KECS-CR-23-01

FED 5 SP1

Certification Report

Certification No.: KECS-CISS-1207-2023

2023. 1. 2.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.1.2.	-	Certification report for FED 5 SP1 - First documentation

This document is the certification report for FED 5 SP1 of Fasoo Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the FED 5 SP1 developed by Fasoo Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (“TOE” hereinafter) is used to enable the user to access various business systems and use the service through a single user login without additional login action. Also, the TOE shall provide a variety of security features: security audit, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on December 05, 2022.

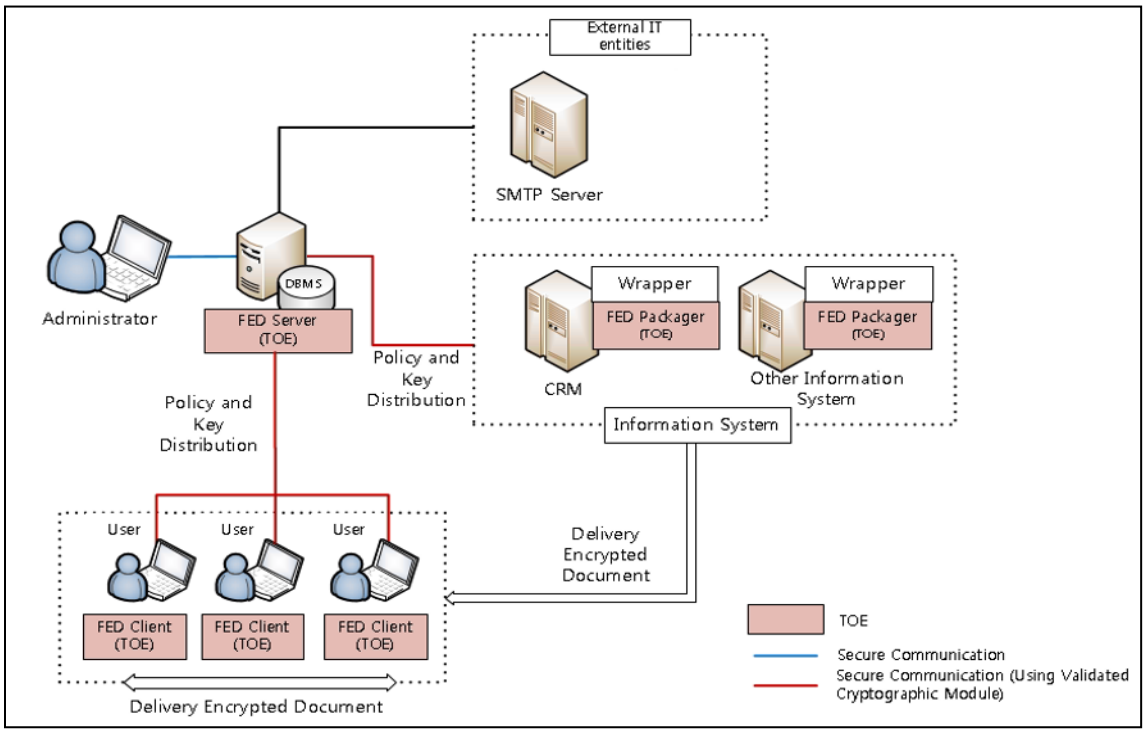
The ST claims conformance to the Korean National Protection Profile for Electronic Document Encryption V1.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the PP, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

'FED 5 SP1' (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 or decrypt documents to be protected by specifying individual documents, document types, document paths, etc., and the TOE encrypt the entire contents of the documents.

The TOE is “Electronic Document Encryption” that prevents information leakage by encrypting/decrypting important documents within the organization and is provided as software. The TOE supports both of “user device encryption” type and “information system encryption” type.

[Figure 1] shows the operational environment of the TOE. The TOE is composed of the FED server which manages the security policy and cryptographic key, the FED client that performs Electronic Document encryption/decryption installed in the user PC, and the FED packager that performs Electronic Document encryption installed in the information system in the form of API module. A wrapper is used for compatibility between the FED packager and various information systems, but it is excluded from the scope of the TOE.



[Figure 1] Operational Environment of the TOE

The administrator sets the policy for each document user or information system through the FED server, which distributes the policy and cryptographic key configured by the administrator to the FED client and FED packager. The FED client performs Electronic Document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted/decrypted document is stored in the user PC as a file. Upon the request from the information system, the FED packager performs Electronic Document encryption/decryption using the validated cryptographic module according to the distributed policy, and the encrypted document is stored in the user device and information system.

The validated cryptographic module, ‘Fasoo Crypto Framework V2.4’, is used for the cryptographic operation of the major security features of the TOE. For the

communication between the TOE component and the administrator (e.g., when the administrator accesses the FED server using the web browser and web server to configure policies), TLS 1.2 is used.

As other external entities necessary for the operation of the TOE, there are the email server to send alerts by email to the authorized administrator.

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

Component		Requirement
FED Server	HW	CPU: Intel Xeon 2 GHz or higher Memory: 8 GB or higher HDD: 500 GB or higher for the installation of TOE NIC: 100/1000 Mbps 1Port or higher
	SW	Jetty 10 OpenJDK 17 MariaDB 10.6
	OS	Linux Ubuntu 20.04 [Kernel 5.4] (64bit)
FED Packager	HW	CPU: Intel Xeon 2 GHz or higher Memory: 4 GB or higher HDD: 1 GB or higher for the installation of TOE NIC: 100/1000 Mbps 1Port or higher
	SW	OpenJDK 17
	OS	Linux Ubuntu 20.04 [Kernel 5.4] (64bit)
FED Client	HW	CPU: Intel Core2 Duo 2 GHz or higher Memory: 4 GB or higher HDD: 200 GB or higher for the installation of TOE NIC: 100/1000 Mbps 1Port or higher
	OS	Windows 10 Pro (32, 64)
	SW	Visual C++ 2008 redistributable 9.0.30729.17

[Table 1] TOE Hardware and Software specifications

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

Component		Requirement
S/W	Web Browser	Chrome 98

[Table 2] Administrator PC Requirements

Validated cryptographic modules included the TOE are as follows.

Classification	Description
Cryptographic Module	Fasoo Crypto Framework V2.4
Validation No.	CM-193-2026.11
Developer	Fasoo Co.,Ltd.
Validation Date	2021.11.18.

[Table 3] Validated Cryptographic Module

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

TOE	FED 5 SP1
Version	5.4.0.2
TOE Components	- FED 5 Server 1.4.0.2 - FED 5 Client 1.4.0.2 - FED 5 Packager 1.4.0.2
Manuals	- FED 5 SP1_AGD_OPE(admin)_1.2 - FED 5 SP1_AGD_OPE(user)_1.2 - FED 5 SP1_AGD_OPE(developer)_1.2 - FED 5 SP1_AGD_PRE_1.2

[Table 4] TOE identification

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	FED 5 SP1
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Electronic Document Encryption V1.1
Developer	Fasoo Co., Ltd.
Sponsor	Fasoo Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	December 05, 2022

[Table 5] Additional identification information

3. Security Policy

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

- Security Audit

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Prtoection of the TSF
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [4]

4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 3])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the FED Server, FED Client, FED Packager, and guidance documents. Verified Cryptographic Module(Fasoo Crypto Framework V2.4) is embedded in the TOE components. Hardware, operating system, DBMS, WAS, JDK, Wrapper which are operating environments of the TOE are excluded from the physical scope of the TOE.

Category	Identification	Type
TOE component	FED 5 Server 1.4.0.2 (FED5_Server_1.4.0.2.tar)	Software (Distributed as a CD)
	FED 5 Client 1.4.0.2 (FED5_Client_1.4.0.2.exe, FED5_Client_1.4.0.2_x64.exe)	
	FED 5 Packager 1.4.0.2 (FED5_Packager_1.4.0.2.tar)	
guidance	FED 5 SP1_AGD_OPE(admin)_1.2	PDF

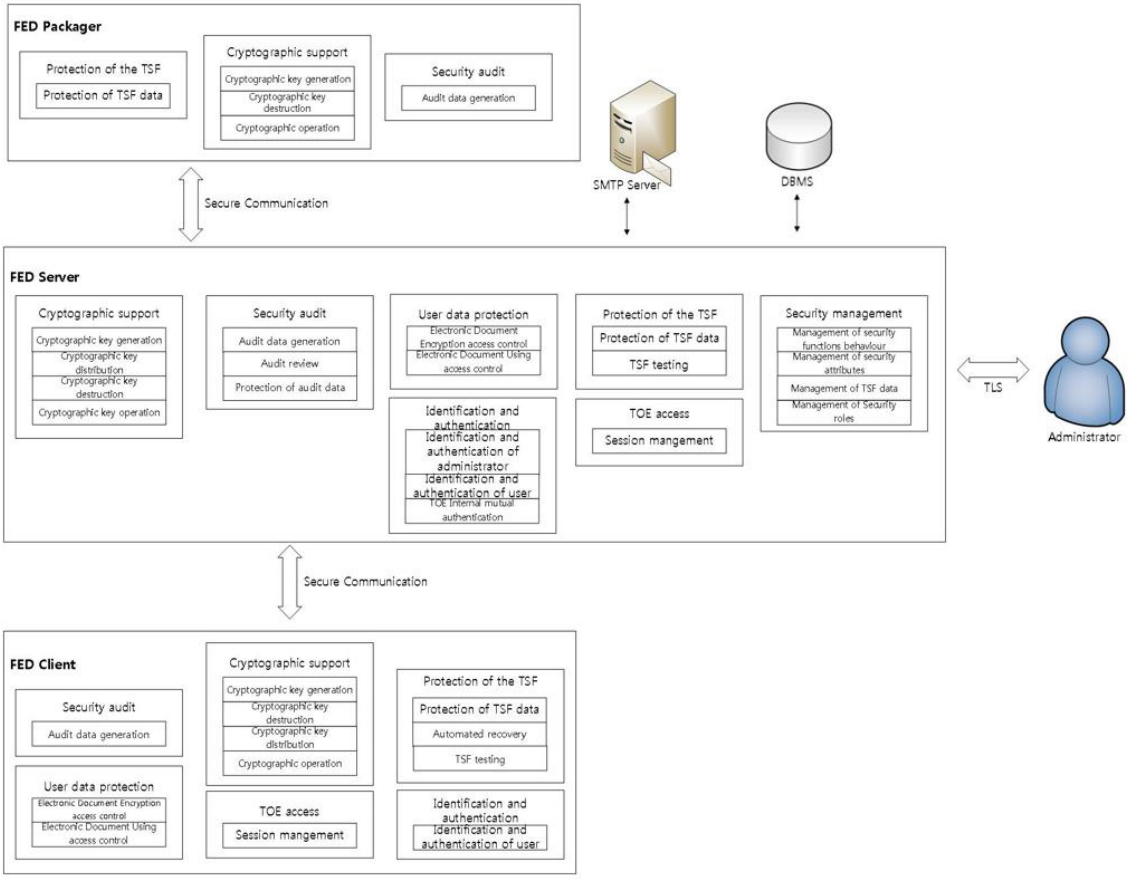
documents	(FED 5 SP1_AGD_OPE(admin)_1.2.pdf)	(Distributed as a CD)
	FED 5 SP1_AGD_OPE(user)_1.2 (FED 5 SP1_AGD_OPE(user)_1.2.pdf)	
	FED 5 SP1_AGD_OPE(developer)_1.2 (FED 5 SP1_AGD_OPE(developer)_1.2.pdf)	
	FED 5 SP1_AGD_PRE_1.2 (FED 5 SP1_AGD_PRE_1.2.pdf)	

[Table 6] Physical scope of TOE

The ‘FED 5 Packager’ is installed as an API module in the information system server and provides the document encryption function in the information system through the wrapper, and does not provide the security function by itself.

2. Logical Scope of TOE

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



[Figure 2] TOE Logical scope

▣ Security Audit

The TOE creates and records audit data of the events relating to the start/end of the audit functions and security functions in the DBMS. Among the audit data, the document usage log can selectively generate audit data by event type. The authorized administrator can view the stored audit records and search for the records by various criteria such as ID, date and event type.

If any potential security violation such as integrity violation, self-test failure, and audit trail amount exceed is detected, the TOE sends an email to the administrator to inform the administrator of the potential violation.

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

▣ Cryptographic support

The TOE performs cryptographic operation and cryptographic key management such as generation, distribution and destruction through Fasoo Crypto Framework V2.4. HASH_DRBG is used to generate document encryption key (DEK) and RSAES-OAEP algorithm is used to generate the key pair based on the public key. The key encryption key

(KEK) is also generated using HASH_DRBG in the same way as the document encryption key (DEK). For secure key distribution among components, RSAES-OAEP is used.

The TOE performs operation in the ARIA-CTR mode for encryption/decryption of document, and in the ARIA-CBC or RSA-OAEP mode for encryption/decryption of encryption key. For generating the message authentication code in the header of the secured document, HMAC_SHA-256 is used, and for the signature of transmission data and policy file, RSASSA-PSS is used. The authentication data of the administrator and document user are saved (one-way encryption) using SHA-256. For destruction of the encryption key after use, it is overwritten with '0' three times in memory.

▣ Identification and authentication

The TOE protects user data.

- The TOE creates a secured document by encrypting a plain document and protects the secured document by controlling access to the secured document according to the policy by user set by the administrator. The policy is set differently depending on the user ID, group, role, job title, group head, document owner, or document class. Permissions to access the secured documents are view, edit, print, screen capture, change permission, extract, decrypt, change class, macro, allowed time period to view, revoke, etc. and depending on the permissions granted, access to the secured document is controlled.
- The secured document is encrypted through the cryptographic support function so that only authorized users can use the secured document. Even if the secured document is sent through a distribution path, unauthorized users cannot access the document.

The FED Client of the TOE encrypts a document as a secured document when it is saved or downloaded in a user PC and protects the secured document. Also, the FED Packager of the TOE encrypts a document as a secured document upon a request from the information system and protects the document in transit.

The file formats that the FED client of the TOE supports encryption are as follows.

Application	File format (extension)
Hancom Office	hwp
MS Office Word	doc, docx
MS Office Powerpoint	ppt, pptx
MS Office Excel	xls, xlsx
Adobe Reader	pdf
Autodesk AutoCAD	dwg
NOTEPAD	txt
MS Paint	jpg, png
Wordpad	rtf

▣ Identification and authentication

The TOE provides identification and authentication process based on ID/PW for the

administrators and document users. Only the authorized administrators can manage the security functions through the web browser. The identification and authentication process of a user are performed through the FED Client, and when the user login to the FED Client, the FED Server and FED Client go through a mutual authentication process.

When an administrator or user enters password to login to the FED Server or FED Client, it is masked to prevent disclosure and in case of authentication failure, the reason is not provided. In addition, the password must be at least 12 characters in length, with at least one alphabetic character, numeric character, and special character. If the number of authentication failures by the administrator or user exceeds the threshold, the account will be locked.

The reuse of the authentication information used when an administrator login to the FED Server is prevented. Also, The reuse of the authentication information used when a user login to the FED Client is prevented.

▣ Security Management

Only the authorized administrator who can access the management interface provided by TOE can performs security management. In case of initial access to the interface, the administrator ID/PW should be registered first. The authorized administrator can manage security function, security attribute and TSF data, and provide security functions using the general setting, document class and security policy menus provided by TOE's management interface. In addition to this, the administrator can add more document users and create or modify user IDs and passwords. Administrators can be added more if needed, but the newly authorized administrators can access only the menus allowed by the initial administrator.

▣ Protection of the TSF

The TOE communicates securely to protect transmission data between components and secures confidentiality and integrity. The TOE also protects TSF data against unauthorized exposure and modification through encryption, digital signature and proprietary encoding.
The TOE periodically performs self-tests and integrity checks when operating, and prevents process termination and file deletion by conducting mutual monitoring between TOE related processes so that the running agent is not terminated. In case of integrity corruption, the TOE provides automated recovery function.

▣ 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 or document user. If logging in with an account, after logging in with the same account from one device, from another device is tried, the new connection attempt is blocked, and administrators can access only from the devices whose IP is designated as accessible.

6. Documentation

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

Identification	Date
FED 5 SP1_AGD_OPE(admin)_1.2 (FED 5 SP1_AGD_OPE(admin)_1.2.pdf)	November 01, 2022
FED 5 SP1_AGD_OPE(user)_1.2 (FED 5 SP1_AGD_OPE(user)_1.2.pdf)	November 01, 2022
FED 5 SP1_AGD_OPE(developer)_1.2 (FED 5 SP1_AGD_OPE(developer)_1.2.pdf)	November 01, 2022
FED 5 SP1_AGD_PRE_1.2 (FED 5 SP1_AGD_PRE_1.2.pdf)	November 01, 2022

[Table 7] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [5], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test case
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [4]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing

effort, the testing approach, configuration, depth, and results are summarized in the Penetration Testing Report [6].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: FED 5 SP1 (5.4.0.2)

- FED 5 Server 1.4.0.2
- FED 5 Client 1.4.0.2
- FED 5 Packager 1.4.0.2

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 6 were evaluated with the TOE

9. Results of the Evaluation

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

1. Security Target Evaluation (ASE)

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

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

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict **PASS** is assigned to the assurance class ASE.

2. Development Evaluation (ADV)

The functional specifications specify a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

The verdict **PASS** is assigned to the assurance class ADV.

3. Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict **PASS** is assigned to the assurance class AGD.

4. Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

The verdict **PASS** is assigned to the assurance class ALC.

5. Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation.

Therefore, the verdict PASS is assigned to ATE_IND.1. Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict **PASS** is assigned to the assurance class ATE.

6. Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing basic attack potential to violate the SFRs.

The verdict **PASS** is assigned to the assurance class AVA.

7. Evaluation Result Summary

Assurance	Assurance	Evaluator Action	Verdict

Class	Component	Elements	Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 8] Evaluation Result Summary

10. Recommendations

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

- The administrator should periodically check the free space of the audit data storage in preparation for the loss of the audit records, and perform backups of the audit records so that the audit records are not exhausted.
- The FED Server must be installed and operated in a physically secure environment that is accessible only to authorized administrators and should not allow remote administration from outside.
- If a cryptographic key is lost due to administrator's wrong cryptographic key management, document users may not be able to decrypt the encrypted file stored on the user's PC, so administrator has to be careful with cryptographic key management
- If the TOE is operated in a ‘Information system encryption’ method, it is recommended that those who are good at using the API.

11. Security Target

FED 5 SP1 Security Target 1.2 [4] is included in this report for reference.

12. Acronyms and Glossary

(1) Acronyms

CC Common Criteria

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

SAR Security Assurance Requirement

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

(2) Glossary

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

Authorized Document User

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

Authorized Administrator

Authorized user to securely operate and manage the TOE

Data Encryption Key (DEK)

Key that encrypts the data

Decryption

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

Encryption

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

External Entity

An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE.

Key Encryption Key (KEK)

Key that encrypts another cryptographic key.

Validated Cryptographic Module

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

Wrapper

Interface to connect the TOE with various types of information system

13. Bibliography

The evaluation facility has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April, 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April, 2017

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

[4] FED 5 SP1 Security Target 1.2, November 01, 2022

[5] FED 5 SP1 Independent Testing Report(ATE_IND.1) V1.00, December 02, 2022

[6] FED 5 SP1 Penetration Testing Report (AVA_VAN.1) V2.00, December 31, 2022