KECS-CR-20-56

MagicDBPlus v2.0

Certification Report

Certification No.: KECS-CISS-1042-2020

2020. 9. 8.

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2020.09.08.	-	Certification report for MagicDBPlus v2.0 - First documentation

This document is the certification report for MagicDBPlus v2.0 for Dreamsecurity Co., LTD.

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 evaluation facility on the results of the MagicDBPlus v2.0 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 ("TOE" hereinafter) 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 July 29, 2020.

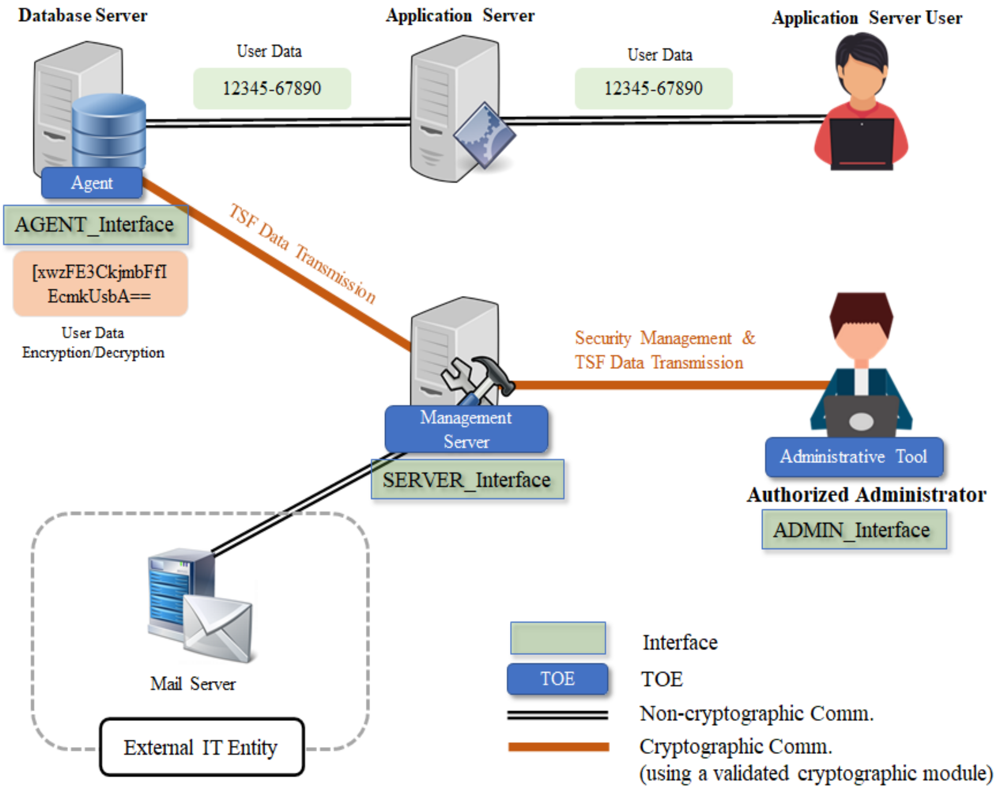
The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs. Therefore, the ST and the resulting TOE is CC Part 3 conformant. 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 comprised of MagicDBPlus v2.0 Server("Management Server"), MagicDBPlus v2.0 Admin("Administrative Tool"), MagicDBPlus v2.0 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 events(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).

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

Component			Requirement
MagicDBPlus v2.0 Server (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	CentOS 7.8 (Linux Kernel 3.10.0) 64 bit
MagicDBPlus v2.0 Admin (Administrative Tool)	HW	CPU	Intel(R) Core (TM) i5 CPU @ 2.50GHz 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	Windows 10 Pro 64 bit
MagicDBPlus v2.0 Agent (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	CentOS 7.8 (Linux Kernel 3.10.0) 64 bit
		DBMS to be protected	Oracle 12.2.0.1.0 64 bit

[Table 1] TOE Hardware and Software specifications

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is software consisting of the following software components and related guidance documents.

TOE	MagicDBPlus v2.0	
Version	v2.0.3.0	
TOE Components	MagicDBPlus v2.0 Server (Management Server)	MagicDBPlus v2.0 Server v2.0.3.0 (`MagicDBPlus_v2.0_Server_v2.0.3.0.sh`)
	MagidDBPlus v2.0 Admin (Administrative Tool)	MagicDBPlus v2.0 Admin v2.0.3.0 (`MagicDBPlus_v2.0_Admin_v2.0.3.0.exe`)
	MagicDBPlus v2.0 Agent (Agent)	MagicDBPlus v2.0 Agent v2.0.3.0 (`MagicDBPlus_v2.0_Agent_v2.0.3.0.sh`)
Guidance Document	MagicDBPlus v2.0 Installation Guide v1.2 (`MagicDBPlus_v2.0_PRE_v1.2.pdf`) MagicDBPlus v2.0 Operational Guidance v1.2 (`MagicDBPlus_v2.0_OPE_v1.2.pdf`)	

[Table 2] TOE identification

Note that the TOE is delivered contained in a CD-ROM.

[Table 3] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (September 12, 2017)
TOE	MagicDBPlus v2.0

Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
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	July 29, 2020
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The ST [4] for the TOE claims strict to the Korean National PP for Database Encryption V1.1 [3], and complies security policies defined in the PP by security requirements. Thus, the TOE provides security features defined in the PP as follows:

- Security audit: The TOE generates audit records of security relevant events such as the start-up/shutdown of the audit functions, integrity violation, self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic key management such as key generation, distribution, and destruction, and cryptographic operations such as encryption and decryption using the cryptographic modules (MagicCrypto V2.2.0) validated under the KCMVP.
- User data protection: The TOE provides encryption and decryption for the user data in a column of a database.
- Identification and authentication: The TOE identifies and authenticates the administrators using their ID/password and mutually authenticates TOE components.
- Security management: The TOE allows only an authorized administrator to access the management interface provided by the TOE.
- Protection of the TSF: The TOE implements secure communications between

the TOE components to protect the transmitted data. The TOE encrypts the stored TSF data to protect them from unauthorized exposure and modification. The TOE performs self-tests on the TOE components, which includes the self-test on the validated cryptographic module.

- TOE access: The TOE manages authorized administrators' sessions based on access IP addresses and administrator rights, and terminates the sessions after predefined time interval of inactivity.

4. Assumptions and Clarification of Scope

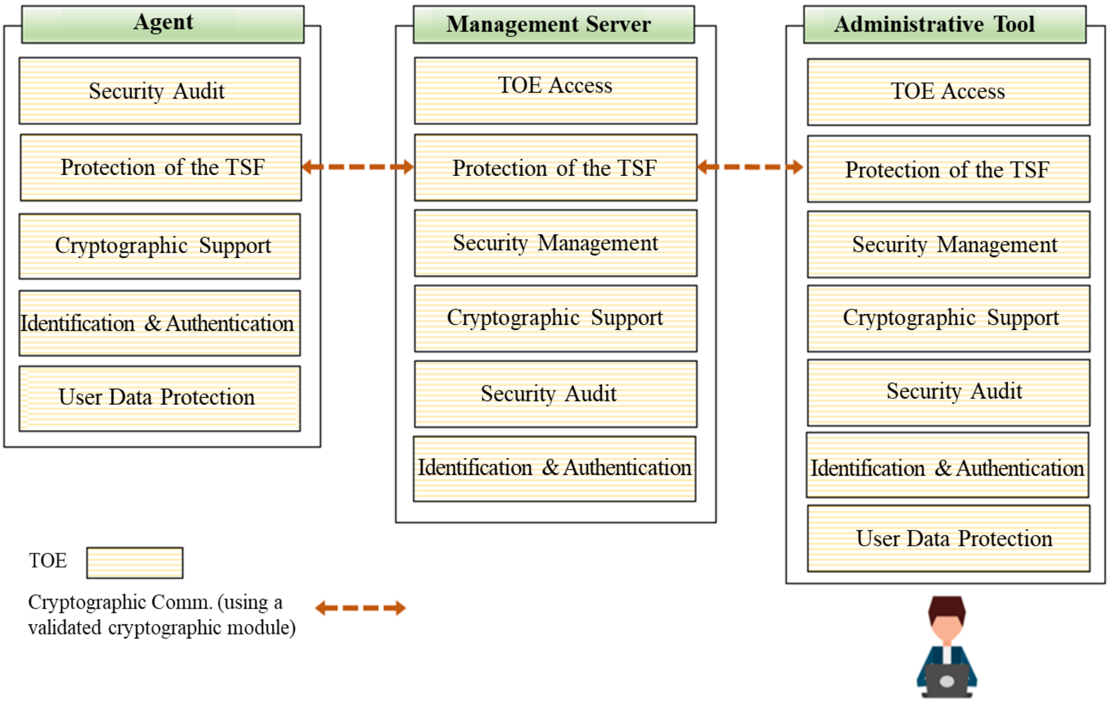
There is no explicit Security Problem Definition chapter, therefore no Assumptions secti on in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [3] in which the TOE will be used or is intended to be used (For the detailed and precise definition of the security objectives of the operational environment, refer to the ST [4], chapter 3.).

5. Architectural Information

The TOE is software consisting of the following components:

- Agent (MagicDBPlus v2.0 Agent)
- Management Server (MagicDBPlus v2.0 Server)
- Administrative Tool (MagicDBPlus v2.0 Admin)

In [Figure 2], the three components perform the same functionalities of audit data generation, cryptographic key management, cryptographic operations, protection of TSF data, and mutual authentication between the components. For the detailed description on the architectural information, refer to the ST [4].



[Figure 2] Logical scope of the TOE

6. Documentation

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

Identification	Date
MagicDBPlus v2.0 Installation Guide v1.2 (MagicDBPlus_v2.0_PRE_v1.2.pdf)	July 10, 2020
MagicDBPlus v2.0 Operational Guidance v1.2 (MagicDBPlus_v2.0_OPE_v1.2.pdf)	July 10, 2020

[Table 4] Documentations

7. TOE Testing

The developer 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. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules 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 developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator installed and prepared the TOE in accordance to the preparative procedures, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities.

The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: MagicDBPlus v2.0 (v2.0.3.0)

- MagicDBPlus v2.0 Server v2.0.3.0
- MagicDBPlus v2.0 Admin v2.0.3.0
- MagicDBPlus v2.0 Agent v2.0.3.0

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 provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components.

9.1 Security Target Evaluation (ASE)

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

9.3 Guidance Documents Evaluation (AGD)

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

9.4 Development Evaluation (ADV)

The functional specification specifies 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.

9.5 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 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		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.
- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default 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 Security Target v1.3 [4] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
Critical Security Parameter (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).
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.
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
Validated Cryptographic Module	A cryptographic module that is validated and given a validation number by validation authority

13. Bibliography

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

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

[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] MagicDBPlus v2.0 Security Target v1.3, July 10, 2020

[5] MagicDBPlus v2.0 Evaluation Technical Report(ETR) Lite V1.00, July 29, 2020