KONICA MINOLTA bizhub C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514, DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514

Security Target

This document is a translation of the evaluated and certified security target written in Japanese.

Version : 2.00

Issued on : February 27, 2020

Created by : KONICA MINOLTA, INC

— 【 Contents 】 ————————————————————

— 【 List of Figures 】 ——————————————————

— 【 List of Tables 】 ——————————————————

1. ST Introduction

1.1. ST Reference

- ST Title : KONICA MINOLTA bizhub C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514, DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514 Security Target
- ST Version : 2.00
- Created on : February 27, 2020
- Created by : KONICA MINOLTA, INC.

1.2. TOE Reference

- TOE Name : KONICA MINOLTA bizhub C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514, DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514
- Version : G00-45

The physical components of the TOE are the MFP body and the FAX kit. "KONICA MINOLTA bizhub C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514" is equipped with FAX kit (product name FK-514, corresponding identification information A883) on the MFP body (KONICA MINOLTA bizhub C360i, KONICA MINOLTA bizhub C300i, KONICA MINOLTA bizhub C250i, KONICA MINOLTA bizhub C036DNi, KONICA MINOLTA bizhub C030DNi or KONICA MINOLTA bizhub C025DNi, and its version (G00-45)). "DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514" is equipped with FAX kit (product name FK-514, corresponding identification information A883) on the MFP body (DEVELOP ineo+ 360i, DEVELOP ineo+ 300i or DEVELOP ineo+ 250i and its version (G00-45)).

1.3. TOE Overview

1.3.1. TOE Type

The TOE is the multi-function printer (MFP) used in the network environment (LAN) and has the function to accumulate documents in addition to copy, scan, print and FAX functions.

1.3.2. Usage of the TOE

TOE's use environment is shown below, and the usage for the TOE is described. The hardware and software necessary for using the TOE, which are not the TOE, is described in 1.3.3.

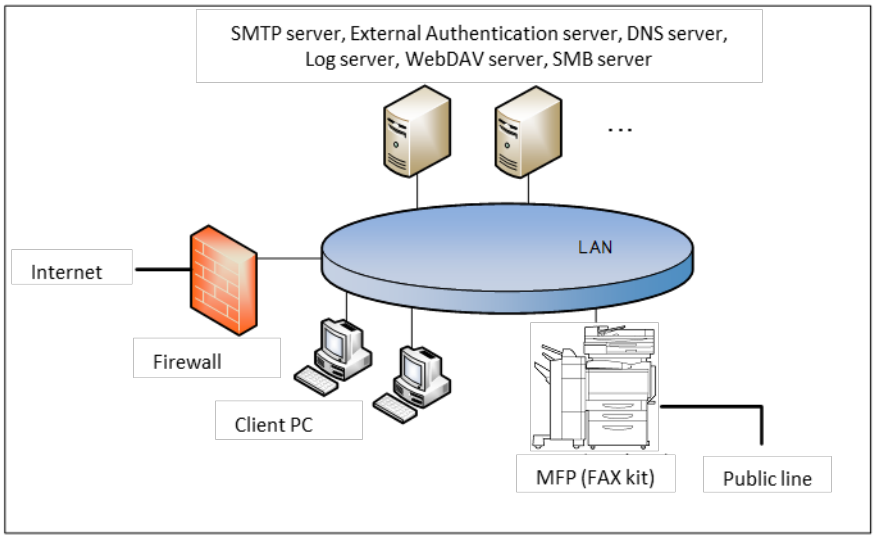


Figure 1-1 TOE's use environment

The TOE is used by connection LAN and public line, as shown in Figure 1-1. The User can operate the TOE by communication through the LAN or the operation panel with which the TOE is equipped.

(1) TOE (MFP)

TOE is connected to the intra-office LAN and the public line and performs the following function.

・Electronic documents' RX
・Fax RX

The User can perform the following from the operation panel.

・MFP's various settings
・Paper documents' Copy, Fax TX, Accumulation as electronic documents, Network TX
・Accumulated documents' Print, Fax TX, Network TX, Deletion

(2) FAX kit

A device that is necessary for use Fax function. Set to TOE.

(3) LAN

Network used for the TOE setup environment

(4) Public line

Telephone line for transmitting the external fax

(5) Firewall

Device for protecting against the network attacks to intra-office LAN from the internet

(6) Client PC

By connecting to the LAN, this works as the client of the TOE. The user can access TOE from the client PC and operate the following by installing the printer driver in the client

PC.

・Accumulation, Print of electronic documents

Also, the user can access TOE from the client PC and operate the following by installing the Web browser in the client PC.

・MFP's various settings

・Accumulation, Print of electronic documents

・Accumulated documents' Network TX, Download, Deletion

(7) SMTP server

Server used for sending the electronic documents stored in the TOE and scanned data.

(8) External Authentication server

Server to identify and authenticate TOE users. This is used only when external server authentication method is used. Kerberos authentication is used in the external server authentication method.

(9) DNS server

Server for converting domain name to IP address

(10) Log server

Server to be destination of audit log TX function. The user can specify a WebDAV server as a destination for files recorded audit logs.

(11) WebDAV server

Server used for stored the electronic documents stored in the TOE and scanned data that are sent from TOE.

(12) SMB server

Server used for stored the electronic documents stored in the TOE and scanned data that are sent from TOE.

1.3.3. Necessary Hardware/Software for the TOE

As the hardware and software necessary for using the TOE, the configuration that was used for the TOE evaluation is as follows.

Hardware/Software	Used version for evaluation
Client PC (Web Brower)	Microsoft Internet Explorer 11
Printer Driver	KONICA MINOLTA C360iSeries PCL / PS
External Authentication Server	Active Directory installed in Microsoft Windows Server 2012 R2 Standard
DNS Server	Active Directory installed in Microsoft Windows Server 2012 R2 Standard
SMTP Server	Black Jumbo Dog Ver. 5.9.5
Log Server	IIS 8.0 accompanying Microsoft Windows Server 2012 R2

Hardware/Software	Used version for evaluation
	Standard
WebDAV Server	IIS 8.0 accompanying Microsoft Windows Server 2012 R2 Standard
SMB Server	File sharing by Microsoft Windows Server 2012 R2 Standard

1.3.4. TOE's Main Security Functions

The TOE is connected to the LAN and a public line and provides the function for users to print, scan, copy, fax and store and retrieve documents and to communicate with the network. Also, in order to protect user documents and security-related data, the following security functions are provided.

Identification and authentication function to specify users, Access control function to restrict access to documents and various operations of TOE in accordance with the authority given to users, Security management function to restrict to users with administrator authority to set security functions, Audit function to record security-related events and send them to the log server, Trusted communication function to protect communication between TOE and external IT devices by IPsec, Encryption function to use for encrypting communication data in the trusted communication function, FAX separation function to ensure separation between PSTN and LAN, and Trusted operation function to prevent updating by illegal FW and detect unauthorized falsification FW during operation.

1.4. TOE Description

This paragraph explains the overview of the physical scope and logical scope of the TOE.

1.4.1. Physical Scope of the TOE

The TOE, as shown in Figure 1-2, is the MFP composed of main/sub power, operation panel, scanner unit, MFP controller unit, printer unit and FAX kit.

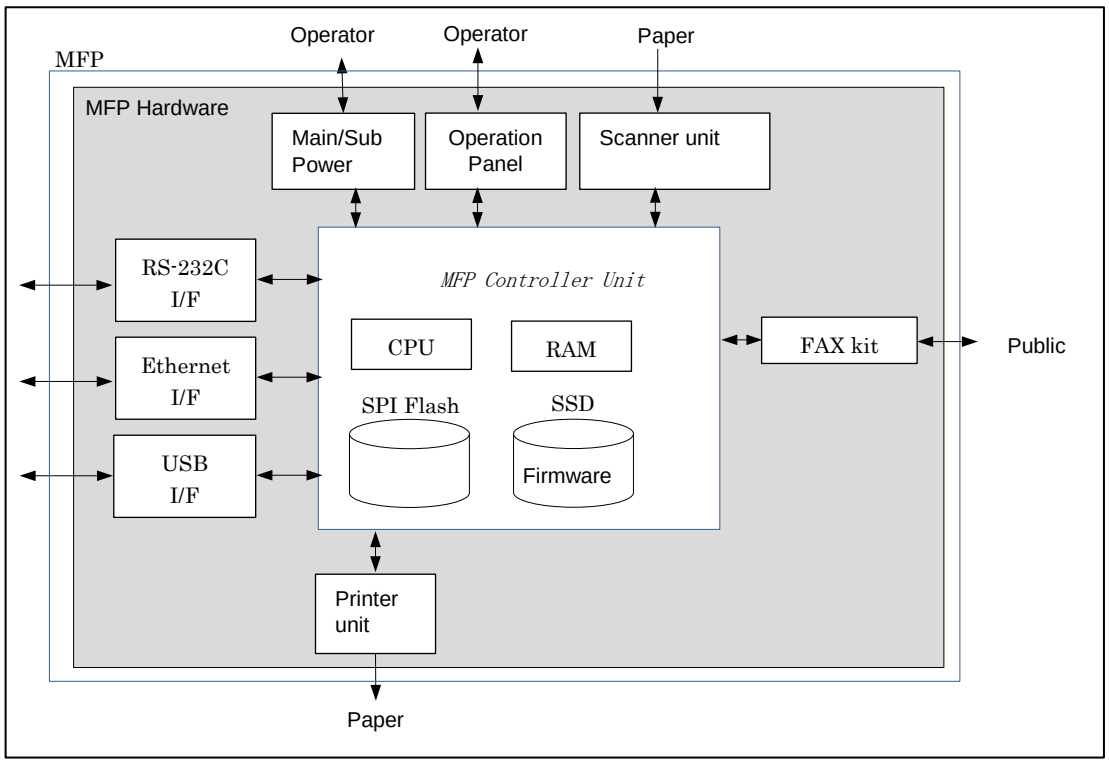


Figure 1-2 Physical scope of the TOE

(1) Main/sub power supply

Power switches for activating MFP.

(2) Operation Panel

An exclusive control device for the operation of MFP, equipped with a touch panel of a liquid crystal monitor.

(3) Scanner unit

A device that scans images and photos from paper and converts them into digital data.

(4) MFP Controller unit

A device that controls MFP.

(5) CPU

Central processing unit.

(6) RAM

A volatile memory used as the working area.

(7) SPI Flash

A nonvolatile memory that stores TSF data that decides MFP action. (Field-nonreplaceable)

(8) SSD

Field-nonreplaceable storage medium of 250GB. Stores the message data expressed in

each country's language to display the response to access through the firmware, operation panel and network, and various settings that the MFP needs. Additionally, electronical file is stored as a file.

(9) Firmware

Software that controls MFP operations.

(10)Printer unit

A device to print the image data which were converted for printing when receiving a print request from the MFP controller.

(11)RS-232C I/F

Interface which is usable for serial connection using D-sub 9-pin connectors. The maintenance function can be used through this interface at the time of a breakdown.

(12)Ethernet I/F

Interface which supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet.

(13)USB I/F

Used for rewriting the firmware according to the guidance.

(14)FAX kit

A device that is used for communications for FAX-data transmission via the public line.

1.4.2. Guidance

The following show the list of guidance which compose this TOE.

Table 1-1 Guidance which compose TOE

Type	Guidance Name	Ver.	Language
FULL	bizhub C360i/C300i/C250i User's Guide	1.00	Japanese
	bizhub C360i/C300i/C250i User's Guide (*)	1.00	English
	ineo+ 360i/300i/250i User's Guide	1.00	English
Security Functions	bizhub C360i/C300i/C250i User's Guide Security Functions	1.02	Japanese
	bizhub C360i/C300i/C250i/C036DNi/C030DNi/C025DNi User's Guide [Security Operations]	1.02	English
	ineo+ 360i/300i/250i User's Guide [Security Operations]	1.02	English

*Supports bizhub C036DNi, bizhub C030DNi and bizhub C025DNi.

1.4.3. TOE's each part and identification

TOE is delivered in unit of MFP hardware, FAX kit, firmware and guidance.

Table 1-2 Delivery format and method of MFP hardware, FAX kit, firmware

Delivery unit	Identification	Format	Delivery method
MFP hardware (Any of the right)	bizhub C360i	hardware	Delivered by original box.
	bizhub C300i		
	bizhub C250i		
	bizhub C036DNi		
	bizhub C030DNi		
	bizhub C025DNi		
	ineo+ 360i		
	ineo+ 300i		
	ineo+ 250i		
FAX kit	FK-514	hardware	Delivered by original box.
Firmware	AA2J0Y0-F000-G00-45	file (exe) (with digital signature)	Customer engineer (CE) bring.

Table 1-3 Delivery format and method of Guidance

Guidance	Format	Delivery method	other
FULL	file (exe) (with digital signature)	CE brings the exe file. Can get html file by executing the exe file.	Delivery the guidance corresponding to the MFP hardware. (FULL and Security functions). The language (Japanese/English) is upon user's request.
Security Functions		CE brings the exe file. Can get pdf file by executing the exe file.	

1.4.4. Logical Scope for the TOE

TOE security functions and the basic functions are described below.

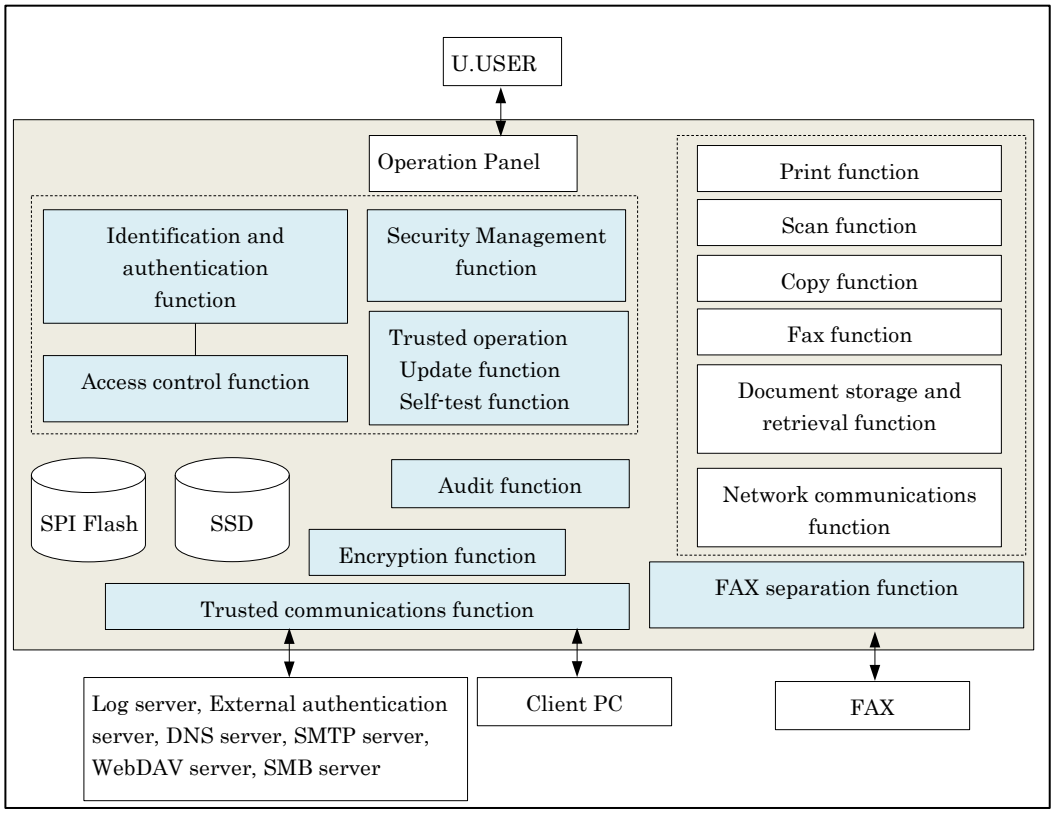


Figure 1-3 Logical scope of the TOE

1.4.4.1. Basic functions

TOE basic functions are described below.

(1) Print function

This function stores temporarily the print data received via LAN by using a printer driver of client PC or WC in the ID & Print user box or the password encrypted PDF user box and prints.

(2) Scan function

This function scans a paper document by user's operation from operation panel and generates a document file and sends (E-mail, WebDAV, SMB).

(3) Copy function

This function scans a paper document by user's operation from operation panel and copies a scanned image.

(4) FAX function

This function sends and receives documents through Public switched telephone network (PSTN) by using standard facsimile protocol.

TOE can accumulate documents and perform Fax TX the accumulated documents. The documents accumulated in the TOE that can perform Fax TX are Fax TX document. Also, Fax RX documents are accumulated in TOE and can print, delete, send (FAX, E-mail,

WebDAV, SMB) and download.

・Fax TX function

Function to send a paper document and Fax TX document to the external fax device from the telephone line. The paper document is scanned by the operation on the panel and performs Fax TX. Fax TX document performs Fax TX by the operation on the panel.

・Fax RX function

Function to receive documents through the telephone line from the external fax.

(5) Document strange and retrieval function

This function stores electronic documents in Personal user box, Memory RX user box and Password Encrypted PDF used box or retrieve the stored electronic documents.

This function can store the electronic documents by scanning a paper document from operation panel, can store the document from the printer driver or WC of a client PC and can store the Fax document by Fax RX function. Stored electronic documents can retrieve from the operation panel and WC.

(6) Network communications function

This function sends and receives documents via local area network (LAN).

1.4.4.2. Security Functions

TOE security functions are described below.

(1) Identification and authentication function

This function verifies a person who intends to use the TOE is the authorized user using identification and authentication information obtained from the user, and to permit the use of the TOE only to a person who is determined to be an authorized user. There are two types of Authentication Method: MFP authentication method that TOE itself identifies and authenticates, and External server authentication method using external authentication server. This function includes the following functions.

- Function to stop the authentication when the number of continuous authentication failures reaches to the setting value.
- Function to display the input password in dummy characters at login.
- Function to register only password that satisfy the condition of minimum character of password, set by administrator for protecting the password quality.
- Function to terminate that session when no operation is performed for a certain period of time (the time set by the administrator) by the user who is identified and authenticated.
- Function to permit the access, only when requesting the password input and verifying the input password and confirm that it is correct password, when accessing the Memory RX user box (except FAX RX).

(2) Access control function

This function restricts the access to the assets in the TOE only to the permitted users.

(3) Encryption function

This function prevents (encrypts) from accessing to the data assets during the communication through LAN. Encryption keys are stored in RAM (volatile memory) and SSD.

(4) Trusted communications function

This function ensures that the communication is performed between known terminations. When communicating with the client PC, SMTP server, external authentication server, DNS server, Log server, WebDAV server and SMB server, this verifies the rightfulness of the connections and protects by encrypting the assets on the network using the Encryption function.

(5) Security management function

This function ensures that the ability to compose the security settings of TOE can be used only by the user with authorized administrator roles.

(6) Audit function

This function records logs of the events related to the TOE use and security with data and time information as a log file and provides it in the auditable form.

The log file is sent to log server by using the trusted communication function and can be viewed by the log server.

(7) Trusted operation function

This function verifies the authenticity of firmware to be updated and confirm that it is the correct one before starting the TOE firmware update, and self-test.

(8) FAX separation function

This function prevents the TOE's fax I/F to be used for creating a network bridge between the PSTN that TOE is connected and the network.

1.4.5. Glossary

The meanings of terms used in this ST are defined.

Table 1-4 Glossary

Designation	Definition
Electronic document	Document data that digitized information such as characters and figures.
Paper document	Paper documents with information such as characters and figures.
WC	Web Connection. Function/Interface to operate TOE through Web browser.
Role	Role of U.USER. There are U. NORMAL and U.ADMIN. Moreover, U. ADMIN is divided into U. BUILTIN_ADMIN and U.USER_ADMIN.

Designation	Definition
SMB TX	Function which transmits to a computer and a public folder of server by converting scanned data, and electronic document saved in the TOE, to the available file on the computer.
U. BUILTIN_ADMIN (Built-in administrator)	Role of U.USER. Role given only to the administrator implemented in the TOE beforehand (built-in administrator).
U.USER_ADMIN (User administrator)	Role of U.USER. Role given by the U.ADMIN. Able to operate as this role by being succeed at the login from the interface for U.USER_ADMIN. Same as U. BUILTIN_ADMIN, exceeding the availability of addition and deletion of the role, and the handling at the time of failure.
WebDAV TX	Function which uploads to WebDAV server by converting scanned data, and the electric document saved in the TOE, to the available file on the computer. Also, used for when sending the log to log server.
Customer Engineer	Role of bringing the firmware and supporting the installation of TOE.
System Auto Reset	Function which logs out automatically when there is not access for a period of set time during logging-in.
System Auto Reset Time	Setup time by administrator. It logs out automatically after these time passes. Operation from the panel is an object.
Job	Document processing task which is sent to hard copy device. Single processing task can process more than one document.
Enhanced security settings	Function to set setting which is related to the behavior of the security function, collectively to the secure values and maintain it. When this function is activated, the use of the update function of the TOE through the network, maintenance function (use RS-232C I/F), and the initializing function of the network setting are prohibited, or alert screen is displayed when it is used. The alert screen is displayed when the setting value is changed. Then, Enhanced security settings become invalid if the setting value is changed (only administrator can do).
Session Auto terminate function	Function to terminate session automatically. Terminate the session automatically when no operation is performed for a certain period of time on each of operation panel and WC.
Print job input function	Function that the TOE receives the User ID, the login password and the print data which are sent from client PC. Only when the identification and authentication of User ID and login password succeeded, the print data are received.
User box	Directory to store documents. Stored documents include the accumulated documents, and documents included in the executing job.

Designation	Definition
	User who can save documents and operate, is different according to a user box.
User box password	Password set for Memory RX user box
User ID (User ID)	Identification that is given to a user. The TOE specified a user by that identification. At the external server authentication, this is composed of User ID + External server ID. On the interface such as operation panel, it is displayed as “User Name”.
Temporary suspension and Release of User ID	Temporary suspension: to temporarily suspend the login of the considered User ID. Release: to release the temporary suspension.
User management function	Function to perform registration / deletion of user and addition / deletion / change of the access authority. Addition / deletion of role (U.USER_ADMIN) * Access authority: Authority to access the information related to documents and document process.
Management function of User Authentication	Function which sets authentication methods. (MFP authentication/External server authentication)
User authentication function	Function to authenticate TOE users. There are two types. MFP authentication (Internally authentication) and External server authentication (Externally authentication). U. BUILTIN_ADMIN is authenticated only by MFP authentication.
Login	To identify and authenticate on the TOE by user ID and login password.
Login Password (LOGIN PASSWORD)	Password for logging in the TOE
External sever authentication setting data	Setting data related to the external authentication server. (Including domain name which external server belongs to)
Audit log management function	Function as follows. ・Set the accumulated amount of audit log ・Set the TX date and time of audit log 監査ログの送信日時の設定 ・Send audit log ・Delete audit log
Audit log function	Function to obtain audit logs.
Operation prohibition release time of Administrator authentication	Time until a lock is released, when the number of continuous authentication failure is reached to the settings and the authentication of U. BUILTIN_ADMINISTRATOR is locked.
Trusted Channel Management Function	Function to perform Trust Channel function, and to manage cryptographic method
Trusted communication function	Function to protect transmitting data via LAN by encryption.
Time information	Information of time. When any event occurred, the time information is recorded on audit log.
Auto logout time	Times set by administrator. Automatically logs out after the setting time. Web Connection is an object.

Designation	Definition
Accumulated document	Documents for storing and retrieving
ID & Print function (AUTH PRINT)	Function to save the document which has user name and password which is sent from PC on the network as the directed print document.
Authentication Failure Frequency Threshold	Threshold that administrator sets. Authentication function is locked when number of continuous authentication failure reached this threshold.

1.4.6. User Box

This paragraph describes the user box that the TOE provides. The TOE provides the following types of User box. (This is categorized base on the characteristic of user box, but this does not necessarily match to the display on the operation panel. Also, Bulletin Board User Box, etc., exists other than this, but except the types of user box described here, cannot be used.)

Table 1-5 System User Box

User box Type	Description
Memory RX user box	User box using for Fax function and Document storage and retrieval function. U. ADMIN preforms Memory RX setting. Password is set by U.ADMIN. The following operations are available on the documents stored in this user box. U. ADMIN ・Delete U. NORMAL who knows the password. ・Print ・Change document name ・Download ・Preview ・Delete
Password Encrypted PDF user box	User box that stores the encrypted PDF (PDF file that requires inputting password when it opened.) By specifying the document and inputting the password, the document can be printed. Used for Print function and Document storage and retrieval function.
ID & Print user box	User box that stores documents by ID & Print function. The ID & Print function is the print function that user sends print data including credentials from the printer driver or WC of the client PC and the TOE temporarily stores it in the ID & Print user box and then, user prints by logging in from the operation panel.

Table 1-6 Function user box

User box Type	
Personal user box	User box using for Fax function and Document storage and retrieval function. U. ADMIN and the owner of the corresponding user box (user logging in by User ID that match to the corresponding user box's Box User ID) can operate. The following operations are available on the documents stored in this user box. U. ADMIN ・Delete ・Change of owner of the document in the corresponding user box by changing the user box owner.

User box Type	
	Owner of the user box ・Modify ・Print ・Fax TX ・Delete ・Copy/Move to the same user box by the owner ・E-mail TX ・WebDAV TX ・SMB TX ・Download ・Preview ・Change of owner of the document in the corresponding user box by changing the user box owner

2. Conformance Claims

2.1. CC Conformance Claims

This ST conforms to the following Common Criteria (hereinafter referred to as “CC”).

CC version	:	Version 3.1 Release 5
CC conformance	:	CC Part 2 (CCMB-2017-04-002) extended, CC Part 3 (CCMB-2017-04-003) conformant

2.2. PP Claim

This ST conforms to the following PP.

PP Name	:	Protection Profile for Hardcopy Devices
PP Version	:	1.0 dated September 10, 2015
Errata	:	Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.3. PP Conformance Rationale

This satisfies the following conditions required by PP and is "Exact Conformance" as required by PP. Therefore, the TOE type is consistent with PP

・Required Uses
Printing, Scanning, Copying, Network communications, Administration

・Conditionally Mandatory Uses
PSTN faxing, Storage and retrieval

・Optional Uses
None

3. Security Problem Definition

3.1. Users

The user roles in the TOE are as follows.

Table 3-1 User Categories

Designation			Definition
U.USER (Authorized user)			Any identified and authenticated User.
	U. NORMAL (Normal User)		A User who has been identified and authenticated and does not have an administrative role
	U. ADMIN (Administrator)	U. BUILTIN_ADMIN (built-in administrator)	A User who has been identified and authenticated and has an administrative role
		U.USER_ADMIN (User administrator)	

*Refer to 1.4.5 Glossary about U. BUILTIN_ADMIN and U.USER_ADMIN

3.2. Assets

The assets in the TOE are as follows.

Table 3-2 Asset categories

Designation	Asset category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

3.2.1. User Data

User Data is composed from the following two types.

Table 3-3 User Data types

Designation	User Data type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

3.2.2. TSF Data

TSF Data is composed from the following two types.

Table 3-4 TSF Data types

Designation	User Data type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3. Threat Definitions

Threats are defined by a threat agent that performs an action resulting in an outcome that has the potential to violate TOE security policies.

Table 3-5 Threats

Designation	Definition
T. UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T. UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4. Organizational Security Policy Definitions

OSPs that TOE realizes is as follows.

Table 3-6 Organizational Security Policies

Designation	Definition
P. AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P. AUDIT	Security-relevant activities must be audited, and the log of such actions must be protected and transmitted to an External IT Entity.
P. COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

3.5. Assumption Definitions

Assumptions are conditions that must be satisfied in order to the Security Objectives and functional requirements to be effective.

Table 3-7 Assumptions

Designation	Definition
A. PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A. NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A. TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A. TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4. Security Objectives

4.1. Definitions of Security Objectives for the Operational Environment

Table 4-1 Security Objectives for the Operational Environment

Designation	Definition
OE. PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE. NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE. ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE. ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

5. Extended Components Definition

This ST defines the following extended components. These are a part of extended components defined by PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015, Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017).

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

Family Behavior:

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

Component leveling:

FAU_STG_EXT.1: Extended: External Audit Trail Storage	1

FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management:

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

- The TSF shall have the ability to configure the cryptographic functionality.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

Rationale:

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.2. FCS_CKM_EXT Extended: Cryptographic Key Management

Family Behavior:

This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

Component leveling:

FCS_CKM_EXT.4: Extended: Cryptographic Key Material	4

FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

Rationale:

Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

This extended component protects the cryptographic key and key materials against exposure,

and it is therefore placed in the FCS class with a single component.

5.3. FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family Behavior:

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

Component leveling:

FCS_RBG_EXT.1 Extended: Random Bit Generation	1

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security strength table for hash functions”, of the keys and hashes that it will generate.

Rationale:

Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.4. FIA_PMG_EXT Extended: Password Management

Family Behavior:

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component leveling:

FIA_PMG _EXT.1 Extended: Password Management	1

FIA_PMG _EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FIA_PMG _EXT.1 Extended: Password management

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG _EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper- and lower-case letters, numbers, and the following special characters: [selection: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")",* [assignment: *other characters*]];
- Minimum password length shall be settable by an Administrator and have the capability to require passwords of 15 characters or greater.

Rationale:

Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.5. FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

Component leveling:

FPT_SKP_EXT.1 Extended: Protection of TSF Data	1

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is

included in the PP/ST:

・There are no auditable events foreseen.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Rationale:

Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

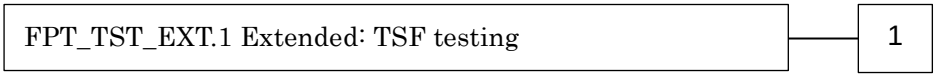
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.6. FPT_TST_EXT.1 Extended: TSF testing

Family Behavior:

This family addresses the requirements for self-testing the TSF for selected correct operation.

Component leveling:



FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF

Rationale:

TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.7. FPT_TUD_EXT Extended: Trusted Update

Family Behavior:

This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

Component leveling:

FPT_TUD_EXT.1 Extended: Trusted Update	1

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)].

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] prior to installing those updates.

Rationale:

Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.8. FDP_FXS_EXT Extended: Fax Separation

Family Behavior:

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

Component leveling:

FDP_FXS_EXT.1 Extended: Fax Separation	1

FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・There are no auditable events foreseen.

FDP_FXS_EXT.1 Extended: Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

Rationale:

Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.

This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

5.9. FCS_IPSEC_EXT Extended: IPsec selected

Family Behavior:

This family addresses requirements for protecting communications using IPsec.

Component leveling:

FCS_IPSEC_EXT.1 Extended: IPsec selected	1

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management:

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

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

・Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; *IKEv2 as defined in RFCs 5996* [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2*.23], and [selection: no other RFCs for hash functions, *RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on [selection: number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]; IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*, [assignment: *other DH groups that are implemented by the TOE], no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys

Rationale:

IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.10. FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family Behavior:

This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

Component leveling:

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	1

FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates.

Management:

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

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [selection: [assignment: *other supported lengths], no other length*hs];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].

Rationale:

Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

6. Security Requirements

6.1. Security Functional Requirements

In this chapter, the TOE security functional requirements for achieving the security objectives specified in Chapter 4.1 are described. This quoted from the security functional requirements specified in the CC Part 2. The security functional requirements which are not specified in the CC Part 2 are quoted from the extended security functional requirements specified in the PP (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015, Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017).

<Method of specifying security functional requirement "Operation">

"Bold" indicates parts of an SFR completed or refined in [PP] and are related to the original SFR definition or extended component definition in Common Criteria Part 2.

"Italic" indicates parts that is necessary to select and/or complete in ST and it is selected and/or completed in [ST].

"Bold" and "Italic" indicate parts of an SFR completed or refined in [PP] and are related to the original SFR definition or extended component definition in Common Criteria Part 2. These are also selected and/or completed in the ST.

SFR component with a character in the parentheses such as (a), (b) etc. means that it is used repeatedly. Extended components are identified by adding "_EXT" to the SFR identification.

6.1.1. Mandatory Requirements

6.1.1.1. Class FAU: Security Audit

FAU_GEN.1	**Audit data generation**		
(for O. AUDIT)			
	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) **All auditable events specified in Table 6-1,**[assignment: *other specifically defined auditable events*].		
	[assignment: *other specifically defined auditable 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 PP/ST, **additional information specified in Table 6-1,** [assignment: *other audit relevant information*].

Table 6-1 Auditable Events

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

[assignment: *other audit relevant information*]

None

FAU_GEN.2	**User identity association**		
(for O. AUDIT)			
	Hierarchical to	:	No other components.
	Dependencies	:	FAU_GEN.1 Audit data generation
			FIA_UID.1 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.		

FAU_STG_EXT.1	**Extended: External Audit Trail Storage**		
(for O. AUDIT)			
	Hierarchical to	:	No other components.
	Dependencies	:	FAU_GEN.1 Audit data generation, FTP_ITC.1 Inter-TSF trusted channel.
FAU_STG_EXT.1.1	The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.		

6.1.1.2. Class FCS: Cryptographic Support

FCS_CKM.1(a)	**Cryptographic Key Generation (for asymmetric keys)**
(for O. COMMS_PROTECTION)	

	Hierarchical to	:	No other components.
	Dependencies	:	[~~FCS_CKM.2 Cryptographic key distribution, or~~ FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)] FCS_COP.1(i) Cryptographic operation (Key Transport)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_CKM.1.1(a)	**Refinement**: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [selection:** ・ ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*** ・ ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ・ ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes*** **] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**		
	[selection: ・ ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*** ・ ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ・ ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***] ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***		

FCS_CKM.1(b)	**Cryptographic Key Generation (Symmetric Keys)**		
(for O. COMMS_PROTECTION, O. STORAGE_ENCRYPTION)			
	Hierarchical to	:	No other components.
	Dependencies	:	[~~FCS_CKM.2 Cryptographic key distribution, or~~ FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption) FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption) FCS_COP.1(e) Cryptographic Operation (Key Wrapping) FCS_COP.1(f) Cryptographic operation (Key Encryption)] FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FCS_CKM.1.1(b)	**Refinement:** The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [selection: *128 bit, 256 bit*] that meet the following: No Standard.**		
	[selection: *128 bit, 256 bit*] ***128 bit, 256 bit***		

FCS_CKM_EXT.4	**Extended: Cryptographic Key Material Destruction**		
(for O. COMMS_PROTECTION, O. STORAGE_ENCRYPTION, O. PURGE_DATA)			
	Hierarchical to	:	No other components.
	Dependencies	:	[FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction
FCS_CKM_EXT.4.1	The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.		

FCS_CKM.4	**Cryptographic key destruction**		
(for O. COMMS_PROTECTION, O. STORAGE_ENCRYPTION, O. PURGE_DATA)			
	Hierarchical to	:	No other components.
	Dependencies	:	[FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or

			FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
FCS_CKM.4.1	**Refinement:** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection**: ***For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].*** ***For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;***] that meets the following: [**selection:** ***NIST SP800-88, no standard***].		
	[**selection**: ***For volatile memory, the destruction shall be executed by [selection: powering off a device,[assignment: other mechanism that ensures keys are destroyed]].*** ***For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;***] ***For volatile memory, the destruction shall be executed by [selection: powering off a device,[assignment: other mechanism that ensures keys are destroyed]].*** ***For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;***		
	[selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]] ***powering off a device***		
	[assignment: other mechanism that ensures keys are destroyed] ***メモリの解放 Free of memory***		
	[selection: single, three or more times] ***single***		
	[selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern] ***a static pattern***		
	[selection: read-verify, none] ***none***		
	[**selection:** ***NIST SP800-88, no standard***] ***no standard***		

FCS_COP.1(a)	**Cryptographic Operation (Symmetric encryption/decryption)**

(for O.COMMS_PROTECTION)			
	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(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(a)	**Refinement**: The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [assignment: *one or more modes*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following: **・ FIPS PUB 197, "Advanced Encryption Standard (AES)"** **・ [Selection: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*]**		
	[assignment: *one or more modes*] ***CBC***		
	[Selection: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*] ***NIST SP 800-38A***		

FCS_COP.1(b)	**Cryptographic Operation (for signature generation/verification)**		
(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)			
	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.1(a) Cryptographic Key Generation (for asymmetric keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(b)	**Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a [selection: ***・ Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment:2048 bits or greater],*** ***・ RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*** ***・ Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*** that meets the following **[selection:** ***Case: Digital Signature Algorithm*** ***・ FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: RSA Digital Signature Algorithm*** ***・ FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: Elliptic Curve Digital Signature Algorithm*** ***・ FIPS PUB 186-4, "Digital Signature Standard"***		

	・The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").]
	[selection: *・Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment:2048 bits or greater],* *・RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or* *・Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]* *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]*
	[assignment: 2048 bits or greater] *2048 bits, 3072bits*
	[selection: *Case: Digital Signature Algorithm* *・FIPS PUB 186-4, "Digital Signature Standard"* *Case: RSA Digital Signature Algorithm* *・FIPS PUB 186-4, "Digital Signature Standard"* *Case: Elliptic Curve Digital Signature Algorithm* *・FIPS PUB 186-4, "Digital Signature Standard"* *・The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").*] *FIPS PUB 186-4, "Digital Signature Standard"*

FCS_RBG_EXT.1	**Extended: Cryptographic Operation (Random Bit Generation)**		
(for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)			
	Hierarchical to	:	No other components.
	Dependencies	:	No dependencies.
FCS_RBG_EXT.1.1	The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].		
	[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] *NIST SP 800-90A*		
	[selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*] *CTR_DRBG (AES)*		
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: *number of software-based*		

	sources] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.
	[selection: [assignment: *number of software-based sources*] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)] [assignment: *number of software-based sources*] software-based noise source(s)
	[assignment: *number of software-based sources*] *one software-based source*
	[selection: *128 bits, 256 bits*] *256 bits*

6.1.1.3. Class FDP: User Data Protection

FDP_ACC.1	**Subset access control**		
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)			
	Hierarchical to	:	No other components.
	Dependencies	:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	**Refinement:** The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 6-2 D.USER.DOC** Access Control SFP **and Table 6-3 D.USER.JOB** Access Control SFP**.**		

FDP_ACF.1	**Security attribute based access control**		
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)			
	Hierarchical to	:	No other components.
	Dependencies	:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	**Refinement:** The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 6-2 D.USER.DOC** Access Control SFP **and Table 6-3 D.USER.JOB** Access Control SFP**.**		
FDP_ACF.1.2	**Refinement:** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 6-2 D.USER.DOC*** Access Control SFP ***and Table 6-3 D.USER.JOB*** Access Control SFP.		
FDP_ACF.1.3	**Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*].		
	[assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*] *None*		

FDP_ACF.1.4	**Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*].
	[assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*] *None*

Table 6-2 D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	***Operation :***	***Submit a document to be printed***	***View image or Release printed output***	***Modify stored document***	***Delete stored document***
	Job owner	(note 1)	permitted	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Scan	***Operation :***	***Submit a document for scanning***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	denied	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	***Operation :***	***Submit a document for copying***	***View scanned image or Release printed copy output***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	permitted	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	***Operation :***	***Submit a document to send as a fax***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	denied	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	***Operation:***	***Receive a fax and store it***	***View fax image or Release printed fax output***	***Modify image of received fax***	***Delete image of received fax***
	Fax owner	(note 3)	permitted	permitted	(注 1)
	U.ADMIN	(note 4)	denied	denied	(注 1)
	U.NORMAL	(note 4)	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Storage/ retrieval	***Operation :***	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***
	Job owner	(note 1)	permitted	permitted	permitted
	U.ADMIN	permitted	denied	denied	permitted

	U.NORMAL	permitted	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied

Table 6-3 D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	*Operation :*	*Create print job*	*View print queue / log*	*Modify print job*	*Cancel print job*
	Job owner	(note 1)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	denied	denied
Scan	*Operation :*	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	(note 2)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	denied	denied
Copy	*Operation :*	*Create copy job*	*View copy status / log*	*Modify copy job*	*Cancel copy job*
	Job owner	(note 2)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	denied	denied
Fax send	*Operation:*	*Create fax send job*	*View fax job queue / log*	*Modify fax send job*	*Cancel fax send job*
	Job owner	(note 2)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	denied	denied
Fax receive	*Operation:*	*Create fax receive job*	*View fax receive status / log*	*Modify fax receive job*	*Cancel fax receive job*
	Fax owner	(note 3)	permitted	denied	permitted
	U.ADMIN	(note 4)	permitted	denied	permitted
	U.NORMAL	(note 4)	permitted	denied	denied
	Unauthenticated	(condition 1)	permitted	denied	denied
Storage / retrieval	*Operation :*	*Create storage / retrieval job*	*View storage / retrieval log*	*Modify storage / retrieval job*	*Cancel storage / retrieval job*
	Job owner	(note 1)	permitted	denied	permitted
	U.ADMIN	permitted	permitted	denied	permitted
	U.NORMAL	permitted	permitted	denied	denied
	Unauthenticated	(condition 1)	permitted	denied	denied

Condition 1: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.

Note 1: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.

Note 2: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.

Note 3: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.

Note 4: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.

Table 6-4 Supplement of Table 6-2 and Table 6-3

Item	Description
Note 1	A fax received document is saved as a stored document in the Memory RX user box or the specified user box (Personal user box). U.ADMIN is possible for canceling a job being received, and by canceling it, documents before saving (documents being received) are also deleted. U.ADMIN or the Fax owner who executed the print job are allowed to cancel the print job of the fax received document. Fax owner and U.ADMIN can delete fax received documents.

6.1.1.4. Class FIA: Identification and Authentication

FIA_AFL.1	**Authentication failure handling**		
(for O.USER_I&A)			
	Hierarchical to	:	No other components.
	Dependencies	:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].		
	[selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] *an administrator configurable positive integer within*[assignment: *range of acceptable values*]		
	[assignment: *range of acceptable values*] *1～3*		
	[assignment: *list of authentication events*] *Authentication of login password in MFP authentication* *Authentication of user box password*		
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *list of actions*].		
	[selection: *met, surpassed*] *met, surpassed*		
	[assignment: *list of actions*] *Suspend authentication by login password*		

	Suspend authentication by user box password *＜Operation for recovering the normal condition＞* *Authentication of U.BUILTIN_ADMIN: Perform the boot process of the TOE. (Release process is performed after time set in the release time setting of operation prohibition for Administrator authentication passed by the boot process.)* *Other (include U.USER_ADMIN): Execute the delete function of authentication failure frequency by U.ADMIN, who is not in the authentication stopped state.*

FIA_ATD.1	**User attribute definition**		
(for O.USER_AUTHORIZATION)			
	Hierarchical to	:	No other components.
	Dependencies	:	No dependencies
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].		
	[assignment: *list of security attributes*]. *User ID* *Role* *Access authority*		

FIA_PMG_EXT.1	**Extended: Password Management**		
(for O.USER_I&A)			
	Hierarchical to	:	No other components.
	Dependencies	:	No dependencies
FIA_PMG_EXT.1.1	The TSF shall provide the following password management capabilities for User passwords: ・Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: *other characters*]]; ・Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;		
	[selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: *other characters*]] “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” [assignment: *other characters*] *“-”, “¥”, “[”, “]”, “:”, “;”, “,”, “.”, “/“, “”, “=”, “~”, “|”, “^”, “{”, “}”, “+”, “<”, “>“, “?”, “_” and space*		

FIA_UAU.1	**Timing of authentication**		
(for O.USER_I&A)			
	Hierarchical to	:	No other components.

	Dependencies	:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	**Refinement:** The TSF shall allow [assignment: *list of TSF mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is authenticated.		
	[assignment: *list of TSF mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] ***Confirm the suspended state of user's use in MFP authentication*** ***Receive Fax*** ***Set the TOE status confirmation and display, etc.*** ***Inquire of the Firmware version from the operation panel***		
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.		

FIA_UAU.7	**Protected authentication feedback**		
(for O.USER_I&A)			
	Hierarchical to	:	No other components.
	Dependencies	:	FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.		
	[assignment: *list of feedback*] *Display "*" or "●" every character data input.*		

FIA_UID.1	**Timing of identification**		
(for O.USER_I&A and O.ADMIN_ROLES)			
	Hierarchical to	:	No other components.
	Dependencies	:	No dependencies
FIA_UID.1.1	**Refinement:** The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is identified.		
	[assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] ***Confirm the suspended state of user's use in MFP authentication*** ***Receive Fax*** ***Set the TOE status confirmation and display, etc.*** ***Inquire of the Firmware version from the operation panel***		
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.		

FIA_USB.1	**User-subject binding**		
(for O.USER_I&A)			
	Hierarchical to	:	No other components.
	Dependencies	:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].		
	[assignment: *list of user security attributes*]. *User ID* *Role* *Access authority*		
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].		
	[assignment: *rules for the initial association of attributes*] *None*		
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].		
	[assignment: *rules for the changing of attributes*] *None*		

6.1.1.5. Class FMT: Security Management

FMT_MOF.1	**Management of security functions behaviour**		
(for O.ADMIN_ROLES)			
	Hierarchical to	:	No other components.
	Dependencies	:	FMT_SMR.1 Security roles
			FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	**Refinement:** The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to **U.ADMIN**.		
	[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] *modify the behaviour of*		
	[assignment: *list of functions*] - Enhanced Security Setting - User Authentication function - Audit Log function - Trusted Channel function		

FMT_MSA.1	**Management of security attributes**		
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)			
	Hierarchical to	:	No other components.

	Dependencies	:	[FDP_ACC.1 Subset access control, ~~or~~ ~~FDP_IFC.1 Subset information flow control]~~ FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	**Refinement:** The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].		
	[selection: *change_default, query, modify, delete, [assignment: other operations]*] *Refer to Table 6-5,Table 6-6*		
	[assignment: *list of security attributes*] *Refer to Table 6-5,Table 6-6*		
	[assignment: *the authorized identified roles*] *Refer to Table 6-5,Table 6-6*		

Table 6-5 Management of Object Security Attribute

Object Security Attribute	Authorized Identified Roles	Operations
User ID of Personal user box	Owner of the corresponding user box U.ADMIN	Modify Create

Table 6-6 Management of Subject Security Attribute

Subject Security Attribute	Authorized Identified Roles	Operations
User ID	U.ADMIN	Create Delete Suspend temporarily / Release of temporary suspension
Role （U.USER_ADMIN）	U.ADMIN	Delete Add
Access authority	U.ADMIN	Delete Add

FMT_MSA.3	**Static attribute initialisation**		
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)			
	Hierarchical t	:	No other components.
	Dependencies:	:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	**Refinement:** The TSF shall enforce the **User Data Access Control SFP** to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.		
	[selection, choose one of: *restrictive, permissive, [assignment: other property]*] *[assignment: other property]*		

	refer to Table 6-7
FMT_MSA.3.2	**Refinement:** The TSF shall allow the **[selection: *U.ADMIN, no role*]** to specify alternative initial values to override the default values when an object or information is created.
	[selection: *U.ADMIN, no role*] ***no role***

Table 6-7 Characteristics Static Attribute Initialization

Object		Attribute	Default values for Object Security Attribute
Print	D.USER.DOC	Job owner	identified by a credential or assigned to an authorized User as part of the process of submitting a print Job
Scan	D.USER.DOC	Job owner	authorized User as part of the process of initiating a scan job
Copy	D.USER.DOC	Job owner	authorized User as part of the process of initiating a copy job
Fax send	D.USER.DOC	Job owner	authorized User as part of the process of initiating a fax send job
Fax receive	D.USER.DOC	Fax owner	U.NORMAL who knows the password of the corresponding user box, when the destination of the object is the Memory RX user box. Owner of the corresponding user box when it is the Personal user box.
Storage / retrieval	D.USER.DOC	Job owner	U.NORMAL who knows the password of the corresponding user box, when the destination of the object is the Memory RX user box. Owner of the corresponding user box when it is the Personal user box.
Print	D.USER.Job	Job owner	identified by a credential or assigned to an authorized User as part of the process of submitting a print Job
Scan	D.USER.Job	Job owner	authorized User as part of the process of initiating a scan job
Copy	D.USER.Job	Job owner	authorized User as part of the process of initiating a copy job
Fax send	D.USER.Job	Job owner	authorized User as part of the process of initiating a fax send job
Fax receive	D.USER.Job	Fax owner	U.NORMAL who knows the password of the corresponding user box, when the destination of the object is the Memory RX user box. Owner of the corresponding user box when it is the Personal user box.
Storage / retrieval	D.USER.Job	Job owner	authorized User as part of the process of initiating a storage job

FMT_MTD.1	**Management of TSF data**		
(for O.ACCESS CONTROL)			
	Hierarchical to	:	No other components.
	Dependencies:	:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	**Refinement:** The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 6-8.**		

Table 6-8 Management of TSF Data

Data	Operation	Authorised role(s)
[assignment: *list of TSF Data* ***owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear,* [assignment: *other operations*]]	**U.ADMIN, the owning U.NORMAL.**
Login password of U.NORMAL	[assignment: *other operations*] *register*	**U.ADMIN**
	modify	**U.ADMIN, the owning U.NORMAL**
User box password	[assignment: *other operations*] *register*	**U.ADMIN**
	modify	
[assignment: *list of TSF Data* ***not owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	**U.ADMIN**
Login password of U.BUILTIN_ADMIN	*modify*	**U.BUILTIN_ADMIN**
Time Information	*modify*	**U.ADMIN**
System auto reset time	*modify*	
Auto logout time	*modify*	
Authentication Failure Frequency Threshold	*modify*	
Number of Authentication Failure (except U.BUILTIN_ADMIN)	*clear*	
Password rule	*modify*	
External server authentication setting data	*modify* [assignment: *other operations*] *register*	
Release time of operation prohibition for Administrator authentication	*modify*	
Network settings	*modify* [assignment: *other operations*] *register*	
[assignment: ***list of software,***	[selection: *change default, query,*	**U.ADMIN**

Data	Operation	Authorised role(s)
firmware, and related configuration data]	*modify, delete, clear*, [assignment: *other operations*]]	
TOE software/ firmware update data (software/firmware to be updated, configuration data related to update)	*modify*	**U.ADMIN**

FMT_SMF.1	**Specification of Management Functions**		
(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: *list of management functions provided by the TSF*].		
	[assignment: *list of management functions provided by the TSF*] *refer to Table 6-9*		

Table 6-9 list of management functions

management functions
Management function of Enhanced Security Setting by U.ADMIN
User management function by U.ADMIN
Management function of User Authentication function by U.ADMIN
Registration and Modification function of External server authentication setting data by U.ADMIN
Trusted Channel management function by U.ADMIN
Registration and Modification function of Network by U.ADMIN
Modification function of date and time information by U.ADMIN
Audit log management function by U.ADMIN
Modification function of system auto reset time by U.ADMIN
Modification function of auto logout time by U.ADMIN
Modification function of release time of operation prohibition of administrator authentication by U.ADMIN
Modification function of Password policy by U.ADMIN
Modification function of Authentication failure frequency threshold by U.ADMIN
Clear function of Authentication failure frequency (except U.BUILTIN_ADMIN) by U.ADMIN
User box management function by U.NORMAL
User box management function by U.ADMIN
Modification function of one's own login password by U.NORMAL
Modification function of one's own login password by U.BUILTIN_ADMIN

FMT_SMR.1	**Security roles**		
(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)			
	Hierarchical to	:	No other components.

	Dependencies:	:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	**Refinement:** The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.		
FMT_SMR.1.2	The TSF shall be able to associate users with roles.		

6.1.1.6. Class FPT: Protection of the TSF

FPT_SKP_EXT.1	**Extended: Protection of TSF Data**		
(for O.COMMS_PROTECTION)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.		

FPT_STM.1	**Reliable time stamps**		
(for O.AUDIT)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies
FPT_STM.1.1	TSF shall be able to provide reliable time stamps.		

FPT_TST_EXT.1	**Extended: TSF testing**		
(for O.TSF_SELF_TEST)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies
FPT_TST_EXT.1.1	The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.		

FPT_TUD_EXT.1	**Extended: Trusted Update**		
(for O.UPDATE_VERIFICATION)			
	Hierarchical to	:	No other components.
	Dependencies:	:	FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
FPT_TUD_EXT.1.1	The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.		
FPT_TUD_EXT.1.2	The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.		
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] prior to installing those updates.		
	[selection: *published hash, no other functions*]		

	no other functions

6.1.1.7. Class FTA: TOE Access

FTA_SSL.3	**TSF-initiated termination**		
(for O.USER_I&A)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].		
	[assignment: *time interval of user inactivity*] *- Time determined by the System auto reset time in case of operation panel* *- Time determined by auto logout time in case of WC* *- No interactive session in case of printer driver or fax*		

6.1.1.8. Class FTP: Trusted Path/Cannels

FTP_ITC.1	**Inter-TSF trusted channel**		
(for O.COMMS_PROTECTION, O.AUDIT)			
	Hierarchical to	:	No other components.
	Dependencies:	:	[FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_ITC.1.1	**Refinement:** The TSF shall **use [selection: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection: *authentication server, [assignment: other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.		
	[selection: *IPsec, SSH, TLS, TLS/HTTPS*] *IPsec*		
	[selection: *authentication server, [assignment: other capabilities]*] *authentication server, [assignment: other capabilities]*		
	[assignment: other capabilities] *SMTP server* *DNS server* *SMB server* *Log server* *WebDAV server*		
FTP_ITC.1.2	**Refinement:** The TSF shall permit **the TSF**, **or the authorized IT entities**, to initiate communication via the trusted channel		
FTP_ITC.1.3	**Refinement:** The TSF shall initiate communication via the trusted channel for		

	[assignment: ***list of services for which the TSF is able to initiate communications***].
	[assignment: ***list of services for which the TSF is able to initiate communications***]. ***External server authentication*** ***Communication with the SMTP server*** ***Communication with the DNS server*** ***Communication with the SMB server*** ***Communication with the Log server*** ***Communication with the WebDAV server***

FTP_TRP.1(a)	**Trusted path (for Administrators)**		
(for O.COMMS_PROTECTION)			
	Hierarchical to	:	No other components.
	Dependencies:	:	[FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_TRP.1.1(a)	**Refinement**: The TSF shall **use** [**selection, choose at least one of:** ***IPsec, SSH, TLS, TLS/HTTPS***] **to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.		
	[**selection, choose at least one of:** ***IPsec, SSH, TLS, TLS/HTTPS***] ***IPsec***		
FTP_TRP.1.2(a)	**Refinement**: The TSF shall permit **remote administrators** to initiate communication via the trusted path		
FTP_TRP.1.3(a)	**Refinement:** The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.		

FTP_TRP.1(b)	**Trusted path (for Non-administrators)**		
(for O.COMMS_PROTECTION)			
	Hierarchical to	:	No other components.
	Dependencies:	:	[FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_TRP.1.1(b)	**Refinement** : The TSF shall **use** [**selection, choose at least one of:** ***IPsec, SSH, TLS, TLS/HTTPS***] **to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.		
	[**selection, choose at least one of:** ***IPsec, SSH, TLS, TLS/HTTPS***] ***IPsec***		

FTP_TRP.1.2(b)	**Refinement**: The TSF shall permit [selection: ***the TSF, remote users***] to initiate communication via the trusted path
	[selection: ***the TSF, remote users***] ***remote users***
FTP_TRP.1.3(b)	**Refinement**: The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

6.1.2. Conditionally Mandatory Requirements

6.1.2.1. PSTN Fax-Network Separation

FDP_FXS_EXT.1	**Extended: Fax separation**		
(for O.FAX_NET_SEPARATION)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies
FDP_FXS_EXT.1.1	The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.		

6.1.3. Selection-based Requirements

6.1.3.1. Protected Communications

FCS_IPSEC_EXT.1	**Extended: IPsec selected**		
(selected in FTP_ITC.1.1, FTP_TRP.1.1)			
	Hierarchical to	:	No other components.
	Dependencies :	:	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption) FCS_COP.1(b) Cryptographic Operation (for signature generation/verification) FCS_COP.1(c) Cryptographic Operation (Hash Algorithm) FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FCS_IPSEC_EXT.1.1	The TSF shall implement the IPsec architecture as specified in RFC 4301.		
FCS_IPSEC_EXT.1.2	The TSF shall implement [selection: *tunnel mode, transport mode*].		
	[selection: *tunnel mode, transport mode*] *transport mode*		
FCS_IPSEC_EXT.1.3	The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.		

FCS_IPSEC_EXT.1.4	The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].
	[selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*] *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC* *AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC*
FCS_IPSEC_EXT.1.5	The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], *and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; *IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307 [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23], and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].
	[selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], *and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; *IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307 [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23], and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]] *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109,* [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]
	[selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*] *RFC 4304 for extended sequence numbers*
	[selection: *no other RFCs for hash functions, RFC 4868 for hash functions*] *RFC 4868 for hash functions*
FCS_IPSEC_EXT.1.6	The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].
	[selection: *IKEv1, IKEv2*] ***IKEv1***

	[selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*] *no other algorithm*
FCS_IPSEC_EXT.1.7 FCS_IPSEC_EXT.1.8	The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode. The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; *IKEv1 SA lifetimes can be established based on* [selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].
	[selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; *IKEv1 SA lifetimes can be established based on* [selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]] *IKEv1 SA lifetimes can be established based on* [selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]
	[selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*] *length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*
FCS_IPSEC_EXT.1.9	The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)),* [assignment: *other DH groups that are implemented by the TOE], no other DH groups*].
	[selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 5 (1536-bit MODP),* [assignment: *other DH groups that are implemented by the TOE], no other DH groups*] *no other DH groups*
FCS_IPSEC_EXT.1.10	The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys.
	[selection: *RSA, ECDSA*] *RSA*

FCS_COP.1(g)	**Cryptographic Operation (for keyed-hash message authentication)**		
(selected with FCS_IPSEC_EXT.1.4)			
	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(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g)	**Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-**[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***], **key size** [assignment: **key size (in bits) used in HMAC**], **and message digest sizes [selection:** ***160, 224, 256, 384, 512***] **bits** that meet the following: "**FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**
	[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***] ***SHA-1*** ***SHA-256*** ***SHA-384*** ***SHA-512***
	[assignment: **key size (in bits) used in HMAC**] *160~512bits*
	[selection: ***160, 224, 256, 384, 512***] ***160*** ***256*** ***384*** ***512***

FIA_PSK_EXT.1	**Extended: Pre-Shared Key Composition**		
(selected with FCS_IPSEC_EXT.1.4)			
	Hierarchical to	:	No other components.
	Dependencies:	:	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FIA_PSK_EXT.1.1	The TSF shall be able to use pre-shared keys for IPsec.		
FIA_PSK_EXT.1.2	The TSF shall be able to accept text-based pre-shared keys that are: 22 characters in length and [selection: [assignment: *other supported lengths*]*, no other lengths*]; composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").		
	[selection: [assignment: *other supported lengths*]*, no other lengths*] [assignment: *other supported lengths*]		
	[assignment: *other supported lengths*] *2~128 characters*		
FIA_PSK_EXT.1.3	The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].		
	[selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] *SHA-1* *SHA-256* *SHA-512* [assignment: *method of conditioning text string*]		

	[assignment: *method of conditioning text string*] *SHA-384*
	[selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*] *use no other pre-shared keys*

6.1.3.2. Trusted Update

FCS_COP.1(c)	**Cryptographic operation (Hash Algorithm)**		
(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)			
	Hierarchical to	:	No other components.
	Dependencies:	:	No dependencies.
FCS_COP.1.1(c)	**Refinement**: The TSF shall perform **cryptographic hashing services** in accordance with [selection: ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].		
	[selection: ***SHA-1, SHA-256, SHA-384, SHA-512***] ***SHA-1, SHA-256, SHA-384, SHA-512***		

6.2. Security Assurance Requirements

The TOE security assurance requirements specified in Table 6-10 provides evaluative activities required to address the threats identified in 3.3 of this ST.

Table 6-10 TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	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_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

6.3. Security Requirements Rationale

6.3.1. The dependencies of security requirements

The dependencies among TOE security functional requirements are shown in the following table.

Table 6-11 The dependencies of security requirements

Functional requirements	Dependencies	ST-satisfied dependencies	Requirements that do not satisfy dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	N/A
	FIA_UID.1	FIA_UID.1	N/A
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1	N/A
	FTP_ITC.1	FTP_ITC.1	N/A
FCS_CKM.1(a)	FCS_COP.1(b) FCS_COP.1(i)	FCS_COP.1(b)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_CKM.1(b)	FCS_COP.1(a) FCS_COP.1(d) FCS_COP.1(e) FCS_COP.1(f) FCS_COP.1(g) FCS_COP.1(h)	FCS_COP.1(a) FCS_COP.1(g)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A
FCS_CKM.4	FCS_CKM.1(a) or FCS_CKM.1(b)	FCS_CKM.1(a) FCS_CKM.1(b)	N/A
FCS_CKM_EXT.4	FCS_CKM.1(a) or FCS_CKM.1(b)	FCS_CKM.1(a) FCS_CKM.1(b)	N/A
	FCS_CKM.4	FCS_CKM.4	N/A
FCS_COP.1(a)	FCS_CKM.1(b)	FCS_CKM.1(b)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_COP.1(b)	FCS_CKM.1(a)	FCS_CKM.1(a)	When Trusted communication function (FCS_IPSEC_EXT.1). In the case of Update function (FPT_TUD_EXT.1), FCS_CKM.1(a) and FCS_CKM_EXT.4 are not satisfied, but no problem since key generation is not performed.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	
FCS_COP.1(c)	No dependencies	No dependencies	N/A
FCS_COP.1(g)	FCS_CKM.1(b)	FCS_CKM.1(b)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_IPSEC_EXT.1	FIA_PSK_EXT.1	FIA_PSK_EXT.1	N/A

Functional requirements	Dependencies	ST-satisfied dependencies	Requirements that do not satisfy dependencies
	FCS_CKM.1(a)	FCS_CKM.1(a)	N/A
	FCS_COP.1(a)	FCS_COP.1(a)	N/A
	FCS_COP.1(b)	FCS_COP.1(b)	N/A
	FCS_COP.1(c)	FCS_COP.1(c)	N/A
	FCS_COP.1(g)	FCS_COP.1(g)	N/A
	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A
FCS_RBG_EXT.1	No dependencies	No dependencies	N/A
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	N/A
	FMT_MSA.3	FMT_MSA.3	N/A
FDP_FXS_EXT.1	No dependencies	No dependencies	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A
FIA_ATD.1	No dependencies	No dependencies	N/A
FIA_PMG_EXT.1	No dependencies	No dependencies	N/A
FIA_PSK_EXT.1	FCS_RBG_EXT.1	—	Because bit-based pre-shared key generation using random bit generator is not selected.
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A
FIA_UID.1	No dependencies	No dependencies	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1	N/A
	FMT_SMF.1	FMT_SMF.1	N/A
FMT_MSA.1	FDP_ACC.1	FDP_ACC.1	N/A
	FMT_SMR.1	FMT_SMR.1	N/A
	FMT_SMF.1	FMT_SMF.1	N/A
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	N/A
	FMT_SMR.1	FMT_SMR.1	N/A
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1	N/A
	FMT_SMF.1	FMT_SMF.1	N/A
FMT_SMF.1	No dependencies	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A
FPT_SKP_EXT.1	No dependencies	No dependencies	N/A
FPT_STM.1	No dependencies	No dependencies	N/A
FPT_TST_EXT.1	No dependencies	No dependencies	N/A
FPT_TUD_EXT.1	FCS_COP.1(b)	FCS_COP.1(b)	N/A
	FCS_COP.1(c)	FCS_COP.1(c)	N/A
FTA_SSL.3	No dependencies	No dependencies	N/A
FTP_ITC.1	FCS_IPSEC_EXT.1 or FCS_TLS_EXT.1 or FCS_SSH_EXT.1	FCS_IPSEC_EXT.1	N/A

Functional requirements	Dependencies	ST-satisfied dependencies	Requirements that do not satisfy dependencies
	or FCS_HTTPS_EXT.1		
FTP_TRP.1(a)	FCS_IPSEC_EXT.1 or FCS_TLS_EXT.1 or FCS_SSH_EXT.1 or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
FTP_TRP.1(b)	FCS_IPSEC_EXT.1 or FCS_TLS_EXT.1 or FCS_SSH_EXT.1 or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A

7. TOE Summary specification

7.1. Random Bit Generation

- Corresponding functional requirements: FCS_RBG_EXT.1

The TOE implements CTR DRBG (AES-256) compliant with NIST SP 800-90A, and also RBG as a noise source by acquiring a timer value that varies due to the effects of CPU cache and branch prediction errors. Above CTR DRBG uses Derivation Function and Reseed, but Prediction Resistance function does not work.

The TOE uses this RBG to generate random numbers and uses to generate cryptographic keys (key lengths 256 bit and 128 bit) of the trusted communication function. When the TOE generates a random number, the necessary size entropy value is obtained and used if the CTR DRBG requires a seed material (Entropy Input and None). This entropy value satisfies the minimum amount of entropy required for Instatiate and Reseed shown in 10.2.1 of NIST SP800-90A (256 bits same as the security strength in the case of TOE) and includes sufficient entropy.

7.2. Identification and Authentication Function

- Corresponding functional requirements: FTA_SSL.3, FIA_AFL.1, FIA_PMG_EXT.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FIA_ATD.1

The TOE verifies that the person who intends to use the TOE is an authorized user by using the identification and authentication information obtained from the user, and permits the use of the TOE only to the person who is determined as the authorized user.

To operate the TOE, specify a role of U.BUILTIN_ADMIN, U.USER_ADMIN or U.NORMAL, identifies and authenticates each specified role, and if the identification and authentication is succeeded, User ID, role and access control are combined as the interactive session.

When performing the print job from the printer driver, not specifies a role, but identifies and authenticates with the credential that is input with a print data, and if it is succeeded, the print data is accepted, only when the access control, which is specified from User ID that obtained from credential, satisfies the condition. In that case, the role of U.NORMAL is combined. Input of Print Job does not generate an interactive session, but generates print data added User ID as an attribute.

When accessing the Memory RX user box (except FAX RX), request the input of the password, verify the entered password, and permit the access only when the correct password is entered.

This password can be registered and changed by U.ADMIN as described in 7.4 Security Management Function.

(1) Authentication method

Identification and authentication have the MFP authentication method that the TOE itself identifies and authenticates, and the external server authentication method that uses external authentication server. When it is external server authentication method, it

sends the input user ID to the external authentication server, and decrypts the returned credential by user key generated from input user password. If the decryption is succeeded, authentication is successful, and the authentication is failed if the decryption failed.

Table 7-1 Authentication method

Authentication method	Possible operation Before success of identification and authentication	SFR
MFP Authentication External Server Authentication	Confirmation of suspension state of User use in MFP Authentication. FAX RX Confirmation of TOE state and Setting of display, etc. Inquiry of firmware version from the operation panel.	FIA_UID.1 FIA_UAU.1

* The setting of authentication method is performed by U.ADMIN. Both MFP authentication and External sever authentication are activated at the same time. When both of them are activated, U.ADMIN set which methods are used. User who U.ADMIN sets both authentication method available, selects by oneself at the time of authentication.

(2) Interface

The relationship between the identification and authentication function and the interface is as follows.

Table 7-2 Relationship between Identification and Authentication Function and Interface

Interface	Operations	
Operation panel	Operation that require Identification and Authentication	Other than the following operations. 【I/F】Login operation on the authentication screen.
	Operation that do not require Identification and Authentication.	Confirmation of suspension state of User use in MFP Authentication. FAX RX ・Table 7-12 Read（Show the Job display） ・Table 7-13 Read（Show the Job display） ・Table 7-14 Read（Show the Job display） ・Table 7-15 Read（Show the Job display） ・Table 7-16 Read（Show the Job display） ・Table 7-17 Read（Show the Job display） Confirmation of TOE state and Setting of display. etc. Inquiry of firmware version from the operation panel.
	Operation that require authentication after Identification and Authentication (login).	Access to the Memory RX user box 【I/F】Select the Memory RX on the functional selection screen
WC	Operation that require Identification and Authentication	Other than the following operations. 【I/F】Login operation on the authentication screen

Interface	Operations	
	Operation that do not require Identification and Authentication.	None
Printer Driver	Operation that requires Identification and authentication	Input the Pint job。 ・Table 7-6 Create Store the documents in user box. ・Table 7-11 Create 【I/F】Performs the print or the save in user box from the PC that the printer driver is installed.
	Operation that do not require Identification and Authentication.	None
Fax RX	Operation that requires Identification and authentication	None
	Operation that do not require Identification and Authentication.	Permitted by Access Control SFP ・Table 7-10 Create (Fax RX from external FAX machine)

(3) Protocol in the External server authentication

The protocols used in the external server authentication are as follows.

TCP/IP (Kerberos V5)

(4) Processing when authentication failed in the MFP authentication

TOE performs the following processing when the authentication failed in the MFP authentication.

Table 7-3 Processing when authentication failed

Target	Processing	SFR
Authentication failure by login password	Authentication is suspended when number of continuous authentication failure reached the value (1 to 3)that U.ADMIN set. The number of authentication failure of U.NORMAL and that of U.USER_ADMIN is totaled. If the user A tries to log in as U.NORMAL and failed (once), and successively the user A tries to log in as U.USER_ADMIN and failed (once), the number of authentication failure of user A is two times. Authentication is also suspended even if the number of continuous authentication failure exceeds the setting value because of the change of setting value by U.ADMIN. When the authentication of U.BUILTIN_ADMIN is suspended, it is released by performing boot process of the TOE and passing the time set in the release time setting of operation prohibition for administrator authentication from boot process. In other cases, it is released by performing deletion function of number of authentication failure by U.ADMIN, who is not in the	FIA_AFL.1

Target	Processing	SFR
	authentication stopped state	
Authentication failure by user box password	Authentication is suspended when number of continuous authentication failure reached the value (1 to 3) that U.ADMIN set. It is released by performing deletion function of number of authentication failure by U.ADMIN, who is not in the authentication stopped state.	

(5) Action allowed before Identification and Authentication

The action permitted before Identification and Authentication are as follows.

- Confirmation of suspension state of User use in MFP Authentication.
- FAX RX
- Confirmation of TOE state and Setting of display, etc.
- Inquiry of firmware version from the operation panel.

(6) Feedback

In the authentication processing of interactive session（Login from the operation panel, Login from the WC and access to the Memory user box other than FAX RX）, it displays "*" or "●" for every one character of input password.

(7) Available characters and the length of minimum password as the user password and the use box password

Available characters are upper and lower case letters in the alphabet, numbers, symbols ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "-", "¥", "[", "]", ":", ";", ",", ".", "/", "'", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?" ,"_" and space), special characters (97 characters), and the minimum password length can be set by U.ADMIN. Also, the minimum password length of 15 characters or more can be set.

(8) Termination of session

The session if terminated if the operation of identified and authenticated user does not last for a certain time (in the time set by the administrator).

Table 7-4 Terminate of interactive session

Target	Session termination	Others
Operation panel	When the time determined by system auto reset time has elapsed since the process of final operation was completed.	System auto reset time is set in the factory and administrator can change it. Factory setting: 1 minute Settable time: 1 to 9 minutes
WC	When the time determined by auto logout time has elapsed since the process of final operation was completed.	Auto logout time is set in the factory and administrator can change it. -Administrator mode Factory setting: 10 minutes Settable time: Select from 1,2,3,4,5,6,7,8,9,10,20,30,40,50,60

Target	Session termination	Others
		minutes. - User mode Factory setting: 60 minutes Settable time: Select from 1,2,3,4,5,6,7,8,9,10,20,30,40,50,60 minutes

7.3. Access Control Function

− Corresponding functional requirements: FDP_ACC.1, FDP_ACF.1

TSF controls access to user data and user data operations. Performs the access control to the job owner based on Tables 6-2 and 6-3 for the operation of user data by specify the owner in the rules shown in Table 7-5 and allowing the access to user data only to the identified and authenticated administrator (U.ADMIN) and owner of the user data.

The TSF interfaces for D.USER.DOC Access Control SFP are shown in Table 7-6 through Table 7-11, and the TSF interfaces for D.USER.JOB Access Control SFP are shown in Table 7-12 through Table 7-17.

The submit of job is permitted based on the access authority combined with FIA_USB.1.

For unapproved operations, the interface is hidden or deactivated. Or an operation request is rejected by displaying a message indicating that operation cannot be performed due to a lack of authority.

Table 7-5 Relationship between Job function and owner

Job function	Job owner/Fax owner
Print	The print job submit is performed from the client PC using the printer driver or the WC interface, but it is necessary to send print data and credentials (User ID/password) to the TOE. TOE treats authorized User with credentials sent in print job submit as Job owner.
Scan	The scan job submit is performed on the operation panel. The operator performs identification and authentication on the operation panel, and after it is succeeded, submits the scan job. Therefore, the authorized User that submits this scan job becomes the Job owner.
Copy	The submit of a copy job is performed on the operation panel. The operator performs identification and authentication on the operation panel, and after it is succeeded, submits the copy job. Therefore, the authorized User that submitted this copy job becomes the Job owner.
Fax send	The submit of the fax TX job is performed on the operation panel. The operator performs identification and authentication on the operation panel and submits the fax TX job after it is succeeded. Accordingly, the authorized User that submits this Fax TX job becomes the Job owner.
Fax receive	The Fax RX document is stored in Memory RX user box or personal user box. The relationship between use box and fax owner is described in the Storage/Retrieval section
	The owner (= fax owner) of the print job for the fax RX document is the person who performs

Job function	Job owner/Fax owner	
	the print.	
Storage / retrieval	Documents are stored in Memory RX user box, password encrypted PDF user box, and personal user box.	
	Memory RX user box	Storage of document is performed by a Storage job generated from fax RX. Storing is performed as a credential of the user box information, and the owner of the saved document is U.NORMAL, which knows the user box password. The print output of the document saved by fax RX and fax RX is controlled according to D.USER.JOB Access Control SFP (Fax receive) as owner = Fax owner.
	Personal user box	Storage of document is accomplished by: a Storage job generated from F-coded fax RX; sending documents from the client PC; saving by scanning on the operation panel; and manipulating (moving documents between personal user boxes, copying) from the operation panel and the client PC. In either case, by specifying the user box to which the document is to be saved, the owner information of the specified user box is saved as a credential. The owner of the saved document is the owner of the user box in which the document is to be stored. The print output of the document stored by fax RX and fax RX is controlled according to D.USER.JOB Access Control SFP (Fax receive) as owner = Fax owner.
	Password Encrypted PDF user box	The document is saved by saving the password encrypted PDF (by performing a direct print from the WC of the client PC). The owner of the saved document is U.NORMAL who instructed to print or save the document.

Table 7-6 TSF interface for D.USER.DOC Access Control SFP (Print)

Operation		Interface
Create	Submit a document to be printed	Select the document from the client PC and print it with the printer driver.
		Select the document from the WC of the client PC and perform a direct print.
		Select the password encrypted PDF document from the WC of the client PC and perform a direct print by specifying print.
Read	View image	On the operation panel, select the document saved by Create operation from the ID & Print user box and display the document preview.
	Release printed output	On the operation panel, select the document temporarily saved by Create operation from the ID & Print user box and perform printing. Temporarily saved document is deleted with the completion of printing.
		On the operation panel, select the document temporarily saved by Create operation from the password encrypted PDF user box and perform printing (inputting password is required.). Temporarily saved document is deleted with the completion of printing.
Modify	Modify stored document	On the operation panel, select the document saved by Create operation from the ID & Print user box and perform the print settings.

Delete	Delete stored document	On the operation panel, select the document saved by Create operation from the ID & Print user box and perform the deletion
		On the operation panel, select the document saved by Create operation from the password encrypted PDF user box and perform the deletion
		Deleted in conjunction with deletion of the job (performed from the operation panel, the WC of the client PC).

Table 7-7 TSF interface for D.USER.DOC Access Control SFP (Scan)

Operation		Interface
Create	Submit a document for scanning	Set the original on the scanner unit and perform the transmission by specifying the destination (excluding the fax destination) from the scan/fax menu screen of the operation panel.
Read	View scanned image	None
Modify	Modify stored image	Perform the application setting in Create operation.
Delete	Delete stored image	Deleted in conjunction with deletion of the job (performed from the operation panel, the WC of the client PC).

Table 7-8 TSF interface for D.USER.DOC Access Control SFP (Copy)

Operation		Interface
Create	Submit a document for copying	Set the original on the scanner unit and copy it from the copy menu screen on the operation panel.
Read	View scanned image	None
	Release printed copy output	Perform Create operation
Modify	Modify stored image	Perform the application setting in Create operation
Delete	Delete stored image	Deleted in conjunction with deletion of the job (performed from the operation panel, the WC of the client PC).

Table 7-9 TSF interface for D.USER.DOC Access Control SFP (Fax send)

Operation		Interface
Create	Submit a document to send as a fax	Set the original on the scanner unit and select the Fax destination from the scan/fax menu on the operation panel to perform the transmission.
Read	View scanned image	None
Modify	Modify stored image	Perform the application setting in Create operation。
Delete	Delete stored image	Deleted in conjunction with deletion of the job (performed from the operation panel, the WC of the client PC).

Table 7-10 TSF interface for D.USER.DOC Access Control SFP (Fax receive)

Operation 作		Interface
Create	Receive a fax and store it	Fax TX from the external fax machine is performed. (Saved in the Memory RX user box)
		Fax TX from the external fax machine is performed by specifying F-code. (Saved in the specified personal user box)
Read	View fax image	On the operation panel, select the document saved by Create operation from the Memory RX user box and display the document

Operation 作		Interface
		preview
		On the WC of the client PC, select the document saved by Create operation from the Memory RX user box and display the document preview
		On the operation panel, select the document saved by Create operation from the Personal user box and display the document preview
		On the WC of the client PC, select the document saved by Create operation from the Personal user box and display the document preview
	Release printed fax output	On the operation panel, select the document saved by Create operation from the Memory RX user box and perform the printing. The document is deleted by the completion of printing.
		On the operation panel, select the document saved by Create operation from the Personal user box and perform the printing. The document is deleted by the completion of printing.
Modify	Modify image of received fax	Perform the application setting in Read operation (printing) in the personal user box. On the operation panel, select and modify the document saved by Create operation from the personal box. Select and modify documents saved by Create operation from the personal user box by the WC of the client PC.
Delete	Delete image of received fax	On the operation panel, select the document saved by Create operation from the Memory RX user box and delete it.
		On the WC of the client PC, select the document saved by Create operation from the Memory RX user box and delete it.
		On the operation panel, select the document saved by Create operation from the Personal user box and delete it.
		On the WC of the client PC, select the document saved by Create operation from the Personal user box and delete it
		Deleted in conjunction with deletion of the job (performed from the operation panel, the WC of the client PC).
		Deleted in conjunction with deletion of the personal user box (performed from the operation panel, the WC of the client PC)

Table 7-11 TSF interface for D.USER.DOC Access Control SFP (Storage/retrieval)

Operation		Interface
Create	Store document	Perform the save in user box from the printer driver of the client PC.
		Perform the direct print by specifying the save in user box from the printer driver of the client PC.

Operation		Interface
		Perform the direct print of password encrypted PDF by specifying the save in user box from the printer driver of the client PC.
		Set the original on the scanner unit and select a personal user box from the user box menu screen of the operation panel to save in the user box
		Perform Fax TX from the external fax machine.
		Perform FAX TX from the external fax machine by specifying the F-code.
Read	Retrieve stored document	On the operation panel, select the document from the Personal user box and display the document preview
		On the operation panel, select the document from the Personal user box and perform the printing
		On the operation panel, select the document from the Personal user box and perform the transmission by specifying the destination (except fax destination) On the operation panel, select the document from the Personal user box and perform the transmission by specifying the fax destination
		On the operation panel, select the document from the Personal user box and move the document by specifying the destination user box.
		On the operation panel, select the document from the Personal user box and copy the document by specifying the copy destination.
		On the WC of the client PC, select the document from the Personal user box and display the document preview
		On the WC of the client PC, select the document from personal user box and perform the transmission by specifying the destination (except Fax destination).
		On the WC of the client PC, select the document from the personal user box and perform the download. On the WC of the client PC, select the document from the personal user box and perform the document move by specifying the destination user box.
		On the WC of the client PC, select the document from the personal user box and perform the document copy by specifying the copy destination user box
		On the WC of the client PC, select the document saved by the Create operation from the Memory RX user box and perform the download.
		On the operation panel, select the document temporarily saved by Create operation from the password encrypted PDF user box and perform the saving. (Password entry is required.) Delete the temporarily saved documents with the completion of storage.
Modify	Modify stored document	Select the document from the personal user box on the operation panel and modify.
		Perform application setting in Read operation (send, print).
		From the WC of the client PC, select the document from the personal user box and modify
		On the operation panel, select the document from the Memory RX user box and modify.
Delete	Delete stored document	On the operation panel, select the document saved by Create operation from the Memory user box and perform deletion.

Operation		Interface
		On the WC of the client PC, select the document saved by the Create operation from the Memory RX user box and perform deletion
		On the operation panel, select the document saved by Create operation from the personal user box and perform deletion. On the WC of the client PC, Select the document saved by Create operation from the personal user box and perform deletion
		On the operation panel, select the document saved by Create operation from the password encrypted PDF user box and perform deletion.
		Deleted in conjunction with deletion of the personal user box (performed from the operation panel, the WC of the client PC)

Table 7-12 TSF interface for D.USER.JOB Access Control SFP (Print)

Operation		Interface
Create	Create print job	After selecting the document from the client PC and performing the printing with the printer driver, select the document temporarily saved in the ID & Print user box on the operation panel and perform the print. This temporarily saved document is also deleted with completion of printing.
		After selecting the document from the WC of the client PC and performing the direct printing, select the document temporarily saved in the ID & Print user box on the operation panel and perform the print. This temporarily saved document is also deleted with completion of printing.
		After selecting the password encrypted PDF document from the WC of the client PC and performing the direct printing, select the document temporarily saved in the Password encrypted PDF user box on the operation panel and perform the print. (Inputting password is required.) This temporarily saved document is also deleted with completion of printing.
Read	View print queue / log	The job display is displayed on the operation panel. (except the jobs for receiving of password encrypted PDF)
		Displays job display after user login in WC. (except the jobs for receiving of password encrypted PDF)
		Displays the job display after the administrator is logged in on the operation panel. (except the jobs for receiving of password encrypted PDF)
		Displays job display after administrator is logged in with the WC. (except the jobs for receiving of password encrypted PDF)
Modify	Modify print job	None
Delete	Cancel print job	After user login on the operation panel, delete the job created by the Create operation from the job display. In the case of ID & Print user boxes, the documents included in the job (D.USER.DOC) will also be deleted
		After user login on the WC, delete the job created by the Create operation from the job display. In the case of ID & Print user boxes, the documents included in the job (D.USER.DOC) will also be deleted

Operation		Interface
		After Administrator login on the operation panel, delete the job created by the Create operation from the job display. In the case of ID & Print user boxes, the documents included in the job (D.USER.DOC) will also be deleted
		After Administrator login form the WC of the client PC, delete the job created by the Create operation from the job display. In the case of ID & Print user boxes, the documents included in the job (D.USER.DOC) will also be deleted

Table 7-13 TSF interface for D.USER.JOB Access Control SFP (Scan)

Operation		Interface
Create	Create scan job	Set the original on the scanner unit and perform the transmission by specifying the destination (excluding the fax destination) from the scan/fax menu screen of the operation panel.
Read	View scan status / log	The job display is displayed on the operation panel.
		The job display is displayed after user login on the WC.
		The job display is displayed after administrator login on the operation panel
		The job display is displayed after administrator login on the WC.
Modify	Modify scan job	None
Delete	Cancel scan job	After the Create operation, during originals reading by scanner unit, the deletion of the suspending job is performed by performing the stop on the original reading screen of the operation panel or pressing the stop key. Documents included in the job (D.USER.DOC) will also be deleted.
		After user login on the operation panel, delete the job created by the Create operation from the job display. Documents included in the job (D.USER.DOC) will also be deleted.
		After user login with the WC, delete the job created by the Create operation from the job display. Documents included in the job (D.USER.DOC) will also be deleted.
		After the Create operation is performed, after the administrator is logged in on the operation panel, the job created by the Create operation is deleted from the job display. Documents included in the job (D.USER.DOC) will also be removed.
		After the Create operation is performed, after the administrator is logged in on the WC of the client PC, the job created by the Create operation is deleted from the job display. Documents included in the job (D.USER.DOC) will also be removed.

Table 7-14 TSF interface for D.USER.JOB Access Control SFP (Copy)

Operation		Interface
Create	Create copy job	Set the original on the scanner unit and copy it from the copy menu screen on the operation panel.
Read	View copy	Displays job display on the operation panel.

Operation		Interface
	status / log	Displays job display after user login in WC
		Displays job display after the administrator is logged in on the operation panel.
		Displays job display after the administrator is logged in from the WC.
Modify	Modify copy job	None
Delete	Cancel copy job	After the Create operation, during originals reading by scanner unit, the deletion of the suspending job is performed by performing the stop on the original reading screen of the operation panel or pressing the stop key. Documents included in the job (D.USER.DOC) will also be deleted.
		After user login on the operation panel, delete the job created by the Create operation from the job display. Documents included in the job (D.USER.DOC) will also be deleted.
		After user login with the WC, delete the job created by the Create operation from the job display. Documents included in the job (D.USER.DOC) will also be deleted
		After the Create operation is performed, after the administrator is logged in on the operation panel, the job created by the Create operation is deleted from the job display. Documents included in the job (D.USER.DOC) will also be removed.
		After the Create operation is performed, after the administrator is logged in on the WC of the client PC, the job created by the Create operation is deleted from the job display. Documents included in the job (D.USER.DOC) will also be removed.

Table 7-15 TSF interface for D.USER.JOB Access Control SFP (Fax send)

Operation		Interface
Create	Create fax send job	Set the original on the scanner unit and select the fax destination from the scan/fax menu screen on the operation panel to perform the transmission.
Read	View fax job queue / log	Displays job display on the operation panel.
		Displays job display after user login in WC
		Displays job display after the administrator is logged in on the operation panel.
		Displays job display after the administrator is logged in from the WC.
Modify	Modify fax send job	None
Delete	Cancel fax send job	After the Create operation, during originals reading by scanner unit, the deletion of the suspending job is performed by performing the stop on the original reading screen of the operation panel or pressing the stop key. Documents included in the job (D.USER.DOC) will also be deleted.
		After user login on the operation panel, delete the job created by the Create operation from the job display. Documents included in the job (D.USER.DOC) will also be deleted.
		After user login with the WC, delete the job created by the Create operation from the job display. Documents included in the job (D.USER.DOC) will also be deleted

Operation		Interface
		After the Create operation is performed, after the administrator is logged in on the operation panel, the job created by the Create operation is deleted from the job display. Documents included in the job (D.USER.DOC) will also be removed.
		After the Create operation is performed, after the administrator is logged in on the WC of the client PC, the job created by the Create operation is deleted from the job display. Documents included in the job (D.USER.DOC) will also be removed.

Table 7-16 TSF interface for D.USER.JOB Access Control SFP (Fax receive)

Operation		Interface
Create	Create fax receive job	After Fax TX from an external fax machine, select the fax RX document from the Memory user box on the operation panel of the TOE and perform the print.
		After Fax TX from an external fax machine by specifying F-code, select the fax RX document from the Personal user box on the operation panel of the TOE and perform the print.
Read	View fax receive status / log	Displays job display on the operation panel.
		Displays job display after user login in WC
		Displays job display after the administrator is logged in on the operation panel.
		Displays job display after the administrator is logged in from the WC.
Modify	Modify fax receive job	None
Delete	Cancel fax receive job	After Administrator login on the operation panel, delete the job created by the Create operation from the job display.
		After Administrator login on the WC of the client PC, delete the job created by the Create operation from the job display.
		After user login on the operation panel, delete the job created by the Create operation from the job display.
		After user login on the WC, delete the job created by the Create operation from the job display

Table 7-17 TSF interface for D.USER.JOB Access Control SFP (Storage/retrieval)

Operation		Interface
Create	Create storage job	Perform the save in user box from the printer driver of the client PC.
		Perform the direct print by specifying the save in user box from the printer driver of the client PC
		Set the original on the scanner unit and select a personal user box from the user box menu screen of the operation panel to save in the user box
		Perform the direct print of password encrypted PDF from the WC of the client PC by specifying the save in user box
		Perform Fax TX from the external fax machine
		Perform FAX TX from the external fax machine by specifying the F-code.
	Create	On the operation panel, select a document from the personal user box and print,

Operation		Interface
	retrieval job	send, fax TX, move, and copy the document. (Excluding printing of FAX RX documents, which is a Create fax receive job in Table 7-16 and is subject to access control by D.USER.JOB Access Control SFP (Fax receive))
		On the WC of the client PC, select a document from the personal user box and send, download, move, and copy it.
		On the WC of the client PC, select Fax RX Document from the Memory RX user box and download it.
		On the operation panel, select the temporarily saved document in Create operation from the password encrypted PDF user box and perform saving. (Password entry is required.) By the completion of storage, the temporarily saved document is also deleted
Read	View storage/retrieval log	Displays job display on the operation panel. (except receiving job of password encrypted PDF)
		Displays job display after user login in WC (except receiving job of password encrypted PDF)
		Displays job display after the administrator is logged in on the operation panel. (except receiving job of password encrypted PDF)
		Displays job display after the administrator is logged in from the WC. (except receiving job of password encrypted PDF)
Modify	Modify storage/retrieval job	None
Delete	Cancel storage job	During originals reading by scanner unit, the deletion of the suspending job is performed by performing the stop on the original reading screen of the operation panel or pressing the stop key. Documents included in the job (D.USER.DOC) will also be deleted.
	Cancel retrieval job	Perform Create retrieval job (Print from Personal user box), and then press the Stop key to delete the stopping job. Documents selected for printing (D.USER.DOC) are not deleted.
	Cancel storage/retrieval job	After user login on the operation panel, delete the job created by the Create operation from the job display.
		After user login in the WC, delete the job created by the Create operation from the job display.
		After administrator login on the operation panel, delete the job created by the Create operation from the job display.
		After administrator login in the WC of the client PC, delete the job created by the Create operation from the job display.

7.4. Security Management Function

- Corresponding functional requirements: FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1, FMT_MOF.1, FMT_SMF.1

The management functions are as follow.

TSF interface related to this case is conformed to FAU_GEN.1, FAU_GEN.2 (Interfaces to perform the management functions)

(1) User management function

U.ADMIN can register, delete, modify, temporally suspend, release of temporally suspend, add and delete of access authority, and add and delete of role (U.USER_ADMIN) of user from the operation panel or WC of client PC to TOE.

If the user is deleted, the document that is owned by the corresponding user is also deleted.

(2) TSF data management function

As shown in table 6-8, the function to manage TSF data is provided.

(3) Maintenance of the role

TOE maintains the role of U.ADMIN and U.NORMAL that was combined at login.

(4) Security function's behavior management function

The TOE provides the following functions only to U.ADMIN.

Table 7-18 Management function of Security function behavior

Function	Interface		
	Operation panel	Client PC	
		Printer Driver	WC
Management function of Enhanced security function	○	×	○
Management function of User authentication function	○	×	○
Audit log management function	○	×	○
Trusted channel management function	○	×	○

(5) User Box Management Function

U.ADMIN can change the User ID of the personal user box. Also, owner of personal user box can change the User ID of the corresponding personal user box. The TOE specifies the owner of the user box by User ID, and so this change means a change of owner of the user box (and documents in the corresponding user box).

U.ADMIN or U.NORMAL who permitted by U.ADMIN can create personal user boxes.

U.ADMIN can delete personal user boxes. Also, owner of personal user box can delete the corresponding personal user box. By deleting the user box, the documents in the corresponding user box is also deleted.

U.ADMIN can register and change the password of Memory RX user box.

(6) Attribute of D.USER.DOC, and D.USER.Job

This allows the attributes (Job owner, Fax owner) to D.USER.DOC and D.USER. Job according to the Table 6-7 during their creation. The relationship between the attributes (Job owner, Fax owner) and the interface is described in table 7-5.

7.5. Trusted Operation Function: Update function

— Corresponding functional requirements: FPT_TUD_EXT.1,FCS_COP.1(b),FCS_COP.1(c)

(1) Firmware version check function

Permitted administrators can confirm the firmware version in the following procedures.

・Login with the WC of the client PC and select Maintenance > ROM version.

・Login on the operation panel and select Maintenance > ROM version.

(2) Firmware update function

Administrator can confirm firmware version on the administer screen after the identification and authentication on the operation panel or WC.

Also, administrator can perform the firmware update function on the administrator screen after installs the USB memory that the firmware data and digital signature data is stored and identifies and authenticate on the operation panel. Firmware data includes various firmware such as system controller and print controller and hash value information (used with self-test function described in 7.7.2) for each firmware that is calculated by SHA-256. Digital signature data is the data signed by RSA digital signature algorithm (key length 2048bit, signature scheme PKCS #1 Ver 1.5) described in FIPS PUB 186-4, “Digital Signature Standard” for the hash value of firmware data calculated by SHA-256.

When the administrator performs the update function, TOE verifies the digital signature of the firmware by using RSA public key (key length 2048bit, installed in TOE at the time of shipment) before starting the installation. If the signature verification fails, a waring is displayed on the operation panel and firmware rewriting process does not performed. If it’s succeeded, the firmware and hash value of each firmware is installed. The procedure of digital signature verification is as follows.

(1) Decrypt by the digital signature data with RSA public key (key length 2048bit) owned by TOE.

(2) Calculate the hash value of the firmware data by SHA-256.

Compare the value of (1) and (2). When the value is matched, the firmware is judged to be correct

7.6. Trusted Operation Function: Self-test function

— Corresponding functional requirement: FPT_TST_EXT.1

The TOE performs the tests shown in the following table in this order when the power is turned on. When an error is detected, displays the warning on the operation panel, stops the operation and does not accept the operation.

This confirms the integrity of the firmware that executes TSF.

Table 7-19 Self-test

No.	Object	Test
1	Controller firmware, other firmware	Confirm that the hash value of each firmware calculated by SHA-256 matches the value recorded in the hash value information installed in TOE by the update function.
2	Library software (SHA, HMAC etc.) in the firmware	Power-up Self-test
3	Library software (DRBG) in the firmware	Set haveged as an entropy source and performs a health test of the DRBG function (Known solution test of Instantiate, Generate, Reseed functions based on "11.3 Health Testing" of NIST SP800-90A).

7.7. Trusted Communication Function

- Corresponding functional requirements: FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b), FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM_EXT.4, FCS_CKM.4, FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1, FCS_IPSEC_EXT.1, FIA_PSK_EXT.1

TOE provides the following function only to the administrator.

(1) FPT_SKP_EXT.1

All pre-shared keys, symmetric keys, and private keys used in the TOE communication protection function are stored in RAM (volatile memory) and SSD. There are no interfaces to access these. There is also no interface for accessing the key stored in RAM (volatile memory).

Table 7-20 Relationship between Key and Storage destination

No.	Object		Destination
1	Pre-shared keys	Pre-shared key set by U.ADMIN	SSD
		Key generated by converting the pre-shared key set by U.ADMIN	RAM
2	Symmetric keys	Shared secret key for IKE (generated in IKEv1 phase 1)	RAM
		Shared secret key for IPsec (generated in IKEv1 Phase2)	RAM
3	Private keys	Private key of the IPsec certification	SSD
		Private key used for key establishment on the IPsec communication. (generated in IKEv1 Phase1)	RAM

(2) FCS_CKM.1(b), FCS_RBG_EXT.1, FCS_COP.1(a)

TOE performs communication encryption using 128-bit and 256-bit AES-CBC encryption algorithms. The encryption keys (128 bits and 256 bits) used are generated by using the 128-bit random number that is generated by the random generation function (FCS_RBG_EXT.1) of library software (DRBG) in the firmware.

See Section 7.1 for details of the entropy used by the random number generator at this time.

(3) FCS_CKM.4, FCS_CKM_EXT.4

The timing when the key is no longer needed and when the key is discarded is same.

Table 7-21 Destruction of keys

Key		Timing of destruction	Method of destruction
Pre-shared key	Pre-shared key set by U.ADMIN	When deleted and modified the pre-shared key by administrator (Trusted channel management function)	Overwritten and deleted by 0x00
	Key generated by converting the pre-shared key set by U.ADMIN	Power OFF	-
Symmetric key	Shared secret key for IKE	Power OFF	-
		After IKE SA lifetime passed	Free of Memory
		When IP address is changed by the administrator	Free of Memory
	Shared secret key for IPsec	Power OFF	-
		After IKE SA lifetime passed	Free of Memory
		When IP address is changed by the administrator	Free of Memory
Private key	Private key of the IPsec certification	When the certification is deleted by the administrator (Trusted channel management function)	Overwritten and deleted by 0x00
	Private key used for key establishment on the IPsec communication.	Power OFF	-

(4) FTP_TRP.1(a), FTP_TRP.1(b)

The TOE performs encrypted communication in communication with other trusted IT devices. The functions that are subject to encrypted communication is as follows.

Table 7-22 Trusted path available to administrator (FTP_TRP.1(a))

Recipient of communication	Details	Protocol
Client PC	Remote administrators establish an interactive session with TOE from the client PC for management, in which case communication is performed using the protocol shown in this table.	IPsec

Table 7-23 Trusted path available to normal user(FTP_TRP.1(b))

Recipient of communication	Description	Protocol
Client PC	The authorised remote users input print jobs from the client PC to TOE and establish interactive sessions with TOE from the client PC to operate, in which case communication is performed using the protocol shown in this table.	IPsec

(5) FTP_ITC.1

The TOE performs encrypted communication in communication with other trusted IT devices. The functions that are subject to encrypted communication is as follows.

Table 7-24 Protocol used in the communications

Recipient of communication	Protocol
External authentication server	IPsec
SMTP server	IPsec
DNS server	IPsec
WebDAV server	IPsec
SMB server	IPsec
Log server	IPsec

(6) FCS_CKM.1(a)

TSF can generate RSA keys as described in the rsakpg1-crt method of NIST SP800-56B, Revision 1 Section 6.3.1.3., and generate IPsec certificates (RSA). The private key of the generated IPsec certificate is stored in the SSD.

The generation of asymmetric keys used for key establishment in cryptographic communication is performed in the method that conforms to the Using the Approved Safe-Prime Groups described in Section 5.6.1.1.1 of NIST SP800-56A, Revision 3.

(7) FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g)

In the IPsec protocol used by TOE, the following settings are available and no other settings are available. Multiple items are items that can be selected by the administrator. Only the administrator can set or change this item.

- IPsec Encapsulation Setting: Transport Mode
- Security Protocol: ESP
  - ESP encryption algorithm: AES-CBC-128, AES-CBC-256
  - ESP authentication algorithm: HMAC-SHA-1, HMAC-SHA-256,

HMAC-SHA-384, HMAC-SHA-512

- Key Exchange Method: IKEv1
  - IKEv1 encryption algorithm: AES-CBC-128, AES-CBC-256
  - Negotiation mode: Main Mode
  - SA lifetime
    - SA of Phase1: 600 - 86400 seconds
    - SA of Phase2: 600 – 28800 seconds
  - Diffie-Hellman Group: Group 14

  - IKE Authentication Method: Digital signature(RSA), Pre-shared key of text base
    - RSA-2048 （signature generation, signature verification）
    - RSA-3072 （signature verification）
    - Authentication algorithm: SHA-256, SHA-384, SHA-512
  - Text-based Pre-shared key
    - Pre-shared key set by U.ADMIN: 2 – 128 characters (ASCII) or HEX value
    - Authentication algorithm: SHA-1, SHA-256, SHA-384, SHA-512

The TOE implements the IPsec Security Policy Database (SPD) and the following settings can be made by the administrator.

- IPsec Policy: Specify the conditions of IP packet and can select which of the protection, passage, and discard operations for IP packets that meet each of these conditions. As the conditions of IP packets, protocols such as TCP and UDP, ports, sender's IP addresses, and destination IP addresses can be set. IPsec policies can be set up to 10 groups of IP policy groups 1 to 10, and preferentially apply to the setting of the group with the lower number.
- Default Action: If the IPsec policy is not matched, you can select the action from the following. (Guidance instructs administrators to choose the discard on this setting.)
  - Discard: Discard IP packets that do not match the IPsec policy setting
  - Passing: Passing IP packets that do not match the IPsec policy setting

7.8. Audit Function

– Corresponding functional requirement: FPT_STM.1, FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1

TOE provides the following functions.

(1) Audit log acquisition function

TOE records the event occurrence time (year / month / day / hour / minute / second), event type, subject identification information and event results.

Table 7-25 Event and Audit log

Interface	Event to be audited	ID(*1)	Result

Interface		Event to be audited		ID(*1)	Result
Operation Panel	Security > Job Log Setting > Job Log Usage Setting > Enable Settings (Set obtaining the job log to ON. After that, it is begun with Power ON.)	Start the Audit log acquisition function	a	Admin ID	OK
WC	Security > Job Log Setting > Job Log Usage Setting > Enable Settings (Set obtaining the job log to ON. After that, it is begun with Power ON.)				
Operation Panel	Security > Job Log Setting > Job Log Usage Setting > Enable Settings (Turn off the power when the obtain of job log is set ON or turn off the obtain of the job log.)	End of Audit log acquisition function		Admin ID	OK
WC	Security > Job Log Setting > Job Log Usage Setting > Enable Settings (Turn off the power when the obtain of job log is set ON or turn off the obtain of the job log.)				
Operation Panel	In the Admin. Mode, Login from Home > Utility > Administrator Setting	Perform of User Authentication	b c	Admin ID /User ID/ Non-registered ID	OK/NG
	In the User login, Log in from the initial screen with the following setting. Operation Rights = User				
WC	In the Admin. Mod, Log in from the initial screen with the following setting. User type = Administrator				
	In the User login, Log in from the initial screen with the following setting User type = registered user Login with Administrative Rights = OFF				
Printer	Perform print				

Interface		Event to be audited		ID(*1)	Result
Driver	Perform save in User box				
Operation Panel	When authenticating by user box password, User Box > System User Box > Memory RX User Box			User ID	
WC	When authenticating by user box password, User Box > System User Box > Memory RX User Box				
Operation Panel	Security > Enhanced Security Mode	Management function of Enhanced security function by U.ADMIN	d	Admin ID	OK
WC	Security > Enhanced Security Mode				
Operation Panel	User Authentication Setting > User Registration	User Management function by U.ADMIN		Admin ID	OK/NG
WC	User Authentication Setting > User Registration				
Operation Panel	User Authentication/Account Track > General Setting	Management function of User authentication function by U.ADMIN		Admin ID	OK
WC	User Authentication/Account Track > General Setting				
Operation Panel	User Authentication/Account Track > External Server Setting	Registration and Modification function of External server authentication setting data by U.ADMIN		Admin ID	OK
WC	User Authentication/Account Track > External Server Setting				
Operation Panel	Network > TCP/IP Setting > IPsec (Register, modify and delete pre-shared key by this interface.)	Trusted Channel management function by U.ADMIN		Admin ID	OK/NG
WC	Network > TCP/IP Setting > IPsec (Registration, modification and deletion of pre-shared key is performed from this interface.)				
WC	Security > PKI Setting > Device Certificate Setting >Device Certificate List (Registration and deletion of the certificate is			Admin ID	OK

Interface		Event to be audited	ID(*1)	Result
	performed from this interface.)			
Operation Panel	Network	Registration and Modification function of Network setting by U.ADMIN	Admin ID	OK/NG
WC	Network			
Operation Panel	Security > Job Log Setting	Audit Log management function by U.ADMIN	Admin ID	OK
WC	Security > Job Log Setting			
Operation Panel	System Setting > Reset Setting > System Auto Reset	Modification function of System auto reset time by U.ADMIN	Admin ID	OK
WC	System Setting > Reset Setting > System Auto Reset			
WC	Security > Auto Logout	Modification function of Auto logout time by U.ADMIN	Admin ID	OK
Operation Panel	Security > Security Details > Prohibit Functions When Auth. Error.	Modification function of Prohibited operation Release time of administrator authentication by U.ADMIN	Admin ID	OK
WC	Security > Security Details > Prohibit Functions When Auth. Error.			
Operation Panel	Security > Security Details > Password Rules	Modification faction of password rules by U.ADMIN	Admin ID	OK/NG
WC	Security > Security Details > Password Rules			
Operation Panel	Security > Security Details > Prohibit Functions When Auth. Error.	Modification function of No. of Authentication Failure threshold by U.ADMIN	Admin ID	OK
WC	Security > Security Details > Prohibit Functions When Auth. Error.			
Operation Panel	Security > Security Details > Prohibit Functions When Auth. Error.	Clear function of No. of Authentication Failure by U.ADMIN（except U.BUILTIN_ADMIN）	Admin ID	OK
WC	Security > Security Details > Prohibit Functions When Auth. Error.			
Operation Panel	・User Login > Home > Utility>User box > User box	User box management function by U.NORMAL	User ID	OK/NG

Interface		Event to be audited		ID(*1)	Result
	list ・User Login > User box > Personal				
WC	User Login > User box > User box list				
Operation Panel	Security > User Box Function Restriction	User box management function by U.ADMIN		Admin ID	OK/NG
	Admin. Mode > Home > Utility>User box > User box list				
WC	Security > User Box Function Restriction				
	Admin. Mode > Home > Utility>User box > User box list				
Operation Panel	Information > Change User Password	Modification function of login password of oneself by U.NORMAL		User ID	OK
WC	Information > Change User Password				OK/NG
Operation Panel	Security > Administrator Password Setting	Modification function of login password of owns elf by U.BUILTIN_ADMIN		Admin ID	OK
Refer to Table 7-6 - Table 7-17		Save of print job	e	User ID	OK/NG
		Print of print job		User ID	OK/NG)
		Send of scan job		User ID	OK/NG
		Print of copy job		User ID	OK/NG
		Send of Fax TX job		User ID	OK/NG
		Receive of Fax RX job		System ID	OK/NG
		Print of Fax RX job		User ID	OK/NG
		Save of Saved job		User ID	OK/NG
		Save of Fax RX job		System ID	OK/NG
		Print of Saved job		User ID	OK/NG
		Send of Saved job		User ID	OK/NG
		Fax TX of Saved job		User ID	OK/NG
		Download of Saved job		User ID	OK/NG
		Move of Saved job		User ID	OK/NG
		Copy of Saved job		User ID	OK/NG
		Delete of Saved job		User ID	OK/NG
Operation Panel	Maintenance > Date/Time Setting	Modification function of Date/Time information by	d f	Admin ID	OK

Interface		Event to be audited		ID(*1)	Result
WC	Maintenance > Date/Time Setting	U.ADMIN			
		Failure of Establishing IPsec session	g h	System ID	errNo (*2)

(a) Start-up and shutdown of the audit functions
(b) Unsuccessful User authentication
(c) Unsuccessful User identification
(d) Use of management functions
(e) Job completion
(f) Changes to the time
(g) Failure to establish session
(h) Failure to establish an IPsec SA
(*1) Subject identification information. The ID of the event to be audited (subject identification information) that occurred before the identification and authentication records a fixed value that is an unregistered ID.
Fax RX does not perform identification and authentication, and so system ID (fixed value: system (MFP)) is recorded.
When IPsec session establishment fails, the system ID (fixed value: system (MFP)) is recorded.
(*2) The predetermined error like "1414" (Failure of Secure communication (IPSec)) etc. is recorded.

Table 7-26 Supplement of Interface

Interface	Details	
Administrator mode	Operation Panel	Login (U.BUILTIN_ADMIN) by inputting administrator password from Home > Utility > Administrator setting
		Select the Administrator on the operation rights of the initial screen and login by inputting User ID and password. (U.USER_ADMIN)
	WC	Select the Administrator on the user type of the initial screen and login by inputting Administrator password. (U.BUILTIN_ADMIN)
		Select the registered user on the user type and administrator on the administrator rights of the initial screen and login by inputting User ID and password. (U.USER_ADMIN)
User login	Operation Panel	Select the user on the operation rights of the initial screen and login by inputting User ID and password. (U.NORMAL)
	WC	Select the registered user on the user type of the initial screen and login by inputting User ID and password (U.NORMAL).
	Printer Driver	Perform the print by inputting User ID and password. Perform the save in User box by inputting User ID and password Input User ID and password on the following screen. Basic > User Authentication / Account Track Setting > User authentication > Registered user
Authentication by User box password	Operation Panel	Enter the password in the following screen. User box > System > Memory RX

Interface	Details	
	WC	Enter the password in the following screen. User box > Open System user box > Memory RX user box
Security	Operation Panel	Admin. Mode > Security
	WC	Admin. Mode > Security
User Authentication / Account Track	Operation Panel	Admin. Mode > User Authentication / Account Track
	WC	Admin. Mode > User Authentication / Account Track
User Authentication Setting	Operation Panel	Admin. Mode > User Authentication / Account Track > User Authentication setting
	WC	Admin. Mode > User Authentication / Account Track > User Authentication setting
Network	Operation Panel	Admin. Mode > Network
	WC	Admin. Mode > Network
System Setting	Operation Panel	Admin. Mode > System setting
	WC	Admin. Mode > System setting
Information	Operation Panel	User login > Home > Utility > Information
	WC	User login > Information
Maintenance	Operation Panel	Admin. Mode > Maintenance
	WC	Admin. Mode > Maintenance

(2) Audit log storage function

The TOE temporarily saves log information as a log file in the local storage area of the TOE and converts it to XML data and sends it to the log server when the set date and time or the set log storage amount is reached or when the administrator performs audit log transmission. The date and time and accumulated amount are set by the administrator.

The log information is transmitted to the log server using the communication protection function. Log files temporarily saved in TOE are deleted after conversion to XML data or when an administrator performs audit log deletion. After transmission to the log server is completed, XML data is deleted when converting next log file to XML data. There is no function to refer or modify temporarily saved log files or XML data in TOE

When log information cannot be sent to the log server due to network failure, etc., and the local storage area in the TOE becomes full, the functions that can be performed are limited to the following functions.

- Terminating of the audit log acquisition function by turning off the power
- Starting of the audit log acquisition function by turning on the power
- User authentication (operation panel only, administrator authentication only)
- Audit Log Management Function (Sending and Deleting Audit Logs) by U.ADMIN

The limitation is released when U.ADMIN performs audit log transmission or audit log deletion and clears the full state of the local storage area.

Table 7-27 Audit Log Data speciation

Handling of audit log data	Overview
Storage area of log information	Stored in the SSD
Size hold log information	Log information is temporarily saved as a log file, converted to XML data and send to the log server. Log files can be saved up to 40MB and converted to XML data for sending to the log server at the any of the following timing. After it's converted, the corresponding log file is deleted. - At the date and time or the accumulated amount set by administrator is reached. - When reached to 36MB - When an administrator performs the Audit log transmission. After sending the XML data to the log server, it is deleted when the next XML data is generated. If the transmission fails, a maximum of 76 MB (40MB log file, 36MB XML data) is stored in the TOE temporarily.

(3) Trusted Timestamp Function

TOE has a clock function and provides a function to change the time of TOE to U.ADMIN. Only U.ADMIN can change it with FMT_SMF.1. The TOE issues timestamp by clock function at audit log generation and records it as audit log.

7.9. FAX Separation Function

－ Corresponding functional requirement: FDP_FXS_EXT.1

TSF prohibits communications via fax I/F other than sending and receiving user data using fax protocols. This prevents the TOE fax I/F is used for creating the network bridge between PSTN that TOE is connected and the network.

Also, the TOE fax I/F is used only for the Fax TX and RX and cannot be used for any other purpose.

The fax modem function that TOE provides is only for Fax TX and RX and supports Super G3 protocol and G3 protocol.

---End---