KONICA MINOLTA bizhub C551i/bizhub C451i/ bizhub C361i/bizhub C301i/bizhub C251i/ bizhub C336DNi/bizhub C330DNi/ bizhub C325DNi with FK-514, DEVELOP ineo+ 551i/ineo+ 451i/ineo+ 361i/ ineo+ 301i/ineo+ 251i with FK-514, Sindoh D741/D740/D472/D471/D470/CM5107/CM4097/CM3095/ CM3037/CM2077/CM5109/CM4099 with FK-514

Security Target

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

Version: 3.03

Issued on：July 14, 2025

Created by：KONICA MINOLTA, INC

—【Table of Contents】--

—【Table of figures】---

—【Table of Contents】--

1. ST Introduction

1.1. ST Reference

- ST name : KONICA MINOLTA bizhub C551i/bizhub C451i/ bizhub C361i/bizhub C301i/bizhub C251i/bizhub C336DNi/bizhub C330DNi/bizhub C325DNi with FK-514,
  DEVELOP ineo+ 551i/ineo+ 451i/ineo+ 361i/ineo+ 301i/ineo+ 251i with FK-514,
  Sindoh D741/D740/D472/D471/D470/CM5107/CM4097/CM3095/
  CM3037/CM2077/CM5109/CM4099 with FK-514 Security Target
- ST version : 3.03
- Created on : July 14, 2025
- Created by : KONICA MINOLTA, INC.

1.2. TOE Reference

- TOE name : KONICA MINOLTA bizhub C551i/bizhub C451i/ bizhub C361i/bizhub C301i/bizhub C251i/bizhub C336DNi/bizhub C330DNi/bizhub C325DNi with FK-514,
  DEVELOP ineo+ 551i/ineo+ 451i/ineo+ 361i/ineo+ 301i/ineo+ 251i with FK-514,
  Sindoh D741/D740/D472/D471/D470/CM5107/CM4097/CM3095/
  CM3037/CM2077/CM5109/CM4099 with FK-514
- Version : G00-R6

The physical components of the TOE are the MFP body and the FAX kit.
This TOE consists of any of the following combinations.

<table>
<tr><th>Sales Area</th><th colspan="2">MFP body</th><th>FAX kit part numbet (Option name)</th></tr>
<tr><td rowspan="2">Japan, North America, Canada, Latin America, Brazil, Mexico, Europe, Russia, South Africa, Argentina, China, Taiwan, Asia Pacific (*1)</td><td>KONICA MINOLTA bizhub C551i</td><td rowspan="6">Firmware (version : AA2J0Y0-F000-G00-R6)</td><td rowspan="6">A883 （FK-514）</td></tr>
<tr><td>KONICA MINOLTA bizhub C451i</td></tr>
<tr><td rowspan="3">Japan, North America, Canada, Latin America, Brazil, Europe, Russia, South Africa, China, Taiwan, Asia Pacific (*1)</td><td>KONICA MINOLTA bizhub C361i</td></tr>
<tr><td>KONICA MINOLTA bizhub C301i</td></tr>
<tr><td>KONICA MINOLTA bizhub C251i</td></tr>
<tr><td>South Korea</td><td>KONICA MINOLTA bizhub C336DNi</td></tr>
</table>

	KONICA MINOLTA bizhub C330DNi		
	KONICA MINOLTA bizhub C325DNi		
Saudi Arabia, Indonesia, Philippines, UAE, China	DEVELOP ineo+ 551i		
	DEVELOP ineo+ 451i		
Saudi Arabia, Indonesia, Philippines, UAE, China, Taiwan	DEVELOP ineo+ 361i		
Europe, Russia, South Africa, Argentina, Taiwan, Saudi Arabia, Indonesia, Philippines, UAE	DEVELOP ineo+ 301i		
Europe, Russia, South Africa, Argentina, China, Taiwan, Saudi Arabia, Indonesia, Philippines, UAE	DEVELOP ineo+ 251i		
South Korea	Sindoh D741		
	Sindoh D740		
	Sindoh D472		
	Sindoh D471		
	Sindoh D470		
	Sindoh CM5107		
	Sindoh CM4097		
	Sindoh CM3095		
	Sindoh CM3037		
	Sindoh CM2077		
	Sindoh CM5109		
	Sindoh CM4099		

*1"Asia Pacific" regions: Hong Kong, South Korea, Singapore, Malaysia, Australia, New Zealand, Saudi Arabia, Latin America, Argentina, Indonesia, Philippines, India, UAE, Kuwait, Thailand, Vietnam, Middle East, Southeast Asia

1.3. TOE Overview

1.3.1. Type of TOE

TOE is a Multi-Function Printer (MFP) used in the network environment (LAN) and has the function of copying, scanning, printing, faxing, and retrieving documents.

1.3.2. Usage and Main Security Functions

The TOE is connected to the LAN and to a public line and has the capability for users to print, scan, copy, fax, store and retrieve documents. 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 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, Update function to prevent updating by illegal firmware, and Trusted operation function by self-test function to verify normal operation of TSF.

The functions related to Storage Encryption are not included in the security functions provided by the TOE.Also, the Internal Audit Log Storage function is not supported in the audit function.

1.3.3. Operating environment

Figure 1-1 shows the operating environment of TOE. The TOE is used by connecting LAN and public line. The User can operate the TOE by communicating through the LAN or the operation panel with which the TOE is equipped.

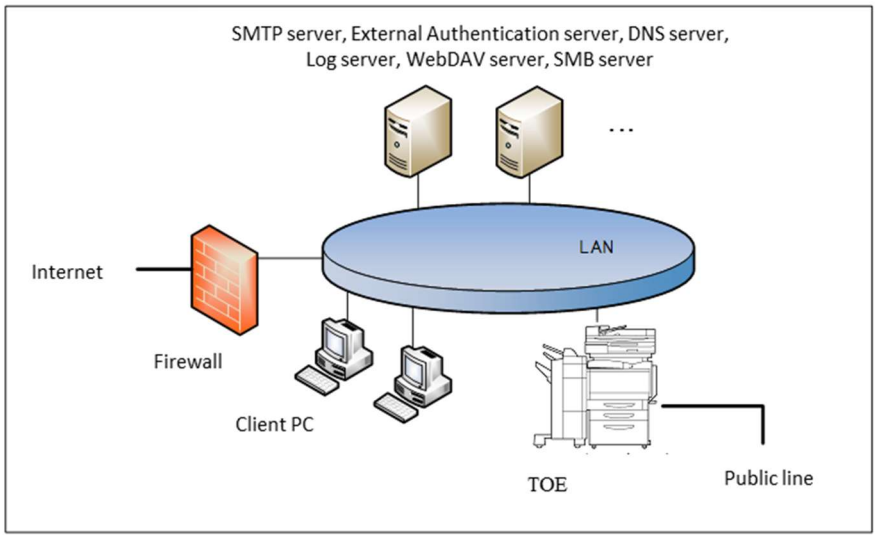


Figure 1-1 TOE's operating environment

(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) TOE (FAX kit)

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

(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.

・WC

(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.

1.3.4. 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.

Table 1-1 Evaluation configuration

Hardware/software			Used version for evaluation
Client PC (OS)			Windows 10 Pro / Windows 11 Home
	Web Browser		Google Chrome 125
	Printer Driver	KONICA MINOLTA bizhub	(c) 2003 KONICA MINOLTA, INC. Universal PCL Version 3.9.737.0 PS Version 3.9.737.0
		DEVELOP ineo	(c) 2003 KONICA MINOLTA, INC. Generic Universal PCL Version 3.9.737.0 PS Version 3.9.737.0
	IPsec		Built-in OS
External Authentication Server			Active Directory installed on Microsoft Windows Server 2019 Std
	DNS Server (note)		Built-in OS
	Ipsec		Built-in OS
SMTP Server			Postfix 3.5.6
	IPsec		strongswan 5.9.2
DNS Server			bind9 9.18.1
	IPsec		strongswan 5.9.2
Log Server			apache2 2.4.46
	IPsec		strongswan 5.9.2
WebDAV Server			apache2 2.4.46
	IPsec		strongswan 5.9.2
SMB Server			samba 4.13.5
	IPsec		strongswan 5.9.2

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 physical scope of TOE is the MFP body with installed optional Fax kit. TOE is delivered in units of MFP (built-in firmware and fax kit installed), Fax kit, and guidance. The hardware/software and guidance that composes TOE are as follows.

USB IF is implemented in the MFP, but it is enabled only for the update function during operation, so users cannot connect and use personal storage devices (portable flash memory devices, etc.). Also, RS-232C IF is implemented in the MFP, but user cannot use this interface since it is disabled during operation.

Table 1-2 Hardware / Software which compose TOE

TOE identification	MFP body	Firmware version	Format	FAX kit part numbet (Option name)	Delivery method
KONICA MINOLTA bizhub C551i with FK-514 G00-R6	KONICA MINOLTA bizhub C551i	AA2J0Y0-F000-G00-R6	Hardware with built-in firmware in binary format	A883 (FK-514)	Customer engineer (CE) brings it with the FAX kit installed.
KONICA MINOLTA bizhub C451i with FK-514 G00-R6	KONICA MINOLTA bizhub C451i				
KONICA MINOLTA bizhub C361i with FK-514 G00-R6	KONICA MINOLTA bizhub C361i				
KONICA MINOLTA bizhub C301i with FK-514 G00-R6	KONICA MINOLTA bizhub C301i				
KONICA MINOLTA bizhub C251i with FK-514 G00-R6	KONICA MINOLTA bizhub C251i				
KONICA MINOLTA bizhub C336DNi with FK-514 G00-R6	KONICA MINOLTA bizhub C336DNi				
KONICA MINOLTA bizhub C330DNi with FK-514 G00-R6	KONICA MINOLTA bizhub C330DNi				
KONICA MINOLTA bizhub C325DNi with FK-514 G00-R6	KONICA MINOLTA bizhub C325DNi				
DEVELOP ineo+ 551i with FK-514 G00-R6	DEVELOP ineo+ 551i				
DEVELOP ineo+ 451i	DEVELOP ineo+ 451i				

with FK-514 G00-R6					
DEVELOP ineo+ 361i with FK-514 G00-R6	DEVELOP ineo+ 361i				
DEVELOP ineo+ 301i with FK-514 G00-R6	DEVELOP ineo+ 301i				
DEVELOP ineo+ 251i with FK-514 G00-R6	DEVELOP ineo+ 251i				
Sindoh D741 with FK-514 G00-R6	Sindoh D741				
Sindoh D740 with FK-514 G00-R6	Sindoh D740				
Sindoh D472 with FK-514 G00-R6	Sindoh D472				
Sindoh D471 with FK-514 G00-R6	Sindoh D471				
Sindoh D470 with FK-514 G00-R6	Sindoh D470				
Sindoh CM5107 with FK-514 G00-R6	Sindoh CM5107				
Sindoh CM4097 with FK-514 G00-R6	Sindoh CM4097				
Sindoh CM3095 with FK-514 G00-R6	Sindoh CM3095				
Sindoh CM3037 with FK-514 G00-R6	Sindoh CM3037				
Sindoh CM2077 with FK-514 G00-R6	Sindoh CM2077				
Sindoh CM5109 with FK-514 G00-R6	Sindoh CM5109				

Sindoh CM4099 with FK-514 G00-R6	Sindoh CM4099				

Table 1-3 Guidance which compose TOE

TOE identification	Guidance type	Guidance Name (*3)	Version	Format	Delivery method
KONICA MINOLTA bizhub C551i with FK-514 G00-R6	FULL	If the sales area is Japan [Japanese] bizhub C651i/C551i/C451i User's Guide If the sales area is other than Japan [English] bizhub C651i/C551i/C451i User's Guide	1.00	exe file (*2)	Customer engineer (CE) bring. (*1)
KONICA MINOLTA bizhub C451i with FK-514 G00-R6					
KONICA MINOLTA bizhub C361i with FK-514 G00-R6		If the sales area is Japan [Japanese] bizhub C361i/C301i/C251i User's Guide If the sales area is other than Japan [English] bizhub C361i/C301i/C251i User's Guide(*4)	1.00		
KONICA MINOLTA bizhub C301i with FK-514 G00-R6					
KONICA MINOLTA bizhub C251i with FK-514 G00-R6					
KONICA MINOLTA bizhub C336DNi with FK-514 G00-R6					
KONICA MINOLTA bizhub C330DNi with FK-514 G00-R6					
KONICA MINOLTA bizhub C325DNi with FK-514 G00-R6					
DEVELOP ineo+ 551i with FK-514 G00-R6		[English] ineo+ 651i/551i/451i User's Guide	1.00		
DEVELOP ineo+ 451i with FK-514 G00-R6					

DEVELOP ineo+ 361i with FK-514 G00-R6		[English] ineo+ 361i/301i/251i User's Guide	1.00		
DEVELOP ineo+ 301i with FK-514 G00-R6					
DEVELOP ineo+ 251i with FK-514 G00-R6					
Sindoh D741 with FK-514 G00-R6		[English] Sindoh D742/D741/D740/ CM6107/CM5107/CM4097/ CM6109/CM5109/CM4099 USER MANUAL	1.00	pdf file	
Sindoh D740 with FK-514 G00-R6					
Sindoh CM5107 with FK-514 G00-R6					
Sindoh CM4097 with FK-514 G00-R6					
Sindoh CM5109 with FK-514 G00-R6					
Sindoh CM4099 with FK-514 G00-R6					
Sindoh D472 with FK-514 G00-R6		[English] Sindoh D472/D471/D470/ CM3095/CM3037/CM2077 USER MANUAL	1.00	pdf file	
Sindoh D471 with FK-514 G00-R6					
Sindoh D470 with FK-514 G00-R6					
Sindoh CM3095 with FK-514 G00-R6					
Sindoh CM3037 with FK-514 G00-R6					
Sindoh CM2077					

with FK-514 G00-R6					
KONICA MINOLTA bizhub C551i with FK-514 G00-R6 KONICA MINOLTA bizhub C451i with FK-514 G00-R6 KONICA MINOLTA bizhub C361i with FK-514 G00-R6 KONICA MINOLTA bizhub C301i with FK-514 G00-R6 KONICA MINOLTA bizhub C251i with FK-514 G00-R6 KONICA MINOLTA bizhub C336DNi with FK-514 G00-R6 KONICA MINOLTA bizhub C330DNi with FK-514 G00-R6 KONICA MINOLTA bizhub C325DNi with FK-514 G00-R6	Security Functions	If the sales area is Japan [Japanese] bizhub C751i/C651i/C551i/C451i/C361i/C301i/C251i User's Guide Security Operations If the sales area is other than Japan [English] bizhub C751i/C651i/C551i/C451i/C361i/C301i/C251i C336DNi/C330DNi/C325DNi AccurioPrint C751i User's Guide Security Operations	1.01 2025.5.26	pdf file	Customer engineer (CE) bring. (*1)
DEVELOP ineo+ 551i with FK-514 G00-R6 DEVELOP ineo+ 451i with FK-514 G00-R6 DEVELOP ineo+ 361i with FK-514 G00-R6 DEVELOP ineo+ 301i with FK-514 G00-R6 DEVELOP ineo+ 251i with FK-514 G00-R6		[English] ineo+ 751i/651i/551i/451i/361i/301i/251i User's Guide Security Operations	1.01 2025.5.26		
Sindoh D741 with FK-514 G00-R6					

Sindoh D740 with FK-514 G00-R6					
Sindoh D472 with FK-514 G00-R6		[English] Sindoh D742/D741/D740/ D472/D471/D470/ CM6107/CM5107/CM4097/ CM3095/CM3037/CM2077/ CM6109/CM5109/CM4099 User's Guide Security Operations	1.00 2025.5.26		
Sindoh D471 with FK-514 G00-R6					
Sindoh D470 with FK-514 G00-R6					
Sindoh CM5107 with FK-514 G00-R6					
Sindoh CM4097 with FK-514 G00-R6					
Sindoh CM3095 with FK-514 G00-R6					
Sindoh CM3037 with FK-514 G00-R6					
Sindoh CM2077 with FK-514 G00-R6					
Sindoh CM5109 with FK-514 G00-R6					
Sindoh CM4099 with FK-514 G00-R6					

(*1) Customer engineer delivers the guidance corresponding to the MFP (FULL and Security Functions).
(*2) Obtain html file by executing the exe file.
(*3) If the sales region (Sales Area) is Japan, the guidance will be distributed in Japanese, and if it is a region other than Japan, the guidance will be distributed in English. If the sales region does not include Japan, only the English guidance will be distributed.
(*4) Also applies to bizhub C336DNi, bizhub C330DNi, bizhub C325DNi.

1.4.2. Logical scope of the TOE

Logical scope of the TOE

TOE security functions and the basic functions are described below.

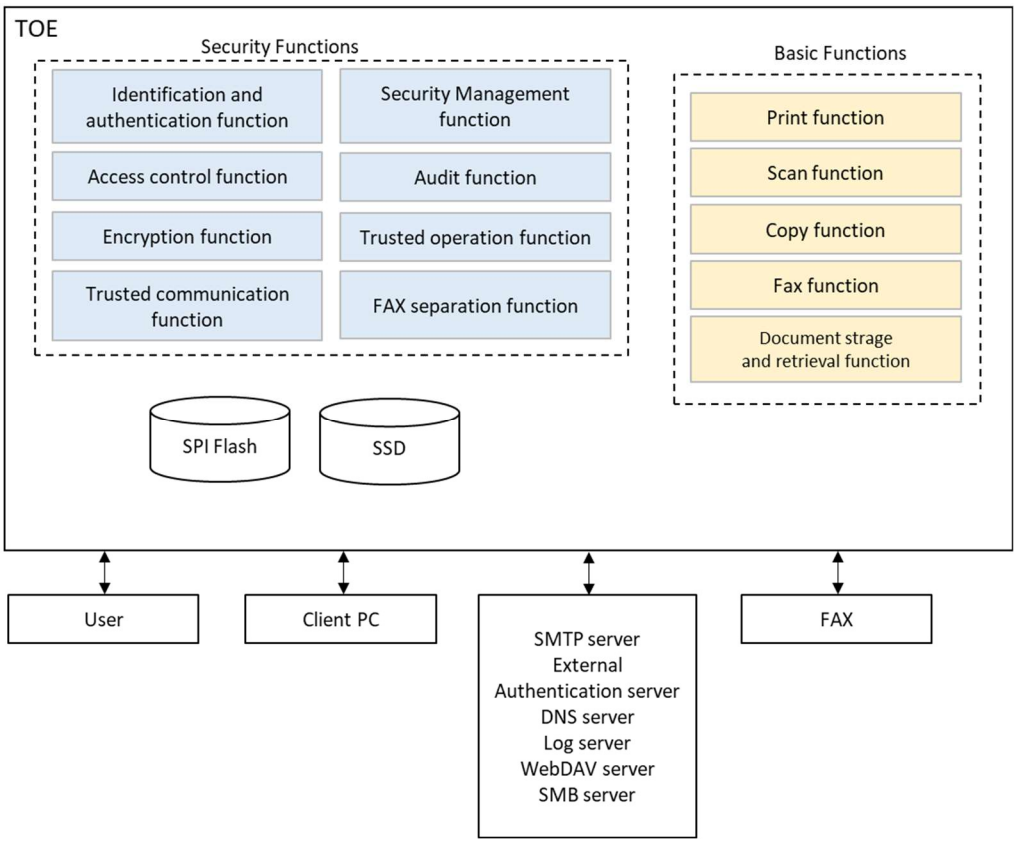


Figure 1-2 The logical scope of TOE

1.4.2.1. Basic functions

TOE basic functions are described below.

Table 1-4 TOE Basic functions

No.	Function	Definition
1	Print function	This function allows users to temporarily save and print electronic documents to TOE via the LAN. Electronic documents can be temporarily saved in the ID & Print user box from the printer driver or WC of the client PC. In addition, electronic documents can be temporarily saved from the WC to the password encrypted PDF user box. When a user prints an electronic document that has been temporarily saved from the operation panel, the relevant electronic document is deleted from the TOE.
2	Scan function	This function scans paper documents, creates electronic documents, and sends them (e-mail, WebDAV, SMB) through the user's operation from the operation panel.
3	Copy function	This function scans paper documents and copies scanned images through the user's operation from the operation panel.
4	Fax function	This function sends and receives documents through Public switched telephone network (PSTN) by using standard facsimile protocol. ・ Fax TX function This function specifies a destination from the operation panel, scans paper documents, creates electronic documents, and sends them to the specified external fax machine. Electronic documents stored in the personal user box can also be sent by fax from the operation panel. ・ Fax RX function Function to receive electronic documents through the telephone line from the external fax.
5	Document Storage 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 To personal user box, this function can store the electronic documents by scanning and converting a paper document, can store the electronic document from the printer driver or WC of a client PC and can store the Fax document with F code by Fax RX function. This function can store the fax documents received by the fax function in Memory RX user box. For Password encrypted PDF user box, electronic documents can be stored from the WC of the client PC. Electronic documents stored in personal user box can be printed, sent files to SMTP server/WebDAV server/SMB server, and Fax TX from the operation panel. Also, it can be sent files to SMTP server/WebDAV server/SMB server, and downloaded from the WC. Electronic documents stored in Memory RX user box can be printed from the operation panel and downloaded from the WC. Electronic documents stored in Password encrypted PDF user box can be stored to personal user box from the operation panel.

1.4.2.2. Security functions

TOE security functions are described below.

The functions related to the encryption on storage device are not included in the security functions provided by the TOE.

Table 1-5 TOE Security functions

No.	Function	Definition
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. The authentication using the Memory RX user box password is performed in addition to the identification and authentication of the user, when accessing the Memory RX user box (except Fax RX). 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 meets or exceeds 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.
2	Access control function	This function restricts the access to the assets in the TOE only to the permitted users.
3	Encryption function	Encryption function that prevents access to data assets during the communication through LAN. The effectiveness of data encryption is assured by the use of internationally accepted encryption algorithms.
4	Trusted communications function	The function to prevent information leakage due to wiretapping on a network when using a LAN. Protects communication path by IPsec. Encrypts the communication data between the client PC, SMTP server, external authentication server, DNS server, log server, WebDAV server, SMB server and TOE. Protects the protected assets flowing over the network by the encryption function (No.3). This function ensures that the communication takes place between known terminations.
5	Security management function	The function that ensures that administrator (U.ADMIN) and normal user (U.NORMAL) who are authenticated by the identification and authentication function can set and refer to the TOE security functions that are provided to each roles.
6	Audit function	The function that records logs of events related to TOE use and security (hereinafter referred to as "audit events") together with date and time information as audit log data. The log file is sent to the log server using the trusted communication function and can be viewed by the log server. WebDAV is used for the protocol. This does not support

		the Internal Audit Log Storage function.
7	Trusted operation function	The function (update function) that verifies the authenticity of the firmware to be updated and verifies that the firmware is legitimate before the TOE starts firmware update. The function (self-test function) to ensure the integrity of firmware by detecting the error at the TOE starts and moving to the status of unaccepting the operation.
8	FAX separation function	The function that ensures that the TOE Fax I/F cannot be used to generate a data bridge between the PSTN and the LAN.

1.4.3. Glossary

The meanings of terms used in this ST are defined.

Table 1-6 Glossary

Designation	Definition
Electronic document	An electronic document is a document data that digitized information such as characters and figures.
Paper document	A paper document is a paper document that contains information such as characters and figures.
Accumulated document	An electronic document (Subject to storage and retrieval operations) that is to be stored and retrieved.
Fax document	Documents sent and received to external fax via public line by fax function.
Job	Document processing task sent to hard copy device. Single processing task can process more than one document.
WC	Web Connection. Function/Interface to operate TOE through the Web browser of the client PC.
Operation panel	The control device for operating TOE. Consists of touch panel liquid crystal displays.
Scanner unit	A device to read graphics and photographs from paper document and convert them into electronic data by TOE.
Printer unit	A device to print out image data converted for printing by TOE.
Controller unit	A device to control TOE.
Firmware	Software to control TOE.
CPU	Central Processing Unit
RAM	A volatile memory used as a working area.
SPI Flash	Field-nonreplaceable nonvolatile memory that stores TSF data that decides TOE operation.
SSD	Field-nonreplaceable storage medium of 250GB. Stores the firmware, the language data of each countries to display the response to access through the operation panel and network, TOE setting data, electronical documents as a file.
Ethernet I/F	The interface for connecting the TOE and LAN. 10BASE-T, 100BASE-TX, and Gigabit Ethernet are supported.
USB I/F	The interface for connection the TOE and USB device.

Designation	Definition
RS-232C I/F	An interface that can be serially connected to the TOE via the D-sub9 pin. Customer engineer shall use this for the maintenance function when TOE fails.
SMB TX	A function that converts scanned data, electronic documents stored in TOE, etc. into computer-handled files and sends them to public folders on computers and servers.
WebDAV TX	A function that converts scanned data, electronic documents stored in TOE, etc. into computer-handled files and uploads them to a WebDAV server. It is also used for when sending the log to the log server.
User Box	A function to store user document data and user job data in TOE for Print function, Fax function, and Document Storage and retrieval function. During operation, ID & Print user box, Password encrypted PDF user box, Memory RX user box, and Personal user box are available.
ID & Print user box	Electronic documents are temporarily saved when a normal user performs the print function from the printer driver or WC of the client PC. The normal user can print electronic documents temporarily saved from the operation panel.
Password encrypted PDF user box	Electronic documents are temporarily saved when a normal user prints or saves a password-encrypted PDF from the WC of the client PC. The normal user can print or store electronic documents temporarily saved from the operation panel.
Memory RX user box	Stores the fax document with no F-code received by Fax function. This function can be used when the administrator has enabled Memory RX in the memory RX setting (enabled during operation). Also, it is protected by the Memory RX user box password set by the administrator in the memory RX setting. Normal user who knows the memory RX user box password can retrieve fax documents from the operation panel and the WC of the client PC.
Personal user box	Normal users can store electronic documents from the operation panel, the printer driver or the WC of the client PC into their own personal user box. If F-code is specified for the job received by the fax function, the fax document is saved in the specified user box. The normal users can retrieve electronic documents from the operation panel or the WC of the client PC form their own personal user box.
Confidential RX	This function saves the fax document with the specified F-code received by the fax function in the personal user box. Normal users and administrators who own the personal user box can set passwords for confidential RX and set valid/invalid for each personal user box.
F-code	Consists of SUB address and sender ID. When sending a fax to the personal user box that confidential RX is set to be valid, enter the registered No. of the relevant personal user box and the password for confidential RX as the SUB address and sender ID of the F-code.
Role	Role of security relevant that is associated with a user when logs in. TOE has the role of normal user (U.NORMAL) and built-in administrator (U.BUILTIN_ADMIN).
Normal User (U.NORMAL)	User authorized to use TOE as normal user (U.NORMAL). When a user successfully logs in with a user name, user password, and without administrator rights, it is identified as a normal user (U.NORMAL). Functions provided on the user screen are available.
Administrator (U.ADMIN)	User authorized to use TOE as administrator (U.ADMIN). The TOE administrators are the user administrator (U.USER_ADMIN) and built-in administrator (U.BUILTIN_ADMIN)

Designation	Definition
	depending on the login method. The security management function provided on the administrator screen can be used.
User administrator (U.USER_ADMIN)	When a user successfully logs in with a user name, user password, and administrator rights, it is identified as a user administrator (U.USER ADMIN).
Built-in administrator (U.BUILTIN_ADMIN)	User who knows the administrator password. When a user successfully logs in with an administrator password, it is identified as a built-in administrator (U.BUILTIN_ADMIN).
Customer Engineer	User who knows the service password. When a user successfully logs in with a service password, the function provided on the service screen can be used. Supports the TOE installation and trouble.
User ID	Identification to which the TOE identifies the user. If the user successfully logs in, it is associated with the user attribute. For normal users and user administrators, the registered No. of the user management function is assigned. Built-in administrator is assigned a special fixed number.
Login	Obtain credentials from users to perform identification and authentication, and if identification and authentication is successful, make TOE available. This can be performed from the operation panel, WC, and printer driver.
User name	Identification entered as credential by the normal user and user administrator when logs in. When MFP Device Authentication, the TOE identifies whether the user is a registered user by user name. This is set when registering a normal user in the user management function and cannot be changed thereafter.
Login password	The password that the user enters as credential at login. When MFP Device Authentication, the TOE authenticates the user by a login password. There are user passwords, administrator passwords, and service passwords.
User password	Login password for normal user. When MFP Device Authentication, the administrator can set the user password for each normal user in the user management function. The normal user can change his or her own user password.
Administrator password	Login password for the built-in administrator. At the time of TOE shipment, the predetermined administrator password is set, and the built-in administrator changes the default value at the time of TOE installation. Thereafter, the administrator can change.
CE password	Login password of the customer engineer.
Suspend temporarily	Function that an administrator suspends the use of TOE by normal user. The administrator can set and release the temporary suspension of use for each User ID registered in the user management function. When a user who has a User ID with a Temporary Suspension is logged in, the TOE discards the relevant user attribute and so user fails to log in and cannot use the TOE.
Administrator Rights	Function that an administrator allows the use of TOE by normal user in the role of administrator. Administrator can set and release the administrator rights for each User ID registered in the user management function. When a user who has a User ID set administrator rights logs in successfully with the administrator authority, TOE can be used in the role of administrator. When a user who has a User ID not set administrator rights performs log in with the administrator authority, TOE discards the relevant user attribute and so user fails to log in and cannot use the TOE.

Designation	Definition
Function Restriction	A function that restricts the functions available to the normal user by the administrator. The administrator can set or release the function restriction for each User ID registered in the user management function. When a normal user with a User ID set a restricted function performs a login, the TOE will hide the UI of the restricted function or display them with the deactivate status and will not be able to use the restricted function.

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 and Errata.

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

TOE users are classified as follows.

Table 3-1 User Categories

Name	Classification name	Definitions
Normal user (U.NORMAL)	Normal User (U.NORMAL)	User who is identified and authenticated by a user name and user password. It has the role of normal user (U.NORMAL).
User administrator (U.USER_ADMIN)	Administrator (U.ADMIN)	User who is identified and authenticated by a user name and user password with administrator rights by assigned an administrator authority by administrator.
Built-in administrator (U.BUILTIN_ADMIN)	Administrator (U.ADMIN)	User who is identified and authenticated by an administrator password. It has the role of administrator (U.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 for 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.

Designation	Definition
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 chapter defines the extended security functional requirements. All extended requirements are used as defined in HCD-PP.

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 Destruction	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.

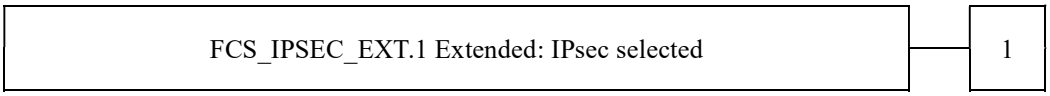
This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3. FCS_IPSEC_EXT Extended: IPsec selected

Family Behavior:

This family addresses requirements for protecting communications using IPsec.

Component leveling:



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

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.

5.4. 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: Cryptographic Operation (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 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.

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.

5.5. 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.

5.6. 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.

5.7. 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 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 lengths*]; ・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].

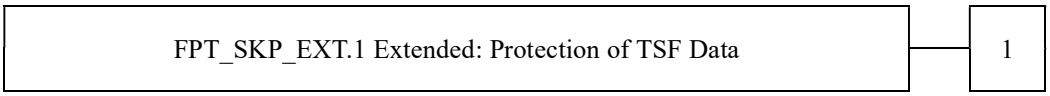
Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

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

5.8. 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 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.		

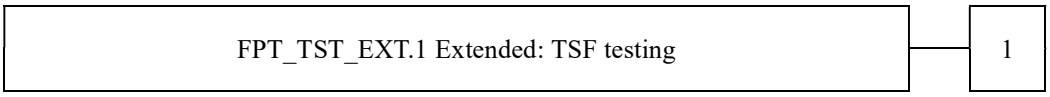
Rationale:
Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

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

5.9. FPT_TST_EXT 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.	

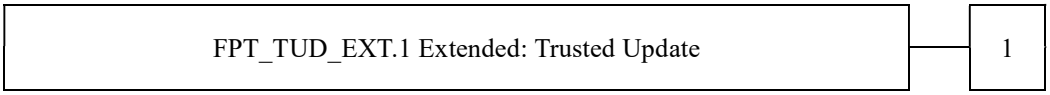
Rationale:
TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing.

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

5.10. 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 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	**Extended: 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.

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).

<Notation>

"Bold" indicates completed or refined in [PP].

"Italic" indicates parts that is necessary to select and/or assign in ST.

"Bold" and "Italic" indicate selected and/or completed in the ST to the parts of an SFR completed or refined in [PP].

The brackets([]) indicate the values selected or assigned by 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**, [*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,** [*None*].

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

Auditable event	Relevant SFR	Additional information
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

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 [**

• 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 800-56B, "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.

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 [*128 bit, 256 bit*] that meet the following: No Standard.**

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 [
***For volatile memory, the destruction shall be executed by* [*powering off a device*].**
For nonvolatile storage, the destruction shall be executed by a* [*single*] *overwrite of key data storage location consisting of* [*a static pattern*]*, followed by a* [*none*]*. If read-verification of the overwritten data fails, the process shall be repeated again;
] that meets the following: [***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 [*CBC mode*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:
• FIPS PUB 197, "Advanced Encryption Standard (AES)"
• [*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 [***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits, 3072 bits]*** that meets the following [***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 [*NIST SP 800-90A*] using [*CTR_DRBG (AES)*].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one*] *software-based noise source*] with a minimum of [*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.

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 and Table 6-3.**

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 and Table 6-3.**
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 and Table 6-3.***.
FDP_ACF.1.3	**Refinement:** The TSF shall explicitly authorise access of subjects to objects based on

the following additional rules: [*none*].

FDP_ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*deny access of user to objective functions based on the function restriction*].

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)			
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Scan	***Operation :***	***Submit a document for scanning***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	denied		
	U.ADMIN	denied	denied	denied	
	U.NORMAL		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)			
	U.ADMIN	denied	denied	denied	
	U.NORMAL		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		
	U.ADMIN	denied	denied	denied	
	U.NORMAL		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)			
	U.ADMIN	(note 4)	denied	denied	
	U.NORMAL	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied
Storage/ retrieval	***Operation :***	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***
	Job owner	(note 5)			
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	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)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Scan	***Operation：***	***Create scan job***	***View scan status / log***	***Modify scan job***	***Cancel scan job***
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Copy	***Operation：***	***Create copy job***	***View copy status / log***	***Modify copy job***	***Cancel copy job***
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		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)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		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)		denied	
	U.ADMIN	(note 4)		denied	
	U.NORMAL	(note 4)		denied	denied
	Unauthenticated	(note 4)		denied	denied
Storage / retrieval	***Operation：***	***Create storage / retrieval job***	***View storage / retrieval log***	***Modify storage / retrieval job***	***Cancel storage / retrieval job***
	Job owner	(note 6)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied

- 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.
- Note 5: Job Owner of the document created by Fax receive shall be Note3, Job Owner of the document sent from the client PC shall be Note 1, Job Owner of the document generated by the scanner shall be Note 2, and Job Owner of the document created by the store from Password encrypted PDF user box shall be Note 1.
- Note 6: Job Owner of the job created by Fax receive on "Create storage job" shall be Note3, Job Owner of the job sent from the client PC shall be Note 1, Job Owner of the job generated by the scanner shall be Note 2, and Job Owner of the job created by the store from Password encrypted PDF user box shall be Note 1. Job Owner of "Create retrieval job" is Note 2.

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 [*an administrator configurable positive integer within* [*1～3*]] unsuccessful authentication attempts occur related to [*Authentication by Login password, Authentication by Memory-RX user box password, Built-in administrator authentication*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met, surpassed*], the TSF shall [*Suspend authentication by login password of the user till it's released, Suspend authentication by Memory RX user box password till it's released, Suspend built-in administrator authentication until the time set in the Prohibited operation Release time setting elapses after the TOE power is turned off and on.*].

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 maintenance the following list of security attributes belonging to individual users: [*User ID, Administrator Rights, Function restriction, Access rights to Memory RX user box*].

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: [*"!", "@", "#", "$", "%", "^", "&",*

"", "(", ")", ["-", "¥", "[", "]", ":", ";", ",", ".", "/", "'", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?", "_", " ", (when Memory RX user box password) ""*]];

- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

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 [*FAX RX, setting of TOE status and display*] on the behalf of the user to be performed before the user is authenticated.

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 [*display "*" or "●" every character data input*] to the user while the authentication is in progress.

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 [*FAX RX, setting of TOE status and display*] on the behalf of the user to be performed before the user is identified.

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 with security attributes with subjects acting on the behalf of the user: [*User ID, Administrator rights, Function restriction, and Access rights to Memory RX user box*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with

subject acting on the behalf of users: [*Discard the security attribute associated to the user if the temporary suspension is set on User ID, Discard the security attribute associated to the user if user without administrator rights logs in with administrator rights.*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subject action on the behalf of users: [*Enable access to the user's Memory RX user box if the user succeeds in authentication of Memory RX user box password, Disable access to the user's Memory RX user box if the user fails to the authentication of Memory RX user box password*].

6.1.1.5. Class FMT: Security Management

FMT_MOF.1 **Management of security functions behavior**

(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 [*disable, enable, modify the behavior of*] the functions [*refer to Table 6-4*] to **U.ADMIN**..

Table 6-4 Management of Security Functions behavior

Security Functions	Operations
Enhanced Security Setting	disable, enable
User Authentication method	modify the behavior
Audit function	modify the behavior
Trusted communications function	modify the behavior
Memory RX	modify the behavior

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 force the **User Data Access Control SFP** to restrict the ability to [*modify, delete,* [*create, suspend temporarily / release of temporary suspension, add, set*]] the security attributes [*Security Attributes in Table 6-5*] to [*Authorised Identified Roles in Table 6-5*].

Table 6-5 Management of Subject Security Attribute

Security Attributes	Authorized Identified Roles	Operations
User ID	U.ADMIN	Create Delete Suspend temporarily / Release of temporary Suspension
	U.ADMIN U.NORMAL	Set of owner of personal user box
	U.ADMIN U.NORMAL who is the owner of the user box	Change of owner of personal user box
Administrator Rights	U.ADMIN	Delete Add
Function Restriction	U.ADMIN	Delete Setting

FMT_MSA.3 Static attribute initialization

(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 [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 **Refinement:** The TSF shall allow the **[*no role*]** to specify alternative initial values to override the default values when an object or information is created.

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 6-6.**

Table 6-6 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.**
User password	[assignment: *other operations*]	**U.ADMIN**

Data	Operation	Authorised role(s)
	registration	
	modify	**U.ADMIN, the owning U.NORMAL**
Memory RX User Box password	[assignment: *other operations*] *registration*	**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**
Administrator password	*modify*	**U.ADMIN**
Date and time information	*modify*	
System auto reset time	*modify*	
Auto logout time	*modify*	
Number of authentication failures threshold	*modify*	
Number of authentication failures (other than U.BUILTIN_ADMIN)	*clear*	
Password rule	*modify*	
External server authentication setting data	*modify* [assignment: *other operations*] *registration*	
Time to release operation of administrator authentication	*modify*	
Network settings	*modify* [assignment: *other operations*] *registration*	
[assignment: ***list of software, firmware, and related configuration data***]	[selection: *change default, query, modify, delete, clear,* [assignment: *other operations*]]	**U.ADMIN**
Firmware	*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: [*refer to Table 6-7*].

Table 6-7 list of management functions

Management functions
Enhanced Security setting function

Management functions
User management function (includes function of register/change a user password, function of managing UserID, Administrator Rights, Function Restriction)
User Authentication setting function
External authentication server setting function
Trusted communication management function
Registration and Modification function of Network setting
Modification function of date and time information
Audit log management function
Modification function of system auto reset time
Modification function of auto logout time
Modification function of release time of operation prohibition of administrator authentication
Modification function of Password policy
Modification function of Authentication failure frequency threshold
Clear function of Authentication failure frequency (except U.BUILTIN_ADMIN)
User box management function (includes function of registering personal user box, managing owner user)
Memory RX setting function (includes function of password registration and modification)
Firmware updating function
Administrator password setting function

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 [*no other functions*] prior to installing those updates.

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 [*time determined by system auto reset time for operation panels, time determined by automatic logout time for WCs, and no interactive session for printer drivers*].

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 [*IPsec*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [*authentication server, [SMTP server, DNS server, Log server, WebDAV server, SMB server]*]** 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**.

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 initial communication via the trusted channel for [***authentication service, mail service, DNS service, log transmission service, WebDAV service, SMB service***].

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 [*IPsec*] 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.**

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 [*IPsec*] 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.**

FTP_TRP.1.2(b)	**Refinement:** The TSF shall permit **[*remote users*]** to initiate communication via the trusted path
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 [*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 [t*he 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: [*IKEv1, using Main Mode for Phase 1 exchanges, as*

defined in RFCs 2407, 2408, 2409, RFC 4109, [*RFC 4304 for extended sequence numbers*]*, and* [*RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [*IKEv1*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [*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 [*IKEv1 SA lifetimes can be established based on* [*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 [*no other DH groups*].

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

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-[*SHA-256, SHA-384, SHA-512*], key size [*256, 384, 512 bits*], and message digest sizes [*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."**

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 [*no other lengths*];
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 [*SHA-256, SHA-512,* [*SHA-384*]] and be able to [*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 **[*SHA-256, SHA-384, SHA-512*]** that meet the following: **[ISO/IEC 10118-3:2004].**	

6.2. Security Assurance Requirements

The TOE security assurance requirements specified in Table 6-8 provides evaluative activities required to address the threats identified in 3.3 of this ST.

Table 6-8 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 between TOE security functional requirements are shown in the table below.

Table 6-9 The dependencies of security requirements

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency
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)	For IPsec communication (FCS_IPSEC_EXT.1). In the case of the update function (FPT_TUD_EXT.1), FCS_CKM.1(a) and FCS_CKM_EXT.4 are not satisfied, but there is no problem because 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
	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

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency
	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 or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
FTP_TRP.1(a)	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1	N/A

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency
	or FCS_TLS_EXT.1 or FCS_SSH_EXT.1 or FCS_HTTPS_EXT.1		
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

Summary specifications for the security functions provided by TOE.

Table 7-1 List of Security Functions

No.	Security function name
1	Identification and Authentication function
2	Access control function
3	Encryption function
4	Trusted communication function
5	Security Management function
6	Audit function
7	Trusted operation function
8	FAX separation function

7.1. Identification and Authentication function

TOE acquires credentials from users, performs identification and authentication, and provides an identification and authentication function, that allows to use TOE, only to those who are judged as authorized users as a result of verification.

FIA_UAU.1, FIA_UID.1

TOE supports the three authentication methods shown in Table 7-2 and an administrator can set in the user authentication setting function.

When using TOE from the operation panel or WC, enter the user name, user password, and administrator rights. When using TOE from the operation panel or WC as the built-in administrator, enter the administrator password from the login screen for the built-in administrator. When using TOE from the printer driver, enter the user name and user password.

TOE performs the identification and the authentication based on the input credentials, and permits the use of TOE only if successful. If the external server authentication method is set, the user enters an external authentication server ID in addition to the user name and user password. TOE sends the user name to the specified external authentication server and decrypts the returned credential by user key generated from the user password. It determines that the authentication is successful when the decryption is successful, and that the authentication is not successful when the decryption is failed. Identification and authentication of Built-in Administrator is always performed by the MFP authentication method, regardless of the authentication method setting.

TOE provides a function for the administrator to set the password to the Memory RX user box in the Memory RX setting function, and Memory RX user box password has been set during operation. When a normal user who succeeds in identification and authentication from the operation panel or WC accesses the Memory RX user box, authentication using the Memory RX user box password is requested, and access is permitted only when authentication is successful. Therefore, a normal user who does not know the Memory RX user box password cannot operate fax documents stored in the Memory RX user box. The authentication of Memory RX user box password is always performed by the MFP authentication method, regardless of the setting of the authentication method.

Since identification and authentication is performed for each of the above interfaces, the normal user can perform identification and authentication from the panel while the administrator is performing the remote management function

from the WC, and if successful, the TOE can be operated. However, because identification and authentication of other administrators is prohibited while an administrator logs in, two or more administrators cannot use TOE simultaneously

When TOE is used by the printer driver, there is no interactive session. When TOE receives electronic document, identification and authentication is performed using the credential (user name, user password) included in the electronic document. If successful, the normal user (U.NORMAL) is assigned as the user's role and stored in TOE as an electronic document owned by relevant normal user. If it fails, the received electronic document is destroyed without storing it. The Printer Driver does not provide a way for administrators to use TOE.

Possible operations before performing identification and authentication are as follows.

・FAX RX

・The following settings can be used to check and display the TOE status.

- Device information display from the operation panel (firmware version etc.)
- Job display from the operation panel
- Enlarge display setting from the operation panel

Table 7-2 User Authentication Setting function

Authorization method	Identification and authentication
MFP device authentication	TOE performs identification and authentication. Confirms that the user name and user password or administrator password or Memory RX user box password match the information registered in the TOE.
External server authentication	TOE performs identification and authentication by using the external authentication server (Active Directory). TOE sends user name to the external authentication server specified by user by using the Kerberos version 5 protocol, and decrypts the returned credential by the user key generated from user password, and performs identification and authentication.
MFP device + External server Authentication	TOE performs identification and authentication using either MFP device authentication or external server authentication. The user selects the authentication method when logging in.

<Related interfaces and functions>

・WebConnection : Password authentication by administrator
Password authentication by normal user
Password authentication by Memory RX user box

・operation panel : Password authentication by administrator (Built-in administrator)
Password authentication by administrator (User administrator)
Password authentication by normal user
Password authentication by Memory RX user box

・printer driver: Password authentication by normal user

FIA_ATD.1

For each normal user registered with the user management function, TOE defines the User ID, administrator rights and the access authority of function restriction as the user attribute. Also, the access authority to Memory RX user box is defined as the user attribute, too. The authority to Memory RX user box is realized with the setting of Memory RX user box password of Memory RX setting functions. Also, User ID is defined as user attributes of the built-in administrator.

<Related interfaces and functions>

・WebConnection : User registration function by administrator
Memory RX user box password authentication setting function by administrator

・operation panel : User registration function by administrator

Memory RX user box password authentication setting function by administrator

FIA_USB.1

TOE associates the user attribute (User ID, administrator rights, function restriction, access authority to Memory RX user box), if a normal user or a user administrator succeeds in identification and authentication. TOE associates the user attribute (User ID), if the built-in administrator succeeds in identification and authentication.

At this time, TOE discards the user attribute associated with the user, if the temporary suspension is set to the User ID. Also, if the administrator rights are not set to the user who performed the login as the user administrator, the user attribute associated with the relevant user is discarded.

When accessing the memory RX user box after a normal user succeeds in identification and authentication, the authentication by memory RX user box password is required. If the authentication is successful, TOE enables access to the memory RX user box that is the user attribute of the relevant user. If the authentication fails, the TOE disables access to the memory RX user box that is the user attribute of the relevant user.

<Related interfaces and functions>

・WebConnection : Password authentication by administrator
Password authentication by normal user
Password authentication by Memory RX user box

・operation panel : Password authentication by administrator
Password authentication by normal user
Password authentication by Memory RX user box

・printer driver: Password authentication by normal user

FIA_AFL.1

The TOE provides an authentication operation prohibition function to stop the user's authentication when the administrator detects a continuous authentication failure more than the number of checks (1 to 3 times) set in advance by the administrator in the user's identification and authentication. If an administrator rights is assigned to a normal user, the number of authentication failures as a normal user and the number of authentication failures as a user administrator are totaled.

When the authentication of the built-in administrator was suspended, turn OFF and ON the TOE power first. Then, the authentication suspension is released when the time set for the operation prohibition release time setting, has passed after the TOE is started. If the authentication of the normal user or the user administrator is suspended, the administrator who is not in the suspended status can release their suspension by performing the deletion function of the number of the authentication failure.

The TOE also performs the above-mentioned authentication failure operation for identification and authentication by an external server authentication method.

The authentication of the memory RX user box password is suspended when the administrator detects a continuous authentication failure more than the number of checks (1 to 3 times) set in advance by the administrator in the identification and authentication of memory RX user box password. If the authentication of memory RX user box password is suspended, the administrator who is not in the suspended status can release the authentication suspension by performing the deletion function of the number of authentication failures.

<Related interfaces and functions>

・WebConnection : Password authentication by administrator
Password authentication by normal user

Password authentication by Memory RX user box

・operation panel : Password authentication by administrator (User administrator)
Password authentication by administrator (Built-in administrator)
Password authentication by normal user
Password authentication by Memory RX user box
・printer driver: Password authentication by normal user
・Main power OFF/ON

FIA_UAU.7

When entering the login password or the memory RX user box password in the authentication processing of the interactive session (login from the operation panel or WC), TOE displays "*" or "●" for each character entered.
<Related interfaces and functions>

・WebConnection : Password authentication by administrator
Password authentication by normal user
Password authentication by Memory RX user box

・operation panel : Password authentication by administrator (User administrator)
Password authentication by administrator (Built-in administrator)
Password authentication by normal user
Password authentication by Memory RX user box

FIA_PMG_EXT.1

Characters that TOE can use as a user password are uppercase and lowercase letters in the alphabet , numbers, symbols (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “-”, “¥”, “[”, “]”, “:”, “;”, “,”, “.”, “/“, “‘”, “=”, “~”, “|”, “`”, “{”, “}”, “+”, “<”, “>“, “?” ,“_” and space). In addition to the above characters, “”” (double quotation) can be used for the memory RX user box password. The administrator can set the minimum password length from 8 to 64 characters. Therefore, the minimum password length of 15 characters or longer can be set.
<Related interfaces and functions>

・WebConnection : User registration function by administrator
Memory RX user box password authentication setting function by administrator
Setting password policy by administrator
Password setting function by normal user

・operation panel : User registration function by administrator
Memory RX user box password authentication setting function by administrator
Setting administrator password by the administrator
Setting password policy by administrator
Password setting function by normal user

FTA_SSL.3

The TOE terminates the session when a user who has been identified and authenticated by the operation panel or WC satisfies the following conditions.

・operation panel : The user is logged out when the system auto reset time (settable between 1 and 9 minutes) has

passed since the process of the final operation was completed.

・WebConnection : The user is logged out when the automatic logout time (settable between 1 and 60 minutes) has passed since the process of the final operation was completed.

There is no interactive session with the printer driver, but it logs in when the requested processing is received from the printer driver and logs out immediately after the processing is completed.

<Related interfaces and functions>

・WebConnection : Login by normal user
Login by administrator

・operation panel : Login by normal user
Login by administrator

7.2. Access control function

FDP_ACC.1, FDP_ACF.1

The TOE restricts the operation of user document data and user job data as described in Tables 7-3 through 7-14, based on the user data access control in Tables 6-2 and 6-3. For unauthorized operations, the interface is hidden or displayed in an inoperable state, or a message is displayed indicating that the operation cannot be performed because there is no authority on the operation request, and the operation is rejected.

When a normal user (U.NORAML) allowed by the identification and authentication performs Create operations in Tables 7-3 through 7-14, the user becomes a Job Owner and TOE records the User ID as the owner information of a document or Job. TOE does not provide an interface for an administrator (U.ADMIN) to perform a Create operation. Since the Fax RX function (Fax receive) performs the Create operation by receiving a fax from an external fax without the TOE operation, the job owner of the document or job until the Fax RX completion is assigned to the administrator (*1). In the case of Fax RX with no F-code specified, the fax document is saved in the Memory RX user box, so the job owner after the Fax RX is the normal user who knows the Memory RX user box password (*2). In the case of Fax RX with the F-code specified, the fax document is saved in the specified personal user box, so the job owner after Fax RX is the normal user who owns the personal user box (*3). Saving from the password encrypted PDF user box (Storage / retrieval) is performed the create operation by retrieving the document, set to be saved, from the password encrypted PDF user box and saving it in the operator's personal user box, when performing the direct print. The job owner of the document or job after saving is the normal user who is the owner of the personal user box.

TOE has a function restriction setting that restricts the functions available to each normal user by the administrator in the user management functions. The TOE displays the interface of the restricted function either hidden or inoperable based on the user attribute function limitations. Therefore, a normal user with a function restriction cannot use the operation using the restricted function from Table 7-3 to Table 7-14.

TOE has Memory RX setting function in which the administrator restricts the access of the normal user to the memory RX user box in the Memory RX setting function. During operation, access is restricted by the memory RX user box password. Based on the access authority to the memory RX user box of user attribute, the TOE allows access to the user's memory RX user box if it is valid, and denies access to the user's memory RX user box if it is invalid. Therefore, normal users who do not know the memory RX user box password cannot use the operations required to access the memory RX user box in Tables 7-3 to 7-14.

In the user box management function, the TOE has a function to set the owner of the personal user box (User ID) by the administrator or normal user. It has a function to change the owner of the personal user box (User ID) by the administrator or the normal user who owns the personal user box. The TOE restricts access to the personal user box and documents stored in the personal user box. If the normal user has the same User ID based on the Personal user Box Owner (User ID), the TOE provides an interface to the Personal User Box and permits access to the Personal User Box. On the other hand, if the normal user has a different User ID, the TOE will hide the interface of the relevant Personal User Box, so the operation that requires the access to the relevant personal user box with Tables 7-3 to 7-14 cannot used.

<Supplement to Table 7-3 through Table 7-14>

The interface provided by TOE is as follows.

PN: Operation panel, WC: Web Connection, PD: Printer driver

The descriptions in the table are as follows.

○: Supported by TOE, -: Not supported by TOE

Notes are as follows.

*1: U.ADMIN

*2: U.NORMAL who knows the memory RX user box password.

*3: U.NORMAL who is the owner of the personal user box specified by F-code.

Table 7-3 D.USER.DOC (Print) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	-	-	○	Perform Printing.
		-	○	-	Perform Direct printing.
		-	○	-	To the password encrypted PDF, specify the print and perform Direct Printing.
Read	Job owner	○	-	-	Select the document from the ID & Print user box to display the document preview.
		○	-	-	Select the document from the ID & Print user box and preform the printing. (Documents will be deleted upon completion of printing.)
		○	-	-	Select the document from the Password Encryption PDF user box and perform the printing. (Password must be entered for printing. Documents will be deleted upon completion of printing.)
Modify	Job owner	○	-	-	Perform print settings for the printing from the ID & Print user bod.
Delete	Job owner	○	-	-	Delete document from ID & Print user box.
		○	-	-	Delete document from password encrypted PDF user box.
	Job owner U.ADMIN	○	○	-	Delete documents due to job deletion.

Table 7-4 D.USER.DOC (Scan) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	Set an original on the scanner unit and perform the transmission by specifying the destination (excluding the fax destination) from the fax/scan menu screen.
Read	-	-	-	-	None.
Modify	Job owner	○	-	-	Perform the application setting with the Create operation.
Delete	Job owner U.ADMIN	○	○	-	Delete documents due to job deletion.

Table 7-5 D.USER.DOC (Copy) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	Set an original on the scanner unit and perform the copy from the copy menu screen.
Read	Job owner	○	-	-	Perform Create operation.
Modify	Job owner	○	-	-	Perform the application setting with the Create operation.
Delete	Job owner U.ADMIN	○	○	-	Delete documents due to job deletion.

Table 7-6 D.USER.DOC (Fax send) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	Set an original on the scanner unit and select the fax destination from the fax/scan menu screen to perform the transmission.
Read	-	-	-	-	None.
Modify	Job owner	○	-	-	Perform the application setting with the Create operation.
Delete	Job owner U.ADMIN	○	○	-	Delete documents due to job deletion.

Table 7-7 D.USER.DOC (Fax receive) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner(*1)	-	-	-	No operation of TOE. Fax without an F-code is received from an external fax.
		-	-	-	No operation of TOE. Fax with an F-code specified is received from an external fax machine.
Read	Job owner	○	○	-	Select the fax document from the Memory RX user box and display the document preview.
		○	○	-	Select the fax document from the personal user box and display the document preview.
		○	-	-	Select the fax document from the Memory RX user box and perform printing. (The fax document will be deleted upon completion of printing.)
		○	-	-	Select the fax document from the personal user box and perform printing. (The fax document will be deleted upon completion of printing.)
Modify	Job owner	○	-	-	Perform application setting when printing fax documents from personal user boxes.
		○	○	-	Select and edit fax documents from the personal user box.
Delete	Job owner U.ADMIN	○	○	-	Delete fax documents from the memory RX user box.
	Job owner	○	○	-	Delete fax document from personal user box.

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
	Job owner U.ADMIN	○	○	-	Deletion of fax documents due to deletion of print job of fax documents.
		○	○	-	Deletion of fax documents due to deletion of personal user boxes.

Table 7-8 D.USER.DOC (Storage/retrieval) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	-	-	○	Save in User Box.
		-	○	-	Specify the Save in User Box and perform direct print.
		○	-	-	Set an original on the scanner unit, specify a personal user box from the user box menu screen, and save in the user box.
		-	○	-	To the password encrypted PDF, specify the Save in User Box and perform direct print.
		○			Select the document from the password encrypted PDF user box and save. (Selected document is moved to the operator's personal user box.)
	Job owner(*2)	-	-	-	No operation of TOE. After receiving a Fax with no F-code from an external Fax, save the fax document in the Memory RX user box.
	Job owner(*3)	-	-	-	No operation of TOE. After receiving a Fax with F-code from the external Fax, save the fax document is the specified personal user box.
Read	Job owner	○	○	-	Select the document from the personal user box and display the document preview. (Except fax documents. Document previews of fax documents are controlled by the Read operation in Table 7-7.)
		○	-	-	Select the document from the personal user box and print, send, fax TX, move, or copy it. (Except the printing of fax documents. The printing of fax documents is controlled by the Read operation in Table 7-7.)
		-	○	-	Select a document from the personal user box and send, download, move, or copy it.
		-	○	-	Select a document from the Memory RX user box and download it.
		○	-	-	Select the document from the Password Encrypted PDF user box and save it. (Password must be entered for storage. Documents will be deleted upon completion of storage.)
Modify	Job owner	○	○	-	Select a document from the personal user box and edit it. (Except fax documents. Editing of fax documents is controlled

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
					by the Modify operation in Table 7-7.)
		○	○	-	Perform application setting in Read operation (send, print). (Except printing of fax documents. The application setting in the printing of fax documents is controlled by the Modify operation in Table 7-7.)
		○	-	-	Select the fax document from the Memory RX user box and edit it (change name).
Delete	Job owner	○	○	-	Delete the document from the personal user box. (Except the deletion of fax documents. Delete of fax documents is controlled by Delete operation in Table 7-7.)
		○	-	-	Delete document from password encrypted PDF user box.
	Job owner U.ADMIN	○	○	-	Deletion of documents due to deletion of personal user boxes. (Except deletion of fax documents. Delete of fax documents is controlled by Delete operation in Table 7-7.)

Table 7-9 D.USER.JOB (Print) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	-	-	○	Select the document from the client PC, perform the print operation using the printer driver, select the document temporarily saved in the ID & Print user box from the operation panel, and perform the print. (Documents will be deleted upon completion of printing.)
		-	○	-	Select the document from the WC of the client PC, perform the direct print, select the document temporarily saved in the ID & Print user box from the operation panel, and perform the print. (Documents will be deleted upon completion of printing.)
		-	○	-	Select the password encrypted PDF document from the WC of the client PC, specify the print, perform the direct print, select the temporarily saved document from the password encrypted PDF user box from the operation panel, and perform the print. (Password must be entered for printing. Documents will be deleted upon completion of printing.)
Read	Job Owner U.ADMIN U.NORMAL	○	○	-	Displays the job. (except the receiving jobs of password encrypted PDF)
	Unauthenticated	○	-	-	
Modify	-	-	-	-	None.
Delete	Job owner U.ADMIN	○	○	-	Delete a job from the job display. (In the case of print jobs from ID & Print user boxes, the document is also deleted by deleting the job.)

Table 7-10 D.USER.JOB (Scan) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORAML	○	-	-	Set an original on the scanner unit and perform the transmission by specifying the destination (excluding the fax destination) from the fax/scan menu screen.
Read	Job owner U.ADMIN U.NORMAL	○	○	-	Displays the job.
	Unauthenticated	○	-	-	
Modify	-	-	-	-	None.
Delete	Job owner	○	-	-	When the scanner unit is reading an original, perform Stop on the original reading screen or press the Stop key to perform deletion of the stopping job. (Documents will also be deleted due to job deletion)
	Job owner U.ADMIN	○	○	-	Delete a job from the job display. (Documents will also be deleted due to job deletion)

Table 7-11 D.USER.JOB (Copy) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORAML	○	-	-	Set an original on the scanner unit and perform copy from the copy menu screen.
Read	Job owner U.ADMIN U.NORMAL	○	○	-	Displays the job.
	Unauthenticated	○	-	-	
Modify	-	-	-	-	None.
Delete	Job owner	○	-	-	When the scanner unit is reading an original, perform Stop on the original reading screen or press the Stop key to perform deletion of the stopping job. (Documents will also be deleted due to job deletion)
	Job owner U.ADMIN	○	○	-	Delete a job from the job display. (Documents will also be deleted due to job deletion)

Table 7-12 D.USER.JOB (Fax send) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	Set an original on the scanner unit and select the fax destination from the fax/scan menu screen to perform transmission.
Read	Job owner U.ADMIN	○	○	-	Displays the job.

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
	U.NORMAL				
	Unauthenticated	○	-	-	
Modify	-	-	-	-	None.
Delete	Job owner	○	-	-	When the scanner unit is reading an original, perform Stop on the original reading screen or press the Stop key to perform deletion of the stopping job. (Documents will also be deleted due to job deletion)
	Job owner U.ADMIN	○	○	-	Delete a job from the job display. (Documents will also be deleted due to job deletion)

Table 7-13 D.USER.JOB (Fax receive) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner(*1)	-	-	-	No operation of TOE. Fax without an F-code is received from an external fax.
		-	-	-	No operation of TOE. Fax with an F-code specified is received from an external fax.
	Job owner(*2)	○	-	-	Select the fax document from the memory user box and perform printing. (The fax document will be deleted upon completion of printing.)
	Job owner(*3)	○	-	-	Select the fax document from the personal user box and perform printing. (The fax document will be deleted upon completion of printing.)
Read	Job owner U.ADMIN U.NORMAL	○	○	-	Displays the job.
	Unauthenticated	○	-	-	
Modify	-	-	-	-	None.
	Job owner U.ADMIN	○	○	-	Delete a job from the job display. (In the case of a print job, the fax document is also deleted by deleting the job.)

Table 7-14 D.USER.JOB (Storage/retrieval) access control

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
Create	Job owner U.NORAML	-	-	○	Save in user box.
		-	○	-	Specify the Save in user box and perform direct print.
		○	-	-	Set an original on the scanner unit, specify a personal user box from the user box menu screen, and save in the user box.
		-	○	-	Specify the Save in User Box and perform a direct print of

Operation	Operable user	Interface			Operation method
		PN	WC	PD	
					password encrypted PDF.
	Job owner(*2)	-	-	-	No operation of TOE. After receiving a fax without an F-code from an external fax, the fax document is saved in the memory RX user box.
	Job owner(*3)	-	-	-	No operation of TOE. After receiving a fax with the specified F-code from an external fax, the fax document is saved in the specified personal user box.
	Job owner U.NORMAL	○	-	-	Select a document from the personal user box and print, send, fax TX, move, or copy it. (Except the printing fax documents. The printing of fax documents is controlled by the Create operation in Table 7-13)
		-	○	-	Select a document from the personal user box and send, download, move, or copy it.
	Job owner U.NORMAL	-	○	-	Select the fax document from the memory RX user box and download it.
	Job owner U.NORMAL	○	-	-	Select the document from the Password Encrypted PDF user box and perform save. (Password must be entered for storage. Documents will be deleted upon completion of storage.)
Read	Job owner U.ADMIN U.NORMAL	○	○	-	Displays the job. (except the receiving jobs of password encrypted PDF)
	Unauthenticated	○	-	-	
Modify	-	-	-	-	None.
Delete	Job owner	○	-	-	When the scanner unit is reading an original, perform Stop on the original reading screen or press the Stop key to perform deletion of the stopping job. (Documents will also be deleted due to job deletion)
		○	-	-	After printing from the personal user box, press the Stop key to delete the job in suspend. (Documents are not deleted after deletion of the job.)
	Job owner U.ADMIN	○	○	-	Delete a job from the job display.

7.3. Encryption function

FCS_CKM.1(a)

The TOE generates an RSA asymmetric key with a key length of 2048 bits in the method described in the rsakpg1-crt method described in Section 6.3.1.3 of NIST SP800-56B, Revision 2 in the generation of IPsec certificates used in the key establishment for IPsec communication. Also, in the key establishment for IPsec communication, an asymmetric key is generated by Diffie-Hellman Group 14 as described in the Using the Approved Safe-Prime Groups described in Section 5.6.1.1.1 of NIST SP800-56A, Revision 3.

<Related interfaces and functions>

- WebConnection: IPsec communication setting
  Using WebConnection administrator setting function
  Using WebConnection normal user setting function
- operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
- printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_CKM.1(b)

The TOE calls the DRBG function (CTR DRBG(AES-256)) to generate a random number using the DRBG and generate a 128-bit or 256-bit symmetric encryption key at the start of IPsec communications or at the key establishment after the SA lifetime.

<Related interfaces and functions>

- WebConnection: Using WebConnection administrator setting function
  Using WebConnection normal user setting function
- operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
- printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_RBG_EXT.1

TOE implements a CTR DRBG (AES-256) conforming to NIST SP 800-90A and an RBG consisting of a single software entropy source. The above CTR DRBG uses the Derivation Function and Reseed, but the Prediction Resistance function does not work. The software entropy source implements a condition branch code etc., that affects the internal state of the CPU, and a clock counter value acquisition process in the loop process. The variation of the loop processing performance time is acquired via the clock counter and obtain the raw data. Conditioning is performed to agitate and compress the entropy included in the raw data into the entire bit using shift operations and XOR, and after increasing the entropy rate of the entire bit, it is output as an entropy value.

The TOE uses this RBG to generate random numbers and uses them to generate encryption keys (key length 256 bit and 128 bit) with a trusted communication function. When the TOE generates a random number, if the CTR DRBG requires a seed material (Entropy Input and Nonce), start the software to be used as the entropy source and obtain and use the required size entropy value. This entropy value satisfies the minimum amount of entropy required for Instantiate and Reseed (in the case of TOE, 256 bits equal to the security strength) shown in 10.2.1 of NIST SP800-90A and contains sufficient entropy.

<Related interfaces and functions>

- WebConnection: IPsec communication setting
  Using WebConnection administrator setting function
  Using WebConnection normal user setting function
- operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FIA_PSK_EXT.1

The TOE uses the following text-based pre-shared key as the pre-shared key for IPsec. The text-based pre-shared key is also converted into a bit string using the hash algorithm described below.

・Text-based pre-shared key
- Length: 22 characters（ASCII String）
- Available Characters: ASCII String (A characters that combines uppercase and lowercase letters, numbers, and special characters ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")"))
- Conditioning methods: SHA-256, SHA-384, and SHA-512

<Related interfaces and functions>

・WebConnection: Using WebConnection administrator setting function
Using WebConnection normal user setting function
・operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_COP.1(a)

TOE uses an AES-CBC with a key length of 128 bits and 256 bits conforming to FIPS PUB 197 and NIST SP 800-38A as an ESP encryption algorithm for IPsec communication. Also, TOE uses an AES-CBC with a key length of 128 bits and 256 bits conforming to FIPS PUB 197 and NIST SP 800-38A as an IKEv1encryption algorithm for IPsec communication.

<Related interfaces and functions>

・WebConnection: Using WebConnection administrator setting function
Using WebConnection normal user setting function
・operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_COP.1(b)

TOE uses the RSA digital signature algorithm with a key length of 2048 bits conforming to FIPS PUB 186-4 in FW verification of the update function. The RSA digital signature algorithm (signature generation) with a key length of 2048 bits conforming to FIPS PUB 186-4 is used for peer authentication of IPsec communications, and the RSA digital signature algorithm (signature verification), with a key length of 2048 bits and 3072 bits, conforming to FIPS PUB 186-4 is used for digital signature verification.

<Related interfaces and functions>

・WebConnection: Using WebConnection administrator setting function
Using WebConnection normal user setting function
・operation panel: Execute firmware update
Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_COP.1(c)

In the update function described in Section 7.7.1, TOE verifies firmware data using digital signature verification as follows. Among them, the calculation of the hash value by SHA-256 conforming to ISO/IEC 10118-3:2004 is performed.

(1) Decrypt the digital signature data with the RSA public key (key length 2048bit) held by the TOE.
(2) Calculate the hash value of the firmware data using SHA-256.
(3) Compare the values of (1) and (2). If they match, it is determined that the firmware data is normal.

Also, In the IPsec communication described in Section 7.4, TOE calculates a hash value conforming to ISO/IEC 10118-3:2004 in each of the following cases.

(1) As IKEv1 authentication algorithms, hash values are calculated using SHA-256, SHA-384, and SHA-512.
(2) SHA-256, SHA-384, and SHA-512 are used as hash algorithms when executing keyed-hash message authentication as the ESP authentication algorithm.
(3) When peer authentication using RSA digital signature is used, SHA-256 is used to calculate the hash value.

<Related interfaces and functions>

・WebConnection: Using WebConnection administrator setting function
Using WebConnection normal user setting function
・operation panel: Execute firmware update
Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_COP.1(g)

In IPsec communication, TOE implements the following ESP by keyed hash message authentication in compliance with The Keyed-Hash Message Authentication Code defined in FIPS PUB 198-1 and Secure Hash Standard defined in FIPS PUB 180-3.

・Message digest length: 256, 384, 512
・Key Length: 256, 384, 512
・Encryption algorithms: HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512

* Use SHA-256, SHA-384, SHA-512 as hash algorithms

<Related interfaces and functions>

・WebConnection: Using WebConnection administrator setting function
Using WebConnection normal user setting function
・operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_CKM.4, FCS_CKM_EXT.4

Table 7-15 shows the storage destination of keys and key materials used for IPsec communication and the method of destruction. The pre-shared key set by the administrator and the private key of the IPsec certificate are stored in the field-nonreplaceable SSD. When the administrator deletes the pre-shared key and IPsec certificate private key, it is overwritten with 0x00. Session keys (temporary encryption keys) used in IPsec are stored in RAM. These items are deleted when the TOE power is turned off since they will be no longer needed.

<Related interfaces and functions>

・WebConnection: Deletion of pre-shared keys for IPsec communication, deletion of digital certificates
・operation panel: Deletion of pre-shared keys for IPsec communication
・Main power OFF/ON

Table 7-15 Storage and Destruction of Key

Key		Storage destination	Timing of destruction	Method of destruction
Pre-Shared Key	Pre-shared key set by the administrator	SSD	Delete Pre-shared key by administrator (Trusted communication management function)	Deleted by 0x00
	Key generated by converting the Pre-shared key set by the administrator	RAM	Power OFF	—
Symmetric key	Shared secret key for IKE (generated in IKEv1 Phase 1)	RAM	Power OFF	—
	Shared secret key for IPsec (Generated in IKEv1 Phase 2)	RAM	Power OFF	—
Private key	Private key of the IPsec certification	SSD	When deleted a certification by an administrator (Trusted communication management function)	Deleted by 0x00
	Diffie-Hellman private key of IPsec (generated in IKEv1 Phase 1)	RAM	Power OFF	—

7.4. Trusted Communication function

FTP_ITC.1

Since the TOE uses the IPsec protocol in communication with the IT device shown in Table 7-16, channel data is not transmitted in plaintext.

Table 7-16 Communication with IT equipment

TSF-permitted IT devices	Protocol
SMTP server	IPsec
External authentication server	IPsec
DNS server	IPsec
Log server	IPsec
WebDAV server	IPsec
SMB server	IPsec

<Related interfaces and functions>

・operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

FTP_TRP.1(a)

TOE provides a WC that runs on the browser of the client PC as a way for the administrator to remotely manage TOE. Communication between TOE and client PC uses the IPsec protocol, which is the trusted communication path. When the TOE is accessed from the client PC for remote management, the TOE starts communication only with the IPsec protocol and guarantees end point identification, protection from communication data leakage, and detection of communication data modification.

<Related interfaces and functions>

・WebConnection: Using WebConnection administrator setting function

FTP_TRP.1(b)

TOE provides WC and printer drivers that run on the browser of the client PC as a way for non-administrator users to access TOE remotely. Communication between TOE and client PC uses the IPsec protocol, which is the trusted communication path. When the TOE is accessed from the client PC for remote access, the TOE starts communication only with the IPsec protocol and guarantees end point identification, protection from communication data leakage, and detection of communication data modification.

<Related interfaces and functions>

・WebConnection: Using WebConnection normal user setting function

・printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

FCS_IPSEC_EXT.1

TOE implements an IPsec architecture conforming to RFC 4301. Only the administrator can set and change the following settings as the IPsec protocol, but cannot use the settings other than followings.

・IPsec Encapsulation Settings: Transport Mode

・Security Protocol: ESP (conform to RFC 4303)

- ESP Encryption Algorithm: AES-CBC-128, AES-CBC-256 (conform to RFC3602)
- ESP Authentication Algorithm: HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512

- Key Exchange Method: IKEv1 (conform to RFC 2407,2408,2409,4109)
  - IKEv1 Encryption Algorithm: AES-CBC-128, AES-CBC-256 (conform to RFC 3602)
  - Negotiation mode: Main Mode
  - SA lifetime
    - Phase 1 of SA: 600 to 86400 seconds
    - Phase 2 of SA: 600 to 28800 seconds
  - Diffie-Hellman Group: Group 14
  - ESN: invalid, valid (conform to RFC 4304)
- IKE Authentication Method: Digital Signature (RSA), Text-Based Pre-shared Key
  - Digital signature
    - RSA-2048 (Signature generation, Signature verification)
    - RSA-3072 (Signature Verification)
    - Authentication Algorithm: SHA-256, SHA-384, and SHA-512 (conform to RFC 4868)
  - Text-based pre-shared key
    - Pre-shared key set by the administrator: 22-character ASCII string
    - Authentication Algorithms: SHA-256, SHA-384, and SHA-512 (conform to RFC 4868)
  - Protocol Setting
    - Protocol Identification Setting: No Selection (Any)
  - IPsec Setting
    - Default Action: Discard
    - Certificate Verification Level Settings: Expiration Date: Check
      Key Usage: No check
      Chain: Check the path of certification
      Expiration Date Confirmation: No check

Also, the TOE implements the IPsec Security Policy Database (SPD) and the followings can be set by the administrator.

- IPsec Policy: Specify the IP packet conditions and select which of the protected, allow, and deny operations to perform for IP packets that meet each of these conditions. Inbound packet and outbound packet are processed with same rule from the view of the IPsec policy. For IP packet conditions, protocols of Any and destination IP addresses (Individual, or Subnet settings) can be set.
  IPsec policy can be set to 10 groups of IP policy groups 1 to 10. When multiple IPsec policies are set, the operation is applied in the following order of precedence, regardless of the order in which IPsec policy groups 1 to 10 are registered.
  Priority: High Protected > Deny > Allow Priority: Low
- Default Action: If the IPsec policy is not matched, select the action from the following. (Guidance instructs administrators to choose to discard in this setting.)
  - Deny: Discard IP packets that do not match the IPsec policy setting
  - Allow: Bypassing IP packets that do not match the IPsec policy setting

<Related interfaces and functions>

- WebConnection: Using WebConnection administrator setting function
  Using WebConnection normal user setting function
- operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
- printer driver: Execute operations using the printer driver as an interface in "7.2. Access control function"

7.5. Security Management function

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

TOE provides the following management functions to users. Each management function is operable only from the interface described. The printer driver does not provide management functions. When transiting the screen of performing the following management functions on the operation panel or WC, identification and authentication to TOE is requested, and so the management function cannot be used without authentication. Roles (U.ADMIN, U.NORMAL) are associated and registered by the user management function. Association of roles (U.ADMIN, U.NORMAL) is made at login and maintained until logout. There are two types of TOE U.ADMIN: U.BUILTIN_ADMIN (built-in administrator) and U.USER_ADMIN (user administrator). The former is authenticated by an administrator password, and the latter is authenticated by a user name, user password, and administrator rights (set administrator rights). Both are associated with U.ADMIN. Cannot use the management functions that are not provided in the user role. In the access control of Tables 6-2 and 6-3, TOE assigns the User ID of the normal user who created the user document data and the user job data as the initial value of the security attribute. User document data and user job data generated by the Fax RX function are created by users other than TOE. Therefore, an administrator's User ID is assigned as the initial value of the security attribute, and the access control of Fax receiving is performed. After Fax RX is completed, Fax document is stored in the Memory RX user box if F-code is not specified, and it is controlled with the access authority of Memory RX user box and so the security attribute is not related. Administrator’s User ID is assigned as the initial value. If Fax RX with F-code, specified personal user box’s User ID is assigned as the initial value of security attributes. Refer to “ 7.2 Access control function” for details. TOE does not have a function to overwrite the User ID assigned as the initial value.

Table 7-17 Management functions provided to Administrator

Management function	Description	Permitted operations	Operable interface
User management function	Register/delete a user with a user attribute User ID of TOE, register/change a user password, set/release a temporarily suspension of use, set/release a function restriction, and assign/delete an administrator rights. When the user registered user creates a document or job, the User ID is set as the initial value of the security attribute, and the user data access control in Tables 6-2 and 6-3 is performed. If the user is deleted, the document in which the user is the owner is also deleted.	Registration, Modification, Deletion	Operation panel, WC
Administrator password setting function	Set the administrator password. The default value is set for the administrator password at the time of shipment. The built-in administrator changes the setting when the setup procedure at the start of operation.	Modification	Operation panel
User Authentication setting function	Set the user authentication method. Select either of MFP device authentication, external server authentication, or MFP device + external server authentication. The Built-in Manager is always identified and authenticated by the MFP device authentication.	Modification	Operation panel, WC
External Authentication server setting function	Sets the external authentication server to be used by the external server authentication method.	Registration, Modification,	Operation panel, WC

Management function	Description	Permitted operations	Operable interface
		Deletion	
Modification function of No. of Authentication Failures Threshold	Set the threshold of the number of authentication failures. When the number of continuous user authentication failures meets or exceeds this set value, the TOE suspends authentication to the relevant user.	Modification	Operation panel, WC
Modification function of Operation prohibition release time of Administrator Authentication	Set the time until releasing the suspension of authentication when the built-in administrator's authentication is suspended due to the number of continuous authentication failures meeting or exceeding the threshold.	Modification	Operation panel, WC
Clear function of No of Authentication Failures (other than the built-in administrator)	Clear the number of authentication failures. This operation can release the authentication suspension of a user other than the built-in administrator.	Execution	Operation panel, WC
Modification function of Password rule	Set and change the password rule (including the setting of the number of minimum password character).	Modification	Operation panel, WC
Enhanced Security setting function	Enable/disable the enhanced security settings. When enabled, the settings related to the behavior of the security function are set to secure values and the settings are maintained. The use of the TOE updating function through the network, the maintenance function (using RS-232C I/F), and the network setting management initialization function is prohibited. When a user performs a prohibited function or a setting change, the enhanced security setting is changed to disable if user instructs to continue the operation after the warning screen is displayed.	Modification	Operation panel, WC
Modification function of Date/Time information	Set the date and time information. If an event under audit occurs, this date and time information is recorded in the audit log.	Modification	Operation panel, WC
Modification function of System Auto reset time	Set the system auto reset time during operation of the operation panel.	Modification	Operation panel, WC
Modification function of Automatic Logout time	Sets automatic logout time during WC operation.	Modification	WC
Trusted Communication Management function	Set IPsec communication, which is a trusted communication function. IPsec communication setting, pre-shared key setting. Registration, modification, and deletion of IPsec certificate setting.	Registration, Modification, Deletion	Operation panel, WC
Network setting function	Register and change the network settings (IP address of TOE, IP address of the DNS server, the port number, NetBIOS name, etc.).	Registration, Modification	Operation panel, WC
Audit Log Management	Enable/disable the audit function, how to obtain the audit	Registration,	Operation panel,

Management function	Description	Permitted operations	Operable interface
function	log, log server, setting of automatic log distribution conditions, and send/delete of the audit log are performed.	Modification	WC
User box Management function	Register the personal user box, change the owner users, and delete.	Registration, Modification, Deletion	Operation panel, WC
Memory RX setting function	Enable/disable the Memory RX, register/change the memory RX user box password.	Registration, Modification	Operation panel, WC
Firmware update function	Perform TOE firmware update using USB memory.	Execution	Operation panel

Table 7-18 Management function provided to normal users

Management function	Description	Permitted operations	Operable interface
User Password setting function	Set the user password. After identification and authentication, the user can change user's own password.	Modification	Operation panel, WC
User Box Management function	Register the personal user box, change the owner users, and delete.	Registration, Modification, Deletion	Operation panel, WC

<Related interfaces and functions: FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1>

・WebConnection: Functions that have WC as an interface in Table 7-17 and Table 7-18

・operation panel: Functions that have operation panel as an interface in Table 7-17 and Table 7-18

<Related interfaces and functions: FMT_SMR.1>

・WebConnection: User registration function by administrator
Password authentication by administrator
Password authentication by normal user

・operation panel: User registration function by administrator
Password authentication by administrator
Password authentication by normal user

・printer driver: Password authentication by normal user

<Related interfaces and functions: FMT_MSA.3>

・WebConnection: The following operations in Tables 7-3 to 7-14 that use WC as an interface.
Table 7-3, Table 7-9: Perform Direct printing.
Table 7-8, Table 7-14: Perform Direct printing.

・operation panel: The following operations in Tables 7-3 to 7-14 that use operation panel as an interface.
Table7-4, Table7-10: The transmission by specifying the destination.
Table7-5, Table7-11: Perform the copy.
Table7-6, Table7-12: The transmission by specifying the destination.
Table7-8, Table7-14: Specify a User Box and execute save in User Box.

・printer driver: The following operations in Tables 7-3 to 7-14 that use printer driver as an interface.

Table7-3, Table7-9: Perform the print.

Table7-8, Table7-14: Save in User Box.

・Fax RX function by fax interface.

FPT_SKP_EXT.1

TOE stores the pre-shared key set by the administrator and the private key of the IPsec certificate, among the encryption keys used for IPsec communication in the SSD that is a Field- nonreplaceable non-volatile storage. Other encryption keys are stored in RAM (see Table 7-15). The TOE does not provide the ability to view stored pre-shared keys, private keys, and encryption keys, so users cannot retrieve them by operating the TOE. The TOE implements RS-232C IF on the MFP itself, but since it is disabled during operation, the user cannot use this interface to retrieve SSD internal data. Other than the RS-232C IF, the interface for retrieving SSD internal data from outside the TOE is not implemented. Because SSD is the field-nonreplaceable storage, user cannot remove SSD and retrieve internal data. Therefore, users cannot read the stored pre-shared key, private key, or encryption key.

7.6. Audit function

TOE generates and records an audit log for the event being audited and sends it to the log server.

FAU_GEN.1, FAU_GEN.2

The TOE defines the following events as the event to be audited and records the event occurrence time (year, month, day, hour, minute, second), event type, subject identification information, and event results.

Table 7-19 List of Events to be Audited

Event to be audited	ID (Subject Identification Information *1)	Operable interface	Results
Perform of User Authentication	Admin ID/User ID/unregistered ID	Operation panel, WC, printer driver	OK/NG
Perform of Memory RX user box password authentication	User ID	Operation panel, WC	OK/NG
Registration, modification, and deletion by the User management function	Admin ID	Operation panel, WC	OK/NG
Modification of User password	User ID	Operation panel, WC	OK/NG
Modification of Administrator password	Admin ID	Operation panel,	OK
Modification of User Authentication Settings	Admin ID	Operation panel, WC	OK
Registration and modification of External Authentication Server settings	Admin ID	Operation panel, WC	OK
Modification of the No. of Authentication Failures threshold	Admin ID	Operation panel, WC	OK
Modification of the Prohibited operation Release time of Administrator authentication	Admin ID	Operation panel, WC	OK
Clearing the No. of Authentication Failures (other than U.BUILTIN_ADMIN)	Admin ID	Operation panel, WC	OK
Password rule modification function	Admin ID	Operation panel, WC	OK/NG
Modification of Enhanced Security mode settings	Admin ID	Operation panel, WC	OK
Modification of Date and time information	Admin ID	Operation panel, WC	OK
Modification of System Auto reset time	Admin ID	Operation panel, WC	OK
Modification of Automatic Logout time	Admin ID	WC	OK
Registration, modification and deletion of Trusted Communication Management settings	Admin ID	Operation panel, WC	OK/NG
Registration and modification of Network settings	Admin ID	Operation panel, WC	OK/NG
Start of the Audit Log acquisition function	System ID	Main power ON, Operation panel, WC	OK
End of the Audit Log acquisition function	System ID Unkown User ID	Main power OFF, Operation panel, WC	OK
Registration and modification of Audit Log management function	Admin ID	Operation panel, WC	OK
Registration, modification, and deletion of personal user box by User box management functions	Admin ID/User ID	Operation panel, WC	OK/NG
Registration, modification of Memory RX setting function	Admin ID	Operation panel, WC	

Execution of Firmware update function	Admin ID	Operation panel	OK/NG
Storing a print job (Table7-3 Operation"Create")	User ID	printer driver, WC	OK/NG
Printing a print job (Table7-3 Operation"Read")	User ID	Operation panel	OK/NG
Sending a scan job (Table7-10 Operation"Create")	User ID	Operation panel	OK/NG
Printing a copy job (Table7-11 Operation"Create")	User ID	Operation panel	OK/NG
Sending a Fax TX job (Table7-12 Operation"Create")	User ID	Operation panel	OK/NG
Receiving a Fax RX job (Table7-13 Operation"Create" Fax without an F code is received from an external fax)	System ID	-	OK/NG
Receiving a Fax RX job (Table7-13 Operation"Create" Fax with an F code is received from an external fax)			
Printing a Fax RX job (Table7-13 Operation"Create" Select the fax document from the memory user box and perform printing)	User ID	Operation panel	OK/NG
Printing a Fax RX job (Table7-13 Operation"Create" Select the fax document from the personal user box and perform printing)			
Storing a saved job (Table7-14 Operation"Create" Save in user box)	User ID	printer driver	OK/NG
Storing a saved job (Table7-14 Operation"Create" Specify the Save in user box and perform direct print)		WC	
Storing a saved job (Table7-14 Operation"Create" Set an original on the scanner unit, specify a personal user box from the user box menu screen, and save in the user box.)		Operation panel	
Storing a saved job (Table7-14 Operation"Create"Specify the Save in User Box and perform a direct print of password encrypted PDF)		WC	
Storing a Fax RX job (Table7-14 Operation"Create"After receiving a fax without an F-code from an external fax, the fax document is saved in the memory RX user box)	System ID	-	OK/NG
Storing a Fax RX job (Table7-14 Operation"Create"After receisving a fax with the specified F-code from an external fax, the fax document is saved in the specified personal user box)			

Printing a saved job (Table7-14 Operation"Create" Select a document from the personal user box and print it)	User ID	Operation panel	OK/NG
Sending a saved job (Table7-14 Operation"Create"Select a document from the personal user box and send it)	User ID	Operation pane, WC	OK/NG
Fax sending a saved job (Table7-14 Operation"Create" Select a document from the personal user box and fax TX it)	User ID	Operation panel	OK/NG
Downloading a saved job (Table7-14 Operation"Create" Select a document from the personal user box and download it)	User ID	WC	OK/NG
Downloading a saved job (Table7-14 Operation"Create" Select the fax document from the memory RX user box and download it)			
Moving a saved job (Table7-14 Operation"Create" Select the document from the Password Encrypted PDF user box and perform save)	User ID	Operation panel	OK/NG
Moving a saved job (Table7-14 Operation"Create" Select a document from the personal user box and move it)		Operation panel, WC	
Duplicating a saved job (Table7-14 Operation"Create" Select a document from the personal user box and copy it)	User ID	Operation panel, WC	OK/NG
Deleting a saved job (Table7-8 Operation"Delete")	User ID	Operation panel, WC	OK/NG
Deleting a saved job (Table7-7 Operation"Delete")	User ID	Operation panel, WC	OK/NG
Failure of IPsec session establishment	System ID	Operation panel, WC, printer driver (*3)	errNo(*2)

(*1) The ID of the event to be audited (subject identification information) that occurred before identification and authentication records a fixed value such as an unregistered ID.
The system ID (fixed value: system (MFP)) is recorded because no identification and authentication is performed for Fax RX.
The system ID (fixed value: system (MFP)) is recoded in the failure of IPsec session establishment.
The start and end of the audit log acquisition function operate according to the use of the audit log management function and the power on/off, and records the system ID (fixed value: system (MFP)) and Unkown User ID.

(*2) A predetermined error such as "501" (Inconsistent proposals during negotiation) is recorded.

(*3) operation panel: Communication with SMTP server, external authentication server, DNS server, log server, WebDAV server, SMB server
WebConnection: Using WebConnection
printer driver: Operations using the printer driver as an interface in "7.2. Access control function"

<Related interfaces and functions>

・WebConnection: Audit log management function

Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

・operation panel: Audit log management function
Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

・printer driver: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

FAU_STG_EXT.1

TOE provides the Audit Log management function performed by the administrator for enabling/disabling the audit function, how to obtain the audit log, log server, setting of automatic log distribution conditions, and sending and deleting the audit log. Use WebDAV server for the log server. IPsec communication between TOE and the log server is set by the trusted communication management function.

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

Log files temporarily saved in TOE are deleted after conversion to XML data or when an administrator performs the audit log deletion. XML data is deleted at the timing of XML data conversion of the next file, after transmission to the log server is completed. The only interfaces that access the log files and XML data stored temporarily in the TOE are the sending and deletion of audit logs by the administrator, and so unauthorized access by normal users or attackers is not possible.

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.

・End of the audit log acquisition function by turning OFF the power supply
・Start of the audit log acquisition function by turning ON the power
・User Authentication (only administrator login from the operation panel is allowed)
・Sending or deleting audit log by administrator

The restriction is released, by an administrator sends an audit log or performs an audit log deletion and clears the full of the local storage area.

Table 7-20 Audit Log Data Specifications

Handling of audit log data	Overview
Storage area of log information	Store on the SSD
Size to hold log information	Log information is temporarily saved as a log file, converted to XML data, and sent to the log server. Log files can be saved up to 40 MB and converted to XML data for transmission to the log server at any of the following timings. After conversion, the corresponding log file is deleted. ・ When the date and time set by the administrator or the accumulated amount are reached ・ Upon reaching 36 MB ・ When an administrator performs an audit log TX XML data is deleted when the next XML data is generated after sending it to the log server. If the transmission fails, a maximum of 76 MB (40 MB of log file, 36 MB of XML data) is temporarily stored in the TOE.

<Related interfaces and functions>

・WebConnection: Audit log management function
Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・operation panel: Audit log management function
Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

FPT_STM.1

TOE has a clock function and provides only the administrator with the function to change the time of TOE. Time information to be recorded in the audit log is provided by the clock function.

<Related interfaces and functions>

・WebConnection: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・operation panel: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"
・printer driver: Operations that generate audit logs described in "Table 7-19 List of Events to be Audited"

7.7. Trusted operation function

7.7.1. Update function

FPT_TUD_EXT.1

The administrator can confirm the firmware version on the administrator screen after the identification and authentication from the operation panel or WC.

In addition, the administrator can install a USB memory storing firmware data and digital signature data in the TOE and perform the firmware update function on the administrator screen after the identification and authentication on the operation panel. Firmware data includes various firmware such as system controller and print controller, and hash value information for each firmware calculated by SHA-256 (used for self-test function described in 7.7.2). Digital signature data is data signed with the RSA digital signature algorithm (key length 2048 bit, 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, the TOE verifies the digital signature of the firmware data by using the RSA public key (key length 2048 bit, installed in TOE at the time of shipment) before starting the installation. If the signature verification fails, a warning is displayed on the operation panel and firmware is not rewritten. If the signature verification is successful, the firmware and the hash value information for each firmware is installed. The procedures for digital signature verification are as follows.

(1) Decrypt the digital signature data with the RSA public key (key length 2048 bit) owned by TOE.
(2) Calculate the hash value of the firmware data by SHA-256.
(3) Compare the values of (1) and (2). The firmware data is judged to be correct if the data are matched.

<Related interfaces and functions>

・WebConnection: Firmware version confirmation function
・operation panel: Firmware version confirmation function
Firmware update function via USB memory
・USB interface for firmware update

7.7.2. Self-test function

FPT_TST_EXT.1

TOE performs the tests described in the table below in sequence, when the power is turned on. If an error is detected, display a warning on the operation panel, stop the operation, and will transit to the status not to accept the operation. This confirms the integrity of the firmware that performs TSF.

Table 7-21 Self-test

No.	Target	Test
1	Various firmware such as system controllers	Confirm that the hash value for each firmware calculated by SHA-256 matches the value recorded in the hash value information installed in TOE by the update function. The encryption library used in TOE is also subject to hash value verification.
2	Encryption Library Algorithm: SHA, HMAC, etc.	Known Answer Test for each encryption algorithm: KAT test for SHA-512, KAT test for HMAC SHA-256, KAT test for AES encryption (CBC, 128-bit key), KAT test for AES decryption (CBC, 128-bit key), KAT for RSA 2048-bit

No.	Target	Test
		(PKCS #1 v1.5), KAT for Diffie-Hellman are performed.
3	Encryption Library Algorithm: DRBG	Set the software to be used as the entropy source and perform the health test of the DRBG function (Known Answer Test of Instantiate, Generate, and Reseed Functions based on "11.3 Health Testing" in NIST SP800-90A).

<Related interfaces and functions>

・Self-test function at main power ON

7.8. Fax separation function

FDP_FXS_EXT.1

TOE implements fax interfaces for receiving faxes from external fax devices via public lines and by sending faxes from the operation panel. The data permitted to be sent and received through the fax interface is only the fax documents described above use.

TOE implements fax modem functions and supports the Super G3 and G3 protocols. The fax modem only performs Fax TX and RX, and does not accept any other commands through the public line. The TOE also does not have a function to form a network bridge between the PSTN and the LAN.

Therefore, user can use the TOE Fax interface only for the Fax TX and RX.

<Related interfaces and functions>

・Fax TX and RX function by fax interface

---End---