KECS-CR-24-30

MagicDBPlus v2.0 SP1

Certification Report

Certification No.: KECS-CISS-1308-2024

2024. 6. 25.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.06.25.	-	Certification report for MagicDBPlus v2.0 SP1 - First documentation

This document is the certification report for MagicDBPlus v2.0 SP1 of Dreamsecurity Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

Certification Report **1**
1. Executive Summary **5**
2. Identification **8**
3. Security Policy **9**
4. Assumptions and Clarification of Scope **10**
5. Architectural Information **10**
1. Physical Scope of TOE 10
2. Logical Scope of TOE 11
6. Documentation **15**
7. TOE Testing **15**
8. Evaluated Configuration **16**
9. Results of the Evaluation **16**
1. Security Target Evaluation (ASE) 16
2. Development Evaluation (ADV) 17
3. Guidance Documents Evaluation (AGD) 17
4. Life Cycle Support Evaluation (ALC) 18
5. Test Evaluation (ATE) 18
6. Vulnerability Assessment (AVA) 18
7. Evaluation Result Summary 19
10. Recommendations **20**
11. Security Target **20**
12. Acronyms and Glossary **20**
13. Bibliography **23**

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the MagicDBPlus v2.0 SP1 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 reffered 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 12, 2024.

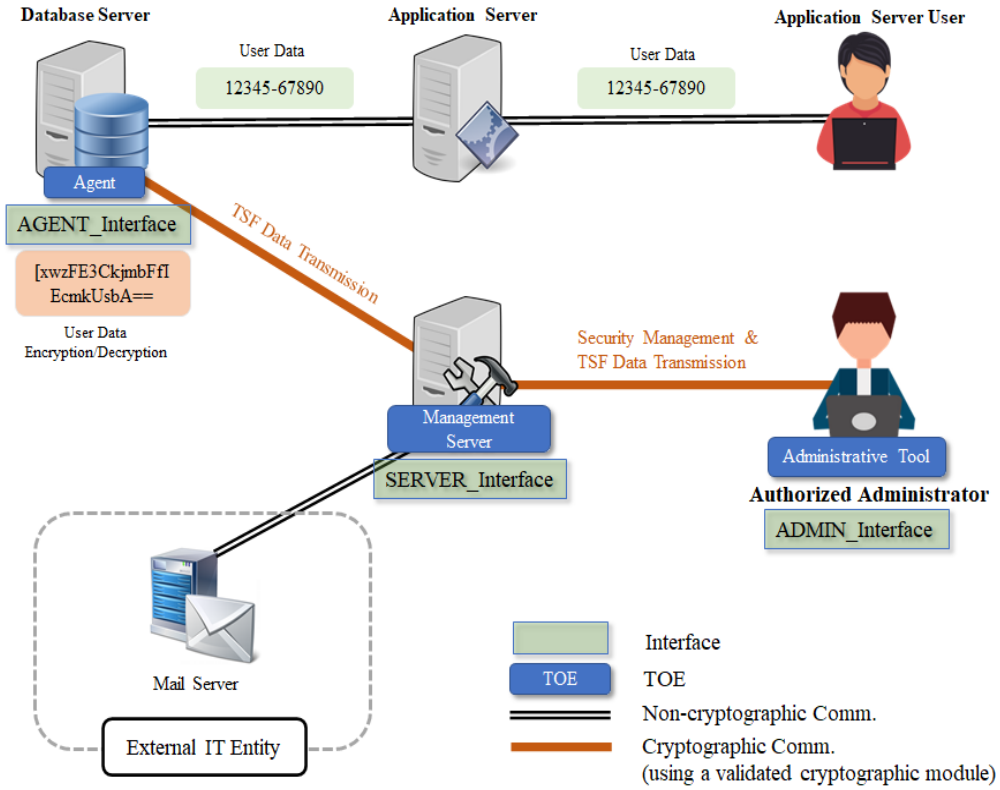
The ST claims conformance to the Korean National Protection Profile for Database Encryption V1.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the ST and the 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.

As shown in [Figure 1], the operational environment is consisted of MagicDBPlus v2.0 SP1 Server(“Management Server”), MagicDBPlus v2.0 SP1 Admin(“Administrative Tool”), MagicDBPlus v2.0 SP1 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

(Agent, Management Server separate type)

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 V2.2.0).

Component			Requirement
MagicDBPlus v2.0 SP1 Server v2.0.4.1 (Management Server)	HW	CPU	Intel(R) Core (TM) i3 CPU @ 2.27 GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE 100 GB or higher
		NIC	100/1000 Mbps Ethernet Port 1 unit or higher
	SW	OS	Ubuntu 22.04 (kernel 6.5.0) 64 bit
MagicDBPlus	HW	CPU	Intel(R) Core (TM) i5 CPU @ 2.50GHz or

v2.0 SP1 Admin v2.0.4.1 (Administrative Tool)			higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE 500 MB or higher
		NIC	100/1000 Mbps Ethernet Port 1 unit or higher
	SW	OS	Windows 10 Pro 64 bit
MagicDBPlus v2.0 SP1 Agent v2.0.4.1 (Agent)	HW	CPU	Intel(R) Core (TM) i5 CPU @ 2.30GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE 500 MB or higher
		NIC	100/1000 Mbps Ethernet Port 1 unit or higher
	SW	OS	Rocky Linux 8.4 (kernel 4.18.0) 64 bit
		DBMS to be protected	IBM DB2 V11.5 64 bit

[Table 1] TOE Hardware and Software specifications

External IT Entity	Description
Mail Server	To be used to notify or send an alarm (a warning mail) to an administrator regarding threats that arise during operation of the Management Server

[Table 2] External IT Entity

3rd party S/W	Description
SQLite v3.45.3	To be used as DB for repository files of TSF data (DEKs for user data, critical security parameters, TOE configuration values and audit data, etc.) in the Management Server

[Table 3] 3rd party S/W(TOE include)

Validated cryptographic modules included the TOE are as follows.

Classfication	Description

Cryptographic Module	MagicCrypto V2.2.0
Validation No.	CM-162-2025.3
Developer	Dream Security Co., Ltd.
Validation Date	2020.03.03
Effective Expiration Date	2025.03.03

[Table 4] Validated Cryptographic Module

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.

Cls.	Contents
TOE Component	MagicDBPlus v2.0 SP1 Server v2.0.4.1 : MagicDBPlus_v2.0_SP1_Server_v2.0.4.1.sh
	MagicDBPlus v2.0 SP1 Admin v2.0.4.1 : MagicDBPlus_v2.0_SP1_Admin_v2.0.4.1.exe
	MagicDBPlus v2.0 SP1 Agent v2.0.4.1 : MagicDBPlus_v2.0_SP1_Agent_v2.0.4.1.sh
Manual	MagicDBPlus v2.0 SP1 Installation Guide v1.1 : MagicDBPlus_v2.0_SP1_PRE_v1.1.pdf
	MagicDBPlus v2.0 SP1 Operational Guidance v1.1 : MagicDBPlus_v2.0_SP1_OPE_v1.1.pdf

[Table 5] TOE identification

[Table 6] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	MagicDBPlus v2.0 SP1
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Database Encryption V1.1
Developer	Dreamsecurity Co., Ltd.
Sponsor	Dreamsecurity Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	June 12, 2024

[Table 6] 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 5])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the Management Server, Administrative Tool, Agent and manuals(Install guide, Operational Guidance). Verified Cryptographic Module(MagicCrypto V2.2.0) is embedded in the TOE components.

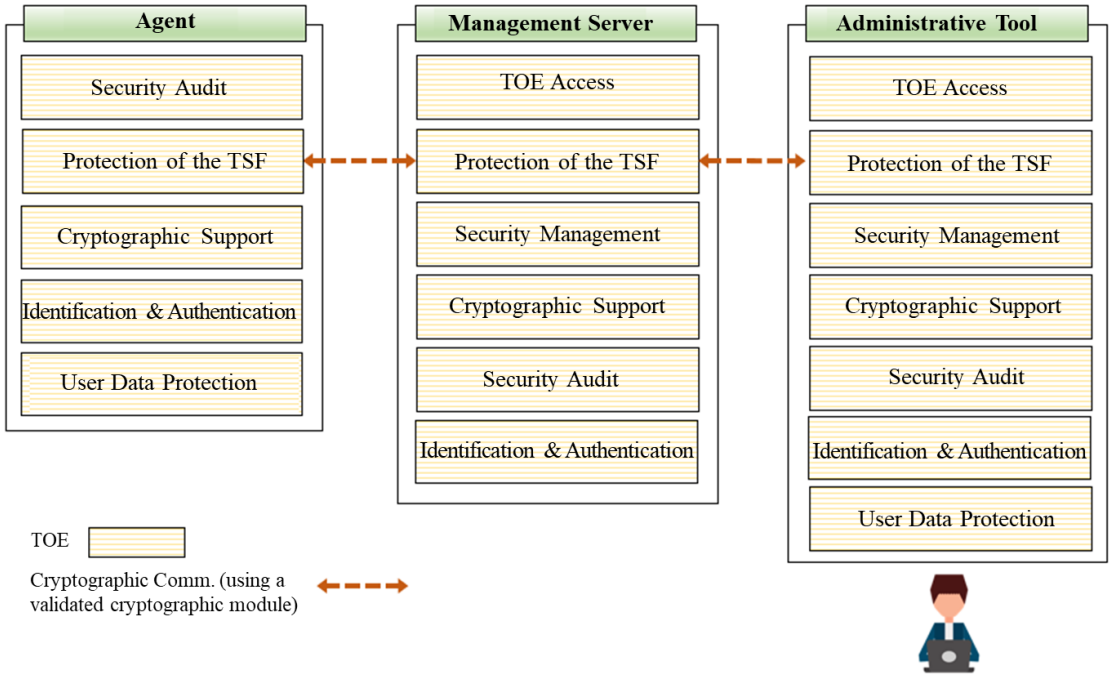
Hardware and OS where the TOE is installed are not included in the scope of the TOE.

Category		Type	Delivery
TOE Component	MagicDBPlus v2.0 SP1 Server v2.0.4.1 : MagicDBPlus_v2.0_SP1_Server_v2.0.4.1.sh	S/W	Included in an installation CD of the product package provided to users
	MagicDBPlus v2.0 SP1 Admin v2.0.4.1 : MagicDBPlus_v2.0_SP1_Admin_v2.0.4.1.exe	S/W	
	MagicDBPlus v2.0 SP1 Agent v2.0.4.1 : MagicDBPlus_v2.0_SP1_Agent_v2.0.4.1.sh	S/W	
Guidance Document	MagicDBPlus v2.0 SP1 Installation Guide v1.1 : MagicDBPlus_v2.0_SP1_PRE_v1.1.pdf	PDF	
	MagicDBPlus v2.0 SP1 Operational Guidance v1.1 : MagicDBPlus_v2.0_SP1_OPE_v1.1.pdf	PDF	

[Table 7] Physical scope of TOE

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 the data/time of an event, an event type, subject identity and authority, results of an event and event details as audit data which are stored and controlled in the MagicDBPlus v2.0 SP1 Server. The audit data generated can be viewed by an administrator, using the Administrative Tool called MagicDBPlus v2.0 SP1 Admin. There is only one super administrator who is capable of viewing security management and audit records as an authorized administrator to which an alarm is send via mail in case of any access from an unauthorized user.

Security audit records can be selectively searched in descending order based on the date of incident occurrence, access IP, access ID, incident type, and incident result.

In addition, the result of a self-test administered at each component of the TOE is stored and controlled in the MagicDBPlus v2.0 SP1 Server as well. In case a self-test fails, an alarm is sent to an email defined by the authorized administrator.

In case the audit data storage reaches a certain threshold defined by the administrator, a warning email is sent to the administrator. Also, if the audit storage is full, audited

obsolete events are overwritten and a warning message is sent to the administrator via email.

All audit data are encrypted and stored in the local file DB of the MagicDBPlus v2.0 SP1 Server, with a limited access only from approved MagicDBPlus v2.0 SP1 Server processes.

▣ Cryptographic support (FCS)

The TOE performs generation, distribution, destruction and operation of cryptographic keys and random bit generation, using a validated cryptographic module, MagicCrypto V2.2.0. The cryptographic module is also used to generate and exchange cryptographic keys during cryptographic communications among TOE components(MagicDBPlus v2.0 SP1 Server ↔ MagicDBPlus v2.0 SP1 Admin, MagicDBPlus v2.0 SP1 Server↔MagicDBPlus v2.0 SP1 Agent) physically separated.

MagicDBPlus v2.0 SP1 Server is generate the cryptographic key is generated, a cryptographic key is generated using a random bit through a random bit generator (HASH_DRBG 256) of the validated cryptographic module, and to encrypt user data of the DBMS to be protected is encrypted, a symmetric key encryption algorithm (ARIA-CBC 128/192/256 bit, SEED-CBC 128 bit, LEA-CBC 128/192/256 bit) and hash algorithm(SHA-256/384/512).

In addition, a symmetric key encryption algorittm (ARIA-CBC 256 bit), digital signature algorittm (RSA-PSS 2048 bit), hash algorithm (SHA-256) and MAC algorithm(HMAC-SHA 256) are used for protction of TSF data.

Cryptograchic key distribution between the TOE components(MagicDBPlus v2.0 SP1 Server↔MagicDBPlus v2.0 SP1 Admin, MagicDBPlus v2.0 SP1 Server↔MagicDBPlus v2.0 SP1 Agent) is safely distributed through public key encryption method (RSAES 2048 bit), and the cryptographic key is overwritten with "0x00" three times to ensure complete destruction.

▣ User data protection (FDP)

MagicDBPlus v2.0 SP1 Agent conducts encryption/decryption in case of storage and modification of user data in DB to be encrypted, using the validated cryptographic module,

MagicCrypto V2.2.0, in accordance with encryption/decryption policy for user data defined by the authorized administrator. Operated as a plug-in, the TOE supports encryption/decryption of user data as per column in the MagicDBPlus v2.0 SP1 Agent.

MagicDBPlus v2.0 SP1 Agent generates different encryption values each time it conducts encryption of the same user data. Once the encryption/decryption is completed, it performs initialization to prevent the restoration of the previous value of the original user data.

▣ Identification and authentication (FIA)

MagicDBPlus v2.0 SP1 Server provides identification and authentication function to an administrator who carries out security management function so that the ID and password have to be changed during the initial login after installation of the product through MagicDBPlus v2.0 SP1 Admin. When the identification and authentication data of an administrator are entered, the password is masked with "*" to protect the authentication feedback.

Moreover, in case of an authentication failure, feedback on a failure reason is not provided, and the account become locked after consecutive authentication failures.

It also blocks an attempt to re-use authentication information regarding the administrator who has logged in to the MagicDBPlus v2.0 SP1 Admin.

MagicDBPlus v2.0 SP1 Server provides the following criteria with respect to verification of the password:

- Length of password: (Min.) 9 characters ~ (Max.) 16 characters
- Characters usable for the password: English upper and low cases, numbers and special characters (~, `, !, @, #, $, %, ^, &, *, (,), -, _, +, =)
- The password has to be a combination of the following three: English upper/lower cases, numbers and special characters.

The TOE carries out mutual authentication, using a self-implemented protocol for secure communications among TOE components(MagicDBPlus v2.0 SP1 Server ↔ MagicDBPlus v2.0 SP1 Admin, MagicDBPlus v2.0 SP1 Server ↔ MagicDBPlus v2.0 SP1 Agent).

▣ Security Management (FMT)

There is only one account for an authorized administrator in the MagicDBPlus v2.0 SP1 Admin and during the initial login, the ID and password have to be changed.

MagicDBPlus v2.0 SP1 Server provides security management functions including generation and destruction of cryptographic keys, registration and deletion of policies, mail notification setting, audit threshold setting and encryption/decryption of user data. The authorized administrator performs security management, using a security management interface available in the MagicDBPlus v2.0 SP1 Admin.

▣ Protection of the TSF (FPT)

MagicDBPlus v2.0 SP1 Server protects TSF data using the TSF data encryption key (DEK) in a storage controlled by the TSF. The key (KEK) that encrypts the TSF data encryption key (DEK) is generated through the password-based derivation (PBKDF2) function, and the TSF data encryption key (DEK) is encrypted and stored. The TOE protects TSF data stored in repositories controlled by the TSF and those transmitted among TOE components(MagicDBPlus v2.0 SP1 Server ↔ MagicDBPlus v2.0 SP1 Admin, MagicDBPlus v2.0 SP1 Server ↔ MagicDBPlus v2.0 SP1 Agent) and conducts inspection on major security function processes based on TSF self-tests. The TOE runs a self-test on the main process, major files and the cryptographic module during the initial start-up of the TOE and normal operation on a periodical basis. In terms of major files, the authorized administrator can manually run such a self-test via a security management screen. In case the self-test shows any abnormal behavior, a warning mail is sent to the administrator.

▣ TOE access (FTA)

The number of management access sessions available for the administrator to enforce security management functions is limited to one. If there is an administrator session already logged in to the MagicDBPlus v2.0 SP1 Server, no more authorized administrator can access. In case no action is detected for a certain period of time after the authorized administrator has logged in to the MagicDBPlus v2.0 SP1 Server via the MagicDBPlus v2.0 SP1 Admin, the session accessible is closed.

In addition, the authorized administrator can have no more than two IPs, and during the

initial installation of the MagicDBPlus v2.0 SP1 Server, one IP accessible during the installation process has to be pre-defined.

6. Documentation

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

Identification	Date
MagicDBPlus v2.0 SP1 Installation Guide v1.1 : MagicDBPlus_v2.0_SP1_PRE_v1.1.pdf	May 14, 2024
MagicDBPlus v2.0 SP1 Operational Guidance v1.1 : MagicDBPlus_v2.0_SP1_OPE_v1.1.pdf	May 14, 2024

[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 v2.0 SP1(v2.0.4.3)
- MagicDBPlus v2.0 SP1 Server v2.0.4.1
- MagicDBPlus v2.0 SP1 Admin v2.0.4.1
- MagicDBPlus v2.0 SP1 Agent v.2.0.4.1

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 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation. (EAL1+).

1. Security Target Evaluation (ASE)

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

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

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

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

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

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

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

2. Development Evaluation (ADV)

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

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

3. Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents consider the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

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

4. Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

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

5. Test Evaluation (ATE)

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

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation.

Therefore, the verdict PASS is assigned to ATE_IND.1. Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

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

6. Vulnerability Assessment (AVA)

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

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

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

7. Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 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.
- 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

MagicDBPlus v2.0 SP1 Security Target v1.2 [4] is included in this report for reference.

12. Acronyms and Glossary

(1) Acronyms

CC Common Criteria
CEM Common Methodology for Information Technology Security Evaluation
EAL Evaluation Assurance Level
ETR Evaluation Technical Report

SAR Security Assurance Requirement
SFR Security Functional Requirement
ST Security Target
TOE Target of Evaluation
TSF TOE Security Functionality
TSFI TSF Interface

(2) Glossary

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.

Database Server

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

DBMS (Database Management System)

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

Data Encryption Key (DEK)

Key that encrypts and decrypts the data

Decryption

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

Encryption

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

External Entity

Human or IT entity possibly interacting with the TOE from outside of 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

Public Key (asymmetric) cryptographic algorithm

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

Random bit generator

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

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

Secret Key

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

13. **Bibliography**

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

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

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

[3] Korean National Protection Profile for Database Encryption V1.1, December 11, 2019

[4] MagicDBPlus v2.0 SP1 Security Target v1.2, May 14, 2024

[5] MagicDBPlus v2.0 SP1 Independent Testing Report(ATE_IND.1) V1.00, May 30, 2024

[6] MagicDBPlus v2.0 SP1 Penetration Testing Report (AVA_VAN.1) V2.00, June 24, 2024