KECS-CR-23-70

CubeOne V3.0

Certification Report

Certification No.: KECS-CISS-1276-2023

2023. 11. 29.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.11.29.	-	Certification report for CubeOne V3.0 - First documentation

This document is the certification report for CubeOne V3.0 of eGlobal Systems 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 certification body on the results of the evaluation of CubeOne V3.0 of eGlobal Systems 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) is database encryption software to prevent unauthorized exposure of the information from DBMS. The TOE is provided as software and provides the following security features: security audit, cryptographic operations using validated cryptographic module, user identification and authentication including mutual authentication between the TOE components, security management, the TOE access session management, and the TSF protection.

The TOE is comprised of the following software components: CubeOne Manager, CubeOne Server, CubeOne Security Server. The TOE uses cryptographic modules validated under the Korea Cryptographic Module Validation Program (KCMVP).

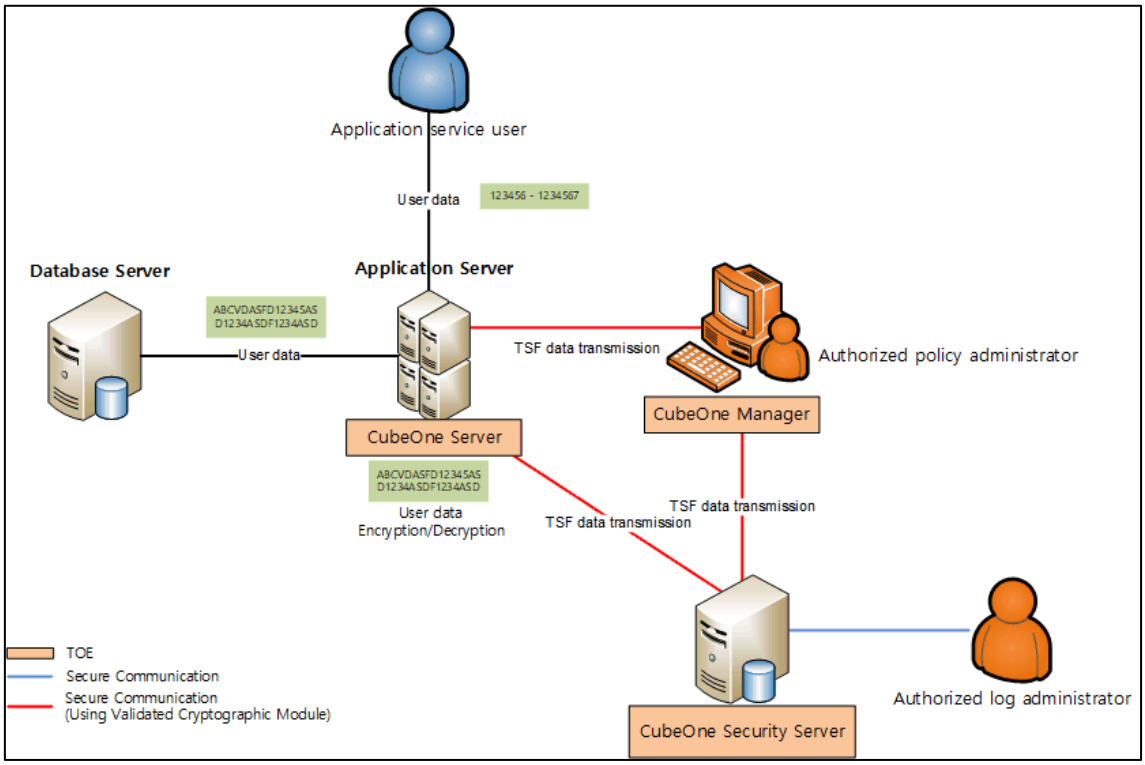
There are two types of the TOE operational environments: plug-in and API types. In the plug-in type, CubeOne Server is installed in a database server. In the API type, CubeOne Server is installed in an application server. The component CubeOne Manager provides security management function to an authorized policy administrator. An authorized log administrator can access to CubeOne Security Server to check if there is security alert and audit log.

The evaluation of the TOE has been carried out by Korea System Assurance (KoSyAs) and completed on 24 November 2023. This report grounds on the evaluation technical report (ETR) KoSyAs had submitted [5] and the Security Target (ST) [6][7].

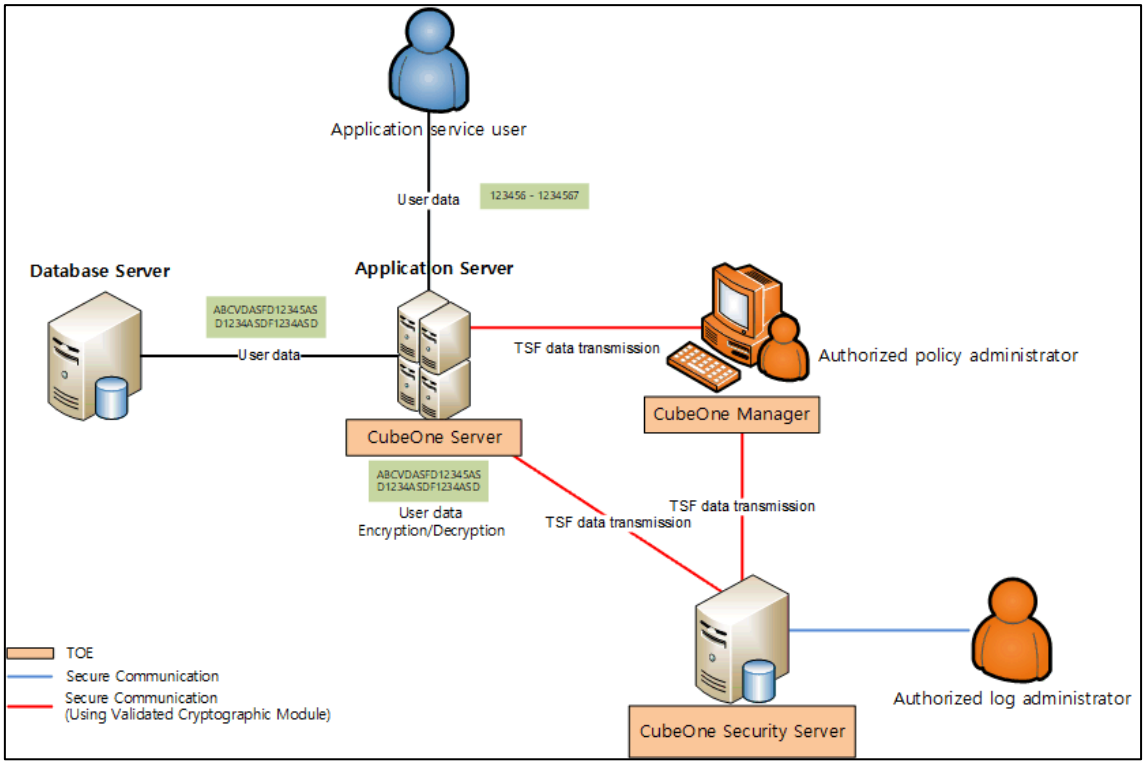
The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.1 [9]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of the PP [9]. Therefore, the ST and the resulting TOE is CC Part 3 conformant.

The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and newly defined components in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] and [Figure 2] show the operational environment of the TOE for the plug-in and API types, respectively.



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



[Figure 2] API-type operational environment of the TOE

[Table 1] shows minimum hardware and software requirements necessary for installation and operation of the TOE.

Classification	Minimum Requirement					
CubeOne Manager	CPU	Intel Core 2 Duo 2.40 GHz or higher				
	Memory	4 GB or higher				
	HDD	At least 200 MB of space for installation of the TOE component				
	NIC	10/100/1000 Mbps X 1 Port or more				
	OS	Windows Server 2019 (64-bit)				
CubeOne Server (Plug-In)	CPU	POWER7 3.0 GHz or higher	Intel Dual Core 1.8 GHz or higher	Intel Dual Core 1.8 GHz or higher		
	Memory	4 GB or higher				
	HDD	At least 200 MB of space for installation of the TOE component				
	NIC	10/100/1000 Mbps X 1 Port or more				
	OS	AIX 7.2 (64-bit)	Rocky Linux 8.7 (64-bit) (kernel 4.18.0)	Windows Server 2019 (64-bit)		
	DBMS	DB2 11.5	Oracle 19c, Tibero 7, Mysql 8.0.35	MSSQL 2019		
CubeOne Server (API)	CPU	POWER7 3.0 GHz or higher	sparcv9 2848 MHz or higher	Intel(R) Itanium 2 1.6 GHz or higher	Intel Dual Core 1.8 GHz or higher	Intel Dual Core 1.8 GHz or higher
	Memory	4 GB or higher				
	HDD	At least 200 MB of space required to install the TOE component				
	NIC	10/100/1000 Mbps X 1 Port or more				
	OS	AIX 7.2 (64-bit)	SunOS 5.11 (64-bit)	HP-UX B.11.31 (64-bit)	Rocky Linux 8.7 (64-bit) (kernel 4.18.0)	Windows Server 2019 (64-bit)
CubeOne Security Server	CPU	Intel Core 2 Duo 2.26 GHz or higher				
	Memory	4 GB or higher				

Classification	Minimum Requirement	
	HDD	At least 200 MB of space required to install the TOE component
	NIC	10/100/1000 Mbps X 1 Port or more
	OS	Rocky Linux 8.7 (64-bit) (kernel 4.18.0)
	Essential S/W	- Mysql 8.0.35 - Apache tomcat 9.0.82

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for a log administrator's PC to access the component CubeOne Security Server using the following web browser.

Category	Contents
Required S/W (Web Browser)	Chrome V118.0 (64-bit)

[Table 2] The minimum requirements for the administrator's PC

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	CubeOne V3.0	
Version	rev.0025	
TOE Components	CubeOne Manager	CubeOne_Manager_V3.0.00.03 (CubeOne_Manager_V3.0.00.03.exe)
	CubeOne Server	[Plug-In type] CubeOne_Server_V3.0.00.03_L64_4.18_OR19C (CubeOne_Server_V3.0.00.03_L64_4.18_OR19C.tar) CubeOne_Server_V3.0.00.03_A64_7.2_DB11.5

		(CubeOne_Server_V3.0.00.03_ A64_7.2_DB11.5.tar) CubeOne_Server_V3.0.00.03_L64_4.18_TI7 (CubeOne_Server_V3.0.00.03_L64_4.18_TI7.tar) CubeOne_Server_V3.0.00.03_L64_4.18_MY8 (CubeOne_Server_V3.0.00.03_L64_4.18_MY8.tar) CubeOne_Server_V3.0.00.03_W64_10_MS19 (CubeOne_Server_V3.0.00.03_W64_10_MS19.exe) [API type] CubeOne_Server_V3.0.00.03_A64_7.2_API (CubeOne_Server_V3.0.00.03_A64_7.2_API.tar) CubeOne_Server_V3.0.00.03_S64_5.11_API (CubeOne_Server_V3.0.00.03_S64_5.11_API.tar) CubeOne_Server_V3.0.00.03_H64_B.11.31_API (CubeOne_Server_V3.0.00.03_H64_B.11.31_API.tar) CubeOne_Server_V3.0.00.03_L64_4.18_API (CubeOne_Server_V3.0.00.03_L64_4.18_API.tar) CubeOne_Server_V3.0.00.03_W64_10_API (CubeOne_Server_V3.0.00.03_W64_10_API.exe)
	CubeOne Security Server	CubeOne_SServer_V3.0.00.03_L64_4.18_MY (CubeOne_SServer_V3.0.00.03_L64_4.18_MY.tar)
Guidance Document	CubeOne_OPE_V3.0.0.3 (CubeOne_OPE_V3.0.0.3.pdf) CubeOne_PRE_V3.0.0.4 (CubeOne_PRE_V3.0.0.4.pdf)	

[Table 3] TOE identification

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

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Scheme for IT Security (May

	17, 2021)
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, KECS-PP-0820a-2017, December 11, 2019
Developer	eGlobal Systems Co., LTD.
Sponsor	eGlobal Systems Co., LTD.
Evaluation Facility	Korea System Assurance (KoSyAs)
Completion Date of Evaluation	November 24, 2023
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [6][7] for the TOE claims strict conformance to the National Protection Profile for Database Encryption V1.1 [9], and complies security policies defined in the PP [9] by security requirements. Thus, the TOE provides security features defined in the PP [9] as follows:

- Security audit: The TOE generates audit records of security relevant events including the start-up/shutdown of the audit functions, integrity violation and self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic operations and cryptographic key management operations using cryptographic module (COLib V1.2.0) validated under the KCMVP.
- Identification and authentication: The TOE provides the identification and authentication operations for administrators using ID and password. The TOE mutually authenticates TOE components when they communicate each other.
- Security management: Security management of the TOE is restricted to only the authorized administrator who can access the management interface provided by TOE.

- Protection of the TSF: The TOE provides secure communications amongst TOE components to protect confidentiality and integrity of the transmitted data between them. The TOE provides the self-test and integrity verification functions of TSF execution code and TSF data.
- TOE access: The TOE manages the authorized administrator's access to itself by terminating and lock interactive sessions after predefined time interval of their inactivity for CubeOne Security Server and CubeOne Manager, respectively.

4. Assumptions and Clarification of Scope

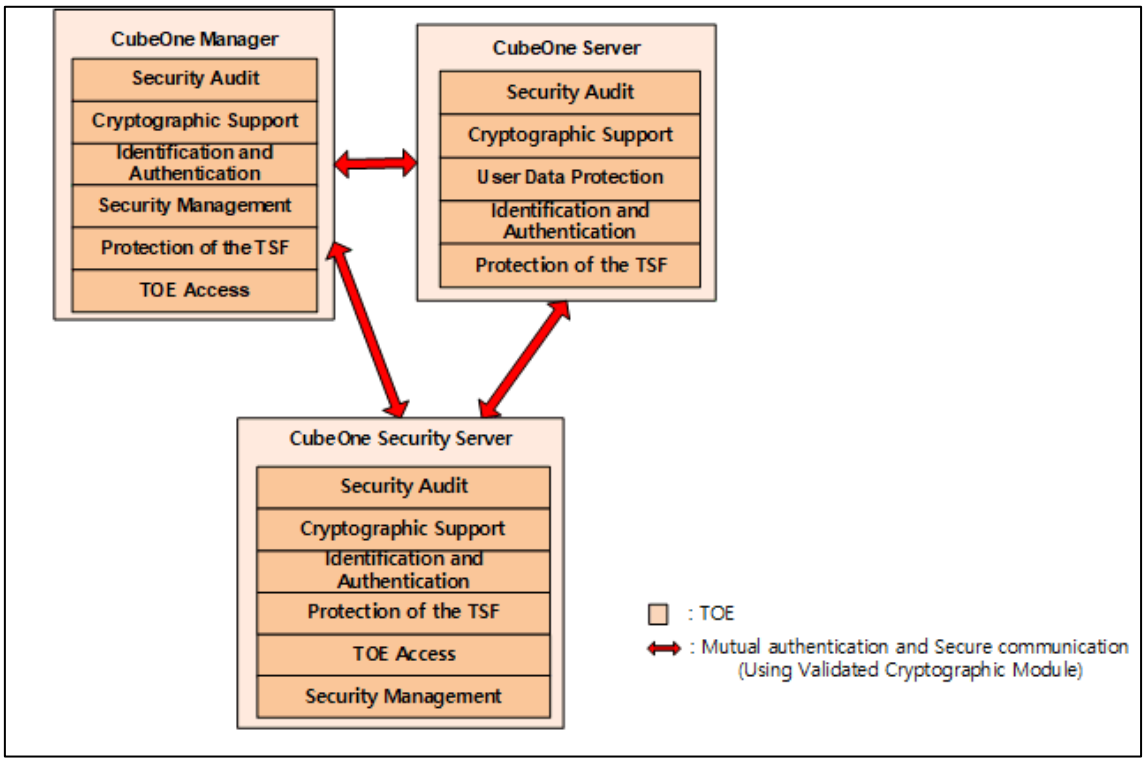
There is no explicit Security Problem Definition chapter, therefore no Assumptions section in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [9] in which the TOE will be used or is intended to be used (For the detailed and precise definition of the security objectives of the operational environment, refer to the ST [6][7], chapter 3.).

5. Architectural Information

The TOE is software consisting of the following components:

- CubeOne Manager
- CubeOne Server, and
- CubeOne Security Server.

Cryptographic module (COLib V1.2.0) validated under the KCMVP are embedded in the TOE Components.



[Figure 3] Architectural Information of the TOE

6. Documentation

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

Identifier	Release	Date
CubeOne_OPE_V3.0.0.3 (CubeOne_OPE_V3.0.0.3.pdf)	V3.0.0.3	October 25, 2023
CubeOne_PRE_V3.0.0.4 (CubeOne_PRE_V3.0.0.4.pdf)	V3.0.0.4	November 22, 2023

[Table 5] Documentation

7. TOE Testing

The developer took a testing approach based on the APIs and security services 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

The evaluator set up the test configuration and testing environment, which are consistent with the ST [6][7]. The evaluator performed all tests provided by developer, 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 CubeOne V3.0 (version number rev.0025). See table 3 for detailed information on the TOE components.
The TOE is installed from the CD-ROM distributed by eGlobal Systems Co., LTD. After installing the TOE, the customer can check the TOE version from 'About CubeOne' menu in the CubeOne Manager. The guidance documents listed in this report chapter 6, [Table 5] 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 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 it is 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 uniquely identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.
The configuration list includes the TOE and the evaluation evidence required by the

SARs in the ST. Therefore, the verdict PASS is assigned to ALC_CMS.1.
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 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.

9.4 Development Evaluation (ADV)

The developer has provided a high-level description of at least 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 TSF, 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, 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_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.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		
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 6] 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 shall be in a physically secure environment to which only the authorized administrator is allowed to access. The TOE shall not allow remote management.
- The authorized administrator of the TOE shall preserve a secure state of the TOE by various methods such as keeping the OS and the DBMS up to date with the latest patch, eliminating unnecessary services, and changing the default ID and password.
- The administrator shall periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data to prevent audit data loss.
- In order to install and operate the TOE, it is recommended that developers of an application server should fully understand the guidance documents (the preparative procedures guidance and the operational user guidance).

11. Security Target

CubeOne V3.0 Security Target V3.0.0.5 [6] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [7] according to the CCRA

supporting document ST sanitizing for publication [8].

12. Acronyms and Glossary

API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HDD	Hard Disk Drive
ID	Identification
IT	Information Technology
KCMVP	Korea Cryptographic Module Validation Program
NIC	Network Interface Card
OS	Operation System
PC	Personal Computer
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
S/W	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

Application server	The application server 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 application server in the operational environment of the TOE reads data from a DB (database), and also sends data to be stored to the DB.
DBMS	A software system composed to configure and apply the

	database. The DBMS related to encryption by column refers to the database management system based on the relational database model.
Encryption	The act that converts the plaintext into the ciphertext using an encryption key

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
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

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

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

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

[5] KOSYAS-2023-11 CubeOne V3.0 Evaluation Technical Report V2.00, 24 November 2023

[6] CubeOne V3.0 Security Target V3.0.0.5, 22 November 2023 (Confidential Version)

[7] CubeOne V3.0 Security Target (ST Lite) V3.0.0.5, 22 November 2023 (Sanitized Version)

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

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