KECS-CR-19-12

CubeOne V2.5

Certification Report

Certification No.: KECS-CISS-0919-2019

2019. 3. 4.

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2019.03.04.	-	Certification report for CubeOne V2.5 - First documentation

This document is the certification report for CubeOne V2.5 of eGlobal Systems Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

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 V2.5 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.

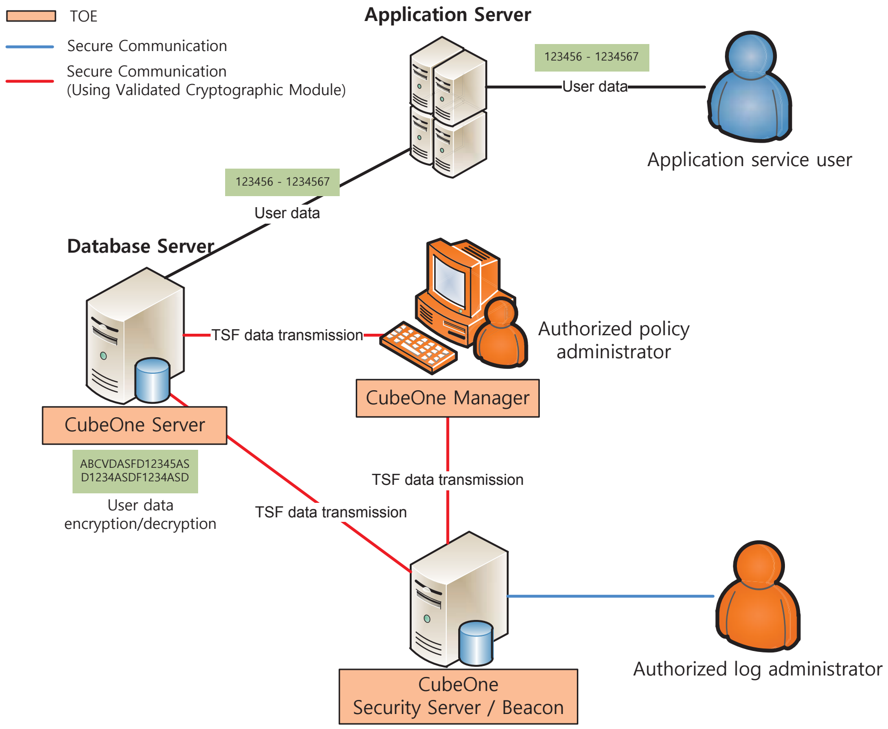
The Target of Evaluation (TOE) is database encryption software that provides encryption and decryption for the user data in a column of a database to be protected. The TOE consists of five software components: CubeOne Manager, CubeOne Server (Plug-In), CubeOne Server (API), CubeOne Security Server, and CubeOne Beacon. CubeOne Manager allows an authorized administrator to access the management interface, CubeOne Server encrypts and decrypts the user data based on the policy set by the authorized administrator, CubeOne Security Server stores the policies configured by the authorized administrator and audit records in the DBMS, and CubeOne Beacon analyzes potential violations and provides the authorized administrator to review all audit records. The TOE includes a cryptographic module validated under the Korea Cryptographic Module Validation Program (KCMVP).

The operational environment of the TOE defined in the Security Target (ST) [6] is classified into two types depending on the location where CubeOne Server installed: plug-in and API types. CubeOne Server is installed in a database server and an application server in the plug-in and API types, respectively. Regardless of the operational environment, CubeOne Security Server and CubeOne Beacon are installed in the same server.

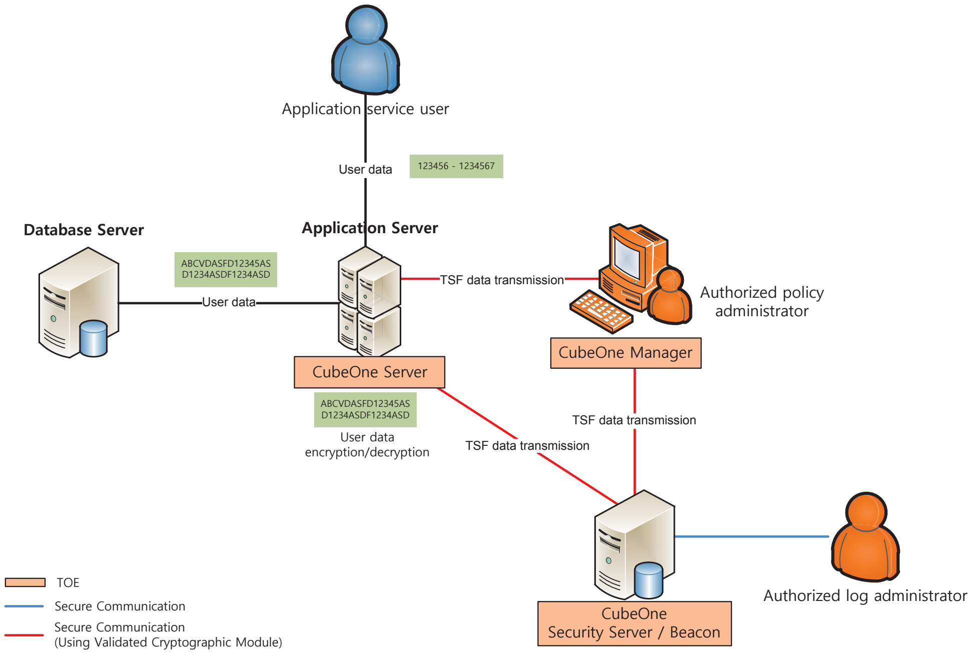
The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on February 7, 2019. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the ST [6].

The ST claims strict conformance to the Korean National PP for Database Encryption V1.0 [7]. 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 [7]. 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.



[Figure 1] Operational environment of the TOE (Plug-in type)



[Figure 2] Operational environment of the TOE (API type)

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

Category		Contents
CubeOne Manager	CPU	Intel Dual Core 2.26 GHz or higher
	RAM	4 GB or higher
	HDD	200 MB or higher space for installation of CubeOne Manager
	NIC	10/100/1000 X 1Port or higher
	OS	Windows 7 Pro 32-bit
	Required S/W	Oracle Client 11g MS Visual C++ 2010 Redistributable Package (x86)
CubeOne Server (Plug-In)	CPU	POWER5 process 1.5 GHz or higher
	RAM	4 GB or higher
	HDD	200 MB or higher space for installation of CubeOne Server (Plug-In)
	NIC	10/100/1000 X 1Port or higher
	OS	AIX 6.1 64-bit
	Required S/W	Oracle Database 11g Release 2 * Software that manages the database to be protected
CubeOne Server (API)	CPU	Intel Dual Core 1.8 GHz or higher
	RAM	4GB or higher
	HDD	200 MB or higher space for installation of CubeOne Server (API)
	NIC	10/100/1000 X 1Port or higher
	OS	CentOS 6.9 (Kernel 2.6.32-696) 64-bit
CubeOne Security Server, CubeOne Beacon	CPU	Intel Dual Core 2.26 GHz or higher
	RAM	4 GB or higher
	HDD	200 MB or higher space for installation of CubeOne Security Server and CubeOne Beacon
	NIC	10/100/1000 X 1Port or higher
	OS	CentOS 6.9 (Kernel 2.6.32-696) 64-bit
	Required S/W	MariaDB 10.0.33 Apache Tomcat 8.5.34

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator’s PC to access CubeOne Beacon.

Category	Contents
CPU	Intel Dual Core 2.26 GHz or higher
RAM	4 GB or higher
HDD	100 GB or higher
NIC	10/100/1000 X 1Port or higher
OS	Windows 7 Pro 32/64-bit
Required S/W	Chrome V 70

[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 consists of the following software component and related guidance documents.

TOE	CubeOne V2.5	
Version	rev.0002	
TOE Components	CubeOne Manager	CubeOne_Manager_V2.5.00.01 (CubeOne_Manager_V2.5.00.01.exe)
	CubeOne Server (Plug-In)	CubeOne_Server_V2.5.00.01_A64_6.1_OR11 (CubeOne_Server_V2.5.00.01_A64_6.1_OR11.tar)
	CubeOne Server (API)	CubeOne_Server_V2.5.00.01_L64_2.6_API (CubeOne_Server_V2.5.00.01_L64_2.6_API.tar)
	CubeOne Security Server	CubeOne_SServer_V2.5.00.01_L64_2.6_MA (CubeOne_SServer_V2.5.00.01_L64_2.6_MA.tar)
	CubeOne Beacon	CubeOne_Beacon_V2.5.00.01 (CubeOne_Beacon_V2.5.00.01.tar.gz)

Guidance Document	CubeOne_PRE_V2.5.1.1.pdf CubeOne_OPE_V2.5.1.2.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 (August 24, 2017) Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)
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 PP for Database Encryption V1.0, KECS-PP-0820-2017, August 18, 2017
Developer	eGlobal Systems Co., Ltd
Sponsor	eGlobal Systems Co., Ltd
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	February 7, 2019
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [6] for the TOE claims strict conformance to the Korean National PP for Database Encryption V1.0 [7], and complies security policies defined in the PP [7] by security requirements. Thus, the TOE provides security features defined in the PP [7] 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, and self-test failures, then 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 module (KLIB V2.2) 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 attributes such as connection IP address, 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 section, in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [7] 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], chapter 3.).

5. Architectural Information

The TOE is software consisting of the following components:

- CubeOne Manager provides security features of identification and authentication of administrators, security management to the TOE and TSF data, access control to CubeOne Manager
- CubeOne Server (Plug-In) and CubeOne Server (API) encrypt and decrypt the user data in a column of a database.
- CubeOne Security Server manages authorized administrators' sessions.
- CubeOne Beacon provides functionality of security management to the TOE and access control to CubeOne Beacon.

Note that all the five 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 [6], chapter 1.4.2.

6. Documentation

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

Identifier	Release	Date
CubeOne_PRE_V2.5.1.1.pdf	V1.1	Oct. 26, 2018
CubeOne_OPE_V2.5.1.2.pdf	V1.2	Jan. 28, 2019

[Table 5] Documentation

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.: Identifier of each test case
- 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 CubeOne V2.5 (version number rev.0002). 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, an administrator can identify the TOE version through the product's Info check menu. 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 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 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 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, 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.2	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	
		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 administrator should install and operate the TOE and DBMS in a physically secure environment that is accessible only by the authorized administrator, and should not allow remote management from the outside.
- Developers who link the encryption function to the application or DBMS should ensure that the security functions of the TOE are applied safely in accordance with the requirements of the manual.
- When operating the product, the administrator's password should be changed periodically.
- It is necessary to maintain the reliability and safety of the operating system by performing reinforcement work on the latest vulnerabilities of the operating system installed and operated by the TOE.
- The authorized administrator should maintain the secure state, such as applying the latest security patches to the operating system and DBMS, and removing unnecessary services, when operating the product.
- The authorized administrator shall periodically check the free space of the audit data storage in preparation for the loss of the audit records and perform the backup of the audit records so that the audit records are not deleted.
- The administrator should perform periodic monitoring through CubeOne Beacon when a potential security violation event occurs after installing the product.
- In order to prevent modification and deletion of the audit log from unauthorized users, the policy manager should manage the PC so that only the authorized policy manager can access the system (PC).

11. Security Target

CubeOne V2.5 Security Target V1.2 [6] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
KCMVP	the Korea Cryptographic Module Validation Program
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

Decryption	The act that restoring the ciphertext into the plaintext using the decryption key
Encryption	The act that converting the plaintext into the ciphertext using the cryptographic key
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

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 (August 24, 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)

[5] TTA-CCE-17-015-ETR-05 CubeOne V2.5 Evaluation Technical Report V1.5, February 26, 2019

[6] CubeOne V2.5 Security Target V1.2, January 31, 2019

[7] Korean National PP for Database Encryption V1.0 (KECS-PP-0820-2017, August 18, 2017)