KECS-CR-18-09

FED 5

Certification Report

Certification No.: KECS-CISS-0858-2018

2018. 3. 27.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2018.3.27.	-	Certification report for FED 5 - First documentation

This document is the certification report for FED 5 of Fasoo.com Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Table of Contents

1. Executive Summary

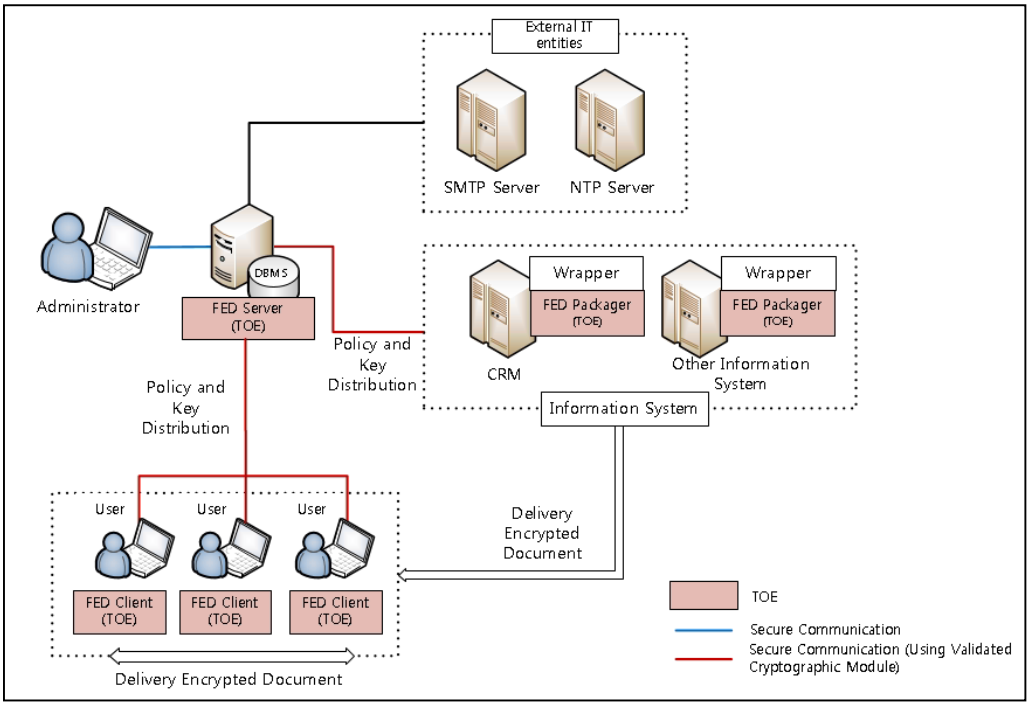
This report describes the certification result drawn by the certification body on the results of the FED 5 developed by Fasoo.com Inc. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation ("TOE" hereinafter) is Electronic Document Encryption designed to protect important documents managed by the organization based on the encryption/decryption. Also, the TOE 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 March 8th, 2018. This report grounds on the Evaluation Technical Report (ETR) [4] KOSYAS had submitted and the Security Target (ST) [5].

The ST claims strict conformance to the Korean National PP for Electronic Document Encryption V1.0 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. The ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the PP, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE. The TOE is composed of the FED Server which manages the security policy and cryptographic key, the FED Client installed in the user PC to encrypt/decrypt Electronic Document, and the FED Packager installed in the information system in the form of API module to encrypt Electronic Document. A wrapper is used for compatibility between the FED Packager and various information systems, but it is outside of the TOE scope.



[Figure 1] Operational Environment of the TOE

The minimum requirements for hardware, software to install and operate the TOE are shown in [Table 1] below:

Component		Requirement
FED Server	HW	CPU: Intel Xeon 2 GHz or higher Memory: 8 GB or higher HDD: 500 GB or higher NIC: 10/100/1000 Mbps 1 Port or higher
	SW	Jetty 9.4 JDK 1.8 Oracle 11g or Microsoft SQL Server 2012 SP3 or MySQL 5.7
		Windows Server 2008 R2 Standard Edition SP1(64) Windows Server 2008 R2 Enterprise Edition SP1(64) Windows Server 2012 Standard Edition (64) Windows Server 2012 [Datacenter Edition (64) CentOS 5.11 (Linux kernel 2.6.18(64))
FED Packager	HW	CPU: Intel Xeon 2 GHz or higher Memory: 4 GB or higher HDD: 500 GB or higher NIC: 10/100/1000 Mbps 1Port or higher
	SW	JDK 1.8
		Windows Server 2008 R2 Standard Edition SP1(64)

		Windows Server 2008 R2 Enterprise Edition SP1(64) Windows Server 2012 Standard Edition (64) Windows Server 2012 Datacenter Edition (64) CentOS 5.11 (Linux kernel 2.6.18(64))
FED Client	HW	CPU: Intel Core2 Duo 2 GHz or higher Memory: 2 GB or higher HDD: 500 GB or higher NIC: 10/100/1000 Mbps 1Port or higher
	SW	Windows 7 Professional SP1(32, 64) Windows 7 Enterprise SP1(32, 64) Windows 7 Ultimate SP1(32, 64) Windows 8.1 Pro (32, 64) Windows 10 Pro (32, 64) Windows 10 Enterprise (32, 64)
		MS Visual C++ 2008 redistributable 9.0.30729.17 MS Notepad, MS Wordpad, MS Paint Microsoft Office 2010, 2013, 2016 Hancom Office 2010 SE, 2014 VP, Neo Acrobat Reader 11, DC

[Table 1] TOE Hardware and Software specifications

Administrator accesses FED for security management using web browser in the Administrator PC, and the PC's minimum requirements are shown in [Table 2] below:

Component	Requirement
HW	CPU: Intel Core2 Duo 2GHz or higher Memory: 2 GB or higher HDD: 500 GB or higher NIC: 10/100/1000 Mbps 1Port or higher
SW	Windows 7 Professional SP1(64)
	Internet Explorer 11

[Table 2] Administrator PC Requirements.

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
Version	5.3.0.4
TOE Components	FED 5 Server 1.3.0.4 FED 5 Client 1.0.0.2 FED 5 Packager 1.2.0.1
Guidance Documents	FED 5 User Operation Guide (admin) 1.2 FED 5 User Operation Guide (user) 1.2 FED 5 User Operation Guide (developer) 1.1 FED 5 Preparative Procedure 1.3

[Table 3] 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 (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (September 12, 2017)
TOE	FED 5
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Protection Profile	Korean National Protection Profile for Electronic Document Encryption V1.0, KECS-PP-0821-2017
Developer	Fasoo.com Inc.
Sponsor	Fasoo.com Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	March 8th, 2018
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [5] by security requirements.

Thus the TOE provides following security features. For more details refer to the ST [5].

TSF	Explanation
Security Audit	The TOE generates audit records of security relevant events such as the start-up/shutdown of the audit functions, integrity violation, self-test failures, and stores them in the DBMS.
Cryptographic Support	The TOE performs cryptographic operation such as encryption/decryption, and cryptographic key management such as key generation/distribution/destruction using Fasoo Crypto Framework v2.3.1
User Data Protection	The TOE protects user's documents by making them Secured Documents by means of encrypting them and controlling access to them in accordance to the access control policy per user set by the administrator.
Identification and Authentication	The TOE identifies and authenticates the administrators and document users based on ID/PW.
Security Management	Only the authorized administrator who can access the management interface provided by TOE can performs security management of the TOE.
Protection of the TSF	The TOE provides secure communications amongst TOE components to protect confidentiality and integrity of the transmitted data between them. The TOE also protects TSF data against unauthorized exposure and modification through encryption, digital signature and proprietary encoding.
TOE Access	The TOE manages the authorized administrator's or document users' access to itself by terminating interactive sessions after defined time interval of their inactivity.

[Table 5] The TOE Security Functions

4. Assumptions and Clarification of Scope

There are no explicit Assumptions in the Security Problem Definition in the Low Assurance ST. The followings are procedural method supported from operational environment in order to provide the TOE security functionality accurately.

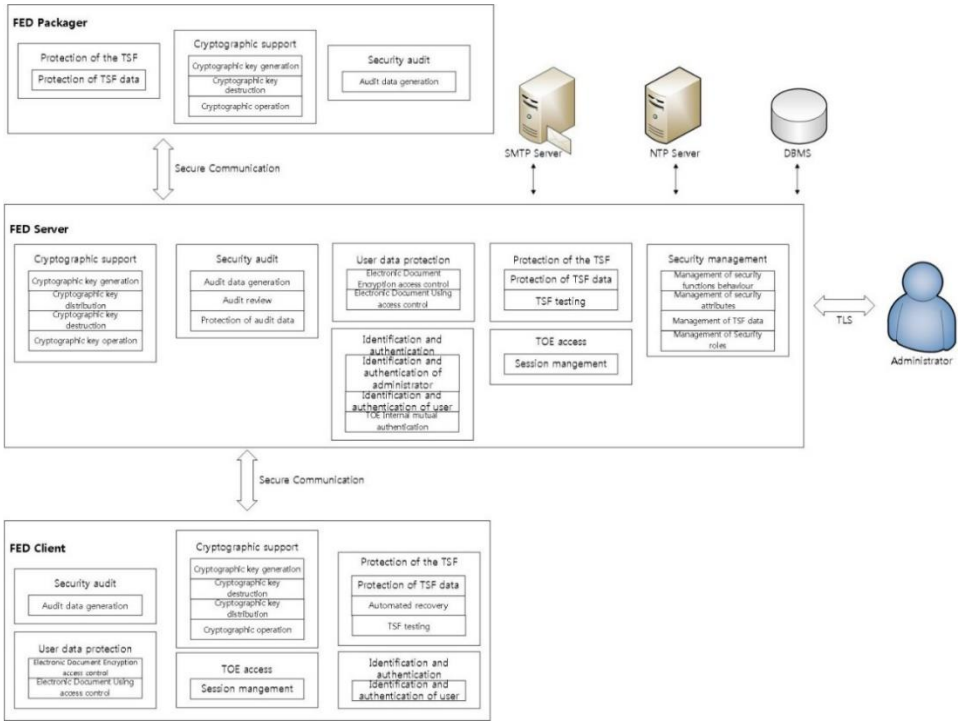
- The place where the management server among the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.
- The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill

the duties in accordance with administrator guidance.

- The authorized administrator shall periodically checks 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.
- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by removing all unnecessary services or means and performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.
- 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.
- The TOE shall accurately record the security related events using the reliable time stamp from the TOE operational environment.
- 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.

5. Architectural Information

The physical scope of the TOE consists of the FED Server, FED Client, FED Packager, and FED guidance documents. The following security functions are provided by the TOE Logical scope and boundary of TOE is shown in [Figure 2]



[Figure 2] TOE Logical scope and boundary

The FED Server is software that provides functions of sending the policy and FSD License defined in ST [3] to the FED Client for the security policy to be applied. The FED Client is software that controls the permissions to use secured documents according to the policy and FSD Licensed sent by the FED Server. The TOE also includes the Fasoo Crypto Framework v2.3.1 validated by KCMVP (Korea Cryptographic Module Validation Program) to perform Electronic Document encryption/decryption. The FED Packager is software that is integrated with the information system server and performs Electronic Document encryption for documents stored in the information system server.

6. Documentation

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

Identifier	Version	Date
FED 5 User Operation Guide (admin) 1.2	1.2	February 08, 2018
FED 5 User Operation Guide (user) 1.2	1.2	February 08, 2018
FED 5 User Operation Guide (developer) 1.1	1.1	February 08, 2018
FED 5 Preparative Procedure 1.3	1.3	February 08, 2018

[Table 6] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. Each test case includes the following information:

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

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [4].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: FED 5 (5.3.0.4)

- FED 5 Server 1.3.0.4
- FED 5 Client 1.0.0.2
- FED 5 Packager 1.2.0.1

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

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [4] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.
The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.
The Security 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.

9.2 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.
The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore the verdict PASS is assigned to ALC_CMS.1.
Also the evaluator confirmed that the correct version of the software is installed in

device.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

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

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

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

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

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

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

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

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By 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.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	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 7] 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 storage is 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 neglectful 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’ type defined in the PP [3], it is recommended that those who are good at using the API.

11. Security Target

FED 5 Security Target Lite V1.5 is included in this report for reference

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
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
Customer relationship management (CRM)	processes implemented to manage a company's interactions with customers and prospects
Data Encryption Key (DEK)	Key that encrypts the data
Decryption	The act that restoring the ciphertext into the plaintext using the decryption key
Encryption	The act that converting the plaintext into the ciphertext using the encryption key
External Entity	An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE
Key Encryption Key (KEK)	Key that encrypts another cryptographic key
Secured document	Documents encrypted by the FED Client or FED Packager and of which the usage is controlled by the FED Client

13. Bibliography

The certification body 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 V1.0, August 18, 2017

[4] FED 5 Evaluation Technical Report Lite V2.00, March 08, 2018

[5] FED 5 Security Target Lite 1.5, March 06, 2018