2023

HDS v1.0 Security Target v1.2

Revision history

Version	Date	Details
1.0	2023.05.23	Initial version
1.1	2023.06.22	Updated
1.2	2023.09.04	Updated

Table of Contents

1. ST introduction

This document is a HDS v1.0 Security Target that targets the Common Criteria EAL1+ level.

1.1. ST reference

This ST is identified as follows.

- Title : HDS v1.0 Security Target
- Version : v1.2
- Created by : Security Operation Team, HD Korea Shipbuilding & Offshore Engineering
- Date : 2023.09.04
- Evaluation Criteria : Common Criteria for Information Technology Security Evaluation
- Common Criteria : v3.1 r5
- Evaluation Assurance Level: EAL1+(ATE_FUN.1)
- Protection Profile : Korean National Protection Profile for Electronic Document Encryption V1.1
- Keywords: Document, Encryption

1.2. TOE reference

TOE is identified as follows.

TOE	HDS v1.0
Version	v1.0.0.2
Components	HDS SERVER v1.0.0.2 : HDS SERVER v1.0.0.2.exe)
	HDS AGENT v1.0.0.2 : HDS AGENT v1.0.0.2.exe, HDS AGENT v1.0.0.2_x64.exe
Guidance documents	HDS v1.0 Operation Guide_admin v1.2 : HDS v1.0 Operation Guide_admin v1.2.pdf
	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
Developer	Security Operation Team, HD Korea Shipbuilding & Offshore Engineering

[Table 1] TOE identification

1.3. TOE overview

'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 (PDF, HWP, Microsoft Excel, Microsoft Word, Microsoft Power point) and the TOE encrypt the entire contents of the documents.

The primary security features provided by TOE are encryption/decryption and cryptographic key management of documents to be protected, and the cryptographic functions applied at this time use the encryption algorithm of the validated cryptographic module that has been verified for stability and implementation through the Korea Cryptographic Module Validation Program (KCMVP), MagicCrypto V2.2.0. In addition, the encryption/decryption and cryptographic key management functions for critical security parameters used by TOE also use the Korea Cryptographic Module Validation Program (KCMVP), MagicCrypto V2.2.0 and the verification target encryption algorithm of the validated cryptographic module that has been verified for safety and implementability.

1.3.1. TOE type

The TOE is 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.

The HDS SERVER, HDS AGENT are the indispensable TOE components that perform the security features of the TOE.

1.3.2. TOE usage and major security features

The TOE performs document encryption/decryption according to the policy set by the administrator in order to protect the important documents managed by the organization, it includes the cryptographic key management function.
Besides, the TOE also provides other functions, such as the security audit function that records major events at the time of starting up the security or management function as the audit data for management, administrator and document user identity verification, mutual authentication

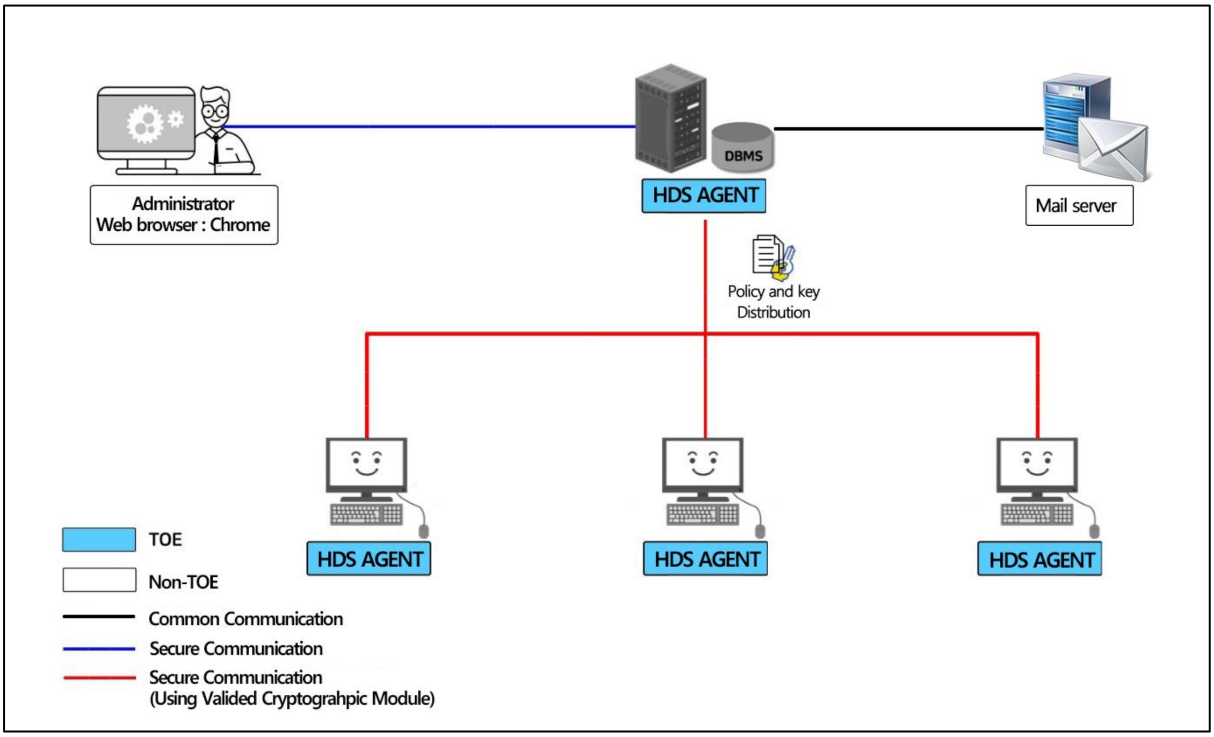
between TOE components, authentication failure processing, and security management function for security function, role definition, and configuration, the function of protecting the data stored in the repository controlled by the TSF , TSF protection function like the TSF's self tests, and the TOE access function to manage the interacting session of the authorized administrator.

The data encryption key (hereinafter referred to as "DEK") can be used for the document encryption/decryption function.

The main body of the protected document is encrypted the security document header with 'The document BODY DEK', and the header of the security document is encrypted and stored with 'The document HEADER DEK'.

The HDS SERVER generates the DEK and distributes mutually-authenticated HDS AGENT. At this time, the cryptographic key is distributed safely. Each component of the TOE provides to safely destruction function covering the cryptographic key in the memory with '0' if the cryptographic key is not used anymore. Only the authorized document user can encrypt/decrypt the document, as the HDS SERVER distributes a cryptographic key to the document user according to policy configured.

1.3.3. Non-TOE and TOE operational environment



[Figure 1] TOE operational environment

[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 administrator sets the policy for each document user through the management web browser and the HDS SERVER distributes the policy and cryptographic key configured by the administrator to the HDS AGENT.

The HDS AGENT installed in the user device performs document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted/decrypted document is stored as a file in the user device.

The requirements for hardware, software and operating system to install the TOE are as follows

Component		Requirement	
HDS SERVER	HW	CPU	Intel(R) Xeon(R) 2.6 GHz or higher
		Memory	16GB or higher
		HDD	300GB or more of space required for TOE installation
		NIC	100 / 1000 Ethernet card 1 port or higher
	OS	Windows SERVER 2019 Standard (64bit)	
	SW	IIS 10.0, MS-SQL 2019-15.0	
HDS AGENT	HW	CPU	Intel Core 3.30 GHz or higher
		Memory	4GB or higher
		HDD	1GB or more of space required for TOE installation
		NIC	100 / 1000 Ethernet card 1 port or higher
	OS	Windows 10 Pro (32/64Bit) Windows 10 Enterprise (32/64Bit)	

[Table 2] TOE installation requirement

The requirements for the administrator PC for TOE security management are as follows.

구분	Requirement
SW	Chrome 114

[Table 3] Administrator (HTTPS Communication)

The external IT entities and software necessary for the operation of the TOE are as in the following, and the following are excluded from the scope of the assessment.

- Mail server used to send security alerts by email to the administrator
- Application for document user
  - Microsoft Office 2016, 2019, 2021

- Hancom Office 2022
- Adobe Acrobat Pro X
- Adobe Acrobat Reader DC

The library for the TOE installation compatibility is included in the HDS installation file.

- Microsoft Visual C++ 2010 Redistributable - 10.0

1.4. TOE description

1.4.1. Physical scope of the TOE

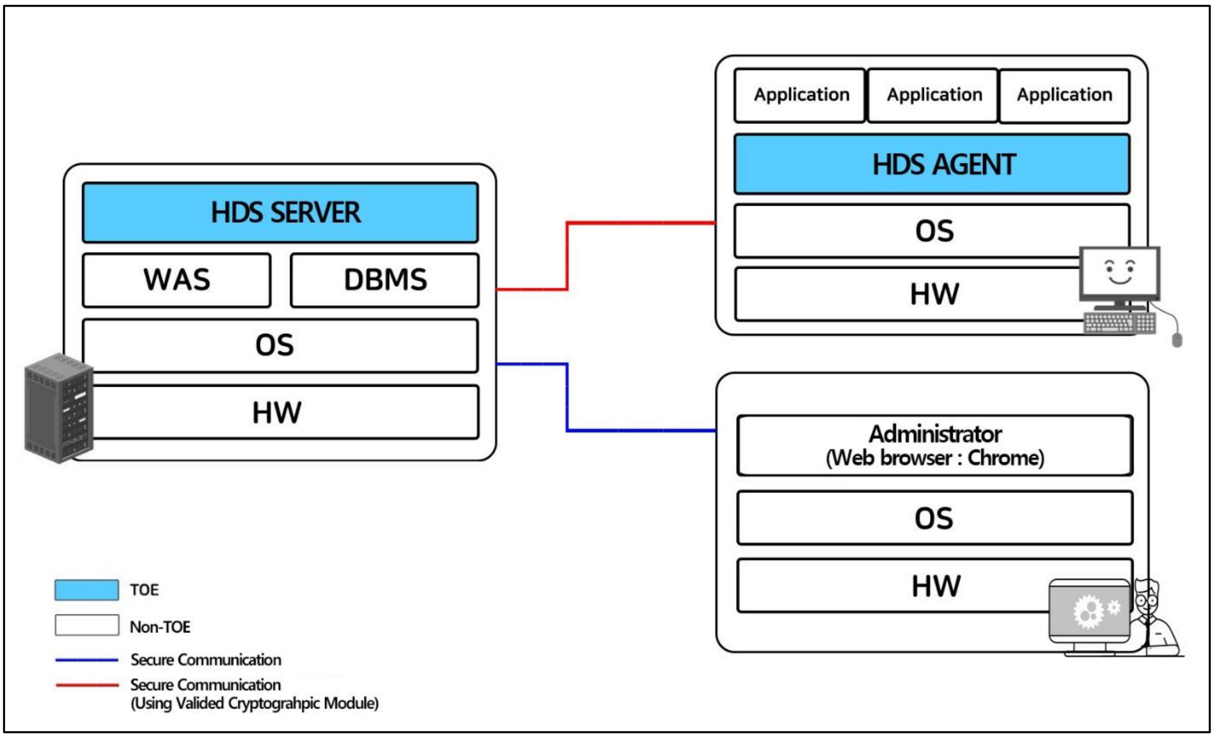
The TOE is composed of the HDS SERVER, HDS AGENT and HDS guidance documents (Operation Guide, Preparative Procedure). The authorized administrator provides the ability to manage policies and security data for document encryption / decryption and apply to HDS AGENT through the management screen of the web browser. The HDS AGENT controls the access rights of document according to the policy applied from the HDS SERVER and performs encryption/decryption of security document.

The components of the distributed TOE are as follows.

Software	HDS SERVER v1.0.0.2 : HDS SERVER v1.0.0.2.exe	Software (CD distribution)
	HDS AGENT v1.0.0.2 : HDS AGENT v1.0.0.2.exe, HDS AGENT v1.0.0.2_x64.exe	
Guidance documents	HDS v1.0 Operation Guide_admin v1.2 : HDS v1.0 Operation Guide_admin v1.2.pdf	PDF (CD distribution)
	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 4] TOE component

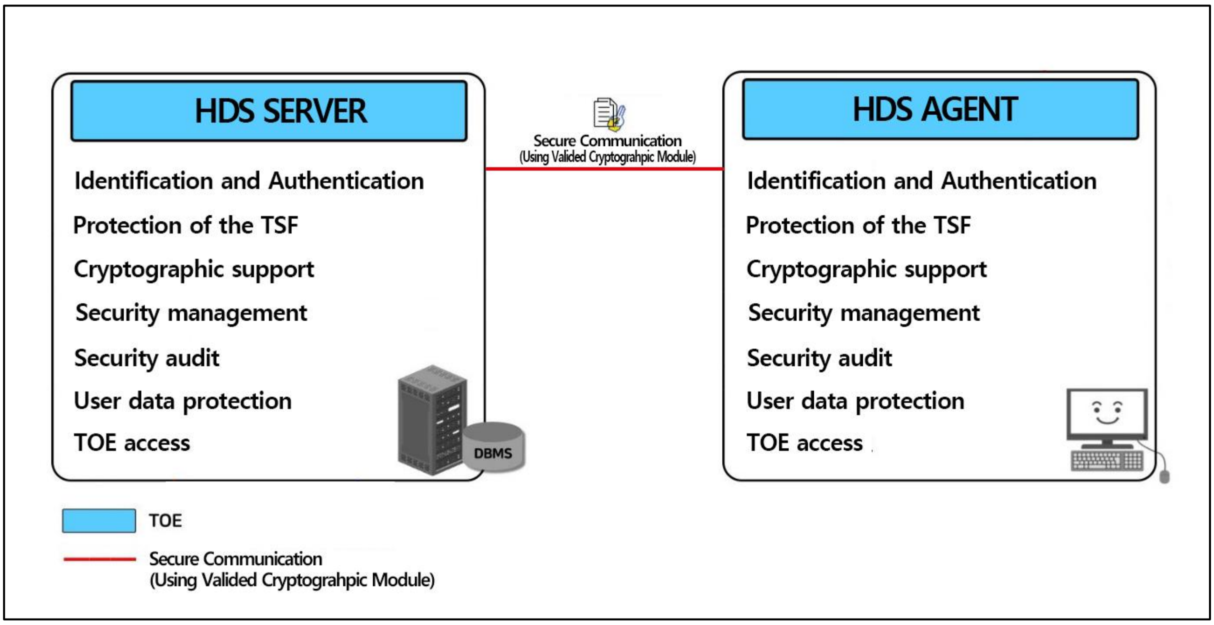
The hardware and operation system where the TOE is installed, application for document user uses and other software necessary to operate the TOE are excluded from the scope of the TOE. The physical scope of the TOE is as follow.



[Figure 2] Physical scope of the TOE

1.4.2. Logical scope of the TOE

The logical scope of the TOE is as follows.



[Figure 3] Logical scope of the TOE

1.4.2.1. Security audit

The TOE generates and stores audit data on events related to start/termination of audit function and security function in the DBMS.

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

The following potential violations are sent to the administrator via email.

- Integrity violation
- TSF self-tests failure
- Mutual authentication failure
- Login failure 5 times
- Unauthorized shutdown/deletion of TOE executables and processes
- Document user failure to encrypt/decrypt documents

In case the audit data storage limit is exceeded by 80%, TOE sends an email alert to the authorized administrator, overwrites existing data (delete audit data for older three days) when the storage limit is exceeded by 90%, and a warning message is sent to the authorized administrator via email.

1.4.2.2. Cryptographic support

HASH_DRBG (256 bit) 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. All encryption keys are used and then destroyed through overwritten with '0' three times in the memory.

1.4.2.3. User data protection

The HDS AGENT of the TOE 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 files 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

[Table 5] File format of the application

1.4.2.4. Identification and Authentication

The TOE provides identification and authentication process based on ID/PW for the administrator and document user. Only the authorized administrator can manage the security functions through the web browser. 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 administrator and document user authentication information, the timestamp of the packet is added, and mutual authentication is performed

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 the Internally Implemented Authentication Protocol when communicating between HDS SERVER and HDS AGENT.

1.4.2.5. 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

1.4.2.6. Protection of the TSF

The TOE performs secure communication to protect transmission data between the components and provides confidentiality and integrity. In addition, the stored TSF date is protected from unauthorized exposure and alteration 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.

1.4.2.7. 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 attempt is blocked, and administrators can access only from the devices whose IP is designated as accessible.

1.5. Convention

This Security Target uses a mixture of English for some abbreviations and clear meanings. The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation.

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST.

Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection

This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as underlined and italicized.

Refinement

This is used to add details and thus further restrict a requirement. The result of refinement is shown in bold text.

1.6. Terms and definitions

Terms used in this ST, which are the same as in the CC, must follow those in the CC.

Private Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Object

Passive entity in the TOE containing or receiving information and on which subjects perform operations

Approved mode of operation

The mode of cryptographic module using approved cryptographic algorithm

Approved cryptographic algorithm

A cryptographic algorithm selected by Korean Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability

Validated Cryptographic Module

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

Attack potential

Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation

Public Security Parameters, PSP

Security related public information whose modification can compromise the security of a cryptographic module

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private keys

Management access

The access to the TOE by using the HTTPS, SSH, TLS, IPSec etc. to manage the TOE by administrator, remotely

Management console

Application program that provides GUI, CLI, etc. to the administrator and provides system management and configuration

Recommend/be recommended

The 'recommend' or 'be recommended' presented in Application notes is not mandatorily recommended, but required to be applied for secure operations of the TOE

Group Based Access Control

As the one of the discretionary access control, performing the access control for the entity based on group identity

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.

Symmetric cryptographic technique

Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique

Data Encryption Key: DEK

Key that encrypts the data

Local access

The access to the TOE by using the console port to manage the TOE by administrator, directly

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.)

Iteration

Use of the same component to express two or more distinct requirements

ST, Security Target

Implementation-dependent statement of security needs for a specific identified TOE

Security Policy Document

Document uploaded to the list of the validated cryptographic module with the module's name and specifying the summary for the cryptographic algorithms and operational environments of the TOE

Security Token

Hardware device that implements key generation and electronic signature generation inside the device to save/store confidential information safely.

PP, Protection Profile

Implementation-independent statement of security needs for a TOE type

Decryption

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

Non-Approved mode of operation

It is a mode that can operate the non-verification target encryption algorithm, and the verification target encryption algorithm can be used

Secret Key

A cryptographic key which is used in a symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

User

See "external entity", a user means authorized administrator and authorized document user

Selection

Specification of one or more items from a list in a component

Identity

Representation uniquely identifying entities (e.g., user, process or disk) within the context of the TOE

Encryption

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

KCMVP, Korea Cryptographic Module Validation Program

A system to validate the security and implementation conformance of cryptographic modules used for the protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions

Element

Indivisible statement of a security need

Role

Predefined set of rules on permissible interactions between a user and the TOE

Role Based Access Control, RBAC

An access control that restricting system access by not the direct relationship (e.g., user-permission) but the role depended on the properties of the organization (e.g., user-role, permission-role), when the user access to the entity

Operation (On a component of the CC)

Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation (On a subject)

Specific type of action performed by a subject on an object

External Entity

Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Threat AGENT

Entity that can adversely act on assets

Authorized Administrator

Authorized user to securely operate and manage the TOE

Authorized Document User

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

Authentication Data

Information used to verify the claimed identity of a user

Application Programming Interface, API

A set of system libraries existing between the application layer and the platform system, enables the easy development of the application running on the platform

TSF self-tests

Pre-operational or conditional test executed by the cryptographic module

Refinement

Addition of details to a component

Access Control List, ACL

The list including entities who are permitted to access the entity and the types of these permission

Information System

Systematic system of devices and software related to the collection, processing, storage, search, sending, receiving, and utilization of the information.

Organizational Security Policies

Set of security rules, procedures, or guidelines for an organization wherein the set is currently given by actual or virtual organizations, or is going to be given

Dependency

Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Subject
Active entity in the TOE that performs operations on objects

Sensitive Security Parameters, SSP
Critical security parameter (CSP) and public security parameter (PSP

Augmentation
Addition of one or more requirement(s) to a package

Component
Smallest selectable set of elements on which requirements may be based

Class
Set of CC families that share a common focus

Key Encryption Key: KEK
Key that encrypts another cryptographic key

TOE, Target of Evaluation
Set of software, firmware and/or hardware possibly accompanied by guidance

EAL, Evaluation Assurance Level
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Family
Set of components that share a similar goal but differ in emphasis or rigor

Assignment
The specification of an identified parameter in a component (of the CC) or requirement

Shall/must

The ‘shall’ or ’must’ presented in Application notes indicates mandatory requirements applied to the TOE

Can/Could

The ‘can’ or ‘could’ presented in Application notes indicates optional requirements applied to the TOE by ST author’s choice

Critical Security Parameters, CSP

Security-related information whose disclosure or modification can compromise the security of a cryptographic module (e.g., secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors)

TSF, TOE Security Functionality

Combined functionality of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

SSL (Secure Sockets Layer)

This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network

TLS (Transport Layer Security)

This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246

Wrapper

Interface to connect the TOE with various types of information system

1.7. Security Target contents

Chapter1 introduces the ST and provides the TOE reference, TOE overview, TOE description, composition rules, terminology definition, and configuration information of the ST.

Chapter2 declares compliance with the CC, PP, and package as a conformance claim and describes the rationale for the declaration of compliance.

Chapter3 describes the security objectives for the TOE operational environment.

Chapter4 define an extended component that is additionally required according to the 'document encryption' property in the extended component definition.

Chapter5 security requirements describe security functional requirements and assurance requirements for satisfying security objectives.

Chapter6 summarizes the security functions of the TOE.

Chapter7 references refer to the data referenced in this ST.

2. Conformance claim

This section describes how this ST complies with the CC, PP, and package.

2.1. CC , PP and package conformance claim

CC		Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 - Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) - Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
Conformance claim	Part 2 security functional components	Extended : FCS_RBG.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1, FPT_PST.2, FTA_SSL.5
	Part 3 Security assurance components	Conformant
	PP	Korean National PP for Electronic Document Encryption V1.1 (2019-12-11)
	Package	Augmented : EAL1 augmented (ATE_FUN.1)

[Table 6] CC and conformance claim

2.2. Conformance claim rationale

This ST claims conformance to security objectives and security requirements by strict adherence to 'Korean National Protection Profile for Electronic Document Encryption V1.1'.

Classification	PP	ST	Rationale
TOE type	Electronic document encryption	Electronic document encryption	Same as PP
Security functional components	FAU_ARP.1	FAU_ARP.1	Same as PP
	FAU_GEN.1	FAU_GEN.1	Same as PP
	FAU_SAA.1	FAU_SAA.1	Same as PP

	FAU_SAR.1	FAU_SAR.1	Same as PP
	FAU_SAR.3	FAU_SAR.3	Same as PP
	FAU_STG.3	FAU_STG.3	Same as PP
	FAU_STG.4	FAU_STG.4	Same as PP
	FCS_CKM.1	FCS_CKM.1(1)	Same as PP
		FCS_CKM.1(2)	Same as PP
	FCS_CKM.2	FCS_CKM.2	Same as PP
	FCS_CKM.4	FCS_CKM.4	Same as PP
	FCS_COP.1	FCS_COP.1(1)	Same as PP
		FCS_COP.1(2)	Same as PP
		FCS_COP.1(3)	Same as PP
	FCS_RBG.1(Extended)	FCS_RBG.1(Extended)	Same as PP
	FDP_ACC.1	FDP_ACC.1(1)	Same as PP
	FDP_ACF.1	FDP_ACF.1(1)	Same as PP
	FIA_AFL.1	FIA_AFL.1	Same as PP
	FIA_IMA.1	FIA_IMA.1	Same as PP
	FIA_SOS.1	FIA_SOS.1	Same as PP
	FIA_UAU.1	FIA_UAU.1	Same as PP
	FIA_UAU.4	FIA_UAU.4	Same as PP
	FIA_UAU.7	FIA_UAU.7	Same as PP
	FIA_UID.1	FIA_UID.1	Same as PP
	FMT_MOF.1	FMT_MOF.1	Same as PP
	FMT_MSA.1	FMT_MSA.1	Same as PP
	FMT_MSA.3	FMT_MSA.3	Same as PP
	FMT_MTD.1	FMT_MTD.1	Same as PP
	FMT_PWD.1(Extended)	FMT_PWD.1(Extended)	Same as PP
	FMT_SMF.1	FMT_SMF.1	Same as PP
	FMT_SMR.1	FMT_SMR.1	Same as PP
	FPT_ITT.1	FPT_ITT.1	Same as PP
	FPT_PST.1(Extended)	FPT_PST.1(Extended)	Same as PP
	FPT_PST.2(Extended)	FPT_PST.2(Extended)	Same as PP
	FPT_TST.1	FPT_TST.1	Same as PP
	FTA_MCS.2	FTA_MCS.2	Same as PP
	FTA_SSL.5(Extended)	FTA_SSL.5(Extended)	Same as PP
	FTA_TSE.1	FTA_TSE.1	Same as PP
Security assurance components	ASE_INT.1	ASE_INT.1	Same as PP
	ASE_CCL.1	ASE_CCL.1	Same as PP
	ASE_OBJ.1	ASE_OBJ.1	Same as PP

	ASE_ECD.1	ASE_ECD.1	Same as PP
	ASE_REQ.1	ASE_REQ.1	Same as PP
	ASE_TSS.1	ASE_TSS.1	Same as PP
	ADV_FSP.1	ADV_FSP.1	Same as PP
	AGD_OPE.1	AGD_OPE.1	Same as PP
	AGD_PRE.1	AGD_PRE.1	Same as PP
	ALC_CMC.1	ALC_CMC.1	Same as PP
	ALC_CMS.1	ALC_CMS.1	Same as PP
	ATE_FUN.1	ATE_FUN.1	Same as PP
	ATE_IND.1	ATE_IND.1	Same as PP
	AVA_VAN.1	AVA_VAN.1	Same as PP

[Table 7] Conformance claim rationale

3. Security objectives

The followings are the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

3.1. Security objectives for the operational environment

OE.PHYSICAL_CONTROL

The place where the management server among the TOE components is installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.

OE.TRUSTED_ADMIN

The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidance.

OE.LOG_BACKUP

The authorized administrator shall periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

OE.OPERATION_SYSTEM_RE_INFORCEMENT

The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

OE.RELIABLE_TIME_STAMP

The TOE shall use reliable time information provided by the TOE operating environment.

OE.PREVENTION_AUDIT_DATA_LOSS

The audit record where the audit trail, such as the DBMS interacting with the TOE, is saved should be protected against unauthorized deletion or modification.

OE.MANAGEMENT_ACCESS

For communication between the web browser of the administrator PC and the web server which is the operation environment of the management server, TLS 1.2 shall be used to guarantee the confidentiality and integrity of the transmitted data.

4. Extended components definition

This section describes the components extended in Part 2 or Part 3 of the Common Criteria of this ST specification.

4.1. FCS, Cryptographic support)

4.1.1. Random bit generation

Family behavior

This family defines requirements for the TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Component leveling

FCS_RBG.1 random bit generation, requires TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Management: FCS_RBG.1

There are no management activities foreseen

Audit: FCS_RBG.1

There are no auditable events foreseen

4.1.1.1. FCS_RBG.1 Ran

Hierarchical to	No other components
Dependencies	No other components

FCS_RBG.1.1 The TSF shall generate random bits required to generate a cryptographic

key using the specified random bit generator that meets the following [assignment: list of standards].

4.2. FIA, Identification and authentication

4.2.1. TOE Internal mutual authentication

Family behavior

This family defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.

Component leveling

FIA_IMA TOE Internal mutual authentication
1

FIA_IMA.1 TOE Internal mutual authentication requires that the TSF provides mutual authentication function between TOE components in the process of user identification and authentication.

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of mutual authentication

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to	No other components
Dependencies	No other components

FIA_IMA.1 The TSF shall perform mutual authentication between [assignment: different parts of TOE] by [assignment: authentication protocol] that meet the following: [assignment: list of standards].

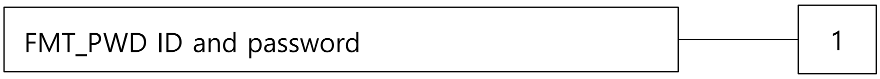
4.3. FMT, Security Management

4.3.1. ID and password

Family behavior

This family defines the capability that is required to control ID and password management used in the TOE, and set or modifies ID and/or password by authorized users.

Component leveling



FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password

4.3.1.1. FMD_PWD.1 Management of ID and password

Hierarchical to	No other components
Dependencies	FMT_SMF.1 Specification of management function FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: list of functions] to [assignment: the authorized identified roles].

1. [assignment: password combination rules and/or length]

2. [assignment: other management such as management of special characters unusable for password, etc.]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: list of functions] to [assignment: the authorized identified roles].

1. [assignment: ID combination rules and/or length]

2. [assignment: other management such as management of special Characters unusable for ID, etc.]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: setting

ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time].

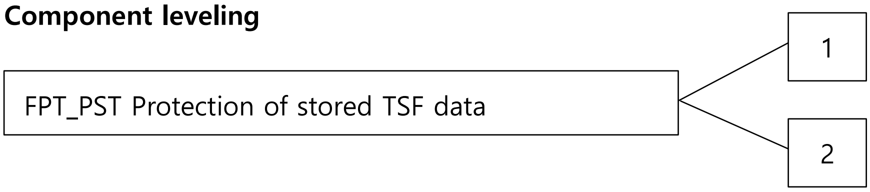
4.4. FPT, Protection of the TSF

4.4.1. Protection of stored TSF data

Family behavior

This family defines rules to protect the TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component leveling



FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.

FPT_PST.2 Availability protection of TSF data requires the TSF to ensure the defined levels of availability for the TSF data.

Management: FPT_PST.1, FPT_PST.2
There are no management activities foreseen.

Audit: FPT_PST.1, FPT_PST.2
There are no audit events foreseen.

4.4.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to	No other components
Dependencies	No other components

FPT_PST.1.1	The TSF shall protect [assignment: TSF data] stored in containers controlled by the TSF from the unauthorized [selection: disclosure, modification].

4.4.1.2. FPT_PST.2 Availability protection of TSF data

Hierarchical to	No other components
Dependencies	No other components

FPT_PST.2.1	The TSF shall [selection: detect, prevent] the unauthorized deletion for [assignment: TSF data].
FPT_PST.2.2	The TSF shall [selection: detect, prevent] the unauthorized termination for [assignment: TSF data].

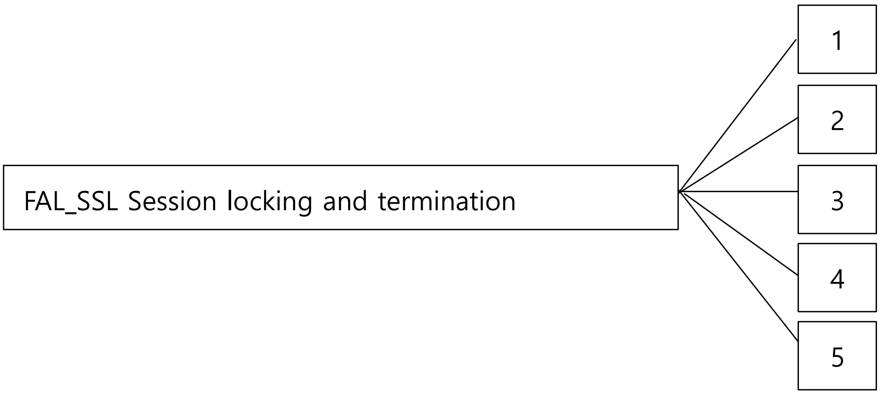
4.5. FTA, TOE Access

4.5.1. Session locking and termination

Family behavior

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Component leveling



In CC Part 2, the session locking and termination family consists of four components. In this ST, it consists of five components by extending one additional component as follows.

※ The relevant description for four components contained in CC Part 2 is omitted.

FTA_SSL.5 The management of TSF-initiated sessions, provides requirements that the TSF locks or terminates the session after a specified time interval of user inactivity.

Management: FTA_SSL.5

The following actions could be considered for the management functions in FMT:

a) Specification for the time interval of user inactivity during which the session locking and termination occurs to each user.

b) Specification for the time interval of default user inactivity during which the session locking and termination occurs.

Audit: FTA_SSL.5

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive session

4.5.1.1. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to	No other components
Dependencies	[FIA_UAU.1 authentication or No dependencies.]

FTA_SSL.5.1 The TSF shall [selection: lock the session and re-authenticate the user before unlocking the session, terminate] an interactive session after a [assignment: time interval of user inactivity].

5. Security requirements

This chapter specifies security functional requirements and assurance requirements that must be satisfied by the TOE.

Subjects, objects, relevant security attributes and operations in this ST are defined as follows:

Subject (User)	Security Attributes of Subject (User)	Object (Information)	Security Attributes of Object (Information)	Operation	SFR or SAR
Authorized administrator	User ID, password, IP address	Administrator password	-	Modify	FMT_MOF.1 FMT_MTD.1 FMT_MSA.1 FMT_PWD.1
		Administrator IP		Query, modify	
		Email setting		Query, modify	
		User registration		Query, modify	
		User password		Modify	
		Decryption right		Query, modify	
		Agent deletion right		Query, modify	
		User deletion		Modify	
		Agent log		Query	
		Server log		Query	
		Send mail log		Query	
		Management log		Query	

Document user	User ID	User document	Designated file type	Encryption, decryption	FDP_ACC.1(1)
					FDP_ACF.1(1)

Evaluator	-	Potential vulnerability	-	Survey	AVA_VAN.1.2E
	-	TOE	Attack potential	Penetration testing	AVA_VAN.1.3E
Developer	-	ST Conformance claim	-	Provide	ASE_INT.1.1D ASE_CCL.1.1D ASE_OBJ.1.1D

		Security objectives Extended components Security requirements Summary specification Functional specification Operational user guidance Preparative procedures TOE configuration list TOE and reference Test documentation			ASE_ECD.1.1D ASE_REQ.1.1D ASE_TSS.1.1D ADV_FSP.1.1D AGD_OPE.1.1D AGD_PRE.1.1D AGD_PRE.1.1D ALC_CMC.1.1D ALC_CMS.1.1D ATE_FUN.1.1D

[Table 8] Definition of subject, object, relevant security attributes and operation

5.1. Security functional requirements

The security functional requirements specify security functional requirements and assurance requirements that conform to the PP and must be satisfied by the TOE. The security functional requirements included in the PP are derived from CC Part 2 and Chapter 4 Extended Components Definition.

The following table summarizes the security functional requirements.

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss

Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (Electronic Document Encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF Data Encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic key operation (Electronic Document Encryption)
	FCS_COP.1(2)	Cryptographic key operation (TSF Data Encryption)
	FCS_COP.1(3)	Cryptographic key operation (One-way Encryption)
	FCS_RBG.1(Extended)	Random bit generation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (Electronic Document Encryption access control)
	FDP_ACF.1(1)	Security attribute based access control (Electronic Document Encryption access control)
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_PST.2(Extended)	Availability protection of TSF data
	FPT_TST.1	TSF testing
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

[Table 9] Security functional requirements

5.1.1. Security audit (FAU)

5.1.1.1. FAU_ARP.1 Security alarms

Hierarchical to No other components

Dependencies FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [an action to send an email to the administrator] upon detection of a potential security violation.

5.1.1.2. FAU_GEN.1 Audit data generation

Hierarchical to No other components

Dependencies FPT_STM.1 Reliable time stamps

FAU_GEN1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audits; and

c) [Refer to the "auditable events" in [Table 10], [None]]

FAU_GEN1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in ST [Refer to the contents of "additional audit record" in [Table 10] Audit events, [None]]

Security Functional Component	Auditable Event	Additional Audit Record
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FCS_CKM.1(2)	Success and failure of the activity	

FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	
FCS_CKM.4	Success and failure of the activity (applying to destruction of key related to Electronic Document Encryption/Decryption)	
FCS_COP.1	Success and failure, and the type of cryptographic operation	
FDP_ACF.1	Successful request of operation execution regarding the object handled by SFP	Object identification information
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	
FIA_IMA.1(Extended)	Success and failure of mutual authentication	
FIA_UAU.1	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	Modified data values
FMT_MSA.1	All modifications to the security attributes	Modified data values
FMT_MSA.3	Modifications to the basic settings of allowance or restriction rules, All modifications to the initial values of security attributes	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1(Extended)	All modifications to the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	

FTA_SSL.5(Extended)	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism, All attempts at establishment of a user session	

[Table 10] Audit events

5.1.1.3. FAU_SAA.1 Potential violation analysis

Hierarchical to No other components
Dependencies FAU_GEN.1 Audit data generation

FAU_SAA1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [auditable events of authentication failure in FIA_UAU.1, auditable events of integrity violation and self-test failure of the validated cryptographic module in FPT_TST.1, auditable events of control rule violation in FDP_ACF.1(1)] known to indicate a potential security violation;
b) [None]

5.1.1.4. FAU_SAR.1 Audit review

Hierarchical to No other components
Dependencies FAU_GEN.1 Audit data generation

FAU_SAR1.1 The TSF shall provide the [authorized administrator] with the capability to read [all the audit data] from the audit records.

FAU_SAR1.2 The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

5.1.1.5. FAU_SAR.3 Selectable audit review

Hierarchical to No other components
Dependencies FAU_SAR.1 Audit review

FAU_SAR3.1 The TSF shall provide the ability to apply [searching in descending order based on the server time] of audit data based on [AND operation].

Audit Data Type	Search Category	Search Condition
Agent log	Search menu	Log date separation, user ID, log content
	Query item	Server time, PC time, user ID, client IP, client MAC, log content, log-generating process
Server log	Search menu	Log date, log content, log-generating process
	Query item	Server time, PC time, log-generating process, process ID, server IP, server PORT, client IP:PORT, log content
Mail sending log	Search menu	Log date, mail title, message body, sender, status
	Query item	Server time, sender, mail title, message body, sending status
Management log	Search menu	Log date, menu name, log content
	Query item	Server time, menu name, event, client IP, log content

[Table 11] Audit review

5.1.1.6. FAU_STG.3 Action in case of possible audit data loss

Hierarchical to No other components

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [send an email to the authorized administrator, [none]] if the audit trail exceeds [80% of the available hard disk space].

5.1.1.7. FAU_STG.4 Prevention of audit data loss

Hierarchical to FAU_STG.3 Action in case of possible audit data loss

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [send an email to the authorized administrator] if the audit trail is full.

5.1.2. Cryptographic support (FCS)

5.1.2.1. FCS_CKM.1(1) Cryptographic key generation (Electronic Document Encryption)

Hierarchical to No other components

Dependencies [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [HASH_DRBG(SHA-256)] and specified cryptographic key sizes [256 bits] that meet the following [ISO/IEC 18031].

5.1.2.2. FCS_CKM.1(2) Cryptographic key generation (TSF Data Encryption)

Hierarchical to No other components

Dependencies [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [algorithms in [Table 12]] and specified cryptographic key sizes [256 bits] that meet the following [list of standards in [Table 12]].

Category	Algorithm	Key Size	List of Standards
DEK for TSF data	HASH_DRBG	256 bits	ISO/IEC 18031
Packet	ECDH(EC_P256_r1)	256 bits	ISO/IEC 11770-3
KEK	PBKDF2 (SALT value is randomly generated with the iteration count of 1024)	256 bits	TTAS.KO-12.0334
DEK for mutual authentication	HASH_DRBG	256 bits	ISO/IEC 18031

[Table 12] Generation algorithm

5.1.2.3. FCS_CKM.2 Cryptographic key distribution

Hierarchical to No other components

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [algorithm in [Table 13]] that meets the following [list of standards in [Table 13]].

Category	Algorithm	Key Size	List of Standards
Packet	ECDH	256 bits	ISO/IEC 11770-3
Document HEADER DEK	ARIA-CBC	256 bits	KS X 1213-1

[Table 13] Distribution algorithm

5.1.2.4. FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting with "0"] that meets the following [none].

5.1.2.5. FCS_COP.1(1) Cryptographic operation (Electronic Document Encryption)

Hierarchical to No other components

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [electronic document encryption and decryption] in accordance with a specified cryptographic algorithm [ARIA_CTR] and cryptographic key size [256 bits] that meet the following [KS X 1213-1].

5.1.2.6. FCS_COP.1(2) Cryptographic operation (TSF data)

Hierarchical to No other components

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [list of cryptographic operations in [Table 14]] in accordance with a specified cryptographic algorithm [cryptographic algorithm in [Table 14]] and cryptographic key size [cryptographic key size in [Table 14]] that meet the following [list of standards in [Table 14]].

Algorithm	List of Standards	Key Size	List of Cryptographic Operations
ARIA-CBC	KS X 1213-1	256 bits	● Encryption/decryption of TSF data ● Encryption/decryption communication
ECDH	ISO/IEC 11770-3	256 bits	● Cryptographic key exchange
PBKDF2 (SALT value is randomly generated with the iteration count of 1024)	TTAS.KO-12.0334	256 bits	● TSF data DEK encryption/decryption

[Table 14] Cryptographic operations

5.1.2.7. FCS_COP.1(3) Cryptographic operation (one-way encryption)

Hierarchical to No other components

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [cryptographic operations in [Table 15]] in accordance with a specified cryptographic algorithm [SHA-256] and cryptographic key size [none] that meet the following [SO/IEC 10118-3].

Cryptographic Algorithm	List of Standards	List of Cryptographic Operations
HASH(SHA-256)	ISO/IEC 10118-3	● TSF data integrity monitoring ● Protection of executable file ● Password encryption

[Table 15] One-way cryptographic operation

5.1.2.8. FCS_RBG.1 Random bit generation (Extended)

Hierarchical to No other components

Dependencies No dependencies

FCS_RBG.1.1 The TSF shall generate random bits using the specified random bit generator that meets the following [[Table 16] Random bit generation].

Random Bit Generation Algorithm	Random Bit Size	List of Standards
HASH-DRBG(SHA-256)	256 bits	ISO/IEC 18031

[Table 16] Random bit generation

5.1.3. User data protection (FDP)

5.1.3.1. FDP_ACC.1(1) Subset access control (Electronic Document Encryption access control)

Hierarchical to No other components

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce [Electronic Document Encryption access control] on [list of subjects, objects, and operations among subjects and objects covered by SFP].

[

- ■ List of subjects: document user
- ■ List of objects: documents that shall be protected
- ■ Operations: read, write, encrypt, decrypt

]

5.1.3.2. FDP_ACF.1(1) Security attribute based access control (Electronic Document Encryption access control)

Hierarchical to No other components

Dependencies FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [Electronic Document Encryption access control] to objects based on [list of subjects and objects controlled by the following SFP, security attribute appropriate for SFP regarding each subject and object].

[

- List of subjects/security attribute: document user / user ID
- List of objects/security attribute: documents that shall be protected / PDF, XLS, XLSX, XLSM, XLSB, XLTX, XLTM, DOC, DOCX, DOTM, DOTX, PPT, PPTX, PPTM, PPS, PPSM, PPSX, POT, POTX, POTM, HWP, HWT
- Operations: read, write, encrypt, decrypt

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

a) If the security attribute for the subject is included to the security attribute which is permitted to access for the object and the operation is matched with the security attribute of the object, the corresponding operation is allowed.

b) [None]

]

FDP_ACF.1.3 The TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [none]

FDP_ACF.1.4 The TSF shall explicitly deny access of the subject to objects based on the following additional rules: [none]

5.1.4. Identification and authentication (FIA)

5.1.4.1. FIA_AFL.1 Authentication failure handling

Hierarchical to	No other components
Dependencies	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *[5]* unsuccessful authentication attempts occur related to [administrator and document user authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [inactivate the identification and authentication function for 10 minutes].

5.1.4.2. FIA_IMA.1 TOE internal mutual authentication

Hierarchical to	No other components
Dependencies	No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication between [HDS SERVER and HDS AGENT] in accordance with a specified [internally implemented authentication protocol] that meets the following [none].

5.1.4.3. FIA_SOS.1 Verification of secrets

Hierarchical to	No other components
Dependencies	No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined combination rule].

[Combination rule:

- English alphabet (differentiating between uppercase and lowercase): a-z, A-Z
- Number: 0-9
- Special character: !, @, #, $, %, ^, &, +, =, -
- Combination of English alphabet, number and special character
- At least 9 up to 20 digits

]

5.1.4.4. FIA_UAU.1 Timing of authentication

Hierarchical to No other components

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [the following list] on behalf of the user to be performed before the document user is authenticated.

[

a) Document user
   A. Enter the password for the encryption key (KEK)
   B. Check the version information
b) Administrator: none

]

FIA_UAU.1.2 The TSF shall require each document user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user, except for the actions specified in FIA_UAU.1.1.

5.1.4.5. FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components

Dependencies No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [ID/PW based authentication mechanism].

5.1.4.6. FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components

Dependencies FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [the following list of feedback] to the user while the authentication is in progress.

[

List of feedback

- All passwords entered are masked with "*" or "•."
- In case of authentication failures, feedback for the cause of failure is not provided.

]

5.1.4.7. FIA_UID.1 Timing of identification

Hierarchical to	No other components
Dependencies	No dependencies

FIA_UID.1.1 The TSF shall allow [the following list] on behalf of the document user to be performed before the user is identified.

[

a) Document user

   A. Enter the password for the encryption key (KEK)

   B. Check the version information

b) Administrator: none

]

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user except for the actions specified in FIA_UID.1.1.

5.1.5. Security management (FMT)

5.1.5.1. FMT_MOF.1 Management of security functions behaviour

Hierarchical to	No other components
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to ***conduct management actions of*** the functions [list of functions in [Table 17]] to [the authorized administrator].

Menu	Category	Management Actions
Basic Settings	Modify administrator password	Modify
	Register administrator IP	Add, modify
	Email settings	Add, modify
User Management	Register user	Add, delete
	Initialize user password	Modify
	Set decryption right	Modify
	Set agent deletion right	Modify

Agent log status	Manage logs	View
Server log status	Manage logs	View
Mail sending log status	Manage logs	View
Management log status	Manage logs	View

[Table 17] List of functions

5.1.5.2. FMT_MSA.1 Management of security attributes

Hierarchical to No other components

Dependencies [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [access control SFP] to restrict the ability to *change_default, modify, delete, [add]* the security attributes [list of security attributes] to [the authorized administrator].

[

List of security attributes

- Decryption right setting
- Agent deletion right setting

]

5.1.5.3. FMT_MSA.3 Static attribute initialization

Hierarchical to No other components

Dependencies FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce [access control SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4. FMT_MTD.1 Management of TSF data

Hierarchical to No other components

Dependencies FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to **manage** the [list of TSF data in [Table 17]] to [the authorized administrator].

Category		Management Actions
Audit data	Agent log	Query
	Server log	
	Mail sending log	
	Management log	
Authentication data	Administrator ID	Query, modify
	Administrator password	Modify
	User ID	Add, query, delete
	User password initialization	Modify
Security management data	Decryption right setting	Add, query, modify, delete
	Agent deletion right setting	Add, query, modify, delete
	Administrator IP registration	Add, query, modify
Mail setting data	Mail setting	Query, modify

[Table 17] List of TSF data

5.1.5.5. FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to No other components
Dependencies FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [none] to [the authorized administrator].

1. [None]
2. [None]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [none] to [the authorized administrator].

1. [None]
2. [None]

FMT_PWD.1.3 The TSF shall provide the capability for *setting ID and password when* installing.

5.1.5.6. FMT_SMF.1 Specification of management functions

Hierarchical to	No other components
Dependencies	No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [list of management functions to be provided by the TSF]

[

- Management actions of TSF function: items specified in FMT_MOF.1
- Management actions of TSF security attributes: items specified in FMT_MSA.1
- Management actions of TSF data: items specified in FMT_MTD.1.1

]

5.1.5.7. FMT_SMR.1 Security roles

Hierarchical to	No other components
Dependencies	FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate users and their **roles defined in FMT_SMR.1.1**.

5.1.6. Protection of the TSF (FPT)

5.1.6.1. FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to	No other components
Dependencies	No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

5.1.6.2. FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to	No other components
Dependencies	No dependencies

FPT_PST.1.1 The TSF shall protect [administrator and document user password, encryption key, TOE configuration values, DB password] stored in containers controlled by the TSF from the unauthorized *disclosure, modification.*

5.1.6.3. FPT_PST.2 Availability protection of stored TSF data (Extended)

Hierarchical to	No other components
Dependencies	No dependencies

FPT_PST.2.1 The TSF shall *prevent* the unauthorized deletion for [HDS AGENT executable file].

FPT_PST.2.2 The TSF shall *prevent* the unauthorized termination for [HDS AGENT process].

5.1.6.4. FPT_TST.1 TSF testing

Hierarchical to	No other components
Dependencies	No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests during *initial start-up, periodically during normal operation* to demonstrate the correct operation of the *TSF.*

FPT_TST.1.2 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of *TSF.*

5.1.7. TOE access (FTA)

5.1.7.1. FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to	FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies	FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [rules for the number of maximum concurrent sessions that restrict the number of maximum concurrent sessions to 1 for administrator management access sessions { the number of maximum concurrent sessions to 1 for document user access sessions }]

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] session per user.

5.1.7.2. FTA_SSL.5 Management of TSF-initiated sessions (Extended)

Hierarchical to No other components

Dependencies FIA_UAU.1 Timing of authentication or no dependencies

FTA_SSL.5.1 The TSF shall *terminate* an interactive session of the **administrator** after [10 minutes of the administrator inactivity].

5.1.7.3. FTA_TSE.1 TOE session establishment

Hierarchical to No other components

Dependencies No dependencies

FTA_TSE.1.1 The TSF shall be able to deny **administrator's management access session** establishment based on [connection IP, *whether or not to activate the management access session of the same account*].

5.2. Security Requirements

In this section specify security functional requirements and assurance requirements that must be satisfied by the TOE.

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operation user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE configuration management coverage
Tests	ATE_FUN.1	Functional testing

	ATE_IND.1	Independent testing: conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

[Table 18] Assurance requirements

5.2.1. Security Target evaluation

5.2.1.1 ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements

ASE_INT.1.1D

The developer shall provide a ST introduction.

Content and presentation elements

ASE_INT.1.1C

The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C

The ST reference shall uniquely identify the ST.

ASE_INT.1.3C

The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C

The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C

The TOE overview shall identify the TOE type.

ASE_INT.1.6C

The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C

The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C

The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E

The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

5.2.1.2 ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D

The developer shall provide a conformance claim.

ASE_CCL.1.2D

The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C

The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C

The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C

The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C

The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C

The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C

The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C

The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C

The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C

The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

ASE_CCL1.1E

The evaluator shall confirm that the information provided meets all requirements for content

and presentation of evidence.

5.2.1.3 ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies

Developer action elements

ASE_OBJ.1.1D

The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1.1C

The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements

ASE_OBJ.1.1E

The evaluator shall confirm that the information provided meets all requirements for content

and presentation of evidence.

5.2.1.4 ASE_ECD.1 Extended components definition

Dependencies: No dependencies

Developer action elements

ASE_ECD.1.1D

The developer shall provide a statement of security requirements.

ASE_ECD.1.2D

The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C

The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C

The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C

The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C

The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C

The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

ASE_ECD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E

The evaluator shall confirm that no extended component can be clearly expressed using existing components.

5.2.1.5 ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.1.1D

The developer shall provide a statement of security requirements.

ASE_REQ.1.2D

The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C

The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C

The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C

All operations shall be performed correctly.

ASE_REQ.1.5C

Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C

The statement of security requirements shall be internally consistent.

Evaluator action elements

ASE_REQ.1.1.E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.6 ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D

The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C

The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

ASE_TSS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E

The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2. Development

5.2.2.1 ADP_FSP.1 Basic function specification

Dependencies: No dependencies

Developer action elements

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3. Guidance documents

5.2.3.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D

The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies

Developer action elements

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4. Life-cycle support

5.2.4.1 ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C

The TOE shall be labelled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies

Developer action elements

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.1.1C

The configuration list shall include the followings: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5. Tests

5.2.5.1 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements

ATE_FUN.1.1D

The developer shall test the TSF and document the results.

ATE_FUN.1.2D

The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C

The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C

The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C

The actual test results shall be consistent with the expected test results.

Evaluator action elements

ATE_FUN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.2 ATE_IND.1 Independent testing: conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements

ATE_IND.1.1D

The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.1.1C

The TOE shall be suitable for testing.

Evaluator action elements

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6. Vulnerability assessment

5.2.6.1 AVA_VAN.1 Vulnerability survey

AGD_PRE.1 Preparative procedures

Developer action elements

AVA_VAN.1.1.D

The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.1.1C

The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and preparation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker processing Basic attack potential.

5.3. Security requirement rational

5.3.1. Dependency of security functional requirements

The following table shows dependency of security functional requirements.

No.	Function component	Dependency	Reference No.

1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.RELIABLE_TIME_STAMP
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	OE.RELIABLE_STORAGE
7	FAU_STG.4	FAU_STG.1	OE.RELIABLE_STORAGE
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	10 or 12
		FCS_CKM.4	11
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	10 or 12
		FCS_CKM.4	11
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8 or 9
		FCS_CKM.4	11
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8 or 9
12	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8 or 9
		FCS_CKM.4	11
13	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8 or 9
		FCS_CKM.4	11
14	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	-
		FCS_CKM.4	-
15	FCS_RBG.1	-	-
16	FDP_ACC.1(1)	FDP_ACF.1	17
17	FDP_ACF.1(1)	FDP_ACC.1	16
		FMT_MSA.3	27
18	FIA_AFL.1	FIA_UAU.1	21
19	FIA_IMA.1	-	-
20	FIA_SOS.1	-	-
21	FIA_UAU.1	FIA_UID.1	24
22	FIA_UAU.4	-	-
23	FIA_UAU.7	FIA_UAU.1	21
24	FIA_UID.1	-	-
25	FMT_MOF.1	FMT_SMF.1	30
		FMT_SMR.1	31

26	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	16
		FMT_SMF.1	30
		FMT_SMR.1	31
27	FMT_MSA.3	FMT_MSA.1	26
		FMT_SMR.1	31
28	FMT_MTD.1	FMT_SMF.1	30
		FMT_SMR.1	31
29	FMT_PWD.1	FMT_SMF.1	30
		FMT_SMR.1	31
30	FMT_SMF.1	-	-
31	FMT_SMR.1	FIA_UID.1	24
32	FPT_ITT.1	-	-
33	FPT_PST.1	-	-
34	FPT_PST.2	-	-
35	FPT_TST.1	-	-
36	FTA_MCS.2	FIA_UID.1	24
37	FTA_SSL.5	FIA_UAU.1	21
38	FTA_TSE.1	-	-

[Table 20] Rationale for dependency

FAU_GEN.1 has the dependency on FPT_STM.1. However, the TOE uses the reliable time stamp (OE.RELIABLE_TIME_STAMP) provided by the TOE operational environment in order to correctly record security-related logs. Therefore, the dependency of FAU_GEN.1 of the security objectives for the operational environment is satisfied by OE.RELIABLE_TIME_STAMP provided by the TOE operational environment, instead of FPT_STM.1.

FAU_STG.3 and FAU_STG.4 have the dependency on FAU_STG.1. However, the TOE uses OE.RELIABLE_STORAGE provided by the TOE operational environment in order to correctly store audit data related to the TOE operation and perform unauthorized deletion or modification. The dependency of FAU_STG.3 and FAU_STG.4 for the operational environment is satisfied by OE.RELIABLE_STORAGE, instead of FAU_STG.1.

Although FCS_COP.1(3) has the dependency on FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, and FCS_CKM.4, it is satisfied as HASH algorithm does not use cryptographic keys.

5.3.2. Dependency rationale of security assurance requirements

As the dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

The augmented ATE_FUN.1 has dependency on ATE_COV.1, but ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation. ATE_COV.1 is not included in the PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

This chapter specifies security functionality that satisfies the security functional requirements.

6.1. TOE security functionality

This chapter describes security functions provided by the TOE and how the TOE satisfies security functional requirements specified in Chapter 5.

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access

6.1.1. Security audit

Security audit performs the following functions:

- Audit data generation
- Audit data view/search
- Protection of audit data

6.1.1.1. Audit data generation

The TOE generates all event logs generated in the TOE security functions. These logs are safely stored in the DBMS.

Audit data are divided into management log, agent log, server log and mail sending log.

Audit Data	Description
Agent log	Log on start/termination of the agent by a document user, self-diagnosis, mutual authentication, integrity, login, encryption key generation/use/destruction, and document viewing/saving
Server log	Log on start/termination of the server, self-diagnosis, mutual authentication, integrity, encryption key generation/use/destruction/distribution, and document user login
Mail sending log	Log on emails sent to the administrator
Management log	Log on login of HDS management web browser through which the

	administrator manages the TOE, menu switching, addition, modification, deletion and query

[Table 21] Description of audit data

Security Functional Component	Auditable Event	Classification of Audit Data
FAU_ARP.1	Actions taken due to potential security violations	Server log, Agent log, Mail sending log, Management log
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	Server log, Agent log
FAU_STG.3	Actions taken due to exceeding of a threshold	Server log
FAU_STG.4	Actions taken due to the audit storage failure	Server log
FCS_CKM.1(2)	Success and failure of the activity	Server log, Agent log
FCS_CKM.2	Success and failure of the activity (applying to distribution of key related to Electronic Document Encryption/Decryption)	Server log, Agent log
FCS_CKM.4	Success and failure of the activity (applying to destruction of key related to Electronic Document Encryption/Decryption)	Server log, Agent log
FCS_COP.1	Success and failure, and the type of cryptographic operation	Server log, Agent log
FDP_ACF.1	Successful request of operation execution regarding the object handled by SFP	Agent log
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal state	Server log, Management log
FIA_IMA.1(Extended)	Success and failure of mutual authentication	Server log, Agent log
FIA_UAU.1	All use of the authentication mechanism	Server log, Agent log

FIA_UAU.4	Attempts to reuse authentication data	Server log, Management log
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	Server log
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	Management log
FMT_MSA.1	All modifications to the security attributes	Management log
FMT_MSA.3	Modifications to the basic settings of allowance or restriction rules, All modifications to the initial values of security attributes	Management log
FMT_MTD.1	All modifications to the values of TSF data	Management log
FMT_PWD.1(Extended)	All modifications to the password	Server log, Management log
FMT_SMF.1	Use of the management functions	Management log
FMT_SMR.1	Modifications to the user group of rules divided	Management log
PT_TST.1	Execution of the TSF self tests and the results of the tests	Server log, Agent log
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	Server log, Agent log, Management log
FTA_SSL.5(Extended)	Locking or termination of interactive session	Management log
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism, All attempts at establishment of a user session	Management log

[Relevant SFR: FAU_GEN.1]

[Table 22] Classification of audit data, based on audit events

The TOE records logs in case of security violation, sends a warning email to the authorized administrator, and take designated actions for each security violation event.

Security Violation Event	Actions Taken
When the threshold (5 times) for the unsuccessful authentication attempts of a document user/administrator is exceeded	● Send an email to the authorized administrator ● Inactivate the authentication

(FIA_AFL.1)	function for 10 minutes
When an error is generated in integrity monitoring of TSF self tests and the performance of self-diagnosis fails (FPT_TST.1)	● Send an email to the authorized administrator
In case of unauthorized termination/deletion of executable files and processes of HDS AGENT and HDS SERVER (FPT_PST.1, FPT_PST.2)	● Send an email to the authorized administrator
In case of failure in mutual authentication between HDS AGENT and HDS SERVER (FIA_IMA.1)	● Send an email to the authorized administrator
In case of failed encryption/decryption of an electronic document by a document user (FDP_ACF.1(1))	● Send an email to the authorized administrator

[Relevant SFR: FAU_GEN.1, FIA_UAU.1, FDP_ACF.1, FPT_TST.1, FAU_SAA.1, FAU_ARP.1]

[Table 23] Security violation event and actions taken

6.1.1.2. Audit data view/search

The TOE provides the function that enables the authorized administrator to retrieve stored audit data as shown in the table below. Audit data can be retrieved in the descending order based on the selectable AND condition and the server time.

Audit Data	Item	Description	Format	Threshold
Agent log status	Log date separation	Time at which log is generated in HDS AGENT	Combo box	● Select between the server time and the PC time
	Date	Period for log generation in HDS AGENT	yyyy-mm-dd	● Year-Month-Day ● The end date is same as the start date. ● The end date is later than the start date.
	User ID	HDS AGENT User ID	English alphabet, number	● Up to 20 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Number: 0-9
	Log content	HDS AGENT log details	English alphabet, numbers, Korean alphabet	● Up to 128 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Number: 0-9 ● Korean alphabet
Server log status	Log date	Period for log generation in HDS SERVER, based on the server time	yyyy-mm-dd	● Year-Month-Day ● The end date is same as the start date. ● The end date is later than the start date.
	Log content	HDS SERVER log details	English alphabet, numbers, Korean alphabet	● Up to 128 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Number: 0-9 ● Korean alphabet
	Process	HDS SERVER log generation process	Combo box	● Select among all, HDS MAIL SENDER, HDS SERVER MANAGER and HDS SERVER
Mail sending log status	Server time	Period for sending emails based on the server time	yyyy-mm-dd	● Year-Month-Day ● The end date is same as the start date. ● The end date is later than the start date.
	Mail title	Title of the sent email	English alphabet, numbers,	● Up to 256 digits including spaces ● English upper/lower case

			Korean alphabet	letters: a-z, A-Z ● Number: 0-9 ● Korean alphabet
	Message body	Message body of the sent email	English alphabet, numbers, Korean alphabet	● Up to 512 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Number: 0-9 ● Korean alphabet
	Sender	Sender of the sent email	English alphabet, numbers, Korean alphabet	● Up to 128 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Number: 0-9 ● Korean alphabet
	Sending status	Sending status of the sent email	Combo box	● Select among all, success, failure, waiting and information error
Management log status	Server time	Period for management log generation based on the server time	yyyy-mm-dd	● Year-Month-Day ● The end date is same as the start date. ● The end date is later than the start date.
	Menu name	Management log menu name	English alphabet, Korean alphabet	● Up to 50 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Korean alphabet
	Log content	Management log details	English alphabet, numbers, Korean alphabet	● Up to 128 digits including spaces ● English upper/lower case letters: a-z, A-Z ● Number: 0-9 ● Korean alphabet

[Relevant SFR: FAU_SAR.1, FAU_SAR.3]

[Table 24] Audit data search conditions

6.1.1.3. Audit data protection

If the audit data take up more than 80% of the hard disk capacity, the TOE sends an email alert to the administrator. If more than 90% of the hard disk space is occupied, leading to a failure in adding audit logs, the TOE deletes the oldest audit records (delete audit records from the oldest three days first), and informs the administrator via email to protect the audit data.

[Relevant SFR: FAU_ARP.1, FAU_SAA.1, FAU_STG.3, FAU_STG.4]

6.1.2. Cryptographic support

Cryptographic support performs the following functions by using MagicCrypto V2.2.0.

- Encryption key generation
- Encryption key distribution
- Encryption task, and key destruction
- Random bit generation
- One-way encryption

Category	Low-level Category	Description
Validated cryptographic module	**Cryptographic module name**	MagicCrypto V2.2.0
	Validation No.	CM-162-2025.3
	Developer	Dream Security Co., Ltd.
	Module type	S/W (library)
	Validation date	March 3, 2020
	Expiration Date	March 3, 2025

[Table 25] Information on validated cryptographic module

6.1.2.1. Encryption key generation

The TOE generates 256-bit symmetric keys by using MagicCrypto V2.2.0 for Electronic Document Encryption, protection of the TSF data and protection of the data communicated between TOE components.

Category	Cryptographic Key Generation Algorithm	Key Size	List of Standards
Document HEADER DEK	HASH_DRBG	256 bits	ISO/IEC 18031
Document BODY DEK	HASH_DRBG	256 bits	ISO/IEC 18031
TSF data DEK	HASH_DRBG	256 bits	ISO/IEC 18031

Packet	ECDH(EC_P256_r1)	256 bits	ISO/IEC 11770-3
KEK	PBKDF2 (SALT value is randomly generated with the iteration count of 1024)	256 bits	TTAS.KO-12.0334
Mutual authentication DEK	HASH_DRBG	256 bits	ISO/IEC 18031

[Relevant SFR: FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1]

[Table 26] Cryptographic key generation algorithm

6.1.2.2. Encryption key distribution

The TOE agent performs mutual authentication with the server, and safely distributes the generated cryptographic keys through the cryptographic algorithm for distribution.

Category	Cryptographic Key Distribution Algorithm	Key Size	List of Standards
Packet	ECDH	256 bits	ISO/IEC 11770-3
Document HEADER DEK	ARIA-CBC	256 bits	KS X 1213-1

[Relevant SFR: FCS_CKM.1(2), FCS_CKM.2, FIA_IMA.1]

[Table 27] Cryptographic key distribution algorithm

6.1.2.3. Encryption and key destruction

The TOE performs cryptographic operations, such as Electronic Document Encryption, TSF data, transmitted data and encryption key encryption, and module self-tests, by using the following cryptographic algorithms, and destroys security parameters by overwriting them with “0” after the operation is completed.

Category	Algorithm	Key Size	List of Standards	Key Destruction	Timing of Destruction
Document HEADER encryption	ARIA-CTR	256 bits	KS X 1213-1	Overwrite with '0'	Immediately after use
Document BODY encryption	ARIA-CTR	256 bits	KS X 1213-1	Overwrite with '0'	Immediately after use
Packet	ARIA-CBC	256 bits	KS X 1213-1	Overwrite with '0'	Immediately after use
TSF encryption	ARIA-CBC	256 bits	KS X 1213-1	Overwrite with '0'	Immediately

					after use
Mutual authentication	ARIA-CBC	256 bits	KS X 1213-1	Overwrite with '0'	Immediately after use
Key exchange	ECDH	256 bits	ISO/IEC 11770-3	Overwrite with '0'	Immediately after use

[Relevant SFR: FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2)]

[Table 28] Encryption key task and key destruction algorithm

6.1.2.4. Random bit generation

The TOE performs random bit generation by using MagicCrypto V2.2.0.

Random Bit Generation Algorithm	Random Number Size	List of Standards
HASH_DRBG	256 bits	ISO/IEC 18031

[Relevant SFR: FCS_RBG.1]

[Table 29] Random bit generation algorithm

6.1.2.5. One-way encryption

The TOE performs one-way encryption by using MagicCrypto V2.2.0.

Cryptographic Algorithm	List of Standards
HASH(SHA-256)	SO/IEC 10118-3

[Relevant SFR: FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1]

[Table 30] One-way encryption algorithm

6.1.3. User data protection

User data protection performs the following functions.

- Electronic Document Decryption access control
- Agent deletion control

6.1.3.1. Electronic Document Decryption access control

The authorized administrator controls a document user’s activity for document decryption via the web browser according to the security policy set in HDS SERVER. Reading, writing, encryption and decryption of a document to be protected (PDF, XLS, XLSX, XLSM, XLSB, XLTX, XLTM, DOC, DOCX, DOTM, DOTX, PPT, PPTX, PPTM, PPS, PPSM, PPSX, POT, POTX, POTM, HWP, HWT) are performed, based on the document user ID.

[Relevant SFR: FDP_ACC.1(1), FDP_ACF.1(1)]

6.1.4. Identification and authentication

Identification and authentication perform the following functions.

- Administrator identification and authentication
- User identification and authentication
- Mutual authentication between HDS SERVER and HDS AGENT

6.1.4.1. Administrator identification and authentication

Upon the installation of the TOE, it is mandatory to create a new administrator ID, and the administrator authentication data are generated by using the ID. The password is the same as ID when the administrator accesses for the first time, which must be changed according to the combination rule. Authentication data and SALT (HASH_DRBG) are stored in the DBMS. No actions are allowed before the administrator is identified and authenticated. The reuse of data is prevented by self-encoding a session ID generated by a random bit generator and time stamp. The password entered during an attempt to access the web browser is masked with "•" so that it is not disclosed on the screen. The authentication succeeds if the ID and password that have been entered are confirmed in the DBMS. In case of authentication failure, a reason for the failure is not provided, and only an error message "the authentication information is invalid" is displayed. If the administrator's authentication attempts fail five times, an email is sent to the authorized administrator and the authentication is inactivated for 10 minutes.

[Password combination rule]

- English alphabet (differentiating between uppercase and lowercase): a-z, A-Z
- Number: 0-9
- Special character: !, @, #, $, %, ^, &, +, =, -
- Combination of English alphabet, number and special character
- At least 9 up to 20 digits

[Relevant SFR: FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1, FMT_PWD.1]

6.1.4.2. User identification and authentication

When the TOE is executed for the first time after a user account is created, the password is the same as the ID and must be changed according to the combination rule. The ID and the password of the document user (SHA-256) are encrypted and transmitted to the server, and then the user is identified and authenticated. The document user is allowed to enter the encryption key (KEK) password and check the version information before that user is identified and authenticated. The document user's identification and information additionally include the time stamp and hash values (SHA-256) to prevent the reuse. The password entered upon the access is masked with "•" so that it is not disclosed on the screen. In case of authentication failure, a reason for the failure is not provided, and only an error message "the authentication information is invalid" is displayed. If the user's authentication attempts fail five times, an email is sent to the authorized administrator and the authentication is inactivated for 10 minutes.

[Password combination rule]

- English alphabet (differentiating between uppercase and lowercase): a-z, A-Z
- Number: 0-9
- Special character: !, @, #, $, %, ^, &, +, =, -
- Combination of English alphabet, number and special character
- At least 9 up to 20 digits

[Relevant SFR: FIA_AFL.1, FIA_IMA.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1]

6.1.4.3. Mutual authentication between HDS SERVER and HDS AGENT

For safe mutual authentication between HDS components, an encryption key is generated through key exchange with ECDH. The generated encryption key is used for secure communication of all packets.

HDS AGENT, after checking whether or not the mutual authentication key is registered, sends Machine ID to HDS SERVER which, then, proceeds with the registration of the mutual authentication key.

HDS SERVER generates mutual authentication ID, KEY and IV through HASH-DRBG, and then encrypts them, including Machine ID, by using DEK and stores them in the DBMS. Then, it sends mutual authentication ID, KEY and IV decrypted with DEK to HDS AGENT, encrypts them with DEK and stores them in the HDS AGENT registry.

If it fails to register mutual authentication ID, KEY and IV in the HDS SERVER, the mutual authentication fails and is finished.

In case the mutual authentication key is registered, HDS AGENT decrypts mutual authentication ID, KEY and IV with DEK, and sends Machine ID, mutual authentication ID and the client nonce generated through HASH-DRBG to HDS SERVER.

HDS SERVER retrieves KEY and IV with Machine ID and mutual authentication ID, decrypts them with DEK, encrypts the client nonce it received through ARIA-CBC, and sends Machine ID, mutual authentication ID, encrypted client nonce, server nonce and server IP to HDS AGENT.

If the data are successfully verified (decrypting the received client nonce, and comparing Machine ID, mutual authentication ID and server IP sent to the server), HDS AGENT proceeds with the second mutual authentication. If the data verification fails, the mutual authentication fails and is finished.

In the second mutual authentication, HDS AGENT encrypts the server nonce through ARIA-CBC, and sends Machine ID, mutual authentication ID, server IP and the encrypted server nonce to HDS SERVER.

If the data are successfully verified (decrypting the server nonce, and comparing server IP, Machine ID and mutual authentication ID sent to the server), the mutual authentication between HDS SERVER and HDS AGENT is completed. If the data verification fails, the mutual authentication fails and is finished.

After the mutual authentication is completed, the encryption key is destroyed, and secure communication of packets is performed by generating another encryption key through ECDH.

6.1.5. Security management

Security management performs the following functions.

- Basic information management
- User management
- Log management
- ID and password management

6.1.5.1. Basic information management

The TOE restricts the role of performing basic configuration management to the administrator, and has the administrator of only one level, that is, the top administrator. The authorized administrator performs the basic configuration of administrator password change, administrator IP registration and email settings through the web browser.

Up to two administrator IPs can be registered in order to fix the location of the administrator, and the maximum number of concurrent sessions is one. In the email settings, the mail server information used to send a warning email to the administrator is set.

6.1.5.2. User management

The TOE allows the authorized administrator to add/delete user accounts, initialize user passwords, and manage decryption right and agent deletion right through the web browser. In user account addition, a document user's ID is registered, the user's name is modified, and user ID is deleted.

In the user password initialization, a document use's password is set to the initial password. In the decryption right, a right to decrypt an encrypted document is assigned to a document user. The agent deletion right means the assignment of a right to delete an agent through HDSUninstall.exe file in the installation folder.

[Relevant SFR: FMT_MOF.1, FMT_MSA.1]

6.1.5.3. Log management

The TOE provides agent logs, server logs, mail sending log status and management log status. The authorized administrator performs log management through the web browser. All logs are sorted in descending order based on the server time.

Classification of Audit Log Status	Query Category	Query Condition
Agent log status	Search menu	Log date separation, user ID, log content
	Query item	Server time, PC time, user ID, client IP, client MAC, log content, log-generating process
Server log status	Search menu	Log date, log content, log-generating process
	Query item	Server time, log-generating process, process ID, 서 server IP, server PORT, client IP:PORT, log content
Mail sending log status	Search menu	Server time, mail title, message body, sender, sending status
	Query item	Server time, mail title, message body, sender, sending status
Management log status	Search menu	Server time, menu ID, log content
	Query item	Server time, menu ID, event, client IP, log content

[Relevant SFR: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]

[Table 31] Audit log management

6.1.5.4. ID and password management

Upon the installation of the TOE, the administrator ID must be set, and the authorized administrator, when accessing the web browser for the first time, is required to change the password initially set to match the ID, in order to gain access. A document user must change his/her password initially set to match the ID to gain access when accessing the agent for the first time.

[Relevant SFR: FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FMT_PWD.1]

6.1.6. Protection of the TSF

Protection of the TSF performs the following functions.

- Protection of stored TSF data
- Protection of transmitted TSF data
- TSF self tests

6.1.6.1. Protection of stored TSF data

Stored TSF data are protected by using the confidentiality (ARIA-CBC, 256 bit) of the validated cryptographic module (MagicCrypto V2.2.0) and one-way (SHA-256) algorithm for storing passwords.

DEK for TSF data encryption is encrypted with KEK and stored. In this case, KEK is generated, using the password-based key derivation method, and is not stored. Document HEADER DEK is encrypted with DEK for TSF data encryption, and stored.

TOE Component	TSF Data	Protection Algorithm	Storage Location
HDS SERVER	DBMS password	ARIA-CBC, 256bit	Registry
	Administrator password	SHA-256	DB
	User password	SHA-256	DB
	Document HEADER DEK	ARIA-CBC, 256 bit	DB
	DEK for TSF data encryption	ARIA-CBC, 256 bit	Registry
HDS AGENT	Mutual authentication key	ARIA-CBC, 256 bit	Registry
	Server IP	ARIA-CBC, 256 bit	Registry
	Document HEADER DEK	Self-encoding	Memory
	Document BODY DEK	ARIA-CTR, 256 bit	File
	DEK for TSF data encryption	ARIA-CBC, 256 bit	Registry

[Relevant SFR: FPT_PST.1]

[Table 32] Protection algorithm for stored TSF data

6.1.6.2. Protection of transmitted TSF data

The following cryptographic algorithms are used for the protection of transmitted TSF data of the TOE.

TOE Component	TSF Data	Protection Algorithm

HDS management web browser <-> HDS SERVER	Transmitted data	TLS 1.2 (cipher suite)
HDS SERVER <-> HDS AGENT	Transmitted data	ARIA-CBC, 256bit, SHA-256

[Table 33] Protection algorithm for transmitted TSF data

6.1.6.3. Agent protection

HDS AGENT protects specific processes from unauthorized termination, and protects executable files subject to the integrity monitoring from unauthorized deletion in the driver.

It prevents unauthorized termination of a process and deletion of an executable file with API hooking, and hides the target process and file.

If HDS AGENT is shut down abnormally, an email is sent to the authorized administrator.

Integrity Monitoring Taret	OS Classification	Item	Description	Prevention of Process Termination	Process Hiding	Prevention of File Deletion
HDS AGENT executable file	32bit, 64bit	HDS.exe	Main executable program	○		○
	32bit, 64bit	HDSAutoEncrypt.exe	Initial encryption program	○	○	○
	32bit, 64bit	HDSDecrypt.exe	Decryption program	○	○	○
	32bit, 64bit	HDSDrvInstall.exe	Driver installation program			○
	32bit, 64bit	HDSEncrypt.exe	Event encryption program	○	○	○
	32bit, 64bit	HDSH.dll	Hooking library			○
	64bit	HDSH32.dll	Hooking library			○
	32bit, 64bit	HDSHook.exe	Message hooking program	○	○	○
	64bit	HDSHook32.exe	Message hooking program	○	○	○
	64bit	HDSLauncher.exe	HDS executable program	○		○
	32bit, 64bit	HDSMonitor.exe	Process monitoring program	○	○	○
	32bit, 64bit	HDSOverlayIcon.dll	Overlay icon library			○
	64bit	HDSOverlayIcon32.dll	Overlay icon library			○

	64bit	HDSProtect.exe	Protection program	○	○	○
	32bit, 64bit	HDSUninstall.exe	Uninstallation program	○	○	○
	32bit	HiDrive.dll	Encryption/decryption engine library			○
	64bit	HiDrive_x64.sys	Encryption/decryption engine driver			○
	32bit, 64bit	HiDriveSVC.exe	Encryption/decryption engine service	○	○	○
	32bit, 64bit	InstHelp.dll	Installation Util			○
	32bit, 64bit	MagicCrypto32V22.dll	KCMVP library			○
	64bit	MagicCryptoV22.dll	KCMVP library			○
	32bit, 64bit	ZsFP.sys	Protection driver			○

[Table 34] List of files to be protected

6.1.6.4 TSF self tests

HDS AGENT and HDS SERVER provides the integrity verification by using SHA-256 algorithm. If an integrity error is found, a warning email is sent to the authorized administrator.

HDS AGENT and HDS SERVER performs self-diagnosis provided by MagicCrypto V2.2.0 when starting the TOE. If it fails, a warning email is sent to the authorized administrator.

TOE Component	Test Targets		Test Interval
HDS AGENT, HDS SERVER	Self-diagnosis	KCMVP	Once every hour upon startup
	Self test	Process monitoring	
		Encryption	
	Integrity monitoring	Executable file	
		Registry	

[Table 35] Self test targets

Integrity Monitoring Target		OS Classification	Item	Description
HDS AGENT	Executable file	32bit, 64bit	HDS.exe	Main executable program
		32bit, 64bit	HDSAutoEncrypt.exe	Initial encryption program
		32bit, 64bit	HDSDecrypt.exe	Decryption program
		32bit, 64bit	HDSDrvInstall.exe	Driver installation program

		32bit, 64bit	HDSEncrypt.exe	Event encryption program
		32bit, 64bit	HDSH.dll	Hooking library
		64bit	HDSH32.dll	Hooking library
		32bit, 64bit	HDSHook.exe	Message hooking program
		64bit	HDSHook32.exe	Message hooking program
		64bit	HDSLauncher.exe	HDS executable program
		32bit, 64bit	HDSMonitor.exe	Process monitoring program
		32bit, 64bit	HDSOverlayIcon.dll	Overlay icon library
		64bit	HDSOverlayIcon32.dll	Overlay icon library
		64bit	HDSProtect.exe	Protection program
		32bit, 64bit	HDSUninstall.exe	Uninstallation program
		32bit	HiDrive.dll	Encryption/decryption engine library
		64bit	HiDrive_x64.sys	Encryption/decryption engine driver
		32bit, 64bit	HiDriveSVC.exe	Encryption/decryption engine service
		32bit, 64bit	InstHelp.dll	Installation Util
		32bit, 64bit	MagicCrypto32V22.dll	KCMVP library
		64bit	MagicCryptoV22.dll	KCMVP library
		32bit, 64bit	ZsFP.sys	Protection driver
	Registry	32bit, 64bit	Auth	KEK normal operation check value
		32bit, 64bit	DEK	DEK
		32bit, 64bit	DEK_IV	DEK IV
		32bit, 64bit	IV	KEK IV
		32bit, 64bit	MutualID	Mutual authentication ID
		32bit, 64bit	MutualIV	Mutual authentication IV
		32bit, 64bit	MutualKey	Mutual authentication KEY
		32bit, 64bit	SALT	KEK SALT
		32bit, 64bit	ServerIP	Server IP

HDS SERVER	Executable file	64bit	HDSCrypt.dll	C# KCMVP wrapper DLL
		64bit	HDSMailSender.exe	Mail sending program
		64bit	HDSSvr.exe	Server program
		64bit	HDSSvrMgr.exe	Server management program
		64bit	HDSSvrMonitor.exe	Server monitoring program
		64bit	MagicCryptoV22.dll	KCMVP library
		64bit	ZsFramework.Data.dll	Mail sending library
	Registry	64bit	Auth	KEK normal operation check value
		64bit	DBPW	DB password
		64bit	DEK	DEK
		64bit	DEK_IV	DEK IV
		64bit	IV	KEK IV
		64bit	SALT	KEK SALT

[Table 36] Items subject to integrity monitoring

6.1.7. TOE access

TOE access performs the following function.

- Session management

6.1.7.1. Session management

The IP address that can access the web browser must be allocated upon the initial access. The maximum number of IPs that can access is limited to two. When the administrator logs in, access is allowed only from the allowed IP addresses. In addition, the number of maximum concurrent sessions is restricted to one for administrator management access sessions, and the previous access is terminated if concurrent access is made. The administrator's interactive session is terminated after the period of the administrator inactivity (10 minutes).

For document users, the number of maximum concurrent sessions is limited to one, and the previous access is terminated if concurrent access is made.

[Relevant SFR: FTA_MCS.2, FTA_SSL.5, FTA_TSE.1]

7. References

1) Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5

   - Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001)
   - Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002)
   - Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003)

2) Korean National Protection Profile for Electronic Document Encryption V1.1 (2019-12-11)