KECS-CR-22-61

Document Security V6.0

Certification Report

Certification No.: KECS-CISS-1203-2022

2022. 12. 14.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2022.12.14.	-	Certification report for Document Security V6.0 - First documentation

This document is the certification report for Document Security V6.0 of SoftCamp Co., Ltd.

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 Document Security V6.0 developed by SoftCamp 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.

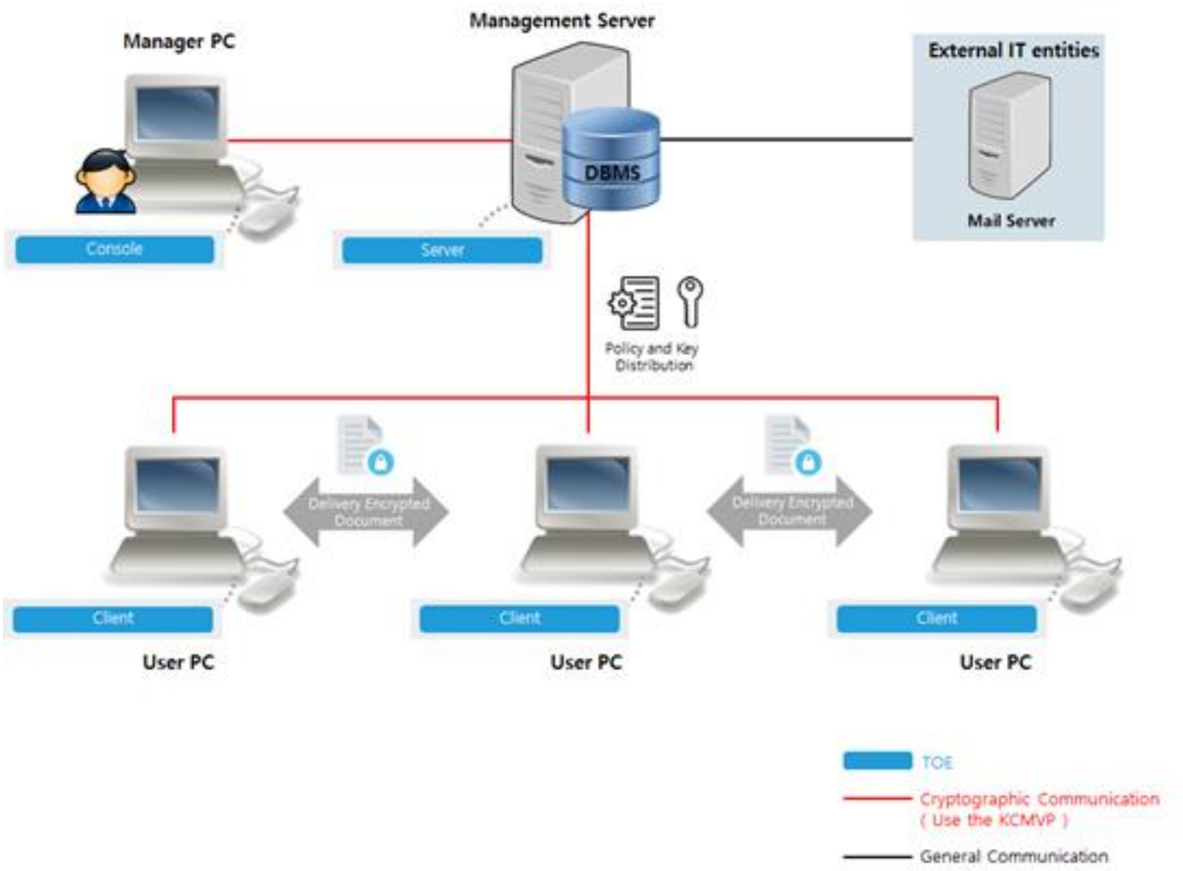
The Target of Evaluation ("TOE" hereinafter) is Electronic Document Encryption designed to protect important documents managed by the organization based on the encryption/decryption. Also, the TOE provides a variety of security features: security audit, the user identification and authentication including 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 November 21, 2022

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 Document Security Server V6.0 (hereinafter 'Server'), Document Security Client V6.0 (hereinafter 'Client'), and Document Security Console V6.0 (hereinafter 'Console') and should be installed and operated inside the internal network of the protected organization.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational Environment of the TOE

[Figure 1] represents the operational environment of "user device encryption" type among other TOE operational environments. In the "user device encryption" type, the TOE is composed of Server that is installed in management server to manage security policy and cryptographic key, Client that is installed in user's PC to perform the encryption/decryption of documents, and Console that is installed in administrator's PC to provide security management interface.

Administrator sets policy for each document user through Console, and Server distributes the policies and cryptographic keys set by administrator to Client. Client installed in user PC performs document encryption/decryption by using validated cryptographic module according to the distributed policy, and the encrypted or decrypted document is stored as a file in the user PC.

In the event of a potential violation, mail server is used as an external IT entity to notify the authorized administrator.

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

Classfication			Requirements for TOE Server	Remarks
Server	H/W	CPU	Intel(R) Xeon(R) E-2226G CPU @ 3.40GHz or higher	-
		HDD	Space required for TOE installation is 20 GB or higher	-
		RAM	8 GB or higher	-
		NIC	10/100/1000 Ethernet Card 1 Port or higher	-
	S/W	OS	Ubuntu Linux release 20.04 LTS (Linux Kernel 5.4, 64bit)	Supported operation systems of the Server
		3rd Party S/W	JRE 1.8 MariaDB 10.7	Third-party software required to run Server
Client	H/W	CPU	Intel(R) Pentium(R) Dual CPU E2200 @ 2.20 GHz or higher	-
		HDD	Space required for TOE installation is 20 GB or higher	-
		RAM	4 GB or higher	-
		NIC	10/100/1000 Ethernet Card 1 Port or higher	-
	S/W	OS	Windows 8.1 32 bit, 64 bit Windows 10 Pro 32 bit, 64 bit Windows 10 Enterprise 32 bit, 64 bit	Supported operation systems of the Client
		3rd Party S/W	Microsoft Visual C++ 2008 redistributable 9.0.30729.4148	Third-party software required to run Client
Console	H/W	CPU	Intel(R) Pentium(R) Dual CPU E2140 @ 1.60GHz or higher	-

		HDD	Space required for TOE installation is 10 GB or higher	-
		RAM	4 GB or higher	-
		NIC	10/100/1000 Ethernet Card 1 Port or higher	-
	S/W	OS	Windows 8.1 32 bit, 64 bit Windows 10 Pro 32 bit, 64 bit Windows 10 Enterprise 32 bit, 64 bit	Supported operation systems of the Console
		3rd Party S/W	Microsoft Visual C++ 2008 redistributable 9.0.30729.4148	Third-party software required to run Console

[Table 1] Hardware/Software Requirements for TOE

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

Classfication	Description
Mail Server	Server that sends a mail to authorized administrator upon a potential security violation detected

[Table 2] External IT entities

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

Classfication	Document Type
Hancom Office	hwp
MS Office Word.	doc, docx
MS Office Powerpoint	ppt, pptx
MS Office Excel	xls, xlsx
Adobe Acrobat	pdf
Notepad	txt
Wordpad	rtf

Mspaint	bmp, jpg, png, gif

[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	Document Security V6.0
Version	V6.0.0.3
TOE Components	Document Security Server V6.0 (V6.0.0.3) Document Security Client V6.0 (V6.0.0.1) Document Security Console V6.0 (V6.0.0.1)
Manuals	Document Security V6.0 Preparative Procedures (PRE) V1.1 Document Security V6.0 Manager Guidance (OPE_A) V1.0 Document Security V6.0 User Guidance (OPE_U) V1.0

[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. 2017-7, 08.24.2017.) Korea Evaluation and Certification Regulation for IT Security (05.17.2021. ITSCC)
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	Document Security V6.0
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National PP for Electronic Document Encryption V1.1 (12.11.2019.)
Developer	SoftCamp Co., Ltd
Sponsor	SoftCamp Co., Ltd

Evaluation Facility	KOREA TESTING & RESEARCH INSTITUTE
Completion Date	November 21, 2022

[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
- 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

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 Document Security Server V6.0, Document Security Client V6.0 and Document Security Console V6.0 as well as guidance documents such as Document Security V6.0 Preparative Procedures and Document Security V6.0 Operational Guidance, which are included in the product, Document Security V6.0. The TOE is offered in the form of software.

Classification	Identification	Type
TOE Component	Document Security Server V6.0 (V6.0.0.3) (SCDS_Server_6.0.0.3.bin)	Software (Distributed as a CD)
	Document Security Client V6.0 (V6.0.0.1) (SCDS_Client_6.0.0.1.exe) (SCDS_Client_6.0.0.1_x64.exe)	
	Document Security Console V6.0 (V6.0.0.1) (SCDS_Console_6.0.0.1.exe) (SCDS_Console_6.0.0.1_x64.exe)	
Guidance	Document Security V6.0_Preparative Procedures (PRE)_V1.1.pdf Document Security V6.0_Manager Guidance (OPE_A)_V1.0.pdf Document Security V6.0_User Guidance (OPE_U) _V1.0.pdf	PDF (Distributed as a CD)

[Table 6] Physical scope of TOE

Validated cryptographic modules included the TOE are as follows.

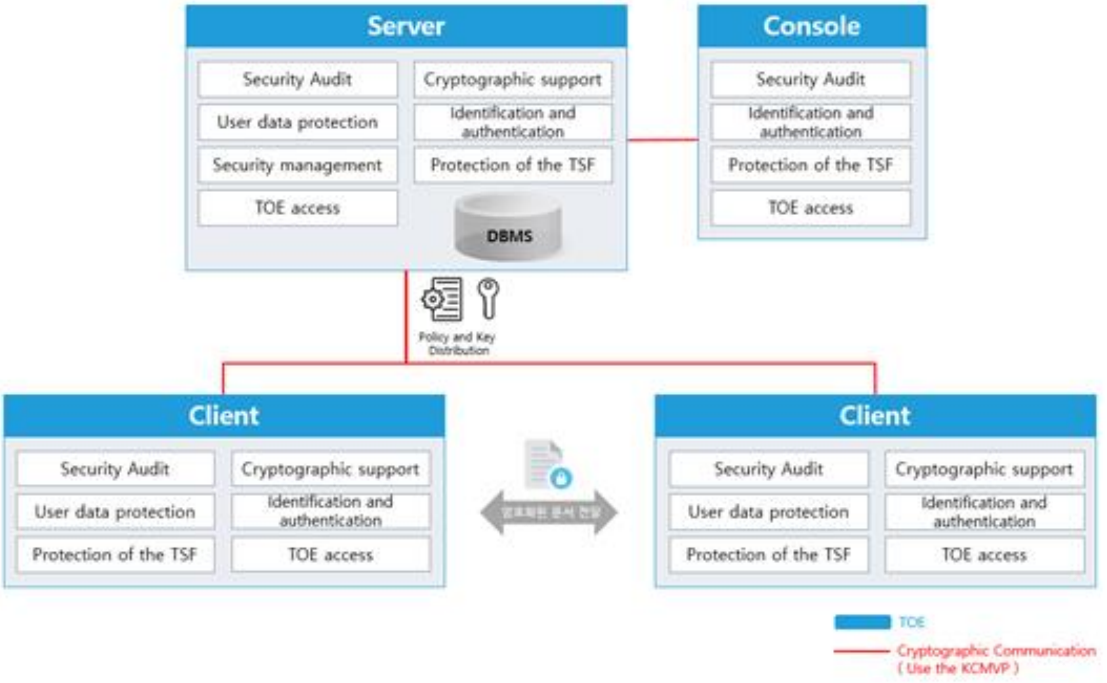
Classfication	Description	
Cryptographic Module	SCCrypto v1.0	MagicJCrypto V3.0.0
Validation No.	CM-122-2021.9	CM-200.2026.12
Developer	SoftCamp Co., Ltd.	Dream Security Co.,Ltd.
Validation Date	2021.11.18	2021.12.31

Expiration Date	2026.11.18	2026.12.31

[Table 7] Validated Cryptographic Module

2. Logical Scope of TOE

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



[Figure 2] Logical scope of TOE

O Security audit

The TOE generates and records audit records for defined auditable events. When audit records are generated, the occurrence time, category, subject information, and processing result of the auditable event are recorded. Server stores audit data it generates and those it receives from Client in DBMS. Also, it provides the function for authorized administrator to view audit data.

When potential security violence is detected, the TOE performs a response action for the relevant act. The TOE provides the function to notify authorized administrator of the relevant information via a mail when the amount of audit trail exceeds the predefined limits. When the audit trail reaches more than 80% of the predefined limit, it sends a warning mail to the administrator, and when the audit trail is full, it sends a warning mail to the administrator after deleting the oldest stored audit data.

O Cryptographic support

The TOE provides functions to generate, distribute and destruct cryptographic key, as well as cryptographic operation function for the protection of data transmitted among the TOE components, the protection of TSF data, and document encryption/decryption.

The TOE generates and distributes a cryptographic key, and performs the cryptographic operation, by using the TOE cryptographic algorithm of the validated cryptographic modules, whose security and implementation conformance are validated by the Korea Cryptographic Module Validation Program (KCMVP). If the cryptographic key is not used anymore, it is destructed. The cryptographic key used in document encryption/decryption is destructed when the encrypted or decrypted document is deleted, while the cryptographic keys created for other purposes are destructed through Zeroization where the key is overwritten by 0.

O User data protection

Through access control policy, the TOE controls read, readable counts, edit, decrypt, print, print marking, authority change, and expiration of documents to be protected according to document user, document user group and category. In the TOE, document user shall go through user identification and authentication and comply with access control policy set by administrator, in order to access to documents and use them.

O Identification and authentication

The TOE performs mutual verification using Internally Implemented Mutual Authentication Protocol between its components, and verifies the identity of administrator and document user based on ID/password. Password shall be not less than 9 digits in combination of alphabet letter, number, and special character.

If administrator or document user fails authentication attempts for five consecutive times during identification and authentication, the administrator or user shall try to access after five minutes as the access of the relevant account is blocked for five minutes.

The TOE shall mask password to make it unrecognizable on the screen for the sake of protected authentication feedback. Also, when user identification or authentication fails, the TOE shall not provide the feedback for the cause of the failure.

The TOE ensures the uniqueness of a session ID using time stamp to prevent the reuse of authentication data.

O Security management

The TOE provides security management function for authorized manager to set and manage security policy and key data. Authorized manager performs security management function through Console, and manages accounts, keys, policies, security management interface setting, password combination rules and password length.

O Protection of the TSF

The TOE conducts self-tests on the major processes during initial start-up or at regular intervals. It verifies the integrity of the TOE execution files during initial start-up or at regular intervals or upon authorized administrator's request, and if the verification fails, notifies the administrator in real time.

When TSF data is transmitted between separate parts of the TOE, validated cryptographic module is used to protect the data from disclosure and modification, and to protect the passwords of authorized manager and user, cryptographic key, critical security parameters, TOE configuration values (security policy and configuration parameters) and audit data, which are stored in TSF data storage, from unauthorized disclosure and modification.

O TOE access

The TOE controls any access to the TOE by allowing only registered IP (one IP by default) to access the security management interface, and limits the number of cocurrent sessions up to 1 to block simultaneous access to the same account and and the same authority. When there is an attempt at simultaneous access, it blocks new connection and maintains the existing connection.

The TOE terminates a session if there is no activity during a certain amount of idle time (five minutes by default) after authorized administrator logs in.

6. Documentation

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

Identification	Date
Document Security V6.0 Preparative Procedures (PRE) V1.1 (Document Security V6.0_Preparative Procedures (PRE)_V1.1.pdf)	August 29, 2022
Document Security V6.0 Manager Guidance (OPE_A) V1.0 (Document Security V6.0_Manager Guidance (OPE_A)_V1.0.pdf)	May 15, 2022
Document Security V6.0 User Guidance (OPE_U) V1.0 (Document Security V6.0_User Guidance (OPE_U)_V1.0.pdf)	May 15, 2022

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: Document Security V6.0
Version: V6.0.0.3

- Document Security Server V6.0 (V6.0.0.3)
- Document Security Client V6.0 (V6.0.0.1)
- Document Security Console V6.0 (V6.0.0.1)

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+).

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	
		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		

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:

- O 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.

- O 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.

- O 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 prvent audit data loss.

11. Security Target

Document Security V6.0 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 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, 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, 2012

[3] Korean National Protection Profile for Electronic Document Encryption V1.1, December 11, 2019

[4] Document Security V6.0 Security Target V1.2, October 18, 2022

[5] Document Security V6.0 Independent Testing Report(ATE_IND.1) V1.01, December 5, 2022

[6] Document Security V6.0 Penetration Testing Report(AVA_VAN.1) V1.01, December 5, 2022