit, SEED-CBC 128-bit, LEA-CBC 128/192/256-bit) and hash algorithms (SHA-256/384/512).

TSF data is protected using symmetric key encryption algorithm (ARIA-CBC 256-bit), digital signature algorithm (RSA-PSS 2048-bit), hash algorithm (SHA-256), and MAC algorithm (HMAC-SHA 256-bit).

Distribution of encryption keys between TOE components is performed securely using public key encryption (RSAES 2048-bit), and encryption keys are overwritten three times with '0x00'.

The KEK is derived using the PBKDF2(SHA-256) algorithm of the validated cryptographic module (KCMVP) with the password entered at startup, Salt (16 bytes) stored in the configuration file, and Iteration Count of 1024. The entered password is

destroyed by overwriting it with zeros three times.

▣ User Data Protection (FDP)

The TOE uses the validated cryptographic module (KCMVP) MagicCrypto V2.3.0 through the user data encryption/decryption policy set by the authorized administrator to perform encryption/decryption when storing and modifying user data in the target DB.
The TOE operates as a plug-in and supports column-level user data encryption/decryption in the Agent.
The TOE generates different encryption result values each time encryption is performed on the same user data.
When encryption/decryption is complete, the TOE initializes so that the previous original user data value cannot be recovered.

▣ Identification and authentication (FIA)

The TOE provides identification and authentication functions for administrators who perform security management functions, and the ID and password must be changed upon first login after product installation. To protect authentication feedback during administrator identification and authentication data input, '*' is displayed as a protection indicator when entering a password.
Additionally, feedback on the reason for failure is not provided in case of authentication failure, and the account is locked (for 5 minutes) after consecutive authentication failures (5 times).
The TOE blocks authentication information reuse attempts for administrators logging into the TOE.
The TOE provides the following criteria for password verification:

- Password length: minimum 9 to maximum 16 characters
- Available password characters: digits (0-9), uppercase (English), lowercase (English), special characters (~, `, !, @, #, $, %, ^, &, *, (,), -, _, +, =)
- Password must include at least one character from each valid character type

The TOE performs TLS 1.3 communication and performs mutual authentication for secure communication between TOE components.

▣ **Security Management (FMT)**

The TOE has only one authorized administrator account, and the ID and password must be changed upon first login.

The TOE provides security management functions including cryptographic key generation and deletion, policy registration and deletion, mail notification configuration, audit threshold configuration, and user data encryption/decryption. The authorized administrator performs security management through the Administrative Tool's security management interface.

▣ **Protection of the TSF (FPT)**

The TOE protects TSF data using the TSF data encryption key (DEK) in TSF-controlled storage, generates the KEK through password-based derivation (PBKDF2), and encrypts and stores the DEK. The TOE also protects TSF data transmitted between TOE components via TLS 1.3 and performs inspections of major security function processes through TSF self-testing. The TOE performs self-tests on major processes, key files, and cryptographic modules at startup and periodically during operation (every 3 hours after startup). For key files, the authorized administrator can also perform integrity tests manually through the security management screen. If a self-test result is abnormal, an alert email is sent to the administrator.

When RCT/APT test errors occur for the health test on collected entropy noise sources of the validated cryptographic module, or when integrity is compromised, the Administrative Tool, Agent, and Management Server can be manually reinstalled to return to a safe state.

▣ **TOE access (FTA)**

The management access session available for performing security management functions is limited to 1. If an administrator session already logged into the Management Server exists, no further authorized administrator access is permitted.

If no activity is detected for a certain period (default: 10 minutes) after the authorized administrator logs into the Management Server through the Administrative Tool, the session connected to the Management Server is terminated.

Additionally, the authorized administrator IP addresses are limited to 2. During initial Management Server installation, one accessible administrator IP address is pre-specified during the installation process.

6. Documentation

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

Identification	Date
MagicDBPlus v2.1 Installation Guide v1.1 : MagicDBPlus_v2.1_PRE_v1.1.pdf	June 9, 2026
MagicDBPlus v2.1 Operational Guidance v1.1 : MagicDBPlus_v2.1_OPE_v1.1.pdf	June 9, 2026

[Table 8] 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: MagicDBPlus v2.1(v2.1.0.1)

- MagicDBPlus v2.1 Server v2.1.0.1
- MagicDBPlus v2.1 Agent v2.1.0.1
- MagicDBPlus v2.1 Admin v2.1.0.1

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 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+).

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 defined 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		
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 9] 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.

11. Security Target

MagicDBPlus v2.1 Security Target v1.2[4] is included in this report for reference.

12. Acronyms and Glossary

12.1 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

12.2 Glossary

Approved cryptographic algorithm

A cryptographic algorithm selected by Korea Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability

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.

Authorized Administrator

Authorized user to securely operate and manage the TOE

Authorized User

The TOE user who may, in accordance with the SFRs, perform an operation

Column

A set of data values of a particular simple type, one for each row of the table in a relational database

Critical Security Parameters (CSP)

Information related to security that can erode the security of the encryption module if exposed or changed (e.g., verification data such as secret key/private key, password, or Personal Identification Number).

Database

A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this PP, refers to the relational database.

DBMS (Database Management System)

A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this PP, refers to the database management system based on the relational database model.

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

Deterministic Random Bit Generator (DRBG)

An algorithm that generates a bit sequence from an initial value called a seed, producing the same bit sequence when the same seed is input

Encryption

The process of transforming plaintext into ciphertext using an encryption key

External Entity

A human technical system or one of its components that interacts with the TOE from

outside the TOE boundary

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Management Console

Application program such as GUI (Graphical User Interface) or CLI (Command Line Interface) provided to an administrator for management and configuration of a system / It is also used as a synonym with the Administrative Tool in this document.

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

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.

※ *A cryptographic random number generator consists of an entropy source used to construct the seed and a Deterministic Random Bit Generator (DRBG)*

Secret Key

Cryptographic key that is used along with a secret key cryptographic algorithm and can be uniquely combined with an entity or more / It shall not be made public.

Self-test

Pre-operational or conditional test executed by the cryptographic module

Symmetric cryptographic technique

Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

User Data

Data for the user, that does not affect the operation of the TSF

Validated Cryptographic Module

A cryptographic module that has been verified and approved by the cryptographic mod ule validation authority and assigned a validation number

13. Bibliography

The evaluation facility 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

[2] Common Methodology for Information Technology Security Evaluation,
CC:2022 Revision 1, CCMB-2022-11-006, November, 2022

[3] Korean National Protection Profile for Database Encryption V3.1

[4] MagicDBPlus v2.1 Security Target v1.2, July 6, 2026

[5] MagicDBPlus v2.1 Independent Testing Report(ATE_IND.1) V2.00, July 6, 2026

[6] MagicDBPlus v2.1 Penetration Testing Report (AVA_VAN.1) V2.00, July 6, 2026