KECS-CR-23-62

HDS V1.0

Certification Report

Certification No.: KECS-CISS-1268-2023

2023. 10. 16.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.10.16.	-	Certification report for HDS V1.0 - First documentation

This document is the certification report for HDS V1.0 of HD Korea Shipbuilding & Offshore Engineering Co., Ltd.

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 evaluation facility on the results of the HDS V1.0 developed by HD Korea Shipbuilding & Offshore Engineering 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 (hereinafter referred to as “TOE”) is used to protect important documents managed by the organization. The TOE can encrypt/decrypt a document to be protected by specifying document type. The entire content of the protected document, however, must be encrypted. Also, the TOE shall provide 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 System Assurance (KOSYAS) and completed on October 04, 2023.

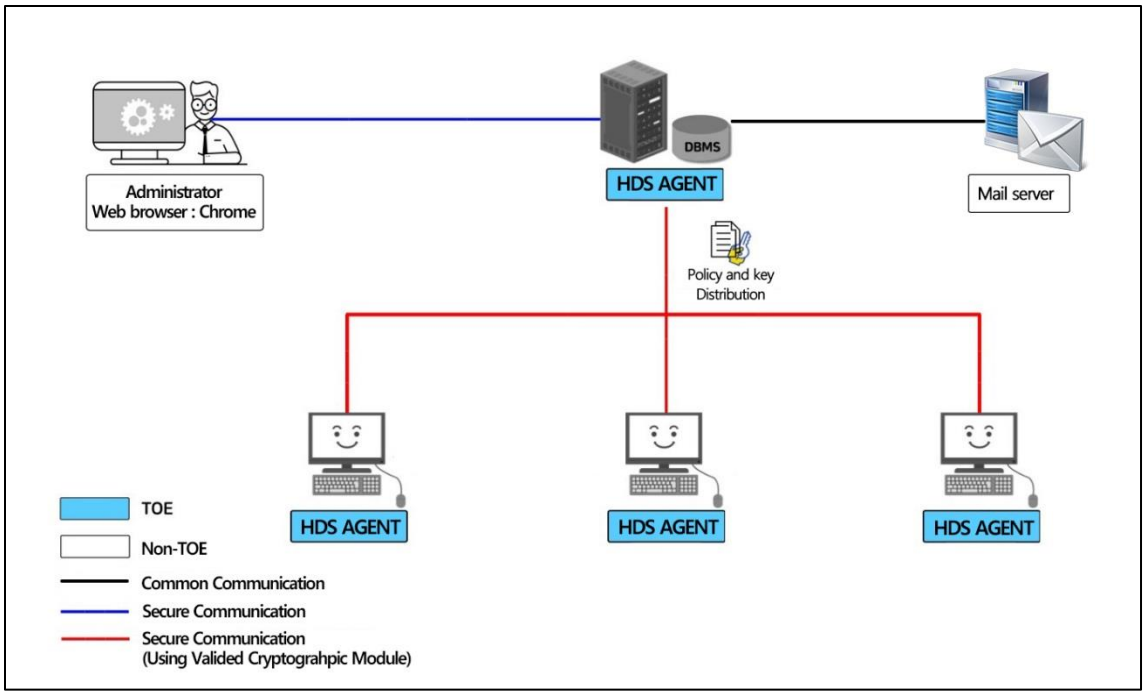
The ST claims conformance to the Korean National Protection Profile for Electronic Document Encryption V1.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the 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.

‘HDS v1.0’(hereinafter referred to as “TOE”) is used to protect important documents managed by the organization. The TOE encrypts electronic documents to protect the important documents managed by the organization according to the policy set by the administrator, and a document is decrypted according to the document user’s request and right.

The TOE can encrypt/decrypt documents to be protected by document types and the TOE encrypts the entire contents of the documents.

The TOE is “Electronic Document Encryption” that prevents information leakage by encrypting/decrypting important documents within the organization and is provided as

software. The TOE supports “user device encryption” type.



[Figure 1] Operational Environment of the TOE

[Figure 1] shows the operational environment of the “user device encryption” type. In the “user device encryption” type, the TOE can be composed of HDS SERVER which manages the security policy and cryptographic key, and the HDS AGENT that performs Electronic Document encryption/decryption installed in the user device.

The validated cryptographic module, ‘MagicCrypto V2.2.0’, 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., when the administrator accesses the HDS SERVER using the web browser and web server to configure policies), TLS 1.2 is used. As other external entities necessary for the operation of the TOE, there is the Mail server to send alerts by email to the authorized administrator.

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

Component		Requirement
HDS SERVER	HW	CPU: Intel(R) Xeon(R) 2.6 GHz or higher Memory: 16 GB or higher HDD: 300 GB or higher for the installation of TOE NIC: 100/1000 Mbps 1Port or higher
	SW	IIS 10 MS-SQL 2019-15.0
	OS	Windows Server 2019 Standard (64 bit)
HDS AGENT	HW	CPU: Intel Core 3.30 GHz or higher Memory: 4 GB or higher HDD: 1 GB or higher for the installation of TOE NIC: 100/1000 Mbps 1Port or higher
	OS	Windows 10 Pro (32, 64 bit) Windows 10 Enterprise (32, 64 bit)

[Table 1] 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]

Component		Requirement
S/W	Web Browser	Chrome 114

[Table 2] Administrator PC Requrements

The S/W required for TOE operation is as follows.

Classfication	Description
Encryption Target Document Program	Microsoft Office 2016, 2019, 2021 Hancom Office 2022 Adobe Acrobat Pro X Adobe Acrobat Reader DC

[Table 3] Encryption Target Document Program

The 3rd party S/W included in the TOE is as follows.

Classfication	Description
S/W	Microsoft Visual C++ 2010 Redistributable -10.0

[Table 4] 3rd party S/W included in the TOE

Validated cryptographic modules included the TOE are as follows.

Classfication	Description
Cryptographic Module	MagicCrypto V2.2.0
Validation No.	CM-162-2025.3
Developer	Dream Security Co., Ltd.
Validation Date	2025.03.03

[Table 5] Validated Cryptographic Module

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	HDS v1.0
Version	V1.0.0.2
TOE Components	HDS SERVER v1.0.0.2 HDS AGENT v1.0.0.2
Manuals	HDS v1.0 Operation Guide_admin v1.2 HDS v1.0 Operation Guide_user v1.2 HDS v1.0 Preparative Procedure v1.1

[Table 6] TOE identification

[Table 7] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	HDS v1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Electronic Document Encryption V1.1
Developer	HD Korea Shipbuilding & Offshore Engineering Co., Ltd.
Sponsor	HD Korea Shipbuilding & Offshore Engineering Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	October 04, 2023

[Table 7] 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 6])

5. Architectural Information

1. Physical Scope of TOE

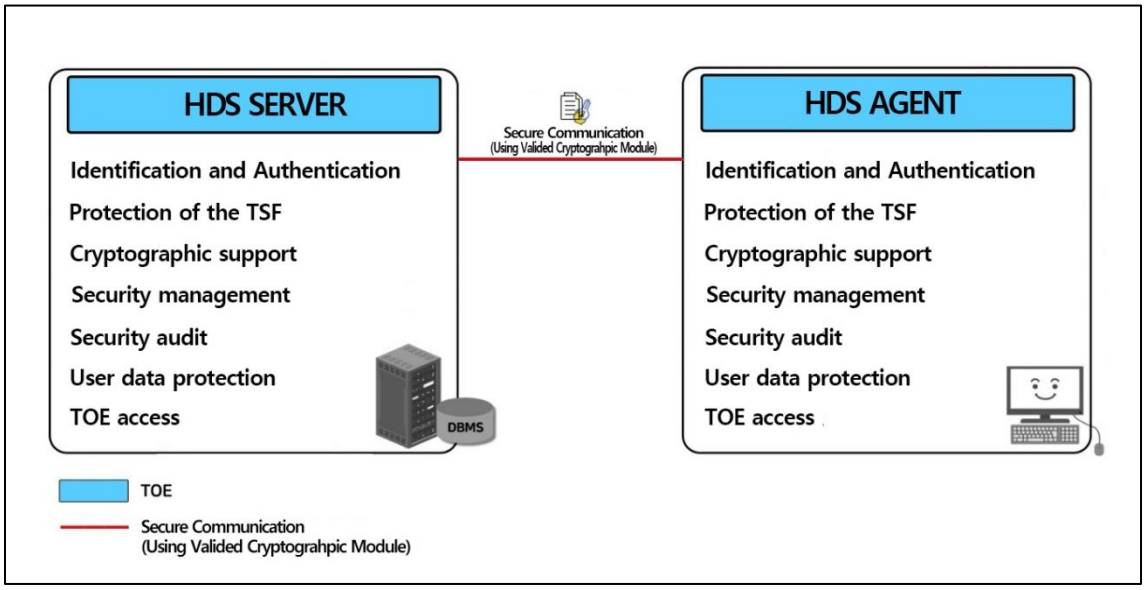
The physical scope of the TOE consists of the HDS SERVER, HDS AGENT, and guidance documents. Verified Cryptographic Module (MagicCrypto V2.2.0) is embedded in the TOE components. Hardware, operating system, DBMS, WAS which are operating environments of the TOE are excluded from the physical scope of the TOE.

Category	Identification	Type
TOE component	HDS SERVER v1.0.0.2 (HDS SERVER v1.0.0.2.exe)	Software (Distributed as a CD)
	HDS AGENT v1.0.0.2 (HDS AGENT v1.0.0.2.exe, HDS AGENT v.1.0.0.2_x64.exe)	
guidance documents	HDS v1.0 Operation Guide_admin v1.2 (HDS v1.0 Operation Guide_admin v1.2.pdf)	PDF (Distributed as a CD)
	HDS v1.0 Operation Guide_user v1.2 (HDS v1.0 Operation Guide_user v1.2.pdf)	
	HDS v1.0 Preparative Procedure v1.1 (HDS v1.0 Preparative Procedure v1.1.pdf)	

[Table 1] Physical scope of TOE

2. Logical Scope of TOE

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



[Figure 2] TOE Logical Scope

▣ Security Audit

The TOE creates and records audit data of the events relating to the start/end of the audit functions and security functions in the DBMS.

The authorized administrator can search through the management screen for the stored audit data. Audit can be retrieved in the descending order based on the selectable AND condition and the server time.

If any potential security violation such as integrity violation, TSF self-tests failure, and Mutual authentication failuer, Login failure 5 times, Unauthorized shutdown/deletion of TOE executables and proccess, Document user failure to encrypt/decrypt documents, Audit trail amount exceed is detected, the TOE sends an email to the administrator to inform the administrator of the potential violation.

In case of a situation when the audit data storage limit exceeds, the TOE sends an alert by email to the administrator and overwrites the old data.

▣ Cryptographic support

The TOE performs cryptographic operation and cryptographic key management such as generation, distribution and destruction through MagicCrypto V2.2.0.

HASH_DRBG is used to generate all DEKs, and the key encryption key (KEK) is generated according to PBKDF2. Key distribution between components is safely distributed using ECDH.

Document encryption/decryption is performed in ARIA-CTR mode, and TSF data encryption/decryption is performed in ARIA-CBC mode. The authentication data of the administrator and document user is stored in one-way encryption with SHA-256. For destruction of the encryption key after use, it is overwritten with '0' three times in memory.

▣ User data protection

The HDS AGENT encrypts the document stored on the user PC to generate secure documents and the authorized document user access them.

The authorized administrator controls the decryption of secure documents according to the policy set by the HDS SERVER of the TOE through the management screen of the web browser.

The file formats that the HDS AGENT of the TOE supports encryption are as follows.

Application	File format (extension)
Hancom Office 2022	HWP, HWT
Adobe Acrobat Pro X	PDF
Acrobat Reader DC	PDF
Microsoft Office 2016, 2019, 2021 (Word, Powerpoint, Excel)	DOC, DOCX, DOTM, DOTX, PPT, PPTX, PPTM, PPS, PPSM, PPSX, POT, POTX, POTM, XLS, XLSX, XLSM, XLSB, XLTX, XLTM

▣ Identification and authentication

The TOE provides identification and authentication process based on ID/PW for the administrators and document users. Only the authorized administrator can manage the security functions through the web browser. The identification and authentication process of a user are performed through the HDS AGEMT. The identification and authentication process of the document user are performed through the HDS AGENT.

When the administrator or user enters password to log in, it is masked to prevent disclosure and in case of authentication failure, the reason is not provided.

The password must be at least 9 characters (max 20) in length, with at least one alphabetic character, numeric character, and special character. If the authentication

failure exceeds 5 times, the login function is disabled for 10 minutes.
In order to prevent the reuse of administrator and document user authentication information, the timestamp of the packet is added, and mutual authentication is performed using Internally Implemented Authentication Protocol when communicating between HDS SERVER and HDS AGENT.

▣ Security Management

The administrators and the document users must change their passwords during the initial access. The authorized administrator performs security management through the management screen on the web browser. The authorized administrator performs security function management, security properties management, and TSF data management and provides the functions through following the menu below.
Change the administrator password of TOE's management web browser
Register administrator IP
Mail setting
Add and delete document user ID
Document decryption rights
Agent deletion rights

▣ Protection of the TSF

The TOE communicates securely to protect transmission data between components and secures confidentiality and integrity. The TOE also protects TSF data against unauthorized exposure and modification through encryption, digital signature and internally implemented encoding.
The TOE performs TSF self-tests and integrity checks periodically and when operating, and prevents process termination and file deletion to prevent the running HDS AGENT from terminating.

▣ TOE access

The TOE terminates the login session after a time interval of inactivity from logging in for secure session management of the authorized administrator. If logging in with an account, after logging in with the same account from one device, from another device is tried, the previous connection is blocked, and administrators can access only from the devices whose IP is designated as accessible.

6. Documentation

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

Identification	Date
HDS v1.0 Operation Guide_admin v1.2 (HDS v1.0 Operation Guide_admin v1.2.pdf)	September 04, 2023
HDS v1.0 Operation Guide_user v1.2 (HDS v1.0 Operation Guide_user v1.2.pdf)	September 04, 2023
HDS v1.0 Preparative Procedure v1.1 (HDS v1.0 Preparative Procedure v1.1.pdf)	September 04, 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.: Identifier of each test case
- Test Purpose: Includes the security functions 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: HDS v1.0 (v1.0.0.2)
- HDS SERVER v1.0.0.2
- HDS AGENT v1.0.0.2

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	
		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 9] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The administrator should periodically check the free space of the audit data storage in preparation for the loss of the audit records, and perform backups of the audit records so that the audit records are not exhausted.
- HDS SERVER must be installed and operated in a physically secure environment that is accessible only to authorized administrators and should not allow remote administration from outside.
- 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

HDS v1.0 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 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.

Validated Cryptographic Module

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

Wrapper

Interface to connect the TOE with various types of information system

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] HDS v1.0 Security Target v1.2, Septemeber 04, 2023

[5] HDS v1.0 Independent Testing Report(ATE_IND.1) V2.00, October 11, 2023

[6] HDS v1.0 Penetration Testing Report (AVA_VAN.1) V1.00, September 27, 2023