FED 5 SP1

Security Target 1.2

Revision history

Document subject	FED 5 SP1 Security Target

Configuration document no.	Version	Details	Created by	Date revised	Reviewed by
FED5 SP1_ST_1.0_en	1.0	Created	Choi Jae-ho	2022.06.28	Choi Woo-sun
FED5 SP1_ST_1.1_en	1.1	Updated	Choi Jae-ho	2022.08.16	Choi Woo-sun
FED5 SP1_ST_1.2_en	1.2	Updated	Choi Jae-ho	2022.11.01	Choi Woo-sun

- Table of Contents -

1. ST Introduction

1.1 ST reference

Item	Specification
Title	FED 5 SP1 Security Target
Version	1.2
Created by	Business Strategy team, Fasoo Co., Ltd.
Date created	2022.11.01
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation
Common Criteria version	CC v3.1 R5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Keywords	Document, Encryption

1.2 TOE reference

Item		Specification	
TOE		FED 5 SP1	
Version		5.4.0.2	
Components	FED Server (Management Server)	FED 5 Server 1.4.0.2	Software (CD)
	FED Client (Agent)	FED 5 Client 1.4.0.2	
	FED Packager (API module)	FED 5 Packager 1.4.0.2	
Guidance Documents		FED 5 SP1_AGD_OPE(admin)_1.2	PDF (CD)
		FED 5 SP1_AGD_OPE(user)_1.2	
		FED 5 SP1_AGD_OPE(developer)_1.2	
		FED 5 SP1_AGD_PRE_1.2	
Developer		Fasoo Co., Ltd.	

1.3 TOE overview

'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 primary security features provided by the TOE include the encryption/decryption of the document to be protected and cryptographic key management. For this encryption function, the TOE uses a validated cryptographic module, Fasoo Crypto Framework V2.4.

1.3.1 TOE type

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.

The FED Server, FED Client, and FED Packager 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 within 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, identification and authentication function (e.g., administrator and document user identity verification, authentication failure processing, and mutual authentication among TOE components), 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-test, and the TOE access function to manage the interacting session of the authorized administrator.

The TOE uses the data encryption key (hereinafter referred to as "DEK") and key encryption key (hereinafter referred to as "KEK") for the document encryption/decryption function. The main body of the protected document is encrypted with the DEK according to the policy set by the administrator, and the DEK is stored in the header of the security document. When the DEK is stored in the header, it is encrypted with the KEK.

The FED Server generates the KEK and distributes it to the mutually-authenticated FED Client. At this time, the cryptographic key is distributed safely through encrypted communication. The FED Client generates the DEK and encrypts the main body of the protected document and decrypts the encrypted main body using the DEK. The FED Client encrypts the DEK using the distributed KEK and stores the encrypted DEK in the header. The FED Packager generates the DEK upon the document encryption request from the information system and encrypts the main body of the protected document. The FED Packager encrypts the DEK using the server's public key issued by the FED Server and stores the encrypted DEK in the document header.

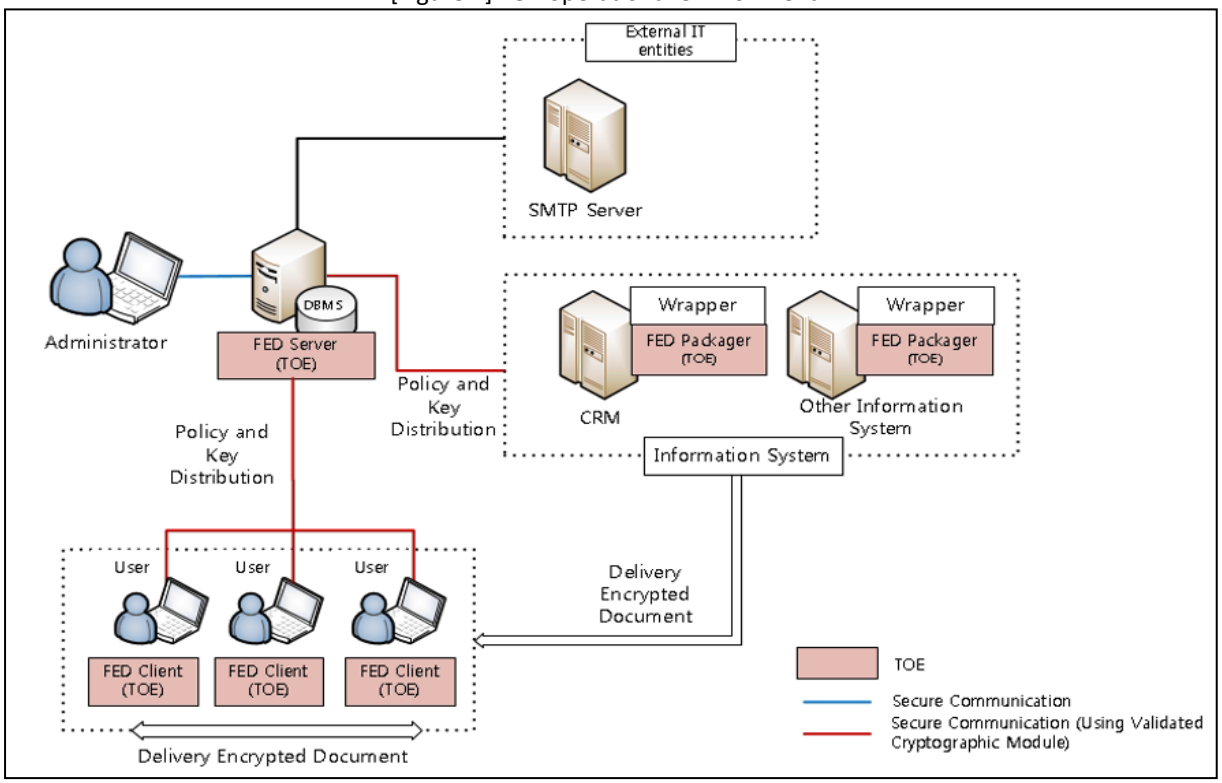
Each component of the TOE provides a cryptographic key destruction function if the cryptographic key is not used anymore.

The administrator can specify documents that shall be encrypted/decrypted through the FED Server, and assign the document access right to the document user. Only the authorized document user can encrypt/decrypt the document, as the FED Server distributes a cryptographic key to the document user according to policy configured.

1.3.3 Non-TOE and TOE operational environment

[Figure 1] shows the operational environment where the TOE is operated. The TOE is composed of the FED Server, FED Client, and FED Packager and should be installed and operated inside the internal network of the protected organization.

[Figure 1] TOE operational environment



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

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 TOP 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 is 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 as in the following.

[Table 1] TOE installation requirements

Component		Requirement
FED Server	HW	CPU : Intel Xeon 2GHz or higher Memory : 8GB or higher HDD : 500GB 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 2GHz or higher Memory : 4GB or higher HDD : 1GB 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 2GHz or higher Memory : 4GB or higher HDD : 200GB 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

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.

- SMTP server used to send security alerts by email to the administrator
- DBMS to store audit data of the FED Server
  - MariaDB 10.6
- Web application server used by the FED Server
  - Jetty 10
- Environment to operate the FED Server and FED Packager
  - OpenJDK 17
- For installation of the FED Client, required library must be installed for compatibility.
  - Visual C++ 2008 redistributable 9.0.30729.17
- Software that supports the document types that FED Client can encrypt
  - MS Notepad, MS Wordpad, MS Paint
  - Microsoft Office 2019
  - Hancom Office 2020
  - Acrobat Reader DC
  - Autodesk AutoCAD 2021

The requirements for the administrator PC for TOE security management are as in the following

Component	Requirement
SW	Chrome 98

1.4 TOE description

1.4.1. Physical scope of the TOE

The TOE is composed of the FED Server, FED Client, FED Packager, and FED guidance documents. The FED Server is software that provides functions of sending the policy and license 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 licensed sent by the FED Server. The FED Packager is software that is integrated

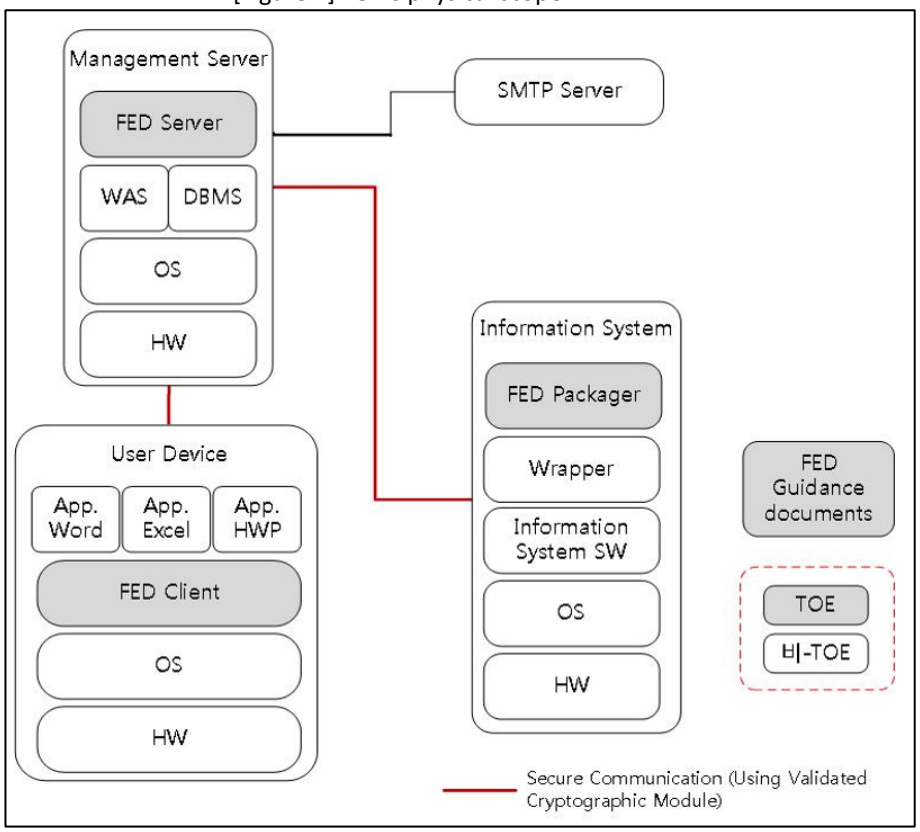
with the information system server and performs Electronic Document encryption for documents stored in the information system server. The components of the distributed TOE are as follows.

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)	
FED Guidance documents	FED 5 SP1_AGD_OPE(admin)_1.2 (FED 5 SP1_AGD_OPE(admin)_1.2.pdf)	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)	

※ The FED 5 Packager 1.4.0.2 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.

The hardware and operation system where the TOE is installed, the word processing program that a user uses, the wrapper for compatibility with information systems and external systems and other software necessary to operate the TOE are excluded from the scope of the TOE.

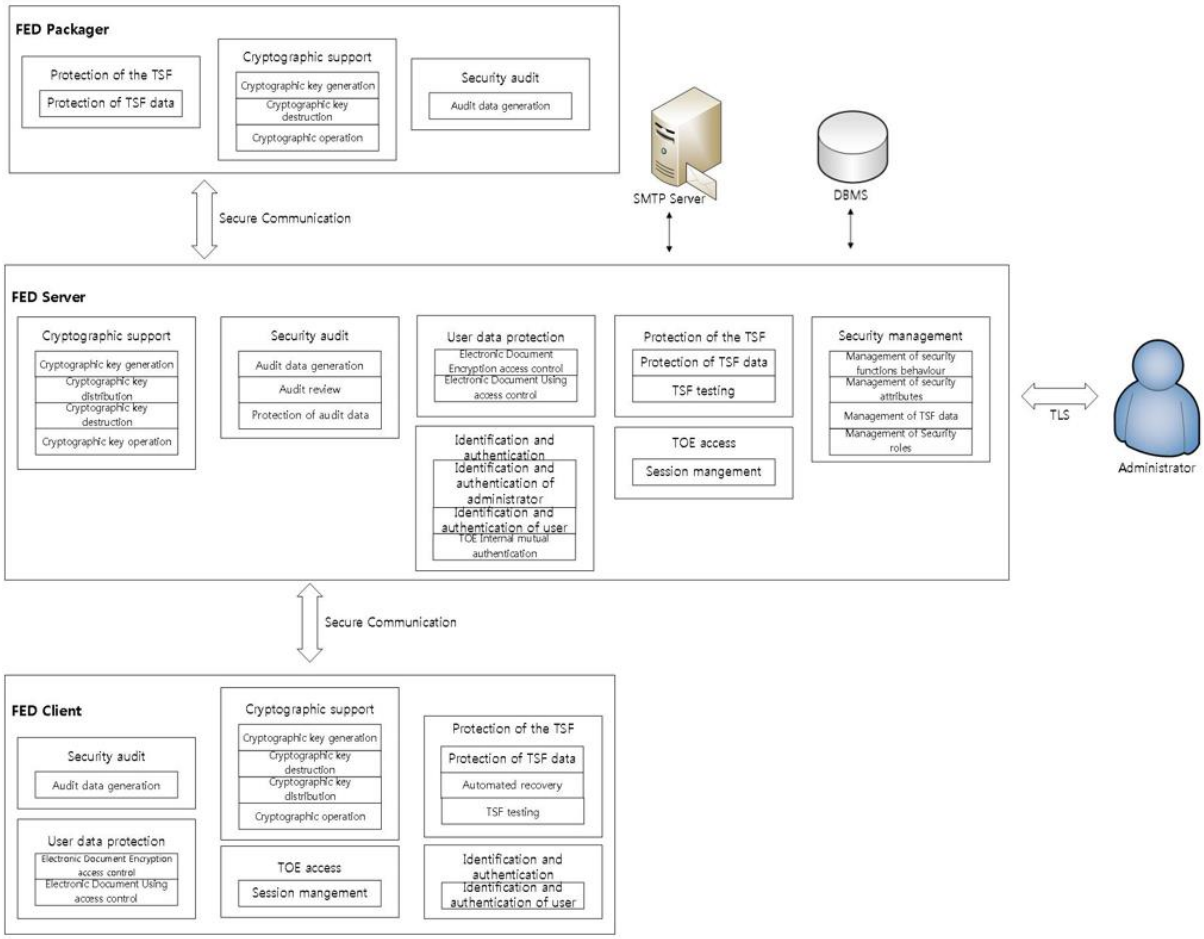
[Figure 2] TOE's physical scope



1.4.2. Logical scope of the TOE

The logical scope of the TOE is as in [Figure 3] below.

[Figure 3] TOE's logical scope



1.4.2.1 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.

1.4.2.2 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.

1.4.2.3 User data protection

The TOE protects user data.

1) 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.
2) 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

1.4.2.4 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. When an administrator attempts to login through a web browser, a NONCE value generated by the random bit generator is first issued from the FED Server and stored in the session. After that, when the administrator attempts to login to the FED Server with the ID and password through the browser, the entered ID, password, and NONCE value are sent to the FED Server. Then, the server checks whether the received NONCE value matches the value stored in the session. If it does match, the authentication process proceeds. When the process is complete, the NONCE value stored in the session is destroyed to prevent reuse.
The reuse of the authentication information used when a user login to the FED Client is prevented. When a user attempts to login, a NONCE value generated by the random bit generator is first issued from the FED

Server and stored in the DB with the user ID. After that, when the user attempts to login to the FED Client with the ID and password, the entered ID, password, and NONCE value are sent to the FED Server. Then, the server checks whether the received user ID and NONCE value match the values stored in the DB. If it does match, the authentication process proceeds. When the process is complete, the NONCE value stored in the DB is destroyed to prevent reuse.

1.4.2.5 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.

1.4.2.6 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.

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 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.

1.5 Terms and definitions

Terms used in this ST, which are the same as in the CC, 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 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 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

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

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

Security Target (ST)
Implementation-dependent statement of security needs for a specific identified TOE

Protection Profile (PP)
Implementation-independent statement of security needs for a TOE type

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

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

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
Authorized user to securely operate and manage the TOE

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

Self-tests
Pre-operational or conditional test executed by the cryptographic module

Assets
Entities that the owner of the TOE presumably places value upon

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

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

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

Evaluation Assurance Level (EAL)
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 rigo

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 that, if exposed or changed, may compromise the security of the cryptographic module (e.g., secret/private key, authentication data such as a password or personal identification number)

TOE Security Functionality (TSF)
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

Secure Sockets Layer (SSL)
This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network

Transport Layer Security (TLS)
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

Document Class
The permission of users for using documents is defined in the document class by the authorized administrator. At least one document class should be set for operating the FED 5 service, and at the time when a FED-N document is created, one of the document classes is selected for the created document.

Permission
Logical unit that allows authorized users to manipulate data in secured documents (e.g., view, edit, print, screen capture, extract, decrypt, change permission, macro, allowed time period to view, revoke, etc.)

Encryption Policy
Policy that defines how to create FED-N documents. There are 4 types of encryption - encryption upon user selection, encryption by application, encryption by extension and batch encryption.

Secured document
Documents encrypted by the FED Client or FED Packager and of which the usage is controlled by the FED Client

Encryption Key Password
Password that acts as an input to derive the actual secure encryption key used for encryption when the FED Server saves important parameters. The administrator should generate the encryption key password at the first login after installing the FED Server and enter it every time when starting the FED Server service.

FED
The abbreviation for Fasoo Enterprise DRM, a digital rights management (DRM) solution provided by Fasoo Co., Ltd.

FED-N Secured Document
Secured document created on a user PC and encrypted according to the document encryption policy. It is subject to the document class where the permission of users for using the document is defined.

FED-R License

Information containing the permission of users for using the FED-R document. It is issued by the FED Server in connection with the ACL of the information system when an authorized user tries to access the document.

FED-R Secured Document
Secured document encrypted by the FED Packager. When a document is downloaded from the information system, the document is encrypted by the FED Packager. Unlike FED-N secured documents, the access to the FED-R secured documents is controlled by the ACL permission policy of the information system.

CRM (Customer relationship management)
Processes implemented to manage a company's interactions with customers and prospects.

1.6 Conventions

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 PP.

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**.

“Application notes” is provided in this ST to clarify the intent of requirements, provide the information for the optional items in implementation, and define "Pass/Fail" criteria for a requirement. The application notes is provided with corresponding requirements if necessary.

2. Conformance claim

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)
Part 2 Security functional components	Extended: FCS_RGB.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 Protection Profile for Electronic Document Encryption V1.1
Package	Augmented : EAL1 augmented(ATE_FUN.1)

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'.

[Table 2] Conformance claim rationale

Item	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_SEL.1	FAU_SEL.1	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.1(3)	Same as PP
		FCS_CKM.1(4)	Same as PP
		FCS_CKM.1(5)	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_COP.1(4)	Same as PP
		FCS_COP.1(5)	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_ACC.1(2)	Same as PP
	FDP_ACF.1	FDP_ACF.1(1)	Same as PP
		FDP_ACF.1(2)	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_RCV.4	FPT_RCV.4	Added when creating ST
	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

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

The following table describes the security objectives for the operational environment.

[Table 3] Security objectives for the operational environment

Item	Description
OE. PHYSICAL_CONTROL	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.
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 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.
OE.OPERATION_SYSTEM_REINFORCEMENT	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.
OE.SECURE_DEVELOPMENT	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.
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.RELIABLE_TIME_STAMP	The TOE shall accurately record the security related events using the reliable time stamp from the TOE operational environment.
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

4.1 Cryptographic support

4.1.1. Random bit generation

Family Behaviour

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 the 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 Random bit generation

Hierarchical to	No other components.
Dependencies	No dependencies.

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*].

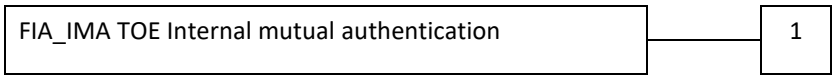
4.2 FIA, Identification & authentication

4.2.1. TOE Internal mutual authentication

Family Behaviour

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

Component leveling



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 dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] by [assignment: *authentication protocol*] that meets the following: [assignment: *list of standards*].

4.3 Security management

4.3.1. ID and password

Family Behaviour

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. FMT_PWD.1 Management of ID and password

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 [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*].

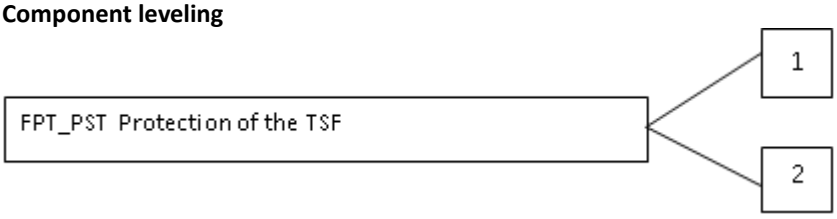
4.4 TSF Protection of the TSF

4.4.1. Protection of stored TSF data

Family Behaviour

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 auditable events foreseen.

4.4.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to No other components.
Dependencies No dependencies.

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 dependencies.

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*].

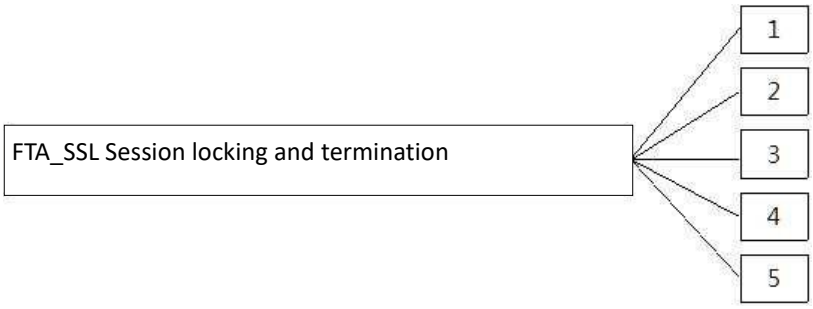
4.5 TOE Access

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

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.

The following table defines all the subjects, objects, operations, security attributes used in the security functional requirements:

[Table 4] Definition of subjects, objects, relevant security properties and operations

Subject (user)	Subject (user) security attributes	Object (information)	Object (information) security attributes	Operation
Authorized administrator	User ID, Password, IP address	Security management data	-	Query, modify
		Authentication data		Query, modify
		Organization chart management data		Query, modify
		Administrator permission setting data		Query, modify
		Security policy setting data		Query, modify
		Audit data		Query
		Cryptographic key data		Query, modify
		Certificate data		Query, modify
Authorized document user	User ID, Group code, Job role, Job title, Head of group	FED-N secured documents	Document class, Owner ID, Owner group code	View
				Edit
				Encrypt
				Decrypt
				Print
				Screen capture
				Change permission
				Extract
				Change class
				Macro
				Period of usage
				Revoke
	User ID	FED-R secured documents	System name, Document ID	View
				Edit
				Encrypt
				Decrypt
				Print
				Screen capture
				Extract

5.1 Security functional requirements

[Table 5] Security functional requirements

Security functional class	Security functional component	
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_SEL.1	Selective audit
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation (Electronic Document Encryption - FED Client)
	FCS_CKM.1(2)	Cryptographic key generation (Electronic Document Encryption - FED Packager)
	FCS_CKM.1(3)	Cryptographic key generation (TSF data encryption - FED Server)
	FCS_CKM.1(4)	Cryptographic key generation (TSF data encryption - FED Client)
	FCS_CKM.1(5)	Cryptographic key generation (TSF data encryption - FED Packager)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Electronic Document Encryption - FED Client)
	FCS_COP.1(2)	Cryptographic operation (Electronic Document Encryption - FED Packager)
	FCS_COP.1(3)	Cryptographic operation (TSF data encryption - FED Server)
	FCS_COP.1(4)	Cryptographic operation (TSF data encryption - FED Client)
	FCS_COP.1(5)	Cryptographic operation (TSF data encryption - FED Packager)
	FCS_RBG.1(Extended)	Random bit generation
FDP	FDP_ACC.1(1)	Subset access control (Electronic Document Encryption access control)
	FDP_ACC.1(2)	Subset access control (Electronic Document Usage access control)
	FDP_ACF.1(1)	Security attribute-based access control (Electronic Document Encryption access control)
	FDP_ACF.1(2)	Security attribute-based access control (Electronic Document Usage access control)
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
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
FPT	FPT_ITT.1	Basic internal TSF data transmission protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_PST.2(Extended)	Availability protection of TSF data
	FPT_TST.1	TSF self-testing
	FPT_RCV.4	Function recovery
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

5.1.1. Security audit

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 [*sending 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_GEN.1.1 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 audit; and
c) [Refer to the “auditable events” in [Table 6] Audit events, [none]].

FAU_GEN.1.2 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 the ST [Refer to the contents of “additional audit record” in [Table 6] Audit events, [none]].

[Table 6] Audit events

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	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)	
FCS_CKM.4	Success and failure of the activity (applying to destruction of key related to Electronic Document Encryption)	
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	
FMT_MSA.1	All modifications to the security attributes	
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 changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	TSF self-testing and the results of the tests	Modified TSF data or module information 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	

5.1.1.3. FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 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_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [integrity violation and self-test failure of the validated cryptographic module, the reaching of the threshold for the unsuccessful login attempts/audit trail, overwriting the oldest stored audit records if the audit trail is full, Control rules violation] 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_SAR.1.1 The TSF shall provide the [authorized administrator] with the capability to read [all the audit data] from the audit records.

FAU_SAR.1.2 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_SAR.3.1: The TSF shall provide the ability to apply [descending order by time] of audit data based on [and operation].

[Table 7] Searching conditions for audit data

Type of audit records	Basic search conditions
Administrator audit log	User ID, name, IP address, period, task type, accessible menu
Document usage log	User ID, name, document name, IP address, period, document type, document class, usage type, result
System usage log	User ID, name, IP address, period, usage type, result

5.1.1.6. FAU_SEL.1 Selective audit

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 TSF Management of TSF data

FAU_SEL.1.1: The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:
a) *event type*
b) [none]

5.1.1.7. 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 [notify the authorized administrator, [none]], if the audit trail exceeds [the threshold set by the authorized administrator].

5.1.1.8. 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 a notification email to the authorized administrator] if the audit trail is full.

5.1.2. Cryptographic support

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

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 [Cryptographic key generation algorithm in [Table 8]] and a specified cryptographic key size [Cryptographic key size in [Table 8]] that meet the following [List of standards in [Table 8]].

[Table 8] Cryptographic key generation algorithm

Cryptographic key generation algorithm	cryptographic key size	List of standards
HASH_DRBG	256bit	TTAK.KO-12.0190

5.1.2.2. FCS_CKM.1(2) Cryptographic key generation (Electronic Document Encryption - FED Packager)

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 [Cryptographic key generation algorithm in [Table 9]] and a specified cryptographic key size [Cryptographic key size in [Table 9]] that meet the following [List of standards in [Table 9]].

[Table 9] Cryptographic key generation algorithm

Cryptographic key generation algorithm	cryptographic key size	List of standards
HASH_DRBG	256bit	TTAK.KO-12.0190

5.1.2.3. FCS_CKM.1(3) Cryptographic key generation (TSF Data Encryption – FED Server)

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 [Cryptographic key generation algorithm in [Table 10]] and a specified cryptographic key size [Cryptographic key size in [Table 10]] that meet the following [List of standards in [Table 10]].

[Table 10] Cryptographic key generation algorithm

Cryptographic key generation algorithm	cryptographic key size	List of standards
RSAES-OAEP	2048bit	KS X ISO/IEC 18033
HASH_DRBG	256bit	TTAK.KO-12.0331
PBKDF	256bit	TTAK.KO-12.0334

5.1.2.4. FCS_CKM.1(4) Cryptographic key generation (TSF Data Encryption – FED Client)

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 [Cryptographic key generation algorithm in [Table 11]] and a specified cryptographic key size [Cryptographic key size in [Table 11]] that meet the following [List of standards in [Table 11]].

[Table 11] Cryptographic key generation algorithm

Cryptographic key generation algorithm	cryptographic key size	List of standards
HASH_DRBG	256bit	TTAK.KO-12.0331
PBKDF	256bit	TTAK.KO-12.0334

5.1.2.5. FCS_CKM.1(5) Cryptographic key generation (TSF Data Encryption – FED Packager)

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 [Cryptographic key generation algorithm in [Table 12]] and a specified cryptographic key size [Cryptographic key size in [Table 12]] that meet the following [List of standards in [Table 12]].

[Table 12] Cryptographic key generation algorithm

Cryptographic key generation algorithm	cryptographic key size	List of standards
HASH_DRBG	256bit	TTAK.KO-12.0331
PBKDF	256bit	TTAK.KO-12.0334

5.1.2.6. 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 the specified cryptographic distribution method [Cryptographic key distribution method of [Table 13] Cryptographic key distribution] that meets the following [List of standards of [Table 13] Cryptographic key distribution].

[Table 13] Cryptographic key distribution

Cryptographic key distribution method	Cryptographic key distribution algorithm	Cryptographic key length	List of standards
Public key cryptographic method	RSAES-OAEP	2048bit	KS X ISO/IEC 18033

5.1.2.7. 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 the specified cryptographic key destruction method [key zeroization] that meets the following: [No other components].

5.1.2.8. FCS_COP.1(1) Cryptographic operation (Electronic Document Encryption- FED Client)

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 the cryptographic operation list [Cryptographic operation list in [Table 14]] in accordance with a specified cryptographic algorithm in [Cryptographic algorithm in Table 14] and a specified cryptographic key size [Cryptographic key size in [Table 14]] that meet the following [List of standards in [Table 14]].

[Table 14] Cryptographic operation

Cryptographic algorithm	Cryptographic key size	List of standards	Cryptographic operation list
ARIA-CTR	256bit	KS X 1213-1	Encryption/decryption of electronic documents

5.1.2.9. FCS_COP.1(2) Cryptographic operation (Electronic Document Encryption – FED Packager)

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 the cryptographic operation list [Cryptographic operation list in [Table 15]] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in [Table 15]] and a specified cryptographic key size [Cryptographic key size in [Table 15]] that meet the following [List of standards in [Table 15]].

[Table 15] Cryptographic operation

Cryptographic algorithm	Cryptographic key size	List of standards	Cryptographic operation list
ARIA-CTR	256bit	KS X 1213-1	Encryption of electronic documents

5.1.2.10. FCS_COP.1(3) Cryptographic operation (TSF Data Encryption – FED Server)

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 the cryptographic operation list [Cryptographic operation list in [Table 16]] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in [Table 16]] and a specified cryptographic key size [Cryptographic key size in [Table 16]] that meet the following [List of standards in [Table 16]].

[Table 16] Cryptographic operation

Cryptographic algorithm	Cryptographic key size	List of standards	Cryptographic operation list
ARIA-CBC	256bit	KS X 1213-1	Encryption/decryption of private key and transmitted data Encryption/decryption of cryptographic key
RSAES-OAEP	2048bit	KS X ISO/IEC 18033	Decryption of data for communication
RSASSA-PSS	2048bit	KS X ISO/IEC 14888	Digital signature
SHA-256	N/A	KS X ISO/IEC 10118	Encryption of authentication data

5.1.2.11. FCS_COP.1(4) Cryptographic operation (TSF Data Encryption – FED Client)

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 the cryptographic operation list [Cryptographic operation list in [Table 17]] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in [Table 17]] and a specified cryptographic key size [Cryptographic key size in [Table 17]] that meet the following [List of standards in [Table 17]].

[Table 17] Cryptographic operation

Cryptographic algorithm	Cryptographic key size	List of standards	Cryptographic operation list
ARIA-CBC	256bit	KS X 1213-1	Encryption of transmitted data Encryption/decryption of password of device cryptographic key file Encryption/decryption of cryptographic key
RSAES-OAEP	2048bit	KS X ISO/IEC 18033	Encryption of data for communication Decryption of electronic document cryptographic key
RSASSA-PSS	2048bit	KS X ISO/IEC 14888	Digital signature and verification
HMAC_SHA-256	256bit	TTAK.KO-12.0330	Integrity check of document header data

5.1.2.12. FCS_COP.1(5) Cryptographic operation (TSF Data Encryption – FED Packager)

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 the cryptographic operation list [Cryptographic operation list in [Table 18]] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in [Table 18]] and a specified cryptographic key size [Cryptographic key size

in [Table 18]] that meet the following [List of standards in [Table 18]].

[Table 18] Cryptographic operation

Cryptographic algorithm	Cryptographic key size	List of standards	Cryptographic operation list
ARIA-CBC	256bit	KS X 1213-1	Encryption/decryption of transmitted data
RSAES-OAEP	2048bit	KS X ISO/IEC 18033	Encryption of electronic document cryptographic key
RSASSA-PSS	2048bit	KS X ISO/IEC 14888	Digital signature and verification
HMAC_SHA-256	256bit	TTAK.KO-12.0330	Integrity check of document header data

5.1.2.13. FCS_RBG.1 Random bit generation (Extended)

Hierarchical to: No other components.
Dependencies: No dependencies

FAU_RBG.1.1 The TSF shall generate random bits using the specified random bit generator that meets the following [[Table 19] Random bit generation].

[Table 19] Random bit generation

Random bit generation algorithm	Cryptographic key size	List of standards
HASH_DRBG (SHA-256)	256bit	TTAK.KO-12.0331

5.1.3. User data protection

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 TSF shall enforce the [electronic document encryption access control SFP] on [list of subjects, objects, and operations among subjects and objects covered by SFP].

[

a) Permission policy by document class
   A. Subject: authorized user
   B. Object : FED-N secured document
   C. Operation list
      i. View
      ii. Edit
      iii. Encrypt
      iv. Decrypt
b) ACL-based access control policy
   A. Subject: authorized user
   B. Object: FED-R secured document
   C. Operation list
      i. View
      ii. Edit
      iii. Encrypt

iv. Decrypt

]

5.1.3.2. FDP_ACC.1(2) Subset access control (Electronic Document Usage access control)

Hierarchical to	No other components.
Dependencies	FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 TSF shall enforce the [electronic document usage access control SFP] on [list of subjects, objects, and operations among subjects and objects covered by SFP].

[

a) Permission policy by document class
   A. Subject: authorized user
   B. Object : FED-N secured document
   C. Operation list
      i. Print
      ii. Screen capture
      iii. Change permission
      iv. Extract
      v. Change class
      vi. Macro
      vii. Period of usage
      viii. Revoke
b) ACL-based access control policy
   A. Subject: authorized user
   B. Object: FED-R secured document
   C. Operation list
      i. Print
      ii. Screen capture
      iii. Extract

]

5.1.3.3. 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 TSF shall enforce the [Electronic Document Encryption access control SFP] on objects based on the [list of subjects and objects controlled by the following SFP, security attribute appropriate for SFP regarding each subject and object, or group of named security attributes].

[

a) Permission policy by document class
   A. Subject: authorized user
   B. Object : FED-N secured document
   C. Security attribute of authorized user: user ID, group code, job role, job title, head of group
   D. Security attribute of secured document: document class, owner's user ID, owner's group code
b) ACL-based access control policy
   A. Subject: authorized user
   B. Object: FED-R secured document
   C. Security attribute of authorized user: user ID
   D. Security attribute of secured document: system name, document ID

]

FDP_ACF.1.2 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 TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [none]

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

5.1.3.4. FDP_ACF.1(2) Security attribute based access control (Document usage access control)

Hierarchical to No other components.

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

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

[

a) Permission policy by document class
   A. Subject: authorized user
   B. Object : FED-N secured document
   C. Security attribute of authorized user: user ID, group code, job role, job title, head of group
   D. Security attribute of secured document: document class, owner's user ID, owner's group code

b) ACL-based access control policy
   A. Subject: authorized user
   B. Object: FED-R secured document
   C. Security attribute of authorized user: user ID
   D. Security attribute of secured document: system name, document ID

]

FDP_ACF.1.2 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 TSF shall explicitly authorize access of the subject to objects based on the following additional rules: [none]

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

5.1.4. Identification and authentication

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 *an administrator configurable positive integer within [3~5]* unsuccessful authentication attempts occur related to [authentication of administrator, document user].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [disable identification and authentication feature (enable after issuing a temporary password].

5.1.4.2. FIA_IMA.1 Internal mutual authentication

Hierarchical to No other components.
Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [FED Server and FED Client, FED Server and FED Client] 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_SOS1.1 The TSF shall provide a mechanism to verify that secrets meet [the following permission criteria].

a) Combination rules
1) 52 English letters (case sensitive)
2) 10 numbers (0~9)
3) 10 special characters (!,@,#,$,%,^,*,+,=,-)
4) The password must be at least 12 characters, but not more than 30 characters in length.
5) Password shall embed one of the above 1) ~ 3) rules

5.1.4.4. FIA_UAU.1 Timing of authentication

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

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

[
a) document user
A. Policy download: domain policy, default policy
b) Administrator: none
]

FIA_UAU.1.2 The TSF shall require each 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].

5.1.4.6. FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components.

Dependencies FIA_UAU.1 authentication

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

[

a) Mask all passwords shown through GUI with "●" instead of the letters or numbers originally typed in.
b) Do not provide feedback for failure causes when authentication failed.

]

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 user to be performed before the user is identified.

[

a) document user
   A. Policy download: domain policy, default policy
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.

5.1.5. Security management

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 administrative actions of*** [the following] List of functions in [Table 20]] to [the authorized administrator].

[

[Table 20] List of functions

Menu	Category	Administrative behaviour
General Setting	User/Group	Modify behaviour, determine behaviour
	Administrator	Modify behaviour, determine behaviour
	System	Modify behaviour, determine behaviour
	Cryptographic key	Modify behaviour, determine behaviour
Document Class	Permission management	Modify behaviour, determine behaviour
Security Policy	Integrated system management	Modify behaviour, determine behaviour
	DRM client policy management	Modify behaviour, determine behaviour
	Document encryption policy management	Modify behaviour, determine behaviour

	Exceptional usage management	Modify behaviour, determine behaviour
Statistics	Statistics management	Enable
Log	Log management	Enable

]

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 of [the following] to [the authorized administrator].

[

a) Administrator permission coverage: accessible menu, scope of management (group)
b) Permission by FED-N secured document class: view, edit, print, screen capture, change permission, extract, decrypt, change class, macro, period of usage, revoke
c) FED-N secured document permission coverage: all, user, team member, direct supervisor
d) Permission assignment criteria of FED-N secured document: user ID, group code, job role, job title
e) FED-R integrated system list
f) Extensions for encryption upon user selection
g) Document identification method upon real time/administrator encryption: extension, document format (MS Office, Hancom Office, PDF)
h) Applications targeted for auto encryption: Hancom HWP, MS Excel, MS Word, MS PowerPoint, MS Notepad, MS WordPad, MS Paint, Adobe Reader, Autodesk Autocad
i) Document class upon encryption
j) Virtual printer to be allowed
k) Capture program to be allowed

]

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 the [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 TSF Data management

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 [the following TSF data list] to [the authorized administrator].

[Table 21] TSF data list

Category		Authorized administrator
Security management data	Number of authentication failure and password validity period	Query, change
	IP setting data for management access	Query, change
	Log threshold setting data	Query, change
Authentication data	ID	Query, change
	PW	change
Organization chart management data		Query, change
Administrator permission setting data		Query, change
Security policy setting data	Document class-specific permission setting	Query, change
	Encryption policy setting	Query, change
	Exception policy setting	Query, change
Audit data	Administrator audit log data	Query
	Document usage statistics data	Query
	Client login statistics data	Query
	Document usage log data	Query
	System usage log data	Query
Cryptographic key data		Query, change
Authentication data		Query, change

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:

[

a) TSF function management: items specified in FMT_MOF.1
b) TSF security attributes management: items specified in FMT_MSA.1
c) TSF data management: 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 role of [the authorized administrator].
FMT_SMR.1.2 TSF shall be able to associate users and their **roles defined in FMT_SMR.1.1**.

5.1.6. Protection of the TSF

5.1.6.1. FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to No other components.
Dependencies No dependencies.

FMT_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.

FMT_PST.1.1 The TSF shall protect [cryptographic data, password of administrator and document user, password for device cryptographic key file and TOE setting value] stored in containers controlled by the TSF from 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 TSF shall *prevent* the unauthorized deletion for [execution file of FED Client, registry value].
FPT_PST.2.2 TSF shall *prevent* the unauthorized termination for [execution file of FED Client].

5.1.6.4. FPT_RCV.4 Function recovery

Hierarchical to No other components.
Dependencies No dependencies.

FPT_RCV.4.1 The TSF shall guarantee a recovery feature capable of returning to the consistent and secure state when one of the [following] is successfully complete or for the specified failure scenarios.

[

a) Integrity error in major setting values or files of the FED client
b) Deletion of major setting values or files of the FED client
c) Termination of the FED client execution process while the operation system is running

]

5.1.6.5. FPT_TST.1 TSF self-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 *TSF*.

FPT_TST.1.2 The TSF shall provide a function that verifies integrity of *TSF data* to the **authorized administrator**.

FPT_TST.1.3 The TSF shall provide a function that verifies integrity of *TSF* to the **authorized administrator**.

5.1.7. TOE access

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 [The maximum number of concurrent sessions for administrator management access session restricted to one, rule for the maximum number of { the maximum number of concurrent sessions for general user access session restricted to one } concurrent sessions].

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

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

Hierarchical to No other components.
Dependencies No dependencies.

FPT_ SSL.5.1 The TSF shall *terminate* an interactive session of the **authorized administrator and document user** after a [time interval of administrator inactivity].

Application notes: The time interval of authorized administrator inactivity is set to 10 minutes and the default value is 10 minutes. The period of document user inactivity depends on the policy set by the administrator and the default value is 5 minutes.

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 assurance requirements

This section defines the assurance requirements for the TOE. Assurance requirements are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

Security assurance class	Security assurance component	
Security Target	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	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

5.2.1. Security target

5.2.1.1. ASE_INT.1 Security target introduction

Dependencies	No dependencies.
Developer action elements	
ASE_INT.1.1D	The developer shall provide an 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 identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarize 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 claim

Dependencies	ASE_INT.1 Security target 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 to a package of the ST 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_CCL.1.1E	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 the existing components.

5.2.1.5. ASE_REQ.1 Stated security requirements

Dependencies	No dependencies
Developer action elements	
ASE_REQ.1.1D	The developer shall provide a statement of security requirements.
ASE_REQ.1.2D	The developer shall provide 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

REQ.1.1E	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. ADV_FSP.1 Basic functional 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 categorization 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 shall 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 display, 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 securely prepared for operation.

5.2.4. Life-cycle support

5.2.4.1. ALC_CMC.1 Labeling of the TOE

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 evaluation evidence required by the TOE and 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 meet requirements for content and presentation of evidence.

5.2.4.2. ALC_CMS.1 TOE CM coverage

Dependencies	ALC_CMS.1 TOE configuration management coverage

Developer action elements

ALC_CMC.1.1D	The developer shall provide the TOE and the TOE reference.

Content and presentation elements

ALC_CMC.1.1C	The TOE shall label for the 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.

5.2.5. 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 plan, expected test results and the 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

Dependencies	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements	
AVA_VAN.1.1D	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 presentation 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 possessing success potential of basic attack.

5.3. Security requirements rationale

5.3.1. Dependency rationale of security functional requirements

The following table shows dependency of security functional requirement.

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE. 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_SEL.1	FAU_GEN.1 FMT_MTD.1	2 36
7	FAU_STG.3	FAU_STG.1	OE. protection of audit data
8	FAU_STG.4	FAU_STG.1	OE. protection of audit data
9	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	14 16

		FCS_CKM.4	15
10	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	14 17 15
11	FCS_CKM.1(3)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	14 18 15
12	FCS_CKM.1(4)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	14 19 15
13	FCS_CKM.1(5)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	14 20 15
14	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - 9, 10, 11, 12, 13 15
15	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	- - 9, 10, 11, 12, 13
16	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - 9 15
17	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - 10 15
18	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - 11 15
19	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - 12 15
20	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - 13 15
21	FCS_RBG.1	-	-
22	FDP_ACC.1(1)	FDP_ACF.1	24
23	FDP_ACC.1(2)	FDP_ACF.1	25
24	FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	22 35
25	FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	23 35
26	FIA_AFL.1	FIA_UAU.1	29
27	FIA_IMA.1	-	-
28	FIA_SOS.1	-	-
29	FIA_UAU.1	FIA_UID.1	32
30	FIA_UAU.4	-	-
31	FIA_UAU.7	FIA_UAU.1	29
32	FIA_UID.1	-	-

33	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	38 39
34	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	22, 23 - 38 39
35	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	34 39
36	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	38 39
37	FMT_PWD.1	FMT_SMF.1 FMT_SMR.1	38 39
38	FMT_SMF.1	-	-
39	FMT_SMR.1	FIA_UID.1	32
40	FPT_PST.1	-	-
41	FPT_PST.2	-	-
42	FPT_ITT.1	-	-
43	FPT_RCV.4	-	-
44	FPT_TST.1	-	-
45	FTA_MCS.2	FIA_UID.1	32
46	FTA_SSL.5	FIA_UAU.1	29
47	FTA_TSE.1	-	-

FAU_GEN.1 has a subordinate relationship with FPT_STM.1. However, as the TOE accurately records security-related events using reliable time stamp provided in the TOE operational environment,
a subordinate relationship with FAU_GEN.1 is satisfied by the security objectives for OE. Time Stamp instead of FPT_STM.1

FAU_STG.3 and FAU_STG.4 has a subordinate relationship with FAU_STG.1. However, as the audit trail protects the audit record from unauthorized deletion or modification (DBMS interacting with the TOE in the TOE operational environment), a subordinate relationship with FAU_STG.3 and FAU_STG.4 is satisfied by the security objectives for OE. Protection of Audit Data instead of FAU_STG.1.

5.3.2. Dependency rationale of security assurance requirements

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. However, 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 this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

This chapter briefly and explicitly specifies how the security functions of the TOE are implemented and how the functions meet the assurance requirements.

6.1 TOE security functions

This chapter describes the security functions provided by the TOE and how the security functions of FED 5 SP1 satisfy all the security requirements specified in Chapter 5.

- Security audit (FAU)
- Cryptographic support (FCS)
- User data protection (FDP)
- Identification and authentication (FIA)
- Security management (FMT)
- Protection of the TSF (FPT)
- TOE access (FTA)

6.1.1. Security audit (FAU)

Security audit performs the following functions:

- Audit data generation
- Audit data lookup/search
- Audit data protection

6.1.1.1 Audit data generation

Audit data generation is a function which creates and stores logs regarding the events incurred from the security functions of the TOE. The logs are created and stored as classified into the following three categories. The document usage log can be selectively collected depending on the usage type such as creation, view, edit, change permission, change owner, print, revoke or decrypt. In addition, the TOE records significant security violations on the system usage logs and sends a notification email to the administrator.

[Table 22] Types of audit data generation

Types of audit records	Description
Administrator audit log	Logs about changes of security policies made by the administrator while executing security management functions.
Document usage log	Logs about users' document usage such as viewing, editing and printing secured documents on users' PC.
System usage log	Booting and termination of the FED Server, user's logging in and out, system usage log such as (policy update on FED Client), violation of integrity, self-test failure, problems regarding protection of audit log, rejection of duplicate login, security alerts including attempts for reusing authentication data

6.1.1.2. Look up/search audit data

The TOE provides the function for looking up the audit data stored in the audit data container (DBMS) for the authorized administrator through management access. Lookup of the audit data is classified as document usage logs, administrator audit logs, and system usage logs, and each type of audit data is shown in the appropriate format for the authorized administrator to interpret. Also, the audit data can be found selectively by the combined search condition of user ID, IP address, data, event type, etc. by the AND operator.

6.1.1.3. Protect audit data

The TOE provides the function for the authorized administrator to set the threshold (default value: 1,000,000) for the audit trail by log type (document usage log, system usage log, and administrator audit log), and when the number of the stored records exceeds 90% of the set threshold, the TOE sends an email warning to the administrator. When the number reaches (exceeds) the threshold, the oldest audit records are overwritten and the administrator is notified by email.

Related SFRS: FAU_SAA.1, FAU_ARP.1, FAU_GEN.1, FAU_SEL.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.3, FAU_SAR.4

6.1.2. Cryptographic support (FCS)

The TOE performs cryptographic key generation, cryptographic operation, and cryptographic key destruction as in the following and distributes the cryptographic key using RSAES-OAEP. For the standard list of each algorithm, refer to 5.1.2 Cryptographic support(FCS).

Key	Used for	Cryptographic key generation Cryptographic operation	Cryptographic key and parameter destruction
DEK	Encrypts documents	HASH_DRBG (256bit) ARIA-CTR	After encryption· decryption, overwrite three times with '0' value and release memory.
	Generates MAC value in the header of the secured document	HASH_DRBG (256bit) HMAC_SHA-256	After encryption· decryption, overwrite three times with '0' value and release memory.
	Encrypts TOE setting	HASH_DRBG (256bit) ARIA-CBC	After encryption· decryption, overwrite three times with '0' value and release memory.
Application server public key	Encrypts the DEK called from the packager. (KEK)	RSA (2048bit) RSAES-OAEP	After encryption· decryption, overwrite three times with '0' value and release memory.
	Encrypts transmitted data (request).	RSA (2048bit) RSAES-OAEP	After encryption· decryption, overwrite three times with '0' value and release memory.
	Digital signature for the transmitted data (response).	RSA (2048bit) RSASSA-PSS	After digital signature, overwrite three times with '0' value and release memory.
Domain key	Encrypts the DEK called from the client. (KEK)	HASH_DRBG (256bit) ARIA-CBC	After encryption· decryption, overwrite three times with '0' value and release memory.
Device public key	Encrypts the DEK in the license file. (KEK)	RSA (2048bit) RSAES-OAEP	After encryption· decryption, overwrite three times with '0' value and release memory.

	Digital signature for the transmitted data (request).	RSA (2048bit) RSASSA-PSS	After digital signature, overwrite three times with '0' value and release memory.
	Encrypts transmitted data (response).	RSA (2048bit) RSAES-OAEP ARIA-CBC	After encryption· decryption, overwrite three times with '0' value and release memory.
Cryptographic key for storing DB	Encrypts key data DB when stored.	PBKDF (256bit) ARIA-CBC	After encryption· decryption, overwrite three times with '0' value and release memory.
Device encryption key	Encrypts the key in the device cryptographic key file (KEK).	HASH_DRBG (256bit) ARIA-CBC	After encryption· decryption, overwrite three times with '0' value and release memory.
Device encryption key for transmission	Encrypts the device cryptographic key for transmission (KEK).	HASH_DRBG (256bit) ARIA-CBC	After encryption· decryption, overwrite three times with '0' value and release memory.

The validated cryptographic module used in cryptographic management is as follows:

Category	Sub category	Description
Validated cryptographic module	Name	Fasoo Crypto Framework V2.4
	Validation number	CM-193-2026.11
	Developer	Fasoo Co., Ltd.
	Date verified	Nov. 18, 2021

Related SFRs: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4), FCS_CKM.1(5), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_RBG.1

6.1.3. User data protection

User data protection performs the following functions:

- Electronic Document Encryption access control
- Electronic Document Usage access control

6.1.3.1. Electronic Document Encryption access control

The authorized administrator can set permissions for encryption or decryption of secured documents (view, edit, encrypt, decrypt) and related policies, and according to the set security policies, document encryption or decryption activities by document users are controlled. Based on the security properties of the document user (user ID, group code, role, and job title) and the security properties of the secured document (document class, owner's user ID, owner's group code, system name, and document ID), access control of electronic document encryption is performed. By comparing the security properties of the document user and the security properties of the secured document with the security policies set by the authorized administrator, if they match, electronic document encryption or decryption is allowed.

6.1.3.2. Electronic Document Usage access control

The authorized administrator can set permissions for use of secured documents (print, screen capture, change permission, extract, change class, macro, period of usage, revoke) and related policies, and according to the set

security policies, document use activities by document users are controlled. Based on the security properties of the document user (user ID, group code, role, and job title) and the security properties of the secured document (document class, owner's user ID, owner's group code), access control of electronic document use is performed. By comparing the security properties of the document user and the security properties of the secured document with the security policies set by the authorized administrator, if they match, electronic document use is allowed.

Related SFRs: FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACC.1(1), FDP_ACF.1(1)

6.1.4. Identification and authentication

Identification and authentication performs the following functions:

- Identification and authentication of administrator
- Identification and authentication of user

6.1.4.1. Administrator identification and authentication

It is mandatory to create a new administrator upon the installation of the TOE, and using the ID and password inputted, administrator authentication data is generated. The generated data is encrypted (SHA-256) and stored in the DBMS. There is no executable action until the identification and authentication of the administrator are complete. The password inputted during the access attempt is masked with "●" to prevent disclosure on the screen and the authentication succeeds if the inputted ID and password are verified by the DBMS. In the case of authentication failure, the reason for the failure is not provided.
The TOE generates a new authentication identification value upon the authentication attempt for management access by the administrator, detects reuse, and if reuse is detected performs administrator authentication failure.
Regarding the authentication attempt for management access by the administrator, if the number of unsuccessful authentication attempts reaches the authentication attempt threshold (3-5 with no timeout value, 5 by default) settable by the authorized administrator, login is permanently blocked and a security alert is sent to the administrator by email. If the login blocking needs to be cleared, the authorized administrator issues a temporary password and the administrator is required to change the password once logging in with the temporary password.
The administrator authentication password must contain at least one alphabetical character, one numeric character, and one special character as in the following and be at least 12 characters in length.

1) 52 alphabetical characters (Capitalization matters.)
2) 10 numeric characters (0-9)
3) 10 special characters (!,@,#,$,%,^,*,+,=,-)

6.1.4.2. User identification and authentication

Before the document user identification and authentication, enter the device password in the device password input window and click the OK button to verify that the device password is the same one set in the certificate registration window at the time of installation. Then, the default policy and the domain policy are received before the identification and authentication of the document user, and the user policy is received after the successful authentication. The TOE provides the ID/password-based authentication function, and the document user is required to change the password upon the initial authentication. The password inputted is masked with "●" to prevent disclosure on the screen, and in the case of authentication failure, the reason for the failure is not provided.
During the authentication of the document user through the FED client, the mutual authentication with the FED server is performed. The FED client authenticates the FED server using the server certificate, encrypts the device ID/authentication data of the FED client using the server's public key, and transmits the encrypted data to the FED server. The FED server decrypts the transmitted data using the server's private key and authenticates the FED client through the authentication process.

The TOE generates a new authentication identification value upon the authentication attempt of the document user, detects reuse, and if reuse is detected performs user authentication failure.
Regarding the authentication attempt of the document user, if the number of unsuccessful authentication attempts reaches the authentication attempt threshold (3-5, 5 by default) settable by the authorized administrator, login is permanently blocked and a security alert is sent to the administrator by email. If the login blocking needs to be cleared, the authorized administrator issues a temporary password and the user is required to change the password once logging in with the temporary password.
The authentication password of the document user must contain at least one alphabetical character, one numeric character, and one special character as in the following and be at least 12 characters in length.

1) 52 alphabetical characters (Capitalization matters.)
2) 10 numeric characters (0-9)
3) 10 special characters (!,@,#,$,%,^,*,+,=,-)

Related SFRs : FIA_AFL.1, FIA_SOS.1, FIA_UAU.4, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1, FIA_IMA.1

6.1.4.3. TOE Internal mutual authentication

Data is transmitted through the internal mutual authentication mechanism among TOE components. When data is transmitted, TLS 1.2 is used for communication by default, and the message transmission between the FED Client and FED Server is as follows:

1) When sending messages from the FED Client to FED Server (verify the client messages)
    i. Data that the FED Client will send
        a. Request data with the digital signature of FED Client device certificate's private key and FED Client device certificate
        b. Encryption of 'a' using the application server certificate
    ii. Data that the FED Server will receive
        a. Decryption using the private key of the application server certificate
        b. Verification of 'a' (digital signature) using the FED Client device certificate
2) When returning messages from the FED Server to FED Client (verify the server messages)
    i. Data that the FED Server will send
        a. Response data with the digital signature of application server certificate's private key and application server certificate
        b. Encryption of 'a' using the FED Client device certificate
    ii. Data that the FED Client will receive
        a. Decryption using the private key of the FED Client device certificate
        b. Verification of 'a' (digital signature) using the application server certificate

6.1.4.4. Prevention of authentication information reuse

1) When an administrator login to the FED Server through a web browser
    a. When a web browser requests a NONCE value from the FED Server, the FED Server stores the NONCE value generated by the random bit generator in the session and send it to the web browser.
    b. When an administrator login by entering the admin ID and password, the NONCE value received at 'a' above is sent together.
    c. The FED Server proceeds authentication process after verifying the admin ID, password and NONCE value stored in the session and destroys the session to prevent the reuse of the stored NONCE.
2) When a user login to the FED Client (DRM Client)
    a. When the FED Client requests a NONCE value from the FED Server, the FED Server stores the

NONCE value generated by the random bit generator in the session and send it to the FED Client.

b. When a user login to the FED Client by entering the user ID and password, the NONCE value received at 'a' above is sent together.

c. The FED Server proceeds authentication process after verifying the user ID, password and NONCE value stored in the session and destroys the session to prevent the reuse of the stored NONCE.

6.1.5. Security management (FMT)

Security management performs the following functions:

- Common management
- Permission policy management of secured documents

6.1.5.1. Common management

The TOE confines the role of executing security management to the authorized administrator, and upon the initial access of the authorized administrator, the ID and password are newly generated. The TOE can register, add, delete group, user, job title, and role and issue temporary passwords through the management access to the FED server. The TOE can control the accessible menu and group management permission on the management access differently depending on the type of the administrator. The TOE also provides the functions for system management such as the settings of the threshold for unsuccessful authentication attempts and audit trail and the IP address setting for administrator's access and the functions for generation and management of the cryptographic keys.

6.1.5.2. Management of permission settings of secured documents

The TOE provides the functions for managing the permissions and policies related to secured documents for the authorized administrator. User permissions for secured documents can be set on the management access screen, and depending on the permission setting, user activities such as view, edit, print, capture screen, change permission, extract, decrypt, change class, macro, and revoke and the period of usage may be restricted. The authorized administrator can specify such permission settings differently by user ID, group head ID, owner, group, document class, role, and job title. Also, the TOE provides the function for setting the policies for encryption upon user selection, encryption by application, encryption by extension, and batch encryption.

6.1.6. Protection of the TSF

Protection of the TSF performs the following functions:

- Protection of the TSF
- Self-testing and recovery

6.1.6.1. Protection of the TSF data

For the safe cryptographic communication among the TOE components, the transmitted TSF data is protected using the confidentiality (ARIA-CBC, 256bit) and integrity (RSASSA-PSS, 2048bit) algorithms of the validated cryptographic module. The types and protection methods for the TSF data stored in the container controlled by TSF are as follows:

TOE component	Container controlled by the TSF			Protection method
	File system	Registry	DBMS	
FED Server			- Domain key - CA private key,	ARIA-CBC

			Application server private key, Device private key	
			- Admin password and user password	SHA-256
FED Client	- Domain key - Device private key			ARIA-CBC
	- Application server public key			RSAES-OAEP
		- User password		SHA-256
	- FED-R license file - Policy file			RSASSA-PSS / proprietary encoding
FED Packager	- Domain key - Application server public key - Device public key - Device private key			ARIA-CBC
	- Policy file			Proprietary encoding

6.1.6.2. Client program recovery

The TOE provides the function for self-testing during the operation to examine the main functions such as the cryptographic function, user authentication, user addition, certificate issuance, policy issuance, etc. if they operate properly regularly (24 hours). The FED client prevents termination of the process using the mutual monitoring among the TOE-related processes so that the running TOE is not to be stopped and prevents file deletion by opening the file handling information about the processes and modules. Also, during the operation of the TOE, integrity check on the TSF (execution file and library file of the FED server, execution file and library file of the FED client) and the TSF data (registry configuration information) is performed regularly (24 hours) for self-protection. The TOE provides the function for recovering the status back to the available status through automatic recovery if the integrity is damaged.

Related SFRs : FPT_ITT.1, FPT_PST.1(Extended), FPT_PST.2(Extended), FPT_TST.1, FPT_RCV.4

6.1.7. TOE access (FTA)

The TOE access performs the following functions:

- Session management

6.1.7.1. Session management

The TOE registers the accessible IP address of the authorized administrator upon the installation, and maximum two IP addresses can be registered. Access from the terminal with an unregistered IP address is not allowed. If access is attempted from the terminal with an unregistered IP address, the error page is displayed instead of the login page. For the management access session of the authorized administrator, the maximum number of concurrent sessions allowed is one, which means concurrent access is not allowed and a new access will be denied, and if a login is attempted with another authorized administrator account in a situation in which there is an administrator who has already logged in, the new access will be denied. If the authorized administrator's period of inactivity for management access reaches 10 minutes, the management access session is terminated.

The maximum number of concurrent sessions for the document user logged in to the FED client is one. After a login session of a specific document user is created, if a login is attempted with the same user account from another terminal, the new access will be denied. The user gets automatically logged out when the inactivity

time elapses, and the inactivity period can be set as the policy (10 minutes by default, 10 – 99,999 minutes) by an administrator.

Related SFRs : FTA_MCS.2, FTA_SSL.5, FTA_TSE.1