KECS-CR-26-33

ShadowCube V8.0
Certification Report

Certification No.: KECS-CISS-1415-2026

2026. 7. 30.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2026. 7. 30.	-	Certification report for ShadowCube V8.0 - First documentation

This document is the certification report

for ShadowCube V8.0 of Duruan Co., Ltd.

The Certification Body

IT Security Certification Center (ITSCC)

The Evaluation Facility

KOREA TESTING & RESEARCH INSTITUTE (KTR)

Table of Contents

1. Executive Summary

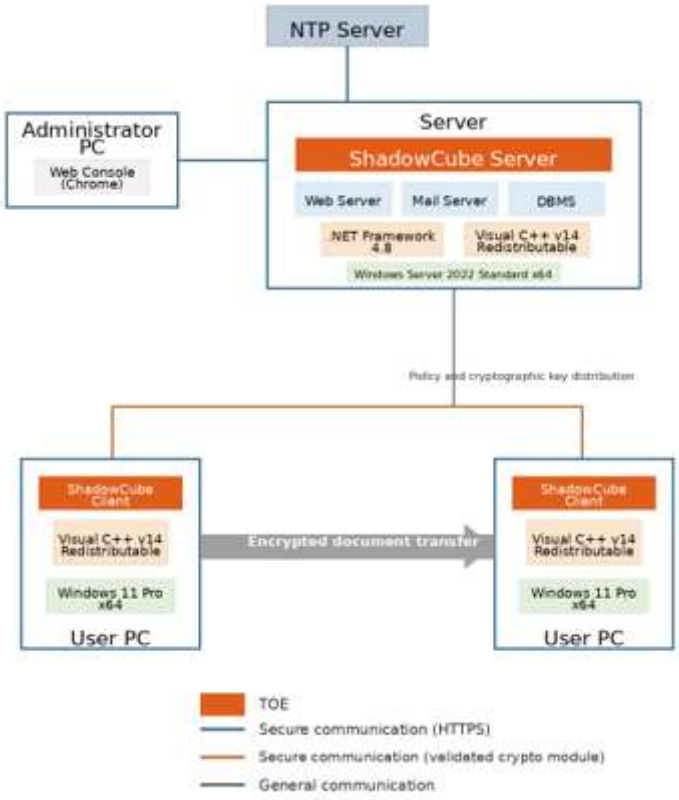
This report describes the evaluation result drawn by the evaluation facility on the results of the ShadowCube V8.0 developed by Duruan Co., Ltd with reference to the Common Criteria for Information Technology Security Evaluation (hereinafter referred to as "CC")[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (hereinafter referred to as "TOE") 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 July 28, 2026

The ST claims conformance to the Korean National Protection Profile for Electronic Document Encryption V3.1[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 ShadowCube Server V8.0.0.4517 (hereinafter referred to as “Server”), ShadowCube Client V8.0.0.4517 (hereinafter referred to as “Client”) and should be installed and operated inside the internal network of the protected organization.



[Figure 1] Operational Environment of the TOE

The TOE encrypts/decrypts documents in accordance with the document group-based access control policy established by an authorized administrator. In addition, it encrypts TSF data in order to protect TSF data when they are transmitted between separate parts of the TOE and when TSF data are stored. The TOE prevents the unauthorized deletion and termination of TSF data, runs self-tests on TSF, and provides the capability to verify the integrity of the TSF and TSF data.

The TOE permits or blocks access by administrators and document users through identification and authentication, provides a password verification mechanism, and disables identification and authentication if login attempts fail more than the number of times configured by the authorized administrator (default: 3). It performs mutual authentication between communication peers using the ECDH algorithm of the validated cryptographic module.

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

Classfication			Requirements	Remarks
Server	H/W	CPU	Intel i7 Quad Core 2.0 GHz or higher	-
		HDD	At least 600MB of free space required for TOE installation	-
		RAM	8 GB or higher	-
		NIC	100/1000 Mbps or higher	-
	S/W	OS	Microsoft Windows Server 2022 Standard (64bit)	Supported operation systems of the Server
		3rd Party S/W	IIS (Internet Information Services) 10.0 Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719 Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719 Microsoft .NET Framework 4.8 Chrome 149.0 PostgreSQL 18.4	Third-party software required to run Server
Client	H/W	CPU	Intel i3 Dual Core 1.0 GHz or higher	-
		HDD	At least 180 MB of space required for TOE	-
		RAM	4 GB or higher	-
		NIC	100/1000 Mbps or higher	-

	S/W	OS	Microsoft Windows 11 Pro (64bit)	Supported operation systems of the Client
		3rd Party S/W	Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719 Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719 MS Office 2024 Hancom Office 2024 Adobe Acrobat Reader DC Autodesk AutoCAD 2026	Third-party software required to run Client

[Table 1] Hardware/Software Requirements for the TOE

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

Classfication	Description
NTP Server	Used for time synchronization to provide trusted timestamps in the TOE.

[Table 2] External IT entities

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

application program	Application Program Version	Document Types (File Extensions)
Notepad	The version included by default in Windows 11 Pro x64, the operational environment for ShadowCube Client	txt
Mspaint		bmp, gif, jpg, png, tif
Wordpad		rtf
MS Office Word	2024	doc, docx
MS Office Excel	2024	xls, xlsx
MS Office Powerpoint	2024	ppt, pptx

Hancom Office 한글	2024	hwp, hwpx
Hancom Office 한셀	2024	nxl, cell
Hancom Office 한쇼	2024	show
Acrobat Reader DC	DC	pdf
Autodesk AutoCAD	2026	dwg, dxf

[Table 3] Encryption/Decryption document types

3rd party Software included in the TOE are as follows.

3rd party S/W	Description
OpenSSL 3.5.4	A third-party module included in the TOE that is used for web management communication between the administrator and the ShadowCube Server.
MagicCrypto V2.3.0	A validated cryptographic module included in the TOE; it is used for the encryption/decryption of protected documents, cryptographic key management, and the encryption/decryption of critical security parameters.

[Table 4] 3rd party S/W(TOE include)

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	ShadowCube V8.0
TOE Version	8.0.0
TOE Components	ShadowCube Server 8.0.0.4517 ShadowCube Client 8.0.0.4517
Manuals	ShadowCube V8.0 Administrator Operational Guidance V1.2 ShadowCube V8.0 User Guidance V1.2 ShadowCube V8.0 Preparative Procedure V1.3

[Table 5] TOE Identification

[Table 6] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, April 7, 2026)
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022 Evaluation methodology, CEM:2022 R1(CCMB-2022-11-006, 2022.11.) Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025
TOE	ShadowCube V8.0
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Electronic Document Encryption V3.1 (June 27, 2025)

Developer	Duruan Co., Ltd
Sponsor	Duruan Co., Ltd
Evaluation Facility	KOREA TESTING & RESEARCH INSTITUTE
Completion Date of Evaluation	July 28, 2026

[Table 6] Additional identification information

3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Document Encryption
- Identification and Authentication
- Security Management
- Protection 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

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the chapter 3.4 of ST[4]):

- The place where the management server among TOE components is installed and operated shall be equipped with access control and protection facilities so that only authorized administrators can access it.
- The authorized administrator of the TOE shall not have malicious intentions, shall be properly trained on TOE management functions, and shall accurately perform duties in accordance with the administrator guidance.
- Developers who use the TOE to integrate document encryption/decryption functions in the operational environment of an information system shall comply with the requirements in the guidance documentation provided with the TOE so that the TOE security functions are applied securely.
- Reinforcement measures shall be performed for the latest vulnerabilities of the operating system on which the TOE is installed and operated, thereby ensuring the reliability and security of the operating system.

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 5])

5. Architectural Information

5.1 Physical Scope of TOE

The TOE components consist of the ShadowCube Server, which manages security policies, and the ShadowCube Client, which performs document encryption/decryption. The physical scope of the TOE consists of the TOE components and the documentation; the TOE components are provided as .exe files, and the documentation is provided as PDF files, all distributed on a CD.

Composition	Subitem	Distribution Format
TOE	ShadowCube V8.0	-
TOE component	ShadowCube Server 8.0.0.4517 (server_8.0.0.4517.exe)	Executable (CD 1)
	ShadowCube Client 8.0.0.4517 (scsetup_8.0.0.4517.exe)	
Guidance	Administrator Operational Guidance: ShadowCube V8.0 Administrator Operational Guidance V1.2.pdf	Electronic Files (CD 1)
	User Guidance: ShadowCube V8.0 User Guidance V1.2.pdf	
	Preparative Procedure: ShadowCube V8.0 Preparative Procedure V1.3.pdf	

[Table 7] Physical scope of the TOE

Validated cryptographic modules included the TOE are as follows.

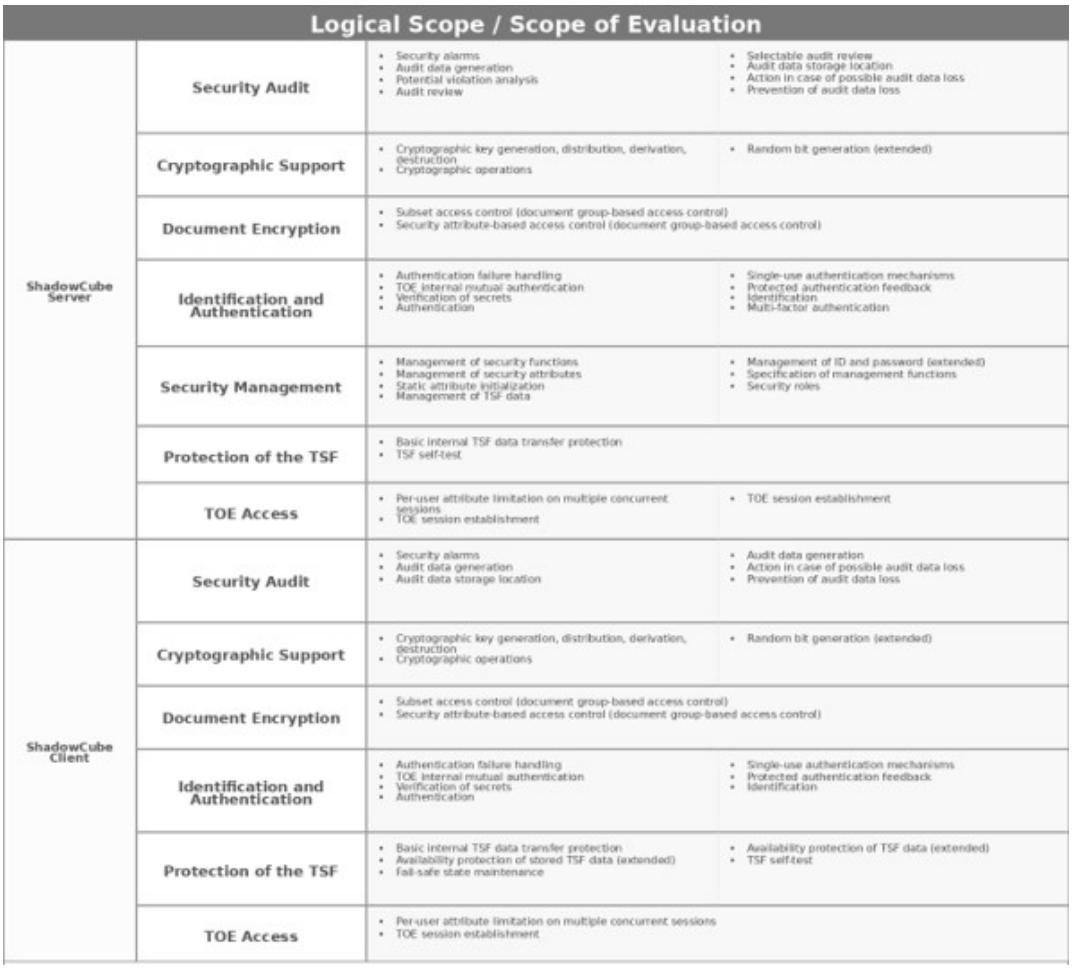
Classfication	Description
Cryptographic Module	MagicCrypto V2.3.0

Validation No.	CM-263-2030.1
Developer	Dream Security Co., Ltd.
Validation Date	January 24, 2025
Expiration Date	January 24, 2030

[Table 8] Validated Cryptographic Module

5.2 Logical Scope of TOE

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



[Figure 2] Logical scope of TOE

▣ Security audit

The TOE generates audit data for all security function operations and, in the event of a potential security violation, sends an email alert to an authorized administrator and logs the incident.

The TOE generates audit data for each TOE components as follows.

ShadowCube Server

- Start/End of Audit Function
- Success/failure of administrator identification and authentication
- Product configuration changes history
- Security function execution history

ShadowCube Client

- Start/End of Audit Function
- Execution of operations on objects
- Successful/Failed Identification and Authentication of Document Users
- Results of TSF self-tests and integrity verification

Audit data includes detailed information on the date and time of the event, the event type, the identity of the entity that triggered the event, the operation details, and the result (success/failure).

Authorized administrators can review all audit data generated by the TOE via the GUI interface. Audit records are generated in a format suitable for interpretation by authorized administrators and allow for selective review based on logical relationship criteria such as AND and OR.

The TOE generates audit data when it predicts a loss of audit data and sends it via email to authorized administrators; to prevent the loss of audit data, it provides a function to overwrite the oldest records when the audit evidence repository becomes full and to send an email notification to authorized administrators.

▣ Cryptographic support

The TOE uses MagicCrypto V2.3.0, the validated cryptographic module developed by Dream Security, in order to apply encryption/decryption algorithms to TSF data according to the security policy, thereby providing assurance of confidentiality, integrity, and

authentication.

The encryption/decryption algorithms used for cryptographic key generation and cryptographic key distribution, and the cryptographic key sizes, are specified below. If cryptographic keys and CSPs loaded in memory are no longer used, they are zeroized and destroyed.

ShadowCube Client: document encryption

- ARIA_CTR 128 bits

ShadowCube Client: Verification of the signature of the document file's author and the ShadowCube Client log creator

- RSA-PSS

ShadowCube Server, ShadowCube Client: Encryption of TSF data and communication data

- ARIA_CBC 256 bits
- RSAES 2048 bits

ShadowCube Server, ShadowCube Client: Hash generation

- SHA-256

ShadowCube Server, ShadowCube Client: Cryptographic Key Distribution

- ARIA_CBC 256 bits

ShadowCube Server, ShadowCube Client: Internal Mutual Authentication Key Agreement Between TOE components

- ECDH

ShadowCube Server, ShadowCube Client: KEK Generation

- PBKDF2

ShadowCube Server, ShadowCube Client: Random Bit Generation

- HASH_DRBG

▣ Document Encryption

On ShadowCube Server, which is a TOE component, the authorized administrator can define the document group-based access control policy required for a document user to encrypt/decrypt a document to be protected. ShadowCube Client, which is a TOE component, provides the function of reading, encrypting (writing) and decrypting a document to be protected, according to the document group-based access control policy

defined by the authorized administrator.

▣ Identification and authentication

The TOE identifies and authenticates the identities of administrators and document users via a GUI interface and restricts access in the event of authentication failure. It does not provide feedback on the reason for failure (e.g., ID error, password error) when identification or authentication fails. The authentication credentials of administrators and document users are processed to prevent reuse. If the number of authentication failures configured by the administrator is reached, authentication is disabled for 5 minutes for administrators and until the system is rebooted for document users.

The TOE performs mutual authentication during communication between the ShadowCube Server and the ShadowCube Client using the ECDH algorithm provided by a validated cryptographic module.

Passwords for administrators and document users must be between 9 and 16 characters long and must consist of a combination of four types of characters: uppercase and lowercase letters, numbers, and special characters.

The TOE identifies and authenticates administrators by administrator ID and email authentication code, and identifies and authenticates document users by document user certificates. In addition, the TOE prevents passwords from being displayed to administrators and users during authentication.

▣ Security management

The TOE provides functionality that allows authorized administrators to configure and manage security functions, security policies, and security roles via a GUI interface.

▣ Protection of the TSF

The TOE protects TSF data from exposure and tampering by encrypting it with a validated cryptographic module when TSF data is transmitted between isolated sections of the TOE. Furthermore, it protects TSF data stored in repositories controlled by the TOE from unauthorized exposure and tampering by encrypting it with a validated cryptographic module.

The ShadowCube Server, a TOE component, performs self-tests and integrity checks at

start-up, periodically during normal operation, and upon request by an authorized administrator. The ShadowCube Client, a TOE component, performs self-tests on key TOE processes and conducts integrity verification of TSF data and the TSF itself at start-up and periodically during normal operation.

Access control policies prevent unauthorized deletion of the configuration files and executable files of the ShadowCube Client, a TOE component, and prevent unauthorized termination of executable files.

The ShadowCube Server and ShadowCube Client, which are TOE components, provide a function to query version information.

▣ TOE access

The TOE terminates the session of an authorized administrator who logged in via the GUI interface if the session timeout has expired. It also provides a function that allows authorized administrators to terminate their own sessions.

TOE limits the number of administrator sessions to one; if a login attempt is made from another device after an administrator has logged in, the new session is allowed, and the previous session is blocked.

Access to the ShadowCube Server is restricted to pre-registered IP addresses only. An authorized administrator can register as many IP addresses as the number of allowed connections.

6. Documentation

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

Identification	Date
Administrator Operational Guidance: ShadowCube V8.0 Administrator Operational Guidance V1.2.pdf	June 29, 2026
User Guidance: ShadowCube V8.0 User Guidance V1.2.pdf	June 29, 2026
Preparative Procedure: ShadowCube V8.0 Preparative Procedure V1.3.pdf	June 29, 2026

[Table 9] 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: ShadowCube V8.0

Version: 8.0.0

- ShadowCube Server V8.0.0.4517
- ShadowCube Client V8.0.0.4517

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 7 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+).

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 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.

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 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.

.

9.5 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_SPD.1	ASE_SPD.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		

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 10] 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 ShadowCube Server must be installed and operated in a physically secure environment accessible only by authorized administrators.
- 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.

11. Security Target

ShadowCube V8.0 Security Target V1.5 [4] is included in this report for reference.

12. Acronyms and Glossary

12.1 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

12.2 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 encryption 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, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022

[2] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-006, November 2022

[3] Korean National Protection Profile for Electronic Document Encryption V3.1, June 27, 2025

[4] ShadowCube V8.0 Security Target V1.5, July 28, 2026

[5] ShadowCube V8.0 Independent Testing Report(ATE_IND.1) V1.01, July 22, 2026

[6] ShadowCube V8.0 Penetration Testing Report(AVA_VAN.1) V1.00, July 01, 2026