KECS-CR-23-30

ubCUBE v3.7

Certification Report

Certification No.: KECS-CISS-1236-2023

2023. 4. 28.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023. 4. 28.	-	Certification report for ubCUBE v3.7 - First documentation

This document is the certification report for ubCUBE v3.7 of Iqpad, Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

KOREA TESTING & RESEARCH INSTITUTE (KTR)

Table of Contents

1. Executive Summary

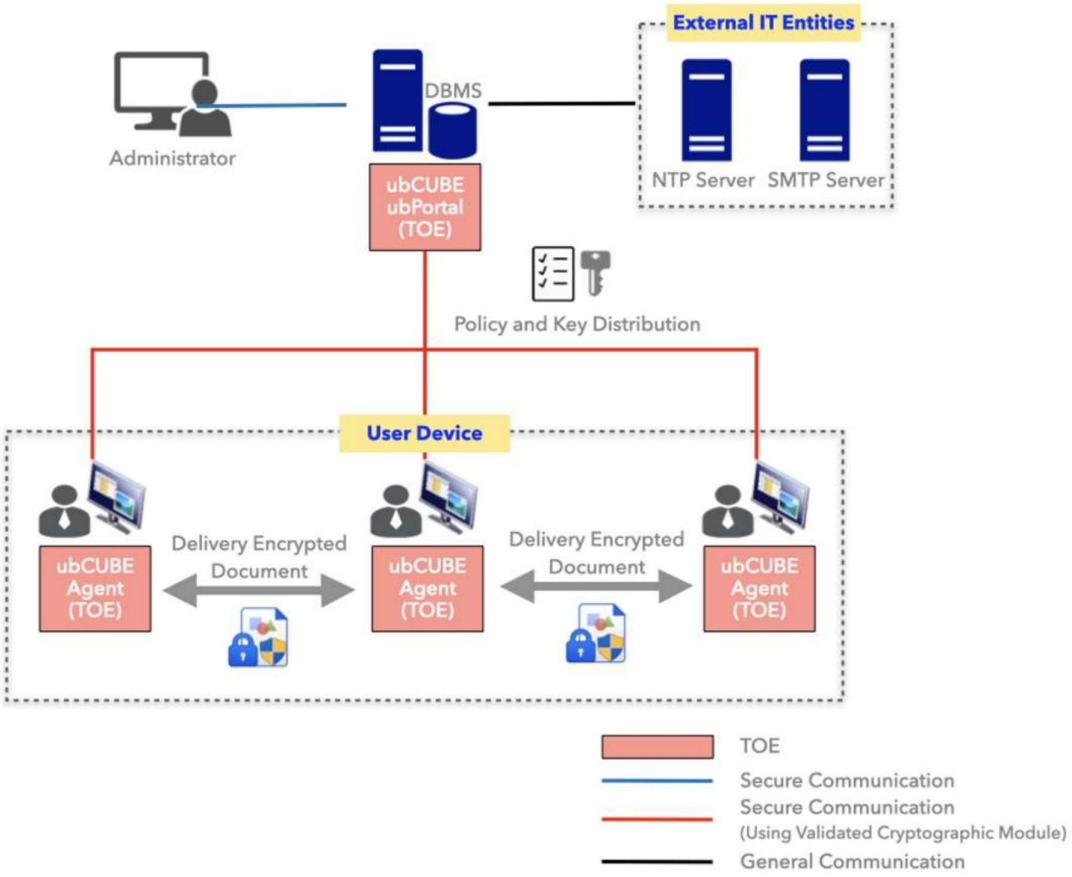
This report describes the evaluation result drawn by the evaluation facility on the results of the ubCUBE v3.7 developed by Iqpad, Inc. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (“TOE” hereinafter) is Electronic Document Encryption designed to protect important documents managed by the organization based on the encryption/decryption. Also, the TOE provides a variety of security features: security audit, 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 TESTING & RESEARCH INSTITUTE(KTR) and completed on April 24, 2023.

The ST claims conformance to the Korean National Protection Profile for Electronic Document 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.

[Figure 1] shows the operational environment where the TOE is operated. The TOE is composed of the ubCUBE ubPortal v3.7.0.3(hereinafter 'ubPortal'), ubCUBE Agent v3.7.0.3 (hereinafter 'Agent') and should be installed and operated inside the internal network of the protected organization.



[Figure 1] Operational Environment of the TOE

The administrator sets the policy for each document user through the ubCUBE ubPortal, which distributes the policy and cryptographic key configured by the administrator to the ubCUBE Agent. The ubCUBE Agent performs Electronic Document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted/decrypted document is stored in the user PC as a file. The 'ubXFS Cryptographic Module V1.1' validated cryptographic module is used for the cryptographic operation of the major security features of the TOE. For the communication between the TOE component and the administrator (e.g., the administrator accesses the ubCUBE ubPortal using the web browser to configure policies), TLS 1.2 is used. There are external entities necessary for the operation of the TOE including the NTP server to synchronize time and email server to notify the authorized administrator in case of audit data loss. The requirements for hardware, software, and operating system to install the TOE are as in [Table 1].

Component			Requirement	Remarks
ubPortal	H/W	CPU	Intel(R) Xeon(R) 3 GHz 6 core or higher	-
		HDD	Space required for TOE installation is 100 GB or higher	-
		RAM	16 GB or higher	-
		NIC	100/1000 Mbps 1 Port or higher	-
	S/W	OS	Microsoft Windows Server 2012 R2 Standard (64bit)	Supported operation systems of the ubPortal
		3rd Party S/W	Microsoft IIS 8.5 Microsoft .NET Framework 4.5 Microsoft .NET Framework 4.7 Microsoft ASP.NET 4.5 Microsoft SQL Server 2016	Third-party software required to run ubPortal
Agent	H/W	CPU	Intel i3 Dual Core 2.50 GHz or higher	-
		HDD	4 GB or higher	-
		RAM	Space required for TOE installation is 10 GB or higher	-
		NIC	100/1000 Mbps 1 Port or higher	-
	S/W	OS	Microsoft Windows 10 Pro (64 bit) Microsoft Windows 10 Enterprise (64 bit)	Supported operation systems of the Agent
		3rd Party S/W	Microsoft Visual C++ 2015 Redistributable Update 3 Microsoft Office 2010, 2013, 2016, 2019 Hancom Office 2010, 2014, 2018, NEO Adobe Acrobat Reader DC	Third-party software required to run Agent

[Table 1] Hardware/Software Requirements for the TOE

External IT entities linked to the TOE operation are as follows.

Classification	Description
SMTP Server	Email server to send security alerts by email to the authorized administrator
NTP Server	Time server to synchronize time to provide reliable time stamp

[Table 2] External IT entities

Word processing programs that support Electronic Document Encryption are as follows.

Application	Document Type (file extension)
MS Office Word	doc, docx
MS Office PowerPoint	ppt, pptx
MS Office Excel	xls, xlsx
Hancom Office	hwp
Adobe Acrobat Reader	pdf

[Table 3] Encryption/Decryption document types

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	ubCUBE v3.7
Version	3.7.0.3
TOE Components	- ubCUBE ubPortal v3.7.0.3 - ubCUBE Agent v3.7.0.3
Manuals	- ubCUBE v3.7 Operation Guide(ubPortal) v1.1 - ubCUBE v3.7 Operation Guide(Agent) v1.1 - ubCUBE v3.7 Preparation Procedure v1.3

[Table 4] TOE Identification

[Table 5] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (MSIT Notice No. 2022-61, October 31, 2022.) Korea Evaluation and Certification Regulation 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
TOE	ubCUBE v3.7
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National PP for Electronic Document Encryption V1.1 (December 11, 2019)
Developer	Iqpad, Inc.
Sponsor	Iqpad, Inc.
Evaluation Facility	KOREA TESTING & RESEARCH INSTITUTE
Completion Date of Evaluation	April 24, 2023

[Table 5] 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
- Prtoection 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 4])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the TOE's components, namely ubCUBE ubPortal v3.7.0.3 and ubCUBE Agent v3.7.0.3 as well as guidance documents such as ubCUBE v3.7 Preparation Procedure and ubCUBE v3.7 Operation Guide, which are included in the product, ubCUBE v3.7. The TOE is offered in the form of software.

Classification	Identification	Type
TOE component	ubCUBE ubPortal v3.7.0.3 (ubCUBE_v3.7_ubPortal_Setup_v3.7.0.3.exe)	Software (Distributed as a

	ubCUBE Agent v3.7.0.3 (ubCUBE_v3.7_Agent_Setup_v3.7.0.3.exe)	CD)
Manuals	ubCUBE v3.7 Operation Guide(ubPortal) v1.1 (OPE-ubCUBE_v3.7_ubPortal-v1.1.pdf)	PDF (Distributed as a CD)
	ubCUBE v3.7 Operation Guide(Agent) v1.1 (OPE-ubCUBE_v3.7_Agent-v1.1.pdf)	
	ubCUBE v3.7 Preparation Procedure v1.3 (PRE-ubCUBE_v3.7-v1.3.pdf)	

[Table 6] Physical scope of TOE

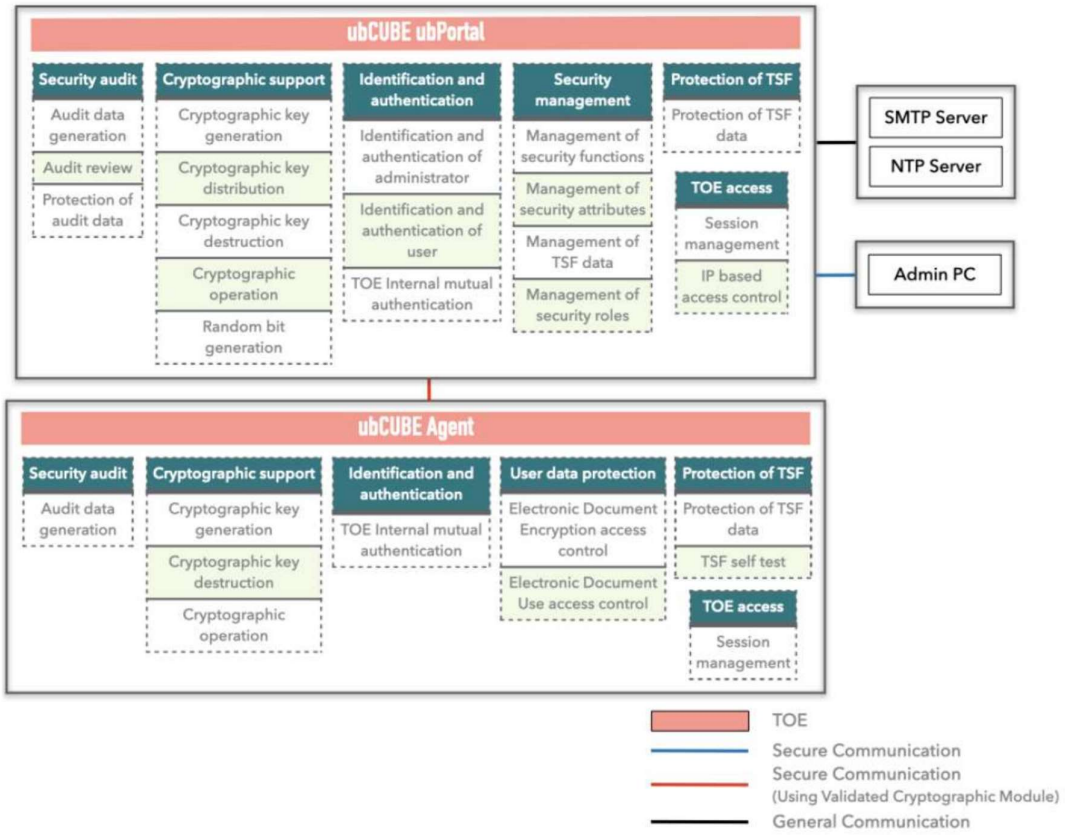
Validated cryptographic modules included the TOE are as follows.

Classification	Description
Cryptographic Module	ubXFS Cryptographic Module V1.1
Validation No.	CM-195-2026.11
Developer	Iqpad, Inc.
Validation Date	2021. 11. 18.
Expiration Date	2026. 11. 18.

[Table 7] Validated Cryptographic Module

2. Logical Scope of TOE

The logical scope of the TOE is shown in the following figure.



[Figure 2] Logical scope of the TOE

▣ Security Audit

The TOE creates and records audit data of the events to the DBMS when a defined audit event occurs. Information including date and time of the event, type of event, subject identity, and result of event (success or failure) are stored in an audit record. The authorized administrator can view the stored audit records and search the records by event type and search conditions. If any potential security violation such as failure of authentication, integrity violation, failure of self-test, exceed of audit trail threshold, exceed of maximum size of audit trail is detected, the TOE sends an email to the administrator to inform the administrator of the potential violation. If audit trail exceeds maximum size, the TOE overwrites the oldest stored audit records to prevent a loss of audit data.

▣ Cryptographic support

The TOE uses the 'ubXFS Cryptographic Module V1.1' validated cryptographic module to perform cryptographic key generation, distribution, destruction, and cryptographic operation. TOE generates 256bit DEK for document and TSF data encryption with Hash_DRBG (SHA-256), KEK for DEK encryption is generated by NIST 800-132 KDF. DEK is securely

distributed with a public key algorithm (RSAES-OAEP, 3072bit) between TOE components. Cryptographic operation for document and TSF data is performed with a symmetric algorithm (ARIA-CBC) whose key size is 256bit. TOE mutual authentication is performed with a public key algorithm (RSAES-OAEP, 3072bit), digital signature of policy data is performed with a digital signature algorithm (RSA-PSS, 3072bit), integration check of TSF data is performed with HMAC(SHA-256), and authentication data is encrypted with SHA-256. A cryptographic key is securely destructed with zeroization in memory after use.

▣ User data protection

The TOE performs access control of the authorized user on document encryption /decryption and use (Expiration date/Modification of permissions/Print) according to the security policy. The authorized administrator can set access control policy per document grade, user/department/group. The access control policy is set based on the security attribute of the user (ID, Allowed document grade, Department ID of the user, Group ID of the user) and the security attribute of protected a document (document type, expiration date).

The following table shows the document types that the TOE supports encryption/decryption.

Application	Document Type (file extension)
MS Office Word	doc, docx
MS Office PowerPoint	ppt, pptx
MS Office Excel	xls, xlsx
Hancom Office	hwp
Adobe Acrobat Reader	pdf

▣ Identification and authentication

The TOE performs mutual authentication between TOE components with the internally implemented authentication protocol, provides identification and authentication of administrator and user based on ID and password. Password is set by combination of each of alphabetical, numerical, and special characters and the length is at least 9 digits and less than 30 digits. The input characters of password are masked with "●" to prevent from disclosure. No feedback is provided on a reason for the failure if authentication fails. When the defined number set by the administrator of unsuccessful authentication attempts has been met, the account is locked out. Reuse of authentication data is prevented with time stamp. The system(global) policy is applied to the user before authentication and the user can access a protected document according to a policy after authentication. The administrator is authenticated through web browser and can perform security management function after authentication.

▣ Security Management

TOE provides management of security functions, security attributes, and TSF data to the authorized administrator. The authorized administrator can manage security function including user and department, security policy, and administrator management through web browser and can manage important TSF data including authentication data, security policy data, and cryptographic key data as well.

▣ Protection of the TSF

The TOE communicates securely to protect transmitted data between TOE components with a public key cryptographic algorithm and assures confidentiality and integrity with a validated cryptographic module. In addition, the TOE protects TSF data that is stored in the repository controlled by the TSF with encryption and digital signature in order to prevent unauthorized disclosure and modification.
The TOE runs a suite of self-tests during initial start-up, periodically during normal operation to prevent unauthorized deletion of agent settings and ensure integrity. The TOE notifies the authorized administrator if an integrity violation is detected. The TOE prevents unauthorized deletion of agent files and unauthorized termination of agent processes with periodic monitoring between agent processes related to the TOE.

▣ TOE access

The TOE provides a management function to register IP addresses that are allowed for management access and performs an access control function that management access is allowed only from a registered IP address. The TOE also restricts the number of maximum concurrent sessions belonging to the same user and permission as 1. The TOE terminates an interactive session of the authorized administrator after 5 minutes of inactivity.

6. Documentation

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

Identification	Date
ubCUBE v3.7 Operation Guide(ubPortal) v1.1 (OPE-ubCUBE_v3.7_ubPortal-v1.1.pdf)	April 6, 2023
ubCUBE v3.7 Operation Guide(Agent) v1.1 (OPE-ubCUBE_v3.7_Agent-v1.1.pdf)	April 6, 2023
ubCUBE v3.7 Preparation Procedure v1.3 (PRE-ubCUBE_v3.7-v1.3.pdf)	April 7, 2023

[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. 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 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: ubCUBE v3.7
Version: 3.7.0.3
- ubCUBE ubPortal v3.7.0.3
- ubCUBE Agent v3.7.0.3

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 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.

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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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 7] 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 Server 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 checks 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.

11. Security Target

ubCUBE v3.7 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

Authorized Document User

The TOE user who may, in accordance with the SFRs, perform an operation

Authorized Administrator

Authorized user to securely operate and manage the TOE

Data Encryption Key (DEK)

Key that encrypts the data

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

External Entity

An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE.

Key Encryption Key (KEK)

Key that encrypts another cryptographic key

Random Bit Generator (RBG)

A device or algorithm that outputs a binary sequence that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the sequence 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.

Validated Cryptographic Module

A cryptographic module that is validated and given a validation number by validation authority

Word Processing Program

Program used to process the important documents, such as generation, modification, manipulation, and print of documents (e.g., Hangul word processor, MS word processor,

Acrobat, Excel, Computer Aided Design(CAD), etc.)

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 Electronic Document Encryption V1.1, December 11, 2019

[4] ubCUBE v3.7 Security Target V1.2, April 10, 2023

[5] ubCUBE v3.7 Independent Testing Report(ATE_IND.1) V1.00, April 10, 2023

[6] ubCUBE v3.7 Penetration Testing Report(AVA_VAN.1) V1.00, April 10, 2023