KECS-CR-20-68

CubeOne V2.5 SP1

Certification Report

Certification No.: KECS-CISS-1054-2020

2020. 11. 26.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2020.11.26.	-	Certification report for CubeOne V2.5 SP1 - First documentation

This document is the certification report for CubeOne V2.5 SP1 of eGlobal Systems Co., ltd

The Certification Body

IT Security Certification Center

The Evaluation Facility

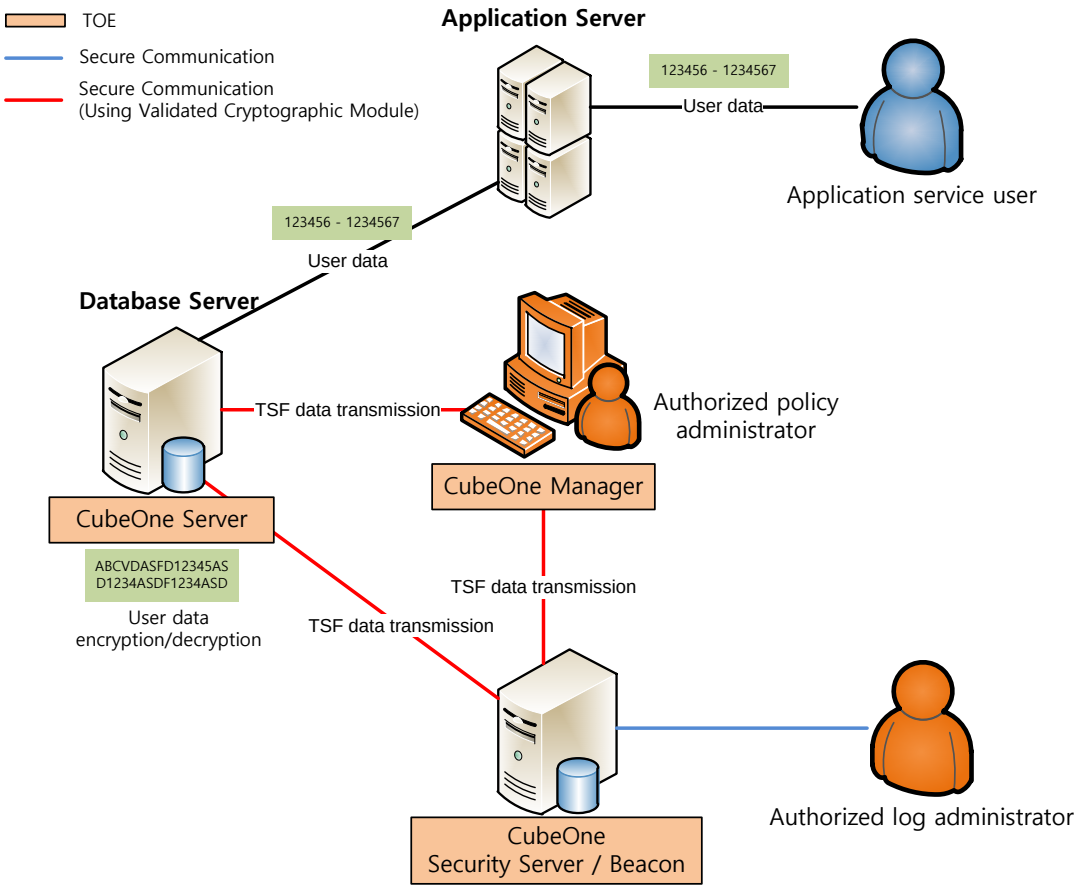
Telecommunications Technology Association (TTA)

Table of Contents

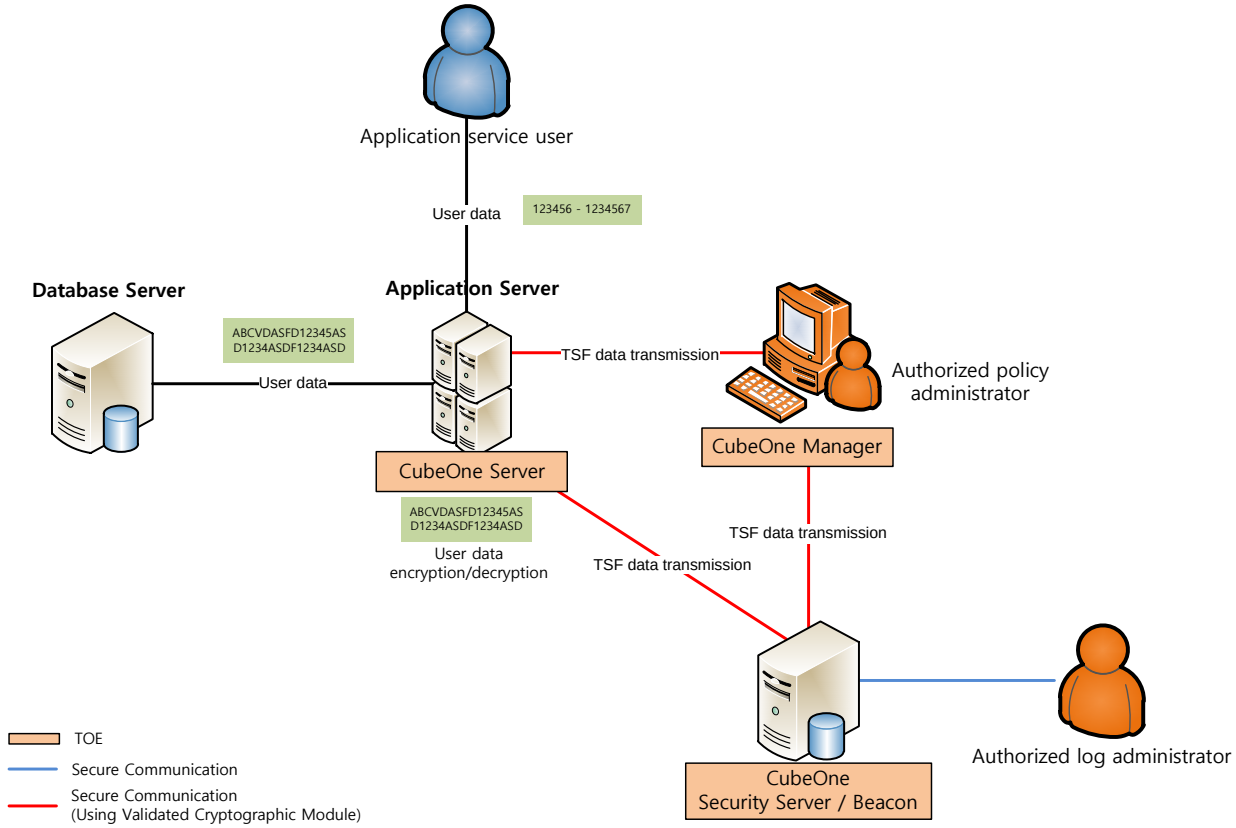
1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the EAL1+ evaluation of CubeOne V2.5 SP1("TOE" hereinafter) 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 TOE is provided as software and provides the encryption/decryption function for the user data by each column of Database. The TOE consists of CubeOne Security Server that save cryptographic policy and security audit log of TOE, CubeOne Manager that configure and control cryptographic policy like role definition of TOE, CubeOne Server that perform cryptographic operation of user data for TOE, and CubeOne Beacon that perform latent violation analysis and security alert of TOE. The plug-in type shown in [Figure 1], which is installed in the protected DB server, performs encryption/decryption of the user data. And API type shown in [Figure 2] which is installed in Application server developed to provide a certain application service, encrypts/decrypts user data on it. CubeOne Beacon and CubeOne Security Server are installed in the same server. The authorized administrator can connect to CubeOne Manager for security control. The authorized user can connect CubeOne Beacon to check security alert and audit log. The TOE is required to use the cryptographic algorithm validated in the Korea Cryptographic Module Validation Program (KCMVP). The TOE is used to encrypt the user data according to the policy set by the authorized administrator to prevent the unauthorized disclosure of the confidential information. In order that the authorized administrator can operate the TOE securely in the operational environment of the organization, the TOE provides various security features such as the security audit function that records and manages major auditable events; cryptographic support

function such as cryptographic key management to encrypt the user and the TSF data, and cryptographic operation; user data protection function that encrypts the user data and protects the residual information; identification and authentication function such as verifying the identity of the authorized administrator, authentication failure handling, and mutual authentication among the TOE components; security management function for security functions, role definition, and configuration; TSF protection functions including protecting the TSF data transmitted among the TOE components, protecting the TSF data stored in the storage that is controlled by the TSF, and TSF self-test; and TOE access function to manage the access session of the authorized administrator. The DEK (Data Encryption Key) used to encrypt/decrypt the user data is protected by encryption with the KEK (Key Encryption Key). The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on November 10, 2020. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the Security Target (ST) [6]. The ST claims strict conformance to the Korean National Protection Profile for Data Encryption V1.1 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. 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. The operational environment of the TOE is shown in [Figure 1, 2] TOE Operational Environment. The operational environment of the TOE includes all the two types(API type, plug-in type) defined in the PP [3].



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



[Figure 2] API Operational environment of the TOE

Item	Minimum operation specification				
CubeOne Server (Plug-In)	CPU	POWER5 2.0Ghz above	sparcv9 2848 MHz above	Intel(R) Itanium 2 1.6 GHz above	Intel Dual Core 1.8GHz above
	Memory	4GB above			
	HDD	At least 200MB of space required to install TOE			
	NIC	10/100/1000 X 1Port above			
	OS	AIX 7.1 64bit	SunOS 5.11 64bit	HP-UX 11.31 64bit	CentOS 7.8.2003 64bit (kernel 3.10.0-1127.el7.x86_64)

Item	Minimum operation specification			
	DBMS	Tibero 6 DB2 10.5	Tibero 6	
CubeOne Server (API)	CPU	POWER5 2.0Ghz above	sparcv9 2848 MHz above	Intel(R) Itanium 2 1.6 GHz above
	Memory	4GB above		
	HDD	At least 200MB of space required to install TOE		
	NIC	10/100/1000 X 1Port above		
	OS	AIX 7.1 64bit	SunOS 5.11 64bit	HP-UX 11.31 64bit
CubeOne Manager	CPU	Intel Core 2 Duo 2.40GHz above		
	Memory	4GB above		
	HDD	At least 200MB of space required to install TOE		
	NIC	10/100/1000 X 1Port above		
	OS	Windows 2012 R2 Standard 64bit		
	essential S/W	- IBM Data Server Client Packages Version 10.5 - Tibero6 ODBC client - MS Visual C++ 2010 Redistributable Package (x86)		
CubeOne Security Server / Beacon	CPU	Intel Core 2 Duo 2.26 GHz above		
	Memory	4GB above		
	HDD	At least 200MB of space required to install TOE		
	NIC	10/100/1000 X 1Port above		
	OS	CentOS 7.8.2003 64bit (kernel 3.10.0-1127.el7.x86_64)		
	essential S/W	- MariaDB 10.5.5 - Apache tomcat 8.5.57		
Authorized log administrator	Web browser	Chrome V 70		

[Table 1] Hardware and software requirements for the TOE

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

2. Identification

The TOE reference is identified as follows.

TOE	CubeOne V2.5 SP1
Version	V2.5 SP1
Detail version	rev.0002
TOE Components	- CubeOne_Manager_V2.5.00.01_SP1 - CubeOne_Server_V2.5.00.01_SP1_A64_7.1_TI6 - CubeOne_Server_V2.5.00.01_SP1_A64_7.1_DB10.5 - CubeOne_Server_V2.5.00.01_SP1_S64_5.11_TI6 - CubeOne_Server_V2.5.00.01_SP1_H64_B.11.31_TI6 - CubeOne_Server_V2.5.00.01_SP1_L64_3.10_TI6 - CubeOne_Server_V2.5.00.01_SP1_A64_7.1_API - CubeOne_Server_V2.5.00.01_SP1_S64_5.11_API - CubeOne_Server_V2.5.00.01_SP1_H64_B.11.31_API - CubeOne_SServer_V2.5.00.01_SP1_L64_3.10_MA - CubeOne_Beacon_V2.5.00.01_SP1
Guidance Documents	CubeOne_OPE_V2.5.1.1_SP1.pdf CubeOne_PRE_V2.5.1.2_SP1.pdf

[Table 2] TOE identification

[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 Scheme for IT Security

	(September 12, 2017)[4]
TOE	CubeOne V2.5 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+ (augmented by ATE_FUN.1)
Developer	eGlobal Systems Co., ltd
Sponsor	eGlobal Systems Co., ltd
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	November 10, 2020
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE provides following security features. For more details refer to the ST [6].

TSF	Explanation
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 operation such as encryption/decryption, and cryptographic key management such as key generation/distribution/destruction using COLib V1.1.0
User data protection	The TOE provides encryption / decryption function for each column of Database to protect user data.
Identification and Authentication	The TOE identifies and authenticates the administrators(Policy administrator, General administrator) based on ID/PW. Mutual authentication between TOE components.
Security	Only the authorized administrator who can access the management

TSF	Explanation
Management	interface provided by TOE can performs security management of the 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 also protects TSF data against unauthorized exposure and modification through encryption.
TOE Access	The TOE manages the authorized administrator's or end user's access to itself by terminating interactive sessions after defined time interval of their inactivity. The TSF restrict the maximum number of concurrent session, and management access session of the administrator based on Access IP, and same administrator right.

[Table 4] Security features

4. Assumptions and Clarification of Scope

There are no explicit Assumptions in the Security Problem Definition in the Low Assurance ST. The followings are procedural method supported from operational environment in order to provide the TOE security functionality accurately.

- The place where the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access
- The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidance.
- 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.
- The authorized administrator of the TOE shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
- The TOE accurately records incidents related to security by receiving reliable time stamps provided by the TOE operating environment.
- DBMS that saves the TSF data and audit data is operated in a physically safe environment.
- All information that is sent when an authorized log administrator connect to the Web server through the Web browser shall be protected through a secure channel.

5. Architectural Information

The physical scope of TOE is CubeOne Manager, CubeOne Server, CubeOne Security Server, CubeOne Beacon and those are inside CD. The major security functions of the TOE and logical scope of the TOE are shown in [Figure 1, 2] and chapter 3, [Table 3].For the detailed description, refer to the ST [6, 7].

6. Documentation

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

Identifier	Release	Date
CubeOne_PRE_V2.5.1.2_SP1.pdf	V1.2	Sep. 11, 2020
CubeOne_OPE_V2.5.1.1_SP1.pdf	V1.1	Sep. 10, 2020

[Table 5] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component 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 has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator 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: CubeOne V2.5 SP1(rev.0002)

- CubeOne_Manager_V2.5.00.01_SP1
- CubeOne_Server_V2.5.00.01_SP1_A64_7.1_TI6
- CubeOne_Server_V2.5.00.01_SP1_A64_7.1_DB10.5
- CubeOne_Server_V2.5.00.01_SP1_S64_5.11_TI6
- CubeOne_Server_V2.5.00.01_SP1_H64_B.11.31_TI6
- CubeOne_Server_V2.5.00.01_SP1_L64_3.10_TI6
- CubeOne_Server_V2.5.00.01_SP1_A64_7.1_API
- CubeOne_Server_V2.5.00.01_SP1_S64_5.11_API
- CubeOne_Server_V2.5.00.01_SP1_H64_B.11.31_API
- CubeOne_SServer_V2.5.00.01_SP1_L64_3.10_MA

- CubeOne_Beacon_V2.5.00.01_SP1

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, [Table 4] were evaluated with the TOE

9. Results of the Evaluation

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 specifications 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 penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.1.
Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing basic attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_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

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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	
		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 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 Beacon when a potential security violation event occurs after installing the product.
- The policy manager should manage the PC so that only the authorized policy manager can access the system to prevent modification and deletion of the audit log from unauthorized users.

11. Security Target

The CubeOne V2.5 SP1 Security Target V1.3, November 5, 2020 [6] is included in this report by 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

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, KECS-PP-0820a-2017, December 11, 2019

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

[5] TTA-CCE-19-008 CubeOne V2.5 SP1 Evaluation Technical Report V1.3, November 10, 2020

[6] CubeOne V2.5 SP1 Security Target V1.3, November 05, 2020