KECS-CR-25-04

DocuRay x v3.5

Certification Report

Certification No.: KECS-CISS-1341-2025

2025. 3. 4.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025. 3. 4.	-	Certification report for DocuRay x v3.5 - First documentation

This document is the certification report for DocuRay x v3.5 of BlueMoonSoft Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the DocuRay v3.5 developed by BlueMoonSoft Inc. 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 used to protect important documents managed by an organization. The TOE performs document encryption according to the policy set by the administrator to protect important documents managed in the organization, and decrypts documents according to the request and permission of the document users.

The TOE encrypts/decrypts the entire contents of the protected documents by specifying the document type (e.g., PDF document, MS Office document, Hangul document, etc.).

The primary security function provided by the TOE is encryption/decryption key management of protected documents. The TOE uses the approved cryptographic algorithm of the validated cryptographic module (MagicCrypto V2.3.0), which has been verified for safety and implementation suitability through the Korea Cryptographic Module Validation Program (KCMVP), for the encryption/decryption of documents, encryption/decryption of critical security parameters used by the TOE and cryptographic key management.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on February 28, 2025.

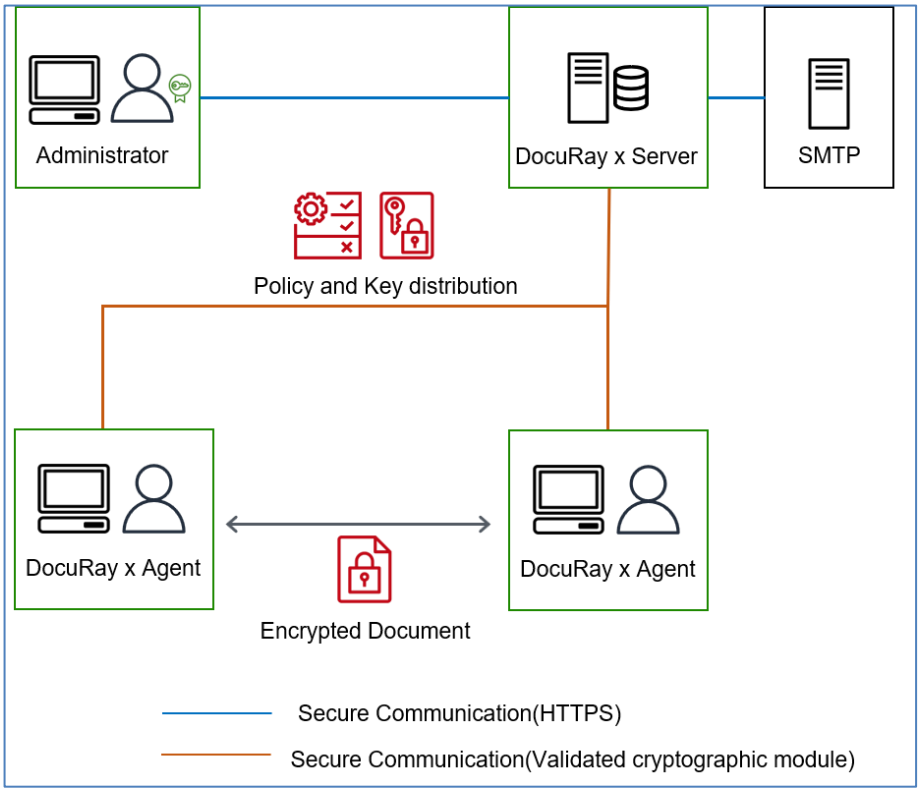
The ST claims conformance to the Korean National Protection Profile for Document Encryption V3.0 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the ST and the 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.

The TOE is 'document encryption' that prevents information leakage by performing encryption/decryption on important documents within an organization, and the TOE

components are provided in the form of software. The TOE supports 'user terminal encryption' method.

The essential TOE components are DocuRay x Server 3.5.5.0 (hereinafter referred to as "DocuRay x Server") and DocuRay x Agent 3.5.5.0 (hereinafter referred to as "DocuRay x Agent").

The TOE has 'user terminal encryption' as its operational environment. [Figure 1] shows the operational environment of the TOE. The TOE consists of DocuRay x Server and DocuRay x Agent, which must be installed and operated on the internal network of the protected organization.



[Figure 1] TOE operational environment

The TOE consists of DocuRay x Server, which manages the security policy and cryptographic key, and DocuRay x Agent, which is installed on the user's PC and performs document encryption/decryption.

The administrator sets the policy for each document user through DocuRay x Server, and DocuRay x Server distributes the policy and cryptographic key set by the administrator to

the agents. The agent installed on the user's device performs encryption/decryption of documents using the validated cryptographic module (MagicCrypto V2.3.0) according to the distributed policy, and the documents are saved as a file on the user's device.

The function to encrypt/decrypt documents when they are delivered outside of an organization where the agent is not installed is not within the scope of the TOE.

Cryptographic operations for the encryption/decryption-related security function use the validated cryptographic module (MagicCrypto V2.3.0). Communication between the TOE components and the administrator (e.g., when accessing DocuRay x Server to set the policy using a web browser) use TLS 1.3 encryption.

The external entity used to operate the TOE uses an SMTP server for email notifications to the authorized administrator.

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

Classification			Minimum Requirement
Server	HW	CPU	Intel Xeon 3.1 GHz or faster
		Memory	8 GB or more
		HDD	500 GB or more of space required for TOE installation
		NIC	10/100/1000 Mbps Ethernet
	SW	OS	Microsoft Windows Server 2019 Standard 64bit
		DBMS	MariaDB 10.11.10
		Etc.	Apache Tomcat 9.0.98 JDK 1.8.0.422 (Azul Zulu)
Agent	HW	CPU	Intel i7 4th Gen 2.2 GHz or faster
		Memory	12 GB or more
		HDD	300 GB or more space required for TOE installation
		NIC	10/100/1000 Mbps Ethernet
	SW	OS	Microsoft Windows 11 Pro 64bit

[Table 2] TOE hardware and software specifications

Administrator uses the pc that can operate web browser to use the security management. Administrator pc minimum requirements are shown in [Table 2].

Classification		Minimum Requirement
SW	Web Browser	Microsoft EDGE - Version: 129.0.2792.52 or later

[Table 2] TOE administrator PC requirements

External IT entities used except for the TOE is as follows.

Type	Description
Mail server	Server to send emails to the authorized administrator

[Table 3] External IT entities

The software required for the TOE operation is as follows.

Encryption Target	Software
MSOFFICE	MS Office 2019
HWP	Hancom Office 2018
ADOBE READER	Adobe Acrobat Reader
TEXTEDIT	MS Notepad
AUTO CAD	Auto Cad 2024
AUTO INVENTOR	Auto Inventor 2024

[Table 4] Supported document editors

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	DocuRay x v3.5
Version	3.5.5.0
TOE Components	DocuRay x Server 3.5.5.0 DocuRay x Agent 3.5.5.0
Manuals	DocuRay x v3.5 Operational Guidance v1.3 DocuRay x v3.5 Installation Guidance v1.4

[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, May 17, 2021)
TOE	DocuRay x v3.5
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1, CCMB-2024-07-002, July 2024
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korea National Protection Profile for Electronic Document Encryption V3.0
Developer	BlueMoonSoft Inc.
Sponsor	BlueMoonSoft Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)

Completion Date of Evaluation	February 28, 2025
Certification Body	IT Security Certification Center

[Table 6] 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
- Trusted Path/Channels

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 5].)

5. Architectural Information

The physical scope of the TOE is identified in the [Table 7] below.

Category		Name	Form	Deploy-ment Types
TOE Name		DocuRay x v3.5	-	-
Version Details		3.5.5.0	-	-
Setup Package	Server	DocuRay x Server 3.5.5.0 (DocuRay_x_Server_Launcher_3.5.5.0.exe)	Software	CD
	Agent	DocuRay x Agent 3.5.5.0 (DocuRay_x_Agent_Setup_3.5.5.0.exe)	Software	
Electronic Documen-tation	User Guide	DocuRay x v3.5 Operational Guidance v1.3 (DocuRay x v3.5 Operations Guidance v1.3.pdf)	PDF	
	Preparation	DocuRay x v3.5 Installation Guidance v1.4 (DocuRay x v3.5 Installation Guidance v1.4.pdf)		
	License certificate	Software_License_Certificate.pdf	PDF	

[Table 7] Physical scope of TOE

Validated cryptographic modules included the TOE are as follows in [Table 8].

Category	Content
Cryptographic Module Name	MagicCrypto V2.3.0
Verification number	CM-263-2030.1
Developer	DreamSecurity Inc.
Verification date	January 24, 2025
Expiration date	January 24, 2030

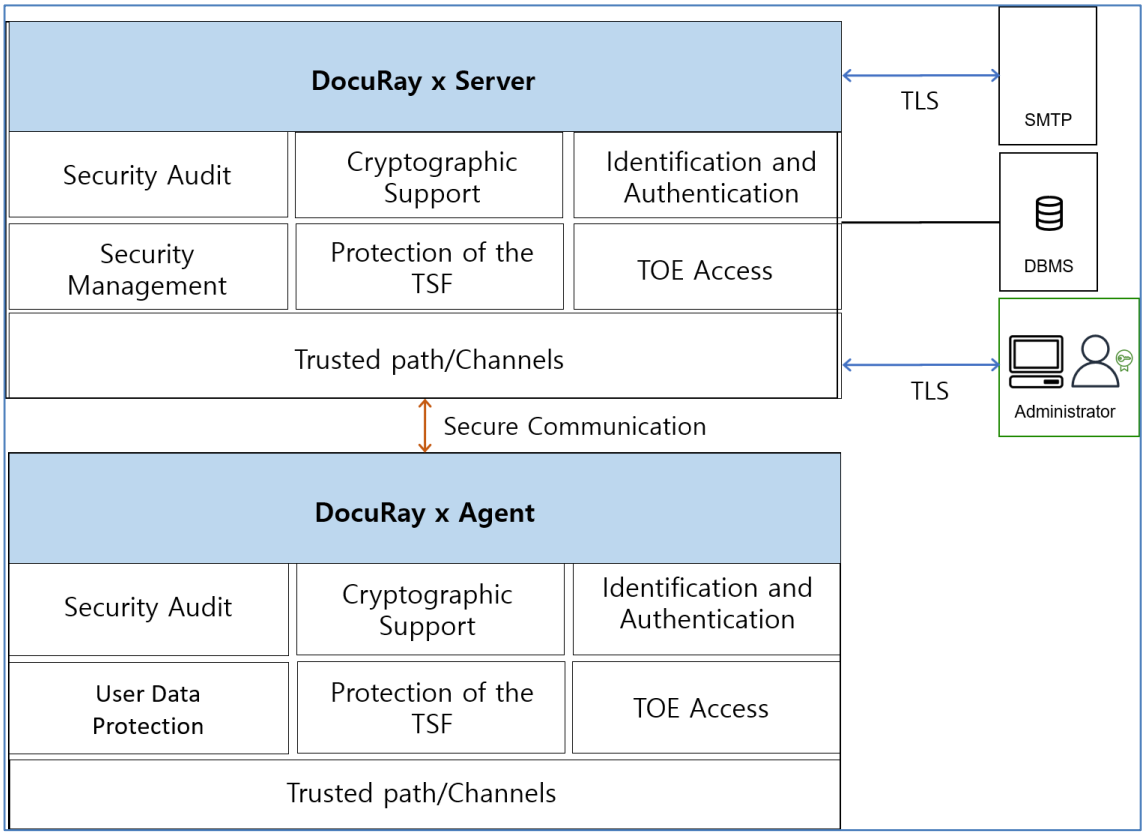
[Table 8] General

The 3rd party software included in the TOE is as follows in [Table 9].

Item		description
DocuRay x Server	OpenSSL 3.4.0	Module for secure communication
	MagicCrypto V2.3.0	Validated Cryptographic Module
DocuRay x Agent	OpenSSL 3.4.0	Module for secure communication
	MagicCrypto V2.3.0	Validated Cryptographic Module

[Table 9] 3rd party software required for TOE operation

The logical scope of the TOE is as in [Figure 2] below.



[Figure 2] Logical scope of TOE

- Security Audit

The TOE stores the audit function's start/stop history and the events related to the security functions as audit records in the DBMS. Among the audit records, document usage history is selectively generated based on encryption/decryption/viewing activities. The audit data includes detailed information such as the date and time of the event, the type of the event, the identity of the subject involved, the operation history, and the result. Time synchronization is performed between servers and agents to ensure accurate time information for key events. The authorized administrator can view the generated audit history and search using various criteria, such as event type, date, or user.

Stored audit records in audit trails do not include any user interface or functionality that allows deletion or modification, even for the authorized administrator.

When a potential security violation is detected, such as an integrity violation, failed testing, or audit threshold exceeded (>90% of total disk capacity), the TOE notifies the authorized administrator via email of the potential violation.

The TOE responds to storage failures by sending an email notification to the administrator when audit data growth exceeds saturation (>95% of total disk capacity) and by sequentially overwriting older audit records.

- Cryptographic support

The TOE uses MagicCrypto V2.3.0 to perform cryptographic operations and cryptographic key management such as generation, distribution, and destruction. HASH_DRBG (SHA-256) is used to generate DEK (data cryptographic key), and RSAES (SHA-256) algorithm is used to generate private and public key pairs. Also, HASH_DRBG (SHA-256) algorithm is used to generate Salt and IV. A KEK (Key Encryption Key) is generated from the runtime password and derived using the PBKDF2 (HMAC-SHA-256) algorithm. The ARIA_CBC mode and RSAES (SHA-256) are used to distribute the cryptographic key between components.

The TOE performs operations through ARIA_CTR mode when encrypting/decrypting the document body, and ARIA_CBC mode is used to encrypt the document header, communication, and cryptographic key. During the communication process, the cryptographic key and authentication information are encrypted with RSAES (SHA-256), and an electronic signature is generated with RSA-PSS (SHA-256) algorithm. The verification code of inter-module communication (IPC), module integrity verification value, and original document validation value recorded in the document header are generated using SHA-512. Passwords of the authorized administrator and document users are stored using HMAC (SHA-256), and settings such as DBMS password are stored using ARIA_CBC mode. When destroying the cryptographic key and authentication information, the memory is overwritten with '0' or '1' at least 3 times.

- User data protection

The TOE protects user documents.

1) The TOE creates protected documents by encrypting plain text documents according to the policy set by the authorized administrator, and protects them by

controlling access to the protected documents. It blocks the clipboard for protected documents and prevents document leakage. Policies are set differently depending on user identifiers, file permissions, and target document types. Access to decrypt documents is controlled according to decryption permissions.

2) Protected documents are encrypted with cryptographic support and can only be accessed by authorized document users. Even if the protected document is leaked externally, unauthorized document users cannot access its contents.

DocuRay x Agent encrypts and stores documents on the user's PC.

DocuRay x Agent supports the following main document types

Encryption Target	Category	Operations			
		Write	View	Manual encryption	Manual decryption
MSOFFICE	Process	winword.exe, excel.exe, powerpnt.exe		-.	
	Document type	MSOffice document header	Secure document header	MSOffice document header, PDF document header	Secure document header
HWP	Process	hwp.exe		-.	
	Document type	Hangul document header	Security document header	Hangul document header	Security document header
ADOBE READER	Process	acrobat.exe		-.	
	Document type	PDF document headers	Secure document header	PDF document header	Secure document header
TEXTEDIT	Process	notepad.exe		-.	
	Document types	All Files	Secure document header	TXT document header	Secure document header
AUTO CAD	Process	acad.exe		-.	
	Document type	Auto Cad document Header	Secure document headers	Auto Cad document header	Secure document header
AUTO INVENTOR	Process	inventor.exe		-.	
	Document type	Auto Inventor document Header	Secure document header	Auto Inventor document header	Secure document header

[Table 10] Supported document type

- Identification and authentication

The TOE provides an identification and authentication process based on IDs and passwords for the administrator and document users. Only authorized administrator can access the administrator page through a web browser to manage security features. When a document user logs in to DocuRay x Agent, the identification and authentication process is performed through mutual authentication between DocuRay x Server and DocuRay x Agent.

When the administrator and document users enter their passwords into DocuRay x Server or DocuRay x Agent, they are masked with '●' to prevent exposure, and if authentication fails, no specific reason for the failure is provided. A password must be at least nine characters long and include at least one uppercase letter, and lowercase letter, one number, and one special character. Additionally, the following rules must be followed: the password cannot be the same as your user ID, the same letter or number cannot be repeated more than 3 times consecutively, more than four consecutive letters or numbers on the keyboard cannot be used, and the last password cannot be reused. If an admin or document user fails to authenticate more than five times, their account will be locked for five minutes.

The credentials of the administrator or document users are timestamped to prevent reuse. A timestamp is sent along with the credentials and saved when authentication is successful. When logging in, the timestamp is used to authenticate the user, and if the timestamp is smaller than the timestamp stored in the DB, authentication fails, and if it is larger, the authentication process proceeds. When the authentication process is completed, the timestamp is saved.

After successful authentication, you can use the security features provided by TOE.

- Security Management

Only the authorized administrator can perform security management through the admin page. Upon initial access, the administrator must change the default password. The authorized administrator can configure security attributes, such as the types of documents to be encrypted, and execute the security functions, including deleting modules and performing server integrity verification, through the policy menu. SMTP account information and connection IP management can be set for security features. The authorized administrator can add, delete, or change the password of document users in organization chart management menu. Only one administrator account is provided.

- Protection of the TSF

The TOE communicates securely to protect transmitted data between components, ensuring confidentiality and integrity.

The TOE prevents unauthorized exposure and tampering of TSF data through encryption, hashing, and digital signatures.

DocuRay x Agent's TSF data is stored in the installation directory and is monitored to prevent unauthorized access and termination. The TOE performs the testing and integrity verification at startup, periodically, and on administrator request to ensure normal operation. If an integrity verification fails, the TOE performs an automated recovery.

- TOE access

In order to ensure secure session management for an authorized administrator, the TOE terminates login sessions after a period of inactivity on the admin page. For secure session management for document users, The TOE also overwrites the display so that the current content is unreadable after a period of inactivity.

The authorized administrator can only sign in from the device specified as the accessible IP. If you try to sign in with the same account, the existing connection is terminated and the sign-in succeeds.

Duplicate document user logins for the agent are blocked using an additional attribute, while the existing connection is maintained.

- Trusted Path/Channels

The TOE provides a trusted channel to protect data from unauthorized changes or exposure when interfacing with a mail server to send mail to the authorized administrator in the event of a potential violation.

6. Documentation

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

Identifier	Date
DocuRay x v3.5 Installation Guidance v1.4 (DocuRay x v3.5 Installation Guidance v1.4.pdf)	January 31, 2025
DocuRay x v3.5 Operational Guidance v1.3 (DocuRay x v3.5 Operations Guidance v1.3.pdf)	January 31, 2025

[Table 11] 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 the 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: DocuRay x v3.5 (3.5.5.0)

- DocuRay x Server 3.5.5.0
- DocuRay x Agent 3.5.5.0

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 results in the ETR [7] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation results were based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation (EAL1+).

As a result of the evaluation, the verdict **PASS** is assigned to all assurance components.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problems that the TOE and TOE operational environment are intended to address. Therefore, the verdict PASS is assigned to ASE_SPD.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 are 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 penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE 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 Results 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_SPD.1	ASE_SPD.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

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 12] Evaluation Results 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 TOE 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 check a spare space of audit data storage in case of the audit data loss, and carry out the audit data backup to prevent audit data loss.
- If a cryptographic key is lost due to administrator's wrong cryptographic key management, document users may not be able to decrypt the encrypted file stored on the user's PC, so administrator has to be careful with cryptographic key management

11. Security Target

Document x v3.5 Security Target v1.6 [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

Random Bit Generator (RBG)

Device or algorithm that outputs a statistically independent, unbiased binary string. Random number generators used for cryptographic applications typically generate bit sequences of zeros and ones, can be combined into random blocks. Random number generators are classified into deterministic and nondeterministic methods. The deterministic random number generator consists of an algorithm that generates a string of bits from an initial value called seed key, whereas the nondeterministic random number generator produces an output that depends on an unpredictable physical source.

Data Encryption Key (DEK)

Key that encrypts the data

Key Encryption Key (KEK)

Key that encrypts and decrypts another encryption key

Encryption

The act that converting the plaintext into the ciphertext using the cryptographic key

Decryption

The act that restoring the ciphertext into the plaintext using the decryption key

Authorized Administrator

Authorized user who operates and manages the TOE safely

Authorized User

Users who can execute functions in accordance with the security functional requirements (SFR)

13. Bibliography

The certification body has used the 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
Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1, CCMB-2024-07-002, July 2024

[2] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, CCMB-2022-11-006, November 2022
Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1, CCMB-2024-07-002, July 2024

[3] Korean National Protection Profile for Electronic Document Encryption V3.0, April 27, 2023

[4] DocuRay x v3.5 Security Target v1.6, February 25, 2025

[5] DocuRay x v3.5 Independent Testing Report (ATE_IND.1) V2.00, February 5, 2025

[6] DocuRay x v3.5 Penetration Testing Report (AVA_VAN.1) V2.00, February 5, 2025

[7] DocuRay x v3.5 Evaluation Technical Report (ETR) Lite V3.00, February 28, 2025