TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci Series with FAX System

Security Target

Version 1.20

December 27, 2023

KYOCERA Document Solutions Inc.

- History of Revisions-

Date	Version	Detail
2019-08-02	0.90	First release
2020-02-06	0.91	Modified for corresponding ORs.
2020-05-18	0.92	Modified for corresponding ORs.
2020-05-21	0.93	Modified for corresponding ORs.
2020-06-12	0.94	Modified for corresponding ORs.
2020-11-11	0.95	Modified for corresponding ORs.
2021-03-04	1.00	Modified for corresponding ORs.
2023-02-02	1.10	Add products.
2023-12-27	1.20	Update version

Table of Contents

List of Figures

List of Tables

1. ST Introduction

1.1. ST Reference

ST Title	TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci Series with FAX System Security Target
ST Version	1.20
Date	December 27, 2023
Author	KYOCERA Document Solutions Inc.

1.2. TOE Reference

TOE Title : TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci, TASKalfa 7054ciG, TASKalfa 6054ciG, TASKalfa 5054ciG, TASKalfa 4054ciG, TASKalfa VFM601ci, TASKalfa VFM501ci, TASKalfa VFM401ci (KYOCERA), 7008ci, 6008ci, 5008ci, 4008ci(TA Triumph-Adler/UTAX), with FAX System

Remarks :
The models with FAX System are the products that comprise the models such as TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci, TASKalfa 7054ciG, TASKalfa 6054ciG, TASKalfa 5054ciG, TASKalfa 4054ciG, TASKalfa VFM601ci, TASKalfa VFM501ci, TASKalfa VFM401ci, 7008ci, 6008ci, 5008ci, 4008ci and the following additional options:

- FAX Option (FAX System 12)

TOE Version : System : 2XC_S0IS.C03.317
FAX : 3R2_5100.003.012

Developer : KYOCERA Document Solutions Inc.

Applicable MFP : KYOCERA TASKalfa 7054ci, KYOCERA TASKalfa 6054ci,
KYOCERA TASKalfa 5054ci, KYOCERA TASKalfa 4054ci,
KYOCERA TASKalfa 7054ciG, KYOCERA TASKalfa 6054ciG,
KYOCERA TASKalfa 5054ciG, KYOCERA TASKalfa 4054ciG,
KYOCERA TASKalfa VFM601ci, KYOCERA TASKalfa VFM501ci,
KYOCERA TASKalfa VFM401ci,
TA Triumph-Adler 7008ci, TA Triumph-Adler 6008ci,

TA Triumph-Adler 5008ci, TA Triumph-Adler 4008ci,
UTAX 7008ci, UTAX 6008ci, UTAX 5008ci, UTAX 4008ci

This TOE is identified by a combination of the respective MFP titles as listed in the TOE title and each version of the two kinds of firmwares, which is installed on the above-described TOE. There are multiple MFP titles as listed above, however the MFP components are all the same. The only differences are print speed and sales destinations.

1.3. TOE Overview

1.3.1. TOE Type

The TOE defined in this ST is a Multi-Function Printer (MFP) manufactured by KYOCERA Document Solutions Inc., namely, “TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci, TASKalfa 7054ciG, TASKalfa 6054ciG, TASKalfa 5054ciG, TASKalfa 4054ciG, TASKalfa VFM601ci, TASKalfa VFM501ci, TASKalfa VFM401ci, 7008ci, 6008ci, 5008ci, 4008ci”, each of which includes mainly Copy function, Scan function, Print function, FAX function and Box function. As for the FAX function, the optional FAX System 12 must be installed on the device to be available.

1.3.2. TOE Usage

This TOE can perform copying (duplication), printing (paper output), sending (electronization) and storing (accumulation) of various documents handled by users. The TOE is located in a common office environment and is not only used as a standalone but also connected to LAN for the use in the network environment. In the network environment, the TOE is assumed to be used by connecting to a server and a client PC on the internal network protected from unauthorized access on the external network by firewall. And, the TOE is assumed to be used by connecting to a Local Port (USB Port). In this user environment, the above-mentioned operational functions can be performed through operations on the operation panel or from the client PCs on the network and of the local connection.

Figure 1-1 shows a normal user environment.

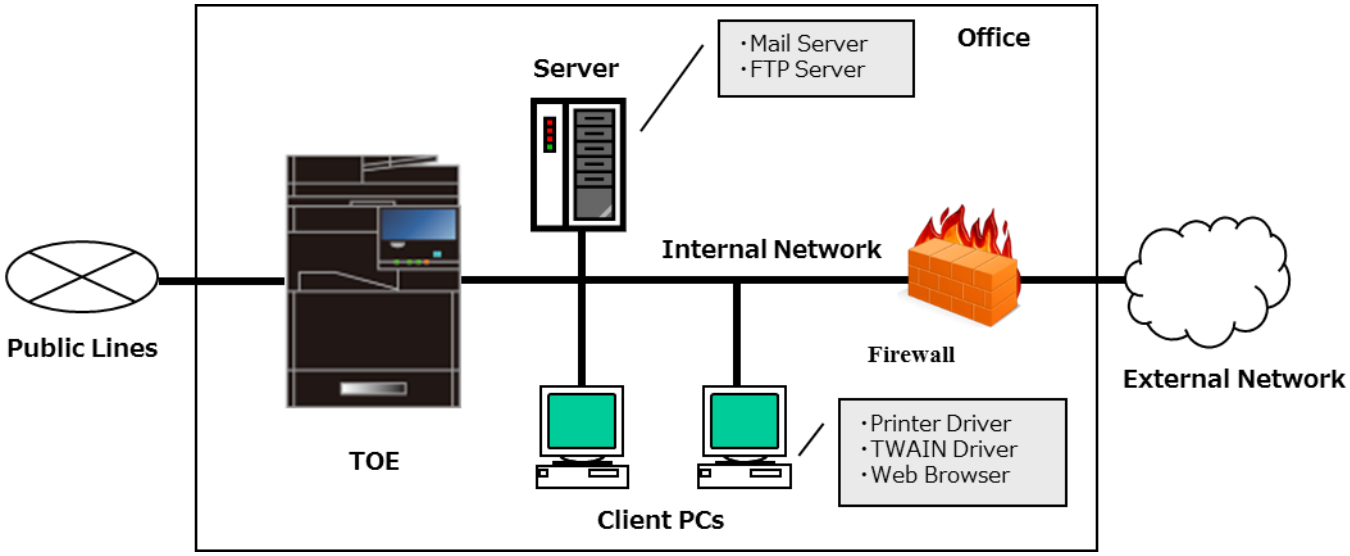

Figure 1-1 Common usage in the offices

The environment to use the common functions of the TOE is illustrated as follows.

- Internal Network :
  The network environment inside the office protected from unauthorized access on the external network by firewall.

- Client PC:
  It is connected to the MFP via the internal network or a Local Port (USB Port). The common functions of the MFP can be available upon receipt of a user instruction.
  Client PC needs the following:
  - Printer Driver
  - TWAIN Driver
  - Web Browser

- Server:
  It is used when sending the documents in the MFP. The following servers are needed.
  - Mail Server
  - FTP Server

- Public Line:
  A public line is needed when sending and receiving the documents in the MFP by the FAX.

1.3.3. Required Non-TOE Hardware, Software and Firmware

Required Non-TOE Hardware, Software and Firmware name is as follows.

- Client PCs:
  - Printer Driver : KX Driver
  - TWAIN Driver : Kyocera TWAIN Driver
  - Web Browser : Microsoft Internet Explorer 11.0
- Mail Server : IPsec(IKEv1) should be available.
- FTP Server : IPsec(IKEv1) should be available.

1.3.4. Major Security Features of TOE

The TOE can perform copying, printing, sending scanned data, FAX (send/receive) and Box storage of various documents handled by users. To prevent alteration and leaks of these documents, the TOE has functions to identify and to authenticate users, to control access to image data, to encrypt image data stored on SSD, to control forwarding the data received from public line to external network, to generate and to refer audit logs, to allow only authorized users to make security function related settings, to perform the TOE self-test, and to protect the network.

1.4. TOE Description

1.4.1. TOE user

User roles related to the use of the TOE are defined as follows.
There are two kinds of users, Normal User and Administrator.

- Normal User
  A person who uses functions provided by TOE, like Copy function, Print function, Scan to Send function, FAX function, and Box function.
- Device Administrator
  A person who manage operations of TOE and registered as an Administrator. A device administrator has privilege to manage device configuration, installation and operation for the TOE correct behavior.

1.4.2. Physical Configuration of TOE

The conceptual figure of physical configuration of the TOE is shown in Figure 1-2.

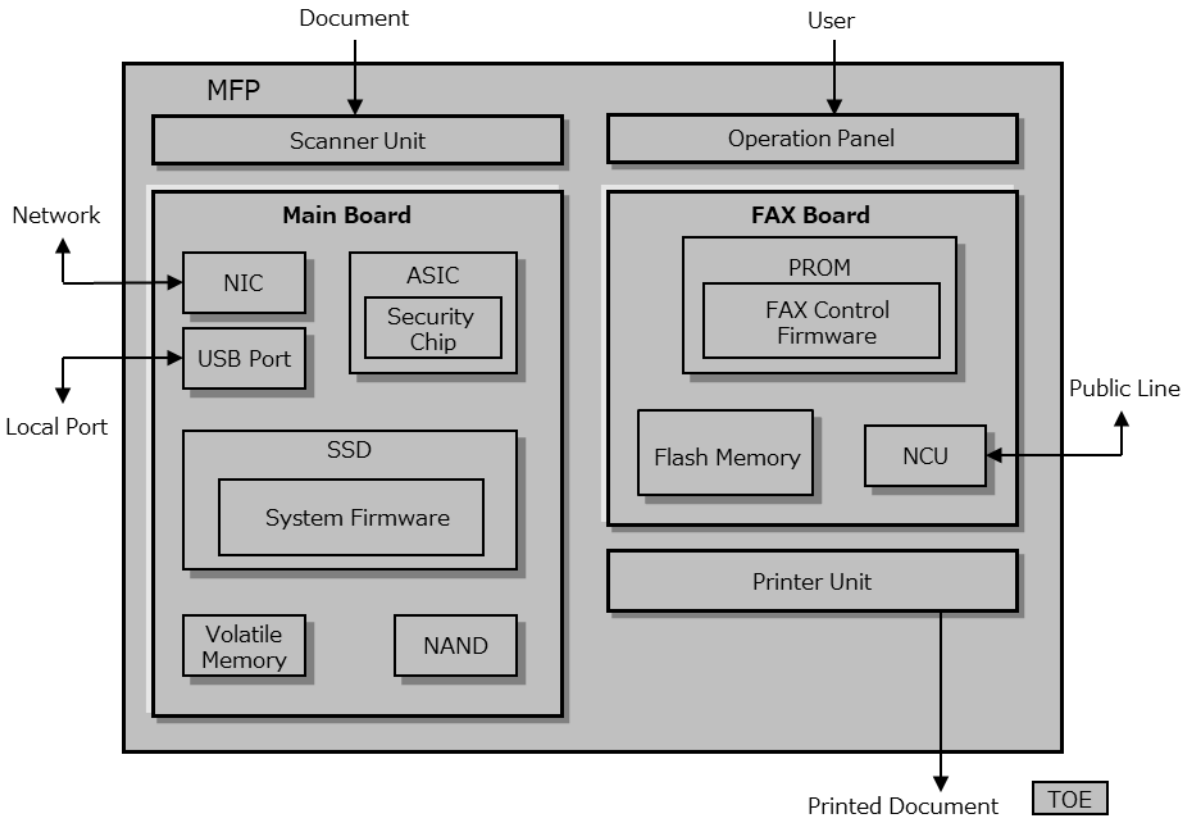

Figure 1-2 Physical Configuration of TOE

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Main Board, a FAX Board, SSD hardware, and firmwares.
The Operation Panel is the hardware that displays status and results upon receipt of input by the TOE user. The Scanner Unit and the Printer Unit are the hardware that input document into MFP and output as printed material.
A Main Board is the circuit board to control entire TOE. A system firmware is installed on a SSD, which is positioned on the Main Board. The Main Board has a Network Interface (NIC) and a Local Interface (USB Port).
ASIC that is also on the Main Board includes a Security Chip, which shares installation of some of the security functions. The Security Chip realizes security arithmetic processing for SSD encryption function
(See below).
A FAX control firmware that controls FAX communication is installed on the PROM, which is positioned on the FAX Board. Additionally, a FAX Board has a NCU as an interface.

As for memory mediums, a NAND that stores device settings, a Volatile Memory that is used as working area and a SSD for the system firmware installation or image data are positioned on the

Main Board. A Flash Memory that stores FAX receive/send image, and a PROM for the FAX control firmware installation are positioned on the FAX Board. Any of the above memory mediums are not removable. Only the FAX receive/send image is stored in the Flash Memory. Image data handled by other basic functions is stored in the SSD.

The delivery method for each TOE components is as follows. Guidance is also a part of TOE.

Table 1-1 Delivery method for each TOE components

TOE Configuration	Form	Delivery Method	Identification Information
MFP Device	MFP Device	Courier	MFP product name and firmware version information described in TOE Reference + Mass storage device: Not installed
Fax	FAX Board	Courier	FAX System 12
Guidance	Paper document, PDF format file in DVD	Included in the box of the MFP device.	Name and version described in Table 1-2.

* Firmware is preinstalled in the MFP

1.4.3. Logical Configuration of TOE

The conceptual figure of logical configuration of the TOE is shown in Figure 1-3.

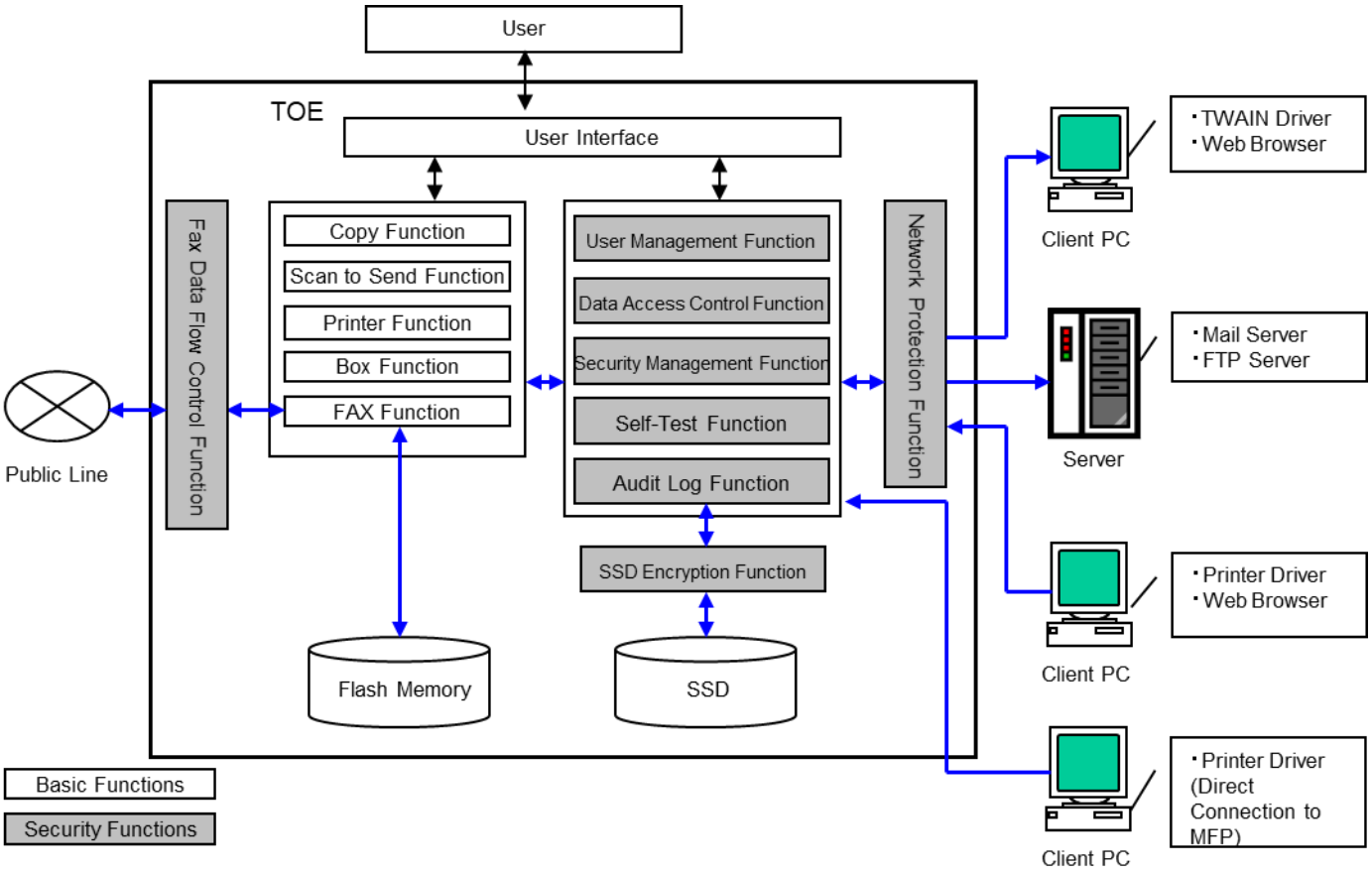

Figure 1-3 Logical Configuration of TOE

1.4.3.1. Basic Functions provided by TOE

The TOE provides the following basic functions.

- Copy Function

  A function that reads image data from the Scanner of the TOE and outputs from the Printer Unit of the TOE by inputting or operating from the Operation Panel by normal users. (Execute a Copy job)

- Scan to Send Function

  A function that sends image data to client PCs or servers connected via LAN by inputting or operating from the Operation Panel and the TWAIN Driver of Client PCs by general users. The following types of send functions are available. (Execute a Scan to Send job)

  - FTP send (FTP Server)
  - E-mail send (Mail Server)

- TWAIN send (TWAIN Driver)

- Print Function

  A function that outputs received image data from the Printer Unit of the TOE by printing instructions from Client PCs connected over LAN or a local port to MFP by normal users. The printing instructions are given from the printer driver installed on Client PCs. The function also supports printing from a USB Memory connected to the local port. The printing instructions are given from the Operation Panel. (Execute a Print job)

- Fax Function

  A function that sends and receives documents by FAX via public line. As for FAX Send, the scanned image data will be sent by FAX to outside. Whereas for FAX Reception, the received image data will be outputted from the Print Unit of the TOE, and then forwarded to outside. (Execute a FAX Send job)

- Box Function

  A function that stores image data in the Box, reads image data from the Box and then sends it or print it by normal users. Image data can also be moved or joined inside the box.

  Inputted image data is stored in the SSD by inputting/operating by normal users from the Operation Panel or the Client PCs connected over LAN or directly connected with MFP. In addition, image data transmitted/received by using the FAX function is stored in the Flash Memory. Stored image data can be outputted from the Print Unit of the TOE or sent to a server such as a Client PC, a mail server and other faxes over public line. Stored image data can also be deleted. When inputting from Client PCs, printer driver is used, and when operating from Client PCs, web browser is used. The following types of send functions are available.

  - FTP send (FTP Server)
  - E-mail send (Mail Server)
  - TWAIN send (TWAIN Driver)
  - FAX send (Other faxes)
  - USB Memory send (USB Memory)

1.4.3.2. Security Functions provided by TOE

TOE provides the following security functions.

- User Management Function

  A function that identifies and authenticates users so that only authorized users can use the TOE. When using the TOE from the Operation Panel and Client PCs, a user will be required to enter his/her login user name and login user password for identification and

authentication. The User Management Function includes a User Account Lockout Function, which prohibits the users access for a certain period of time if the number of identification and authentication attempts consecutively result in failure, a function, which protects feedback on input of login user password when performing identification and authentication and a function, which automatically logouts in case no operation has been done for a certain period of time.

- Data Access Control Function
  A function that restricts access so that only authorized users can access to image data stored in the TOE.

- FAX Data Flow Control Function
  A function that controls forwarding the data received from public line to the TOE's external interface, following to the FAX forward setting.

- SSD Encryption Function
  A function that encrypts information assets stored in the SSD in order to prevent leakage of data stored in the SSD inside the TOE.

- Audit Log Function
  A function that records and stores the audit logs of user operations and security-relevant events on the SSD. This function provides the audit trails of TOE use and security-relevant events. Stored audit logs can be accessed only by a device administrator. The stored audit logs will be sent by email to the destination set by the device administrator.

- Security Management Function
  A function that sets security functions of the TOE. This function can be used only by authorized users. This function can be utilized from an Operation Panel and a Client PC. Operations from a Client PC use a web browser.

- Self-Test Function
  A function that verifies the integrity of TSF executable code and TSF data to detect unauthorized alteration of the executable code of the TOE security functions.

- Network Protection Function
  A function that protects communication paths to prevent leaking and altering of data by eavesdropping of data in transition over the internal network connected to TOE.
  This function verifies the propriety of the destination to connect to and protects targeted information assets by encryption, when using a Scan to Send Function, a Print Function, a Box Function and a BOX Function from a Client PC (web browser), or a Security Management

Function from a Client PC (web browser). However, usage of a Print Function directly connected to a MFP is exception.

1.4.4. Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Maintenance Interface

1.4.5. Guidance

The guidance comprising the TOE is shown below.

Table 1-2 Guidance that comprises TOE

Name	Version
Notice (KYOCERA)	302XC5641003
Notice (KYOCERA VFM)	302XC5644001
Notice (Copystar)	302XC5642001
Notice (TA Triumph-Adler/UTAX)	302XC5643003
FAX System 12 Installation Guide	303RK5671101
TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa VFM601ci / TASKalfa 5054ci / TASKalfa VFM501ci / TASKalfa 4054ci / TASKalfa VFM401ci /TASKalfa 3554ci / TASKalfa VFM351ci / TASKalfa 2554ci / TASKalfa VFM251ci First Steps Quick Guide	302XC5606002
TASKalfa 2554ci / TASKalfa 3554ci / TASKalfa 4054ci / TASKalfa 5054ci / TASKalfa 6054ci / TASKalfa 7054ci Operation Guide	2XCKDEN000
TASKalfa 2554ci / TASKalfa VFM251ci / TASKalfa 3554ci / TASKalfa VFM351ci / TASKalfa 4054ci / TASKalfa VFM401ci / TASKalfa 5054ci / TASKalfa VFM501ci / TASKalfa 5004i / TASKalfa VFM501i / TASKalfa 6054ci / TASKalfa VFM601ci / TASKalfa6004i / TASKalfa VFM601i / TASKalfa 7054ci / TASKalfa 7004i Safety Guide	302XC5628001
FAX System 12 Operation Guide	3RKKDEN300
Data Encryption/Overwrite Operation Guide	3MS2XCKDEN1
Command Center RX User Guide	CCRXKDEN23
TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa 5054ci / TASKalfa 4054ci / TASKalfa 3554ci / TASKalfa 2554ci Printer Driver User Guide	2XCCLKTEN750.2020.02
KYOCERA Net Direct Print User Guide	DirectPrintKDEN2.2019.2

1.4.6. Protected Assets of TOE

Protected Assets of TOE are described below.

(1) Image data

The image data that is stored on the SSD in the TOE when a Normal User uses TOE basic functions such as Copy function, Scan to Send function, Print function, Fax function, and Box function. However when a USB memory locally connected to the TOE is specified in Box function, the image data will be stored in the USB memory. Also when Fax function is used, the image data will be stored in the Flash memory. Other function stores image data on the SSD.

(2) TOE configuration data

The data shown in Table 1-3. They are set or registered by Device Administrator or Normal User to control and use TOE security functions.

(3) Communication data on the internal network

The data flow on the internal network when a Normal User uses basic functions or when a Device Administrator changes or manages security settings of TOE via Web interface. It includes both of document data and TOE setting data.

Table 1-3 TSF Data to be targeted by the TOE

TSF Data	Explanation
Login User Name	User's identification information that is used for the User Management Function.
User Authorization	User's authorization information that is used for the User Management Function. There are two kinds of authorization such as Device Administrator and Normal User in the TOE.
Owner Information	Owner Information that targeted assets hold. Login user name is assigned to the owner information.
Number of Retries until Locked (User Account Lockout Policy Settings)	Number of retries until user account is locked out. This information is used for the user management function.

Lockout Duration (User Account Lockout Policy Settings)	Time duration of rejection before user account is unlocked. This information is used for the user management function.
Lockout List	User list that shows users with their user names who are locked out for user management function. Release of lockout on per user account basis from the list can be instructed by a device administrator.
Auto Logout Time Setting	Time information about automatic termination of login session.
Password Policy Settings	Information that is used for setting Password Policy such as password length, complexity and validity period.
Box Owner	Setting for showing the box owner. Login user name is assigned to the owner information.
Box Permission	Setting for sharing documents inside a box with all users. When box permission is enabled , all the users can access to the box.
Date and Time Settings	Setting information for date and time
Network Encryption Setting	Setting information for TLS and IPsec encryption communication, which is used for Network Protection function.
FAX Forward Setting	Setting for forwarding of received fax data.
Send destination information for Audit Log Report	Destination information when sending audit log report to an administrator.
Login User Password	Authentication information of users that is required for user management function.
Audit Log	Log data that are generated by an audit log function.

2. Conformance Claim

2.1. CC Conformance Claim

The CC conformance claim of this ST and TOE is as follows.

CC version for which this ST and TOE claim conformance:

Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model Version 3.1 Revision 5
Part2: Security functional components Version 3.1 Revision 5
Part3: Security assurance components Version 3.1 Revision 5

Conformity of ST to CC Part 2: CC part 2 conformant
Conformity of ST to CC Part 3: CC part 3 conformant

2.2. PP Claims

No PP to which this ST and TOE are conformant.

2.3. Package Claims

The ST and TOE claim the package: EAL2 and addition. Additional Component is ALC_FLR.2.

2.4. Conformance Rationale

There is no rationale that the ST and TOE conform to PP because no PP is claimed.

3. Security Problem Definitions

This section describes Threats, Organizational Security Policies and Assumptions.

3.1. Threats

Threats is identified shown in Table 3-1. Attacker shall have a basic ability to attack TOE.

Table 3-1 Threats

Threat	Description
T.SETTING_DATA	Malicious person may have unauthorized access to, to change, or to leak TOE setting data via the operation panel or client PCs.
T.IMAGE_DATA	Malicious person may illegally access not authorized image data via the operation panel or Client PC and leak or alter them.
T.NETWORK	Malicious person may illegally eavesdrop or alter image data or TOE setting data on the internal network.

3.2. Organizational Security Policies

Organizational Security Policies that must be conformed by the TOE is shown in Table 3-2.

Table 3-2 Organizational Security Policies

Name	Definition
P.SSD_ENCRYPTION	TOE must encrypt image data and TOE setting data stored on SSD.
P.FAX_CONTROL	TOE must control forwarding data received from public line and send it to external interface according with rules set by authorized roles.
P.SOFTWARE_VERIFICATION	TOE must execute Self Test that verify execution code of TSF to detect corruption of executable code.

3.3. Assumptions

Assumbtions of the TOE is shown in Table 3-3.

Table 3-3 Assumptions

Assumption	Definition
A.ACCESS	The hardware and software that are composed of TOE are located in a protected environment from security invasion such as illegal analysis and alteration.
A.NETWORK	The TOE is connected to the internal network that is protected from illegal access from the external network.
A.USER_EDUCATION	The TOE users are aware of the security policies and procedures of their organization, and are educated to follow those policies and procedures.
A.DADMIN_TRUST	The TOE's administrators are competent to manage devices properly as a device administrator and have a reliability not to use their privileged access rights for malicious purposes.

4. Security Objectives

This section describes Security Objectives for TOE, Security Objectives of Operational Environment and Security Objectives Rationale.

4.1. Security Objectives for the TOE

Security Objectives for the TOE is shown in Table 4-1.

Table 4-1 Security objectives for the TOE

Objective	Definition
O.SSD_ENCRYPTION	The TOE shall provide a function to encrypt image data and TOE setting data stored in SSD in order to prevent unauthorized decryption.
O.AUDIT_LOG	The TOE shall provide a function to record auditable event and provide audit logs in order to monitor unauthorized access.
O.NETWORK_ENCRYPTION	The TOE shall provide encrypted communication function required on network protection in order to protect image data and TOE setting data on the internal network from eavesdropping or alteration.
O.FAX_CONTROL	The TOE shall provide a function to control FAX data flow to forward received data from public line to external interfaces of TOE according with rules set by authorized role.
O.SETTING_DATA	The TOE shall authorize access to the TOE setting data only for authenticated right users, and prevent access to the TOE setting data by unauthorized users, and prevent change or leak of TOE setting data.
O.ACCESS_CONTROL	The TOE shall provide a function to ensure that the TOE identifies and authenticates users, and controls access privilege to image data in order only authorized user can access to the image data.
O.SOFTWARE_VERIFICATION	The TOE shall provide a function to self-verify executable code in the TSF.

4.2. Security Objectives for the operational environment

Security Objectives for the operational environment is shown in Table 4-2.

Table 4-2 Security objectives for the operational environment

Objective	Definition
OE.ACCESS	The TOE shall be placed in a secure or monitored area and Device Administrator can monitor it so that it provides protection from attacks such as unmanaged analyze and alteration to hardware and software in the TOE.
OE.NETWORK_PROTECTION	The internal network that the TOE connected to shall prevent attacks from the external network to the TOE by introducing appliance such as a firewall.
OE.USER_EDUCATION	The organization shall make the TOE users aware of the security policies and procedures of their organization, and make them educated and acquired to follow those security policies and procedures.
OE.DADMIN_TRUST	The device administrator shall be elected a trustworthy person and received enough guidance to comply security policy and operation rules in the belonged organization and to be able appropriate operation following the description in the product's guidance.

4.3. Security Objectives rationale

The relation among assumption, threat, and organizational security policy is shown in the table below. It describes that one Security Objective corresponds at least one assumtion, threat, and organizational security policy.

Table 4-3 Completeness of security objectives

Security Objectives	Assumption, Threat, and Organizational security policy									
	A.ACCESS	A.NETWORK	A.USER_EDUCATION	A.DADMIN_TRUST	T.SETTING_DATA	T.IMAGE_DATA	T.NETWORK	P.SSD_ENCRYPTION	P.FAX_CONTROL	P.SOFTWARE_VERIFICATION
O.SSD_ENCRYPTION								✓		
O.AUDIT_LOG					✓	✓	✓			
O.NETWORK_ENCRYPTION							✓			
O.FAX_CONTROL									✓	
O.SETTING_DATA					✓					
O.ACCESS_CONTROL						✓				
O.SOFTWARE_VERIFICATION										✓
OE.ACCESS	✓									
OE.NETWORK_PROTECTION		✓								
OE.USER_EDUCATION			✓							
OE.DADMIN_TRUST				✓						

Also the Security Objectives Rationale for Assumptions, Threats, and Organizational Security Policy is shown in Table 4-4.

Table 4-4 Sufficiency of security objectives

Assumptions, Threats, and Organizational Security Policy	Security Objectives Rationale
A.ACCESS	Assumptions of A.ACCESS requires that the hardware and software that are composed of TOE are located in a protected environment from security invasion such as illegal analysis and alteration. By OE.ACCESS, the TOE is placed in a secure or monitored area that it provides protection from attacks such as unmanaged analyze and alteration to hardware and software in the TOE. Therefore the methods or opportunities of attacks are restricted and A.ACCESS can be achieved.
A.NETWORK	Assumptions of A.NETWORK requires that the TOE is connected to the internal network that is protected from illegal access from the external network. By OE.NETWORK_PROTECTION, the internal network that the TOE connected to prevents attacks from the external network to the TOE by introducing appliance such as a firewall. Therefore the methods or opportunities of attacks by many and unspecified agents on the external network are restricted and A.NETWORK can be achieved.
A.USER_EDUCATION	Assumptions of A.USER_EDUCATION requires that the TOE users are aware of the security policies and procedures of their organization, and are educated to follow those policies and procedures. By OE.USER_EDUCATION, the organization makes the TOE users aware of the security policies and procedures of their organization, and make them educated and acquired to follow those security policies and procedures. Therefore A.USER_EDUCATION can be achieved.

A.DADMIN_TRUST	Assumptions of A.DADMIN_TRUST requires that the TOE's administrators are competent to manage devices properly as a device administrator and have a reliability not to use their privileged access rights for malicious purposes. By OE.DADMIN_TRUST, the device administrator is elected a trustworthy person and received enough guidance to comply security policy and operation rules in the belonged organization and to be able appropriate operation following the description in the product's guidance. Therefore A.DADMIN_TRUST can be achieved.
T.SETTING_DATA	To counter T.SETTING_DATA, it is required to prevent to have unauthorized access to, to change, or to leak TOE setting data via the operation panel or client PCs. By O.SETTING_DATA and O.AUDIT_LOG, this threat can be countered. By O.SETTING_DATA, the TOE authorizes access to the TOE setting data only for authenticated right users, and prevent access to the TOE setting data by unauthorized users, and prevent change or leak of TOE setting data. Therefore unauthorized access, change, or leak of TOE setting data can be prevented. By O.AUDIT_LOG, the TOE can record auditable event and provide audit logs. Therefore unauthorized access to the setting data can be monitored and tracked.

T.IMAGE_DATA	To counter T.IMAGE_DATA, it is required to prevent to have unauthorized access to, to leak, or to alter image data via the operation panel or client PCs. By O.ACCESS_CONTROL and O.AUDIT_LOG, this threat can be countered. By O.ACCESS_CONTROL, the TOE identifies and authenticates users accessing via operation panel or client PCs, and controls access privilege to image data in order only authorized user can access to the image data. Therefore TOE can prevent unauthorized access, leak or alteration of image data. By O.AUDIT_LOG, the TOE records auditable event and provide audit logs. Therefore unauthorized access to the image data can be monitored and tracked.
T.NETWORK	To counter T.NETWORK, it is required to prevent eavesdropping or alteration on the image data and the TOE setting data on the internal network. By O.NETWORK_ENCRYPTION and O.AUDIT_LOG, this threat can be countered. By O.NETWORK_ENCRYPTION, the TOE provide encrypted communication function required on network protection. Therefore eavesdropping and alteration of the image data and the TOE setting data on the internal network can be prevented. By O.AUDIT_LOG, the TOE records auditable event and provide audit logs. Therefore the behavior of encryption communication function, to protect the image data or the TOE setting data from eavesdropping or alteration, can be monitored and tracked.

P.SSD_ENCRYPTION	P.SSD_ENCRYPTION of the security objective of the organization is supposed to encrypt the image data and the TOE setting data to maintain confidentiality of these data stored on the SSD. By O.SSD_ENCRYPTION, the TOE encrypts image data and TOE setting data stored in SSD. Therefore this security objective can be achieved.
P.FAX_CONTROL	P.FAX_CONTROL in the security objective of the organization is supposed that received data from public line is forwarded to the external interface of TOE according with rules set by authorized roles when the data is forwarded to the external interface. By O.FAX_CONTROL, the TOE controls FAX data flow to forward received data from public line to external interfaces of TOE according with rules set by authorized roles. Therefore this security objective can be achieved.
P.SOFTWARE_VERIFICATION	P.SOFTWARE_VERIFICATION in the security objective of the organization is supposed that the TOE executes Self Test that verifies executable code of TSF in order to detect corruption of executable code. By SOFTWARE_VERIFICATION, the TOE executes Self Test that verifies executable code in the TSF. Therefore this security objective can be achieved.

5. Extended Components Definition

No extended components defined.

6. Security Requirements

This section describes the TOE Security Functional Requirements.

6.1. TOE Security Functional Requirements.

6.1.1. Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
- [assignment: other specifically defined auditable events].

[selection, choose one of: *minimum, basic, detailed, not specified*]

- not specified

[assignment: *other specifically defined auditable events*]

- Auditable data target of TOE shown in Table 6-1

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

[assignment: *other audit relevant information*]

- Target function regarding FDP_ACF.1, Tried user identification regarding FIA_UID.1, IP address of failed trusted channel (Source IP address is not required since it is fixed IP address of TOE itself.)

Table 6-1 Auditable data requirements

Functional Requirement	Auditable event	Actions to be audited defined by CC
FAU_GEN.1	-	There are no auditable events foreseen.
FAU_GEN.2	-	There are no auditable events foreseen.
FAU_SAR.1	[Not specified] -	a) Basic: Reading of information from the audit records.
FAU_SAR.2	[Not specified] -	a) Basic: Unsuccessful attempts to read information from the audit records.
FAU_STG.1	-	There are no auditable events foreseen.
FAU_STG.4	[Not specified] -	a) Basic: Actions taken due to the audit storage failure.
FCS_CKM.1(a)	[Not specified] -	a) Minimum: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_CKM.1(b)	[Not specified] -	a) Minimum: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_CKM.1(c)	[Not specified] -	a) Minimum: Success and failure of the activity. c) Basic: The object attribute(s), and object value(s) excluding any

		sensitive information (e.g. secret or private keys).
FCS_COP.1(a)	[Not specified] -	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FCS_COP.1(b)	[Not specified] -	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FCS_COP.1(c)	[Not specified] -	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FDP_ACC.1	-	There are no auditable events foreseen.
FDP_ACF.1	[Not specified] Successful requests to perform an operation on an object as the following: ・ Image Data: Read ・ Image Data: Delete	a) Minimum: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.

FDP_IFC.1	-	There are no auditable events foreseen.
FDP_IFF.1	[Not specified]	a) Minimum: Decision permitting requested information flow. b) Basic: All decisions regarding requests for information flow. c) Detailed: The specific security attributes used on the decision of information flow. d) Detailed: The specific subset of information that is flow based on the policy goal (e.g. Degraded audit of objects).
FIA_AFL.1	[Minimum] The following actions taken, when reaching of the threshold for the unsuccessful authentication attempts since the last successful authentication. ・ Perform user account lockout, and the following action taken to restore to the normal state. ・ Release the lockout state by a device administrator.	a) Minimum: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_ATD.1	-	There are no auditable events foreseen.
FIA_SOS.1	[Minimum] Rejection by the tested secrete as shown below: ・ Rejection by quality check of the login user password, which was imputed when initially creating the user information.	a) Minimum: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of

	・Rejection by quality check of the login user password, which was changed when editing the user information.	any changes to the defined quality metrics.
FIA_UAU.1	[Basic] Both successful and unsuccessful use of the authentication mechanism	a) Minimum: Unsuccessful usage in the authentication mechanism; b) Basic: All usages of authentication mechanism; c) Detailed: All TSF mediated actions which were done before user authentication.
FIA_UAU.7	-	There are no auditable events foreseen.
FIA_UID.1	[Basic] Both successful and unsuccessful use of the identification mechanism	a) Minimum: Unsuccessful use of user identification mechanism including provided user identity information; b) Basic: All use of user identification mechanism including provided user identity information;
FIA_USB.1	[Not specified] -	a) Minimum: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).
FMT_MSA.1(a)	[Not specified] -	a) Basic: All modifications of the values of security

		attributes.
FMT_MSA.3(a)	[Not specified] -	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
FMT_MSA.1(b)	[Not specified] -	a) Basic: All modifications of the values of security attributes.
FMT_MSA.3(b)	[Not specified] -	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
FMT_MTD.1(a)	[Not specified] -	a) Basic: All modifications to the values of TSF data.
FMT_MTD.1(b)	[Not specified] -	a) Basic: All modifications to the values of TSF data.
FMT_SMF.1	[Minimum] Use of the management functions	a) Minimum: Use of the management functions.
FMT_SMR.1	[Minimum] Modifications to the group of users that are part of a role	a) Minimum: Modifications to the group of users that are part of a role b) Detailed: All use of privilege of roles.
FPT_STM.1	[Minimum] Changes to the time	a) Minimum: Changes to the time. b) Detailed: Provide of time stamps.
FPT_TST.1	[Not specified] -	a) Basic: Execution of the TSF self tests and the results of the tests.
FTA_SSL.3	[Minimum] Termination of an interactive session by the session locking	a) Minimum: Termination of an interactive session by the session locking

	mechanism	mechanism.
FTP_ITC.1	[Minimum] Failure of the trusted channel functions	a) Minimum: Failure of the trusted channel functions. b) Minimum: Identification of the initiator and target of failed trusted channel functions. c) Basic: All trial of use of trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.

FAU_GEN.2 User identify association

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_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

[assignment: *authorised users*]

- Device Administrator

[assignment: *list of audit information*]

- Auditable event of TOE as shown in Table 6-1.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.

[selection: *choose one of: prevent, detect*]

- prevent

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, *choose one of: "ignore audited events", "prevent audited*

events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"] and [assignment*: other actions to be taken in case of audit storage failure*] if the audit trail is full.

[selection: *choose one of: "ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

- "overwrite the oldest stored audit records"

[assignment: *other actions to be taken in case of audit storage failure*]

- None

6.1.2. Class FCS: Cryptographic Support

FCS_CKM.1(a) Cryptographic key generation (Storage Encryption)

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(a) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: cryptographic key generation algorithm]

- KDF(Feedback Mode)

[assignment: cryptographic key sizes]

- 256 bits

[assignment: list of standards]

- NIST SP800-108

FCS_CKM.1(b) Cryptographic key generation (TLS)

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(b) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [multiple primitives described below] and specified cryptographic key sizes [as described below] that meet the following: [multiple standards as described below].

Table 6-2 Key Generation

Algorithm	Key sizes	Standards
RSA	2048, 4096 bits	FIPS 186-4, Appendix B
AES	128, 256 bits	FIPS 197
ChaCha20-Poly1305	256 bits	RFC8439
TLS key generation via DHE or ECDHE	AES 128, 256 bits	SP 800-135 Rev.1
TLS key generation via DHE or ECDHE	HMAC 160, 256, 384 bits	SP 800-135 Rev.1

FCS_CKM.1(c) Cryptographic key generation (IPSec)

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(c) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] implement [assignment: Diffie-Hellman Groups] that meet the following: [assignment: list of standards].

[assignment: cryptographic key generation algorithm]

- IKEv1KDF

[assignment: Diffie-Hellman Groups]

- Diffie-Hellman Group 14, 16, 17, 18, 19, 20, 21, 22, 23, 24

[assignment: list of standards]

- SP 800-135 Rev.1, RFC 2409, RFC 5114

FCS_COP.1(a) Cryptographic operation (Storage Encryption)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(a) The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: list of cryptographic operations]

- Encryption of image data and TOE setting data when writing into the SSD
- Decryption of image data and TOE setting data when reading out from the SSD

[assignment: cryptographic algorithm]

- AES (XTS mode)

[assignment: cryptographic key sizes]

- 256 bits

[assignment: list of standards]

- FIPS PUB 197, SP800-38E

FCS_COP.1(b) Cryptographic operation (TLS)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(b) The TSF shall perform [the operations listed in the table below] in accordance with a specified cryptographic algorithm [multiple algorithms described below] and cryptographic key sizes [as described below] that meet the following: [multiple standards as described below].

Table 6-3 Cryptographic Operations

Operations	Algorithm	Key/Hash Size in Bits	Standards
Encryption, decryption	AES (CBC mode)	128, 256 bits	FIPS 197 SP800-38A SP800-38D
	AES (GCM mode)		
	ChaCha20-Poly1305	256 bits	RFC8439
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS1-v1_5)	2048, 4096 bits	PKCS #1 v2.2 FIPS 186-4
Hashing	SHA-1	160 bits	FIPS 180-4
	SHA-256, SHA-384	256, 384 bits	FIPS 180-4
Keyed Hash Message Authentication Code	HMAC-SHA-1	160 bits	RFC 2104
	HMAC-SHA-256, HMAC-SHA-384	256, 384 bits	

FCS_COP.1(c) Cryptographic operation (IPSec)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(c) The TSF shall perform [the operations listed in the table below] in accordance with a specified cryptographic algorithm [multiple algorithms described below] and cryptographic key sizes [as described below] that meet the following: [multiple

standards as described below].

Table 6-4 Cryptographic Operations

Operations	Algorithm	Key/Hash Size in Bits	Standards
ISAKMP authentication	Pre-shared key	-	RFC 2409 SP800-77 Rev.1
Hashing	SHA-256, SHA-384, SHA-512	256, 384, 512 bits	FIPS 180-4
Data authentication	HMAC-SHA256-128	256 bits	RFC 2104 RFC 4868
	HMAC-SHA384-192	384 bits	
	HMAC-SHA512-256	512 bits	
Encryption, decryption	3DES (CBC mode)	168 bits	FIPS 46-3 SP 800-67 Rev.2
	AES (CBC mode)	128, 192, 256 bits	FIPS 197 SP800-38A

6.1.3. Class FDP: User Data Protection

FDP_ACC.1 Subset access control

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

FDP_ACC.1.1 The TSF shall enforce the [assignment: Access Control SFP**]** on [assignment: List of subjects, objects, and operations among subjects and objects covered in SFP].

[assignment: the list of subjects, objects, and operations among subjects and objects covered in SFP]

- The list of subjects, objects, and operations among subjects and objects shown in Table 6-5.

[assignment: Access Control SFP]

- User Data Access Control SFP

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ ACF.1.1 The TSF shall enforce the [assignment: Access Control SFP] to objects based on the following: [assignment: the list of users as subjects and objects controlled under the indicated SFP and for each the SFP related security attribute or the named group of SFP related security attribute].

[assignment: the list of users as subjects and objects controlled under the indicated SFP and for each the SFP related security attribute or the named group of SFP related security attribute]

- The subjects and the objects listed in Table 6-5, and for each, the indicated security attributes.

[assignment: Access Control SFP]

- User Data Access Control SFP

FDP_ ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules of access control used to the operations for controlled object among controlled subjects and controlled objects].

[assignment: rules of access control used to the operations for controlled object among controlled subjects and controlled objects]

- Access control rules that controls operations among subjects and objects as listed in Table 6-5

FDP_ ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- Explicitly authorize access control rule as shown in Table 6-6

FDP_ ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment:

rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- None

Table 6-5 User Data Access Control SFP

Object (Security attribute)	Target Function	Operation(s)	Subject (Security attribute)	Access control rule
Image data (Owner Information)	Print function Scan to Send function Copy function Fax send function	Read, Delete	Normal User (Login User Name)	Denied, except for his/her own documents. When "Owner Information" of image data matches "Login User Name" of Normal User, operation is permitted.
Image data (Box Owner, Box Permission)	Box function	Read, Delete	Normal User (Login User Name)	Denied, except (1) for his/her own documents, or (2) if authorized by another role or mechanism if such functions are provided by a conforming TOE. (1) When "Owner Information" of image data matches "Login User Name" of Normal User, operation is permitted. (2)When "Box Permission" storing image data is enabled, operation is permitted.
Image data (Owner Information)	Fax receive function	[assignment: other operations] Any Operations	Normal User (Login User Name)	Denied. Any Operations by Normal User is denied.

Table 6-6 User Data Access Control SFP for Device Administrator

Object (Security attribute)	Target Function	Operation(s)	Subject (Security attribute)	Explicitly authorize access control rule
Image data (Owner Information)	Print function	Delete	Device Administrator (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
Image data (Owner Information)	Scan to Send function	Delete	Device Administrator (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
Image data (Owner Information)	Copy function	Delete	Device Administrator (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
Image data (Owner Information)	Fax send function	Delete	Device Administrator (User Authorization)	Regardless of "Owner Information" value, operation is permitted.
Image data (Box Owner)	Box function	Read, Delete	Device Administrator (User Authorization)	Regardless of "Box Owner" value, operation is permitted.
Image data (Owner Information)	Fax receive function	Read, Delete	Device Administrator (User Authorization)	Regardless of "Owner Information" value, operation is permitted.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple Security attributes

FDP_IFC.1.1 The TSF shall enforce [assignment: information flow control SFP] for [assignment: controlled Subjects used by SFP, or the list of Subjects, Information, and Operations that trigger information flow controlled by the Subject].

[assignment: controlled Subjects used by SFP, or the list of Subjects, Information, and Operations that trigger information flow controlled by the Subject]

- The list of Subjects Information, and Operations as listed in Table 6-7

Table 6-7 The list of Subjects, Information, and Operations that triggers information flow

Subject (Security attribute)	Information	Subject (Security attribute)	Operation	Access control rule
A receiving task from public line (FAX Forward setting)	Received data from public line	A sending task to the external interfaces (FAX Forward setting)	Forwarding	To forward (Operation) data (Information) received from public line by receiving task (Subject) to sending task (Subject) for the external interface according with Fax Forward setting (Security attributes).

[assignment: information flow control SFP]

- Fax information flow control SFP

FDP_IFF.1 Simple Security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_ IFF.1.1 The TSF shall enforce the *[assignment: information flow control SFP]* based on the following types of subjects and information security attributes: [assignment: the list of subjects and information controlled under the indicated SFP, and for each, the correspond security attribute].

[assignment: information flow control SFP]

- Fax information flow control SFP

[assignment: the list of subjects and information controlled under the indicated SFP, and for each, the correspond security attribute]

- Subjects and information and for each, the correspond security attribute as listed in Table 6-7

FDP_ IFF.1.2 The TSF shall authorize information flow among controlled subjects and controlled information through controlled operations when the rules below maintained: [assignment: relation, based on security attributes, that must be maintained among subjects and information security attributes for each operations].

[assignment: relation, based on security attributes, that must be maintained among subjects and information security attributes for each operations]

- the rules of information flow control that control operations among subjects and information as listed in Table 6-7

FDP_ IFF.1.3 The TSF shall enforce [assignment: rules of *additional information flow control SFP*].

[assignment: rules of *additional information flow control SFP*]

- None

FDP_ IFF.1.4 The TSF shall explicitly authenticate information flow based on the [assignment: *rules, based on security attributes, that explicitly authorize information flow*].

[assignment: *rules, based on security attributes, that explicitly authorize information flow*]

- None

FDP_ IFF.1.5 The TSF shall explicitly deny information flow based on the [assignment: *rules, based on security attributes, that explicitly deny information flow*].

[assignment: *rules, based on security attributes, that explicitly deny information flow*]

- None

6.1.4. Class FIA: Identification and Authentication

FIA_AFL.1	**Authentication failure handling**

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

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of*

authentication events].

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

- an administrator configurable positive integer within [assignment: range of acceptable values]

[assignment: range of acceptable values]

- 1 to 10

[assignment: *list of authentication events*]

- Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from an operational panel.
- Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from a client PC.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

[selection: *met, surpassed*]

- met

[assignment: *list of actions*]

- Login from the account is locked out between 1 and 60 minutes and until the time designated by a device administrator that elapse, or until a device administrator releases lock status.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]

- Login User Name, User Authorization

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]

- Password Length : At least 8 characters
- Character Type : Alphanumeric or special characters

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is authenticated.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- Obtain a device status
- Display a list of job information
- Display counter information
- Receive FAX data

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

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

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

[assignment: *list of feedback*]

- dummy characters （* ： asterisk）

FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- Obtain a device status
- Display a list of job information
- Display counter information
- Receive FAX data

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

Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

[assignment: *list of user security attributes*]

- Login User Name, User Authorization

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

[assignment: *rules for the initial association of attributes*]

- None

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *rules for the changing of attributes*]

- None

6.1.5. Class FMT: Security Management

FMT_MSA.1 (a)	**Management of security attributes**

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (a) The TSF shall enforce [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

- User Data Access Control SFP

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

- *[assignment: other operations]*

[assignment: other operations]

- Operation(s) as listed in Table 6-8

[assignment: *list of security attributes*]

- Security Attributes as listed in Table 6-8

[assignment: *the authorised identified roles*]

- Role as listed in Table 6-8

Table 6-8 Management of security attributes (Box function)

Security Attributes	Operation(s)	Role
Box Owner	modify	Device Administrator
Box Permission	modify	Device Administrator
		Normal User that matches a Box Owner.

FMT_MSA.3 (a) Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (a) The TSF shall enforce [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

- User Data Access Control SFP

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- restrictive

FMT_MSA.3.2 (a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]
- nobody

FMT_MSA.1 (b) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (b) The TSF shall enforce [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]
- Fax information flow control SFP

[selection: *change_default, query, modify, delete, [assignment: other operations]*]
- [assignment: other operations]

[assignment: *other operations*]
- Operation(s) as listed in Table 6-9

[assignment: *list of security attributes*]
- Security Attributes as listed in Table 6-9

[assignment: *the authorised identified roles*]
- Role as listed in Table 6-9

Table 6-9 Management of security attributes (Fax receive function)

Security Attributes	Operation(s)	Role
Fax Forward setting	modify	Device Administrator

FMT_MSA.3 (b) Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (b) The TSF shall enforce [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

- Fax information flow control SFP

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- permissive

FMT_MSA.3.2 (b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- Nobody

FMT_MTD.1 (a) Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles.
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to

[assignment: *the authorized identified roles*].

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

- Other operations

[assignment: other operations]

- Operation as listed in Table 6-10

[assignment: *list of TSF data*]

- TSF data as listed in Table 6-10

[assignment: *the authorized identified roles*]

- Roles as listed in Table 6-10

Table 6-10 Operation of TSF data

TSF data	Roles	Operation
Login User Name	Device Administrator	modify, delete, [assignment: other operations] [assignment: other operations] ● Create
Login User Password	Device Administrator	modify, delete, [assignment: other operations] [assignment: other operations] ● Create
User Authorization	Device Administrator	modify, delete, [assignment: other operations] [assignment: other operations] ● Create
Number of Retries until locked (User Account Lockout Policy Settings)	Device Administrator	modify
Lockout Duration (User Account Lockout Policy Settings)	Device Administrator	modify
Lockout List	Device Administrator	modify
Auto Logout Time Setting	Device Administrator	modify
Password Policy Settings	Device Administrator	modify
Date and Time Settings	Device Administrator	modify
Network Encryption Setting	Device Administrator	modify
Send Destination Information for Forwarding Audit Log Report	Device Administrator	modify
Encryption Key	Device Administrator	modify

FMT_MTD.1 (b) Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles.
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to

[assignment: *the authorized identified roles*].

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

- Other operations

[assignment: other operations]

- Operation as listed in Table 6-11

[assignment: *list of TSF data*]

- TSF data as listed in Table 6-11

[assignment: *the authorized identified roles*]

- Role as listed in Table 6-11

Table 6-11 Operation of TSF data

TSF data	Roles	Operation
Login User Password associated with Normal User	Normal User	modify

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

[assignment: *list of management functions to be provided by the TSF*]

- Functions that manage security attributes (i.e. Box Owner, Box Permission and Owner Information) related to a Box function, security attributes of Fax Data Flow Control function(Fax forward setting).
- Functions that manage TSF Data (i.e. Login User Name, Login User Password, User authorization, Number of Retries until Locked, Lockout Duration, Auto Logout Time Setting, Password Policy Settings, Date and Time Settings, Network encryption Setting(TLS, IPsec setting), and Send Destination

Information for Audit Log Report).

Table 6-12 Management Functions

Function Requirement	Management Functions	Management Items defined by CC
FAU_GEN.1	-	There are no management activities foreseen.
FAU_GEN.2	-	There are no management activities foreseen.
FAU_SAR.1	Management of Authorization of Device Administrator	a) Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SAR.2	-	There are no management activities foreseen.
FAU_STG.1	-	There are no management activities foreseen.
FAU_STG.4	None (Action is fixed and is not managed.)	a) Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FCS_CKM.1(a)	-	There are no management activities foreseen.
FCS_CKM.1(b)	-	There are no management activities foreseen.
FCS_CKM.1(c)	-	There are no management activities foreseen.
FCS_COP.1(a)	-	There are no management activities foreseen.
FCS_COP.1(b)	-	There are no management activities foreseen.
FCS_COP.1(c)	-	There are no management activities foreseen.
FDP_ACC.1	-	There are no management activities foreseen.
FDP_ACF.1	None (Attributes used to make explicit access or denial based decisions is fixed as Device Administrator, and this is not needed	a) Managing the attributes used to make explicit access or denial based decisions.

	to be managed.)	
FDP_IFC.1	-	None
FDP_IFF.1	None (There is no attributes used to make explicit access based decisions, and this is not needed to be managed.)	a) Managing the attributes used to make explicit access based decisions.
FIA_AFL.1	Management of unsuccessful authentication attempts.	a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure.
FIA_ATD.1	None (There are no additional security attributes and there are no additional security attributes to be managed.)	a) If so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.
FIA_SOS.1	Management of Login User Password Policy	a) The management of the metric used to verify the secrets.
FIA_UAU.1	Management of login user password by Device Administrator. Management of Normal User (him/her) login user password by Normal User.	a) Management of the authentication data by an administrator; b) Management of the authentication data by the associated user; c) Managing the list of actions that can be taken before the user is authenticated.
FIA_UAU.7	-	There are no management activities foreseen.
FIA_UID.1	Management of the user identities	Management of the user identities
FIA_USB.1	None (Subject security attributes are fixed and are not managed.	a) An authorised administrator can define default subject security attributes. b) an authorised administrator can change subject security attributes.

FMT_MSA.1(a)	None (The role group is fixed as Device Administrator and is not managed.)	a) Managing the group of roles that can interact with the security attributes; b) Management of rules by which security attributes inherit specified values.
FMT_MSA.3(a)	None (The role group is fixed as Device Administrator and is not managed.)	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP; c) Management of rules by which security attributes inherit specified values.
FMT_MSA.1(b)	None (The role group is fixed as Device Administrator and is not managed.)	a) Managing the group of roles that can interact with the security attributes; b) Management of rules by which security attributes inherit specified values.
FMT_MSA.3(b)	None (The role group is fixed as Device Administrator and is not managed.)	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP; c) Management of rules by which security attributes inherit specified values.
FMT_MTD.1(a)	None (The role group is fixed as Device Administrator and is not managed.)	a) Managing the group of roles that can interact with the TSF data.
FMT_MTD.1(b)	None (The role group is fixed as Device Administrator and is not managed.)	a) Managing the group of roles that can interact with the TSF data.
FMT_SMF.1	-	There are no management activities foreseen.
FMT_SMR.1	Manage the group of	a) Managing the group of users that are

	users that are user authorization.	part of a role.
FPT_STM.1	Management of system time	Defined by PP: Management of system time
FPT_TST.1	None (Self test executable condition is fixed and is not managed.)	a) Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) Management of the time interval if appropriate.
FTA_SSL.3	Management of auto-logout time.	a) Specification of the time of user inactivity after which termination of the interactive session occurs for an individual user; b) Specification of the default time of user inactivity after which termination of the interactive session occurs.
FTP_ITC.1	Management of data protection on the internal network. (Network encryption settings(TLS, IPsec setting))	a) Configuring the actions that require trusted channel, if supported.

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain [assignment: *the authorised identified roles*].

[assignment: *the authorised identified roles*]
- Device Administrator
- Normal User

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6. Class FPT: TSF Protection

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

[selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]

- during initial start-up

[selection: [assignment: *parts of TSF*], *the TSF*]

- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]

- SSD Encryption Function

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*].

[selection: [assignment: *parts of TSF data*], *TSF data*]

- [assignment: *parts of TSF data*]

[assignment: *parts of TSF data*]

- Encryption Key

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF*].

[selection: [assignment: *parts of TSF*], *TSF*]

- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]

- TSF executable module

6.1.7. Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: *time interval of user inactivity*]

- Operation Panel : No operation after time set by a device administrator elapsed (between 5 seconds and 495 seconds)
- Web browser : No operation after 10 minutes elapsed.

*There are no interactive session exists with the exception of an operation panel and a web browser.

6.1.8. Class FTP: High Trusted Path/Channel

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides

assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.

[selection: the TSF, another trusted IT product]
- TSF
- another trusted IT product

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: the list of functions that require trusted channel].

[assignment: the list of functions that require trusted channel]
- Scan to Send function
- Print function
- Box to Send function
- Box operation by client PCs (via Web browser)
- Security management function operated by client PCs (via Web browser), except printer function use in local connection.

6.2. TOE Security Assurance Requirement

Security assurance requirements are described in **Table 6-13 Security Assurance Requirements**. The evaluation assurance level of this TOE is EAL2. The security assurance component, ALC_FLR.2 is added to the assurance components as shown in the Table 6-13.

Table 6-13 Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims

Assurance Class	Assurance Components
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3. Security Functional Requirements Rationale

6.3.1. Security Functional Requirements Rationale

Table 6-14 shows the TOE security functional requirements and the corresponding security objectives.

Table 6-14 Correspondence between Security Functional Requirements

Security Functional Requirements	Security Objectives						
	O.SSD_ENCRYPTION	O.AUDIT_LOG	O.NETWORK_ENCRYPTION	O.FAX_CONTROL	O.SETTING_DATA	O.ACCESS_CONTROL	O.SOFTWARE_VERIFICATION
FAU_GEN.1		✓					
FAU_GEN.2		✓					
FAU_SAR.1		✓					
FAU_SAR.2		✓					
FAU_STG.1		✓					

Security Functional Requirements	Security Objectives						
	O.SSD_ENCRYPTION	O.AUDIT_LOG	O.NETWORK_ENCRYPTION	O.FAX_CONTROL	O.SETTING_DATA	O.ACCESS_CONTROL	O.SOFTWARE_VERIFICATION
FAU_STG.4		✓					
FCS_CKM.1(a)	✓						
FCS_CKM.1(b)			✓				
FCS_CKM.1(c)			✓				
FCS_COP.1(a)	✓						
FCS_COP.1(b)			✓				
FCS_COP.1(c)			✓				
FDP_ACC.1						✓	
FDP_ACF.1						✓	
FDP_IFC.1				✓			
FDP_IFF.1				✓			
FIA_AFL.1					✓	✓	
FIA_ATD.1						✓	
FIA_SOS.1					✓	✓	
FIA_UAU.1					✓	✓	
FIA_UAU.7					✓	✓	
FIA_UID.1		✓			✓	✓	
FIA_USB.1						✓	
FMT_MSA.1(a)						✓	
FMT_MSA.3(a)						✓	
FMT_MSA.1(b)				✓			
FMT_MSA.3(b)				✓			
FMT_MTD.1(a)					✓		
FMT_MTD.1(b)					✓		
FMT_SMF.1				✓	✓	✓	
FMT_SMR.1				✓	✓	✓	
FPT_STM.1		✓					

Security Functional Requirements	Security Objectives						
	O.SSD_ENCRYPTION	O.AUDIT_LOG	O.NETWORK_ENCRYPTION	O.FAX_CONTROL	O.SETTING_DATA	O.ACCESS_CONTROL	O.SOFTWARE_VERIFICATION
FPT_TST.1							✓
FTA_SSL.3					✓	✓	
FTP_ITC.1			✓				

The rationale for "Table 6-14 Correspondence between Security Functional Requirements" demonstrates below.

O.SSD_ENCRYPTION

O.SSD_ENCRYPTION is the security objective to encrypt Image data and TOE setting data stored in SSD in order to prevent unauthorized decryption.

FCS_CKM.1(a) generates encryption keys in accordance with a specified encryption algorithm.

FCS_COP.1(a) encrypts Image Data and TOE setting data when storing in the SSD using a specified encryption algorithm and encryption key length, and decrypts Image data and TOE setting data when reading out from the SSD.

Therefore, O.SSD_ENCRYPTION ensures the encryption of User Data and TSF Data when storing in SSD.

O.AUDIT_LOG

O.AUDIT_LOG is the security objective to record auditable event and provide audit logs in order to monitor unauthorized access.

FAU_GEN.1 records the audit log of the events, which should be auditable.

By associating FAU_GEN.2 with FIA_UID.1, the auditable events are associated with identification information of users.

FPT_STM.1 provides a trusted time stamp function inside the TOE, and records the times when auditable events occurred.

FAU_SAR.1 provides read capability of audit log information to Device Administrator.

FAU_SAR.2 restricts the access for audit logs except Device Administrator.

FAU_STG.1 protects stored audit logs from unfair deletion or alteration.

FAU_STG.4 overwrites the oldest stored audit log and stores new audit log, when audit logs

are full.
Therefore, O.AUDIT_LOG records auditable event and provides audit logs, and ensures to prevent unauthorized disclosure and alteration.

O.NETWORK_ENCRYPTION

O.NETWORK_ENCRYPTION is the security objective to provide encrypted communication function required on network protection in order to protect image data and TOE setting data on the internal network from eavesdropping or alteration.
FTP_ITC.1 provides trusted channel by encrypt communication in order to protect image data and TOE setting data on the internal network from eavesdropping and alteration.
FCS_CKM.1(b), FCS_CKM.1(c), FCS_COP.1(b), and FCS_COP.1(c) support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission.
Therefore, O.NETWORK_ENCRYPTION ensures to provide encrypted communication function required on network protection in order to protect image data and TOE setting data on the internal network protected.

O.FAX_CONTROL

O.FAX_CONTROL is the security objective to control FAX data flow to forward received data from public line to external interfaces of TOE according with rules set by authorized role.
FDP_IFC.1, FDP_IFF.1 use Fax information flow control function on TOE and received data from public line is forwarded to external interface of TOE according with Fax forward setting that is set by authenticated role.
FMT_MSA.1 (b) manages operations on the security attributes.
FMT_MSA.3 (b) ensure that FAX forward settings have appropriate default value.
FMT_SMR.1 assigns and maintains user authorization of Device Administrator.
FMT_SMF.1 provides Device Administrator with the security management functions.
Therefore, O.FAX_CONTROL ensures to control FAX data flow to forward received data from public line to external interfaces of TOE according with rules set by authorized role.

O.ACCESS_CONTROL

O.ACCESS_CONTROL is the security objective to ensure that the TOE identify and authenticate users, and control access privilege to image data in order to only authorized user can access to the image data.
FIA_UID.1 and FIA_UAU.1 implement identification and authentication of users who try to access from operation panel and client PCs.
FIA_UAU.7 protects authentication feedback to users.
FIA_ATD.1 and FIA_USB.1 maintain user attributes of login user name, user authorization, and bind the subject security attributes to authorized users.
FIA_AFL.1 lockouts user login when users consecutively fail their authentication.

FIA_SOS.1 verifies if the secret of user authentication meet the defined quality metrics.
FTA_SSL.3 manages user session and terminates out of session.
FDP_ACC.1 and FDP_ACF.1 allow the authorized users only to operate image data.
FMT_MSA.1 (a) manages operation on the security attributes.
FMT_MSA.3 (a) ensures that the owner information of image data, or owner and share information of the box storing image data have appropriate default values.
FMT_SMR.1 maintains that user authorization of Device Administrator and Normal User are assigned to the users.
FMT_SMF.1 provides security management function to Device Administrator and Normal User who own the image data.
Therefore, O.ACCESS_CONTROL ensures that that the TOE identify and authenticate users, and control access privilege to image data in order to only authorized user can access to the image data.

O.SETTING_DATA
O.SETTING_DATA is the security objective to authorize access to the TOE setting data only for authenticated right users, and prevent access to the TOE setting data by unauthorized users, and prevent change or leak of TOE setting data.
FIA_UID.1 and FIA_UAU.1 implement identification and authentication of users who try to access from operation panel and client PCs.
FIA_UAU.7 protects authentication feedback to users.
FIA_AFL.1 lockouts user login when users consecutively fail their authentication.
FIA_SOS.1 verifies if the secret of user authentication meet the defined quality metrics.
FTA_SSL.3 manages user session and terminates out of session.
By FMT_MTD.1(a), operation of TOE setting data is restricted to Device Administrator.
By FMT_MTD.1(b), operation of TOE setting data is restricted to Normal Users who are owner of the TOE setting data.
FMT_SMR.1 maintains that user authorization of Device Administrator and Normal User are assigned to the users.
FMT_SMF.1 provides security management function to Device Administrator and Normal User who own TOE setting data.
Therefore, O.SETTING_DATA ensures that that the TOE identify and authenticate users, and control access privilege to TOE setting data in order to only authorized user can access to the TOE setting data.

O.SOFTWARE_VERIFICATION
O.SOFTWARE_VERIFICATION is the security objective to provide self-verification of the TSF executable code.
FPT_TST.1 runs a suite of self-test during the TOE start-up, and verifies the integrity of parts of TSF data and verifies the integrity of parts of TSF by operating at arbitrary timing after the

start-up.
Therefore, O.SOFTWARE_VERIFICATION can provide authorized users with the procedure for self-verification of the TSF executable code.

6.3.2. Dependency Relationship of the TOE Security Functional Requirements

Table 6-15 shows the dependency relationship of the TOE security functional requirements.

Table 6-15 Dependency Relationship of the TOE Security Functional Requirements

Functional Requirements	Dependency Relationship	Dependencies Not Satisfied
FAU_GEN.1	FPT_STM.1	—
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	—
FAU_SAR.1	FAU_GEN.1	—
FAU_SAR.2	FAU_SAR.1	—
FAU_STG.1	FAU_GEN.1	—
FAU_STG.4	FAU_STG.1	—
FCS_CKM.1(a)	FCS_COP.1(a) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_CKM.1(b)	FCS_COP.1(b) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_CKM.1(c)	FCS_COP.1(c) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_COP.1(a)	FCS_CKM.1(a) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_COP.1(b)	FCS_CKM.1(b) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FCS_COP.1(c)	FCS_CKM.1(c) FCS_CKM.4	FCS_CKM.4 See Section 6.3.2.1
FDP_ACC.1	FDP_ACF.1	—
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	—
FDP_IFC.1	FDP_IFF.1	—
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	—

FIA_AFL.1	FIA_UAU.1	—
FIA_ATD.1	No dependencies.	—
FIA_SOS.1	No dependencies.	—
FIA_UAU.1	FIA_UID.1	—
FIA_UAU.7	FIA_UAU.1	—
FIA_UID.1	No dependencies.	—
FIA_USB.1	FIA_ATD.1	—
FMT_MSA.1(a)	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.3(a)	FMT_MSA.1 FMT_SMR.1	—
FMT_MSA.1(b)	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.3(b)	FMT_MSA.1 FMT_SMR.1	—
FMT_MTD.1(a)	FMT_SMF.1 FMT_SMR.1	—
FMT_MTD.1(b)	FMT_SMF.1 FMT_SMR.1	—
FMT_SMF.1	No dependencies.	—
FMT_SMR.1	FIA_UID.1	—
FPT_STM.1	No dependencies.	—
FPT_TST.1	No dependencies.	—
FTA_SSL.3	No dependencies.	—
FTP_ITC.1	No dependencies.	—

6.3.2.1. Rationale for why dependency on FCS_CKM.4 is not needed.

The encryption key to encrypt SSD is generated with a unique value only per device every time main power is turned on, and is stored in the volatile memory. However, the TOE is physically protected by security objectives in operational environment, that is OE.ACCESS, even when the main power is turn off. Therefore the requirement for the encryption key destruction is not needed.

The symmetric session key generated during the handshake by the client, used to encrypt application data exchanged in the TLS session, is not persistently stored by either the client or the server. This session key is held in memory and is only valid for that given session. Once the session is terminated the key cannot be used to decrypt subsequent sessions. The attack potential required attempting to

extract the key from the client memory following session termination to decrypt traffic captured between the client and server is significantly beyond the attack potential of EAL2. Therefore the requirement for the encryption key destruction is not needed.
The pre-shared key authentication method is used for the authentication of the IP-Sec peer. The pre-shared key is set by Device Administrator and not generated and destructed by the device. The symmetric encryption communication key obtained by DH IKEv1 Key Derivation Function is not persistently stored by each peers. This key is held in memory and is only valid with the corresponding Security Association. Once the SA is terminated the key cannot be used. Therefore the requirement for the encryption key destruction is not needed.

6.3.3. Security Assurance Requirements Rationale

Since this TOE is aimed at countering the threat of exposure of image data by an attacker with basic attack capability, it is necessary to guarantee counter-ability against basic level attacks.

EAL2 have an analyze if TOE provides sufficient guidance information for safe use of security functions, including analysis of security measures at development stage in TOE (implementation and analysis of tests based on functional specifications, evaluation of management status of deliverables and delivery procedure). Since the assurance requirement is EAL2 compliant, the selection of EAL2 is reasonable.
ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7. TOE Summary Specification

This section describes the summary specification for the security functions that are provided by the TOE.

Table 7-1 shows the relations between the TOE security functions and security functional requirements

Table 7-1 TOE security functions and security functional requirements

Security Functions / Functional Requirements	TSF.USER_AUTHENTICATION	TSF.DATA_ACCESS	TSF.FAXDATAFLOW	TSF.SSD_ENCRYPTION	TSF.AUDIT_LOG	TSF.SECURITY_MANAGEMENT	TSF.SELF_TEST	TSF.NETWORK_PROTECTION
FAU_GEN.1					✓			
FAU_GEN.2					✓			
FAU_SAR.1					✓			
FAU_SAR.2					✓			
FAU_STG.1					✓			
FAU_STG.4					✓			
FCS_CKM.1(a)				✓				
FCS_CKM.1(b)								✓
FCS_CKM.1(c)								✓
FCS_COP.1(a)				✓				
FCS_COP.1(b)								✓
FCS_COP.1(c)								✓
FDP_ACC.1		✓						
FDP_ACF.1		✓						
FDP_IFC.1			✓					
FDP_IFF.1			✓					
FIA_AFL.1	✓							
FIA_ATD.1	✓							
FIA_SOS.1	✓							

FIA_UAU.1	✓							
FIA_UAU.7	✓							
FIA_UID.1	✓				✓			
FIA_USB.1	✓							
FMT_MSA.1(a)						✓		
FMT_MSA.3(a)		✓						
FMT_MSA.1(b)						✓		
FMT_MSA.3(b)			✓					
FMT_MTD.1(a)						✓		
FMT_MTD.1(b)						✓		
FMT_SMF.1						✓		
FMT_SMR.1						✓		
FPT_STM.1					✓			
FPT_TST.1							✓	
FTA_SSL.3	✓							
FTP_ITC.1								✓

7.1. User Management Function

TSF.USER_AUTHENTICATION

User management function is a function that identifies and authenticates whether persons are authorized users when users intend to operate the TOE from the operation panel or the client PCs.

When the TOE is used from the Operation Panel or a Web browser, the login screen is displayed and a user is required to enter his or her login user name and login password.

When the TOE is accessed from the printer driver or TWAIN driver, the TOE identifies and authenticates if the person is authorized by referring to the login user name and login user password obtained from a user job.

(1) FIA_UID.1 Timing of identification

When a user intends to login to the TOE, the TOE verifies if the entered login user name exists in the user information pre-registered in the TOE.

With reception of the device status, the TOE provides information before the user is identified. With a list of user jobs and counter information, the TOE displays the information before the user is identified. With fax data reception, the TOE receives fax data before the user is identified.

(2) FIA_UAU.1 Timing of authentication

When the user is successfully identified by FIA_UID.1, the TOE verifies if the entered login

user password matches with one pre-registered in the TOE.
With reception of the device status, the TOE provides information before the user is authenticated. With a list of user jobs and counter information, the TOE displays the information before the user is authenticated. With fax data reception, the TOE receives fax data, before the user is authenticated.

(3) FIA_UAU.7 Protected authentication feedback
The TOE displays login user password entered from the operation panel or a client PC on the login screen, which is masked by dummy characters (*: asterisk).

(4) FIA_ATD.1 User attribute definition
The TOE defines and maintains user attributes such as login user name and user authorization.

(5) FIA_SOS.1 Verification of secrets
The TOE verifies that a login user password meets specified quality metrics such as password length: no fewer than the minimum number of characters (8 characters), character and types: Alphanumeric or special characters.

(6) FIA_USB.1 User-subject biding
The TOE associates user attributes such as login user name and user authorization with subjects.

(7) FIA_AFL.1 Authentication failure handling
When the number of consecutive unsuccessful login attempts from the operation panel or a client PC since the last successful authentication, reaches the threshold, the TOE does not allow the users to access to the accounts (i.e. state changes to lockout condition).
The number of unsuccessful authentication attempts set by the device administrator can be within 1 to 10 times.
After changing to lockout state, If time between 1 and 60 minutes and until the lockout time designated by a device administrator that elapse, or until a device administrator releases lockout state, the TOE is then back to the normal state.

(8) FTA_SSL.3 TSF-initiated termination
The auto-logout is activated if no operation is performed from the operation panel or a web browser for certain period of time.

- Operation Panel
  After the user logs on to the TOE and if no operation is performed while the auto-logout time set by the device administrator elapses, the auto-logout is activated.
  The time can be set to 5 to 495 seconds by the device administrator.

- Web browser
  After the user logs on to the TOE and if no operation is performed for 10 minutes, the auto-logout is activated.

7.2. Data Access Control Function

TSF.DATA_ACCESS

The data access control function is a function that allows authorized users only to access to image data stored in the TOE using each of the TOE basic function such as copy, scan to send, print, fax and box function.

(1) FDP_ACC.1 Subset access control
FDP_ACF.1 Security attribute based access control

The TOE allows authorized users only to access to image data handled by respective basic functions in accordance with the access control rules for users as shown in Table 7-2.

In Table 7-2 Access Control Rules, login user names and owner information of targeted assets need to be matched in order to determine if the jobs are executed by themselves.

Table 7-2 Access Control Rules for Data Access Control Functions

Targeted Assets	Operations	Users	Access Control Rules
Image Data (Print Function)	Box Print (Job after print request from a printer driver), Print from a USB memory, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Scan to Send Function)	FTP Send, E-mail Send, TWAIN Send, Preview send image, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Copy Function)	Copy Print, Copy preview image, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Fax Send Function)	FAX Send, Send preview image, Delete	Normal User	It is allowed for a normal user to access to job image data executed by themselves.
	Delete	Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Box Function)	Box print, Box preview, Box Send, Move, Join and Delete documents inside a box	Normal User	It is allowed for a normal user to access to image data stored in their own box set as an owner or a box that permission is enabled.
		Device Administrator	It is allowed for a device administrator to access to all job image data.
Image Data (Fax Reception Function)	Print FAX reception, FAX forward, Delete	Device Administrator	It is allowed for a device administrator to access to image data stored in FAX box.

(2) FMT_MSA.3(a) Static attribute initialization
The TOE sets default values for image data that is initially generated, and a box. Owner information is created using a login user name of the user who initially creates the image data. Box owner is a device administrator who initially creates the box, and the box permission is disabled.

7.3. Fax Data Flow Control Function

TSF.FAXDATA_FLOW

The Fax Data Flow Control function is a function that controls forwarding the data received from public line to the TOE's external interface, following to the FAX forward setting.

(1) FDP_IFC.1 Subset information flow control
FDP_IFF.1 Simple Security attribute
TOE controls information flow according with Fax Forward Setting and send received data from public line to an external interface. Therefore the receiving task from public line forward the data(information) received from public line to sending task to the external interface according with Fax Forward Setting.

(2) FMT_MSA.3(b) Static attribute initialization
TOE set default value of newly created FAX forward setting. The default value of the newly created fax forward setting is an output from printing part.

7.4. SSD Encryption Function

TSF.SSD_ENCRYPTION

Once the basic function of the TOE is executed, image data and TSF data is stored on the SSD. The SSD encryption function is a function that encrypts data and then stores the data on the SSD when storing these data on the SSD.

(1) FCS_CKM.1(a) Cryptographic key generation (Storage Encryption)
The TOE generates a 256 bits encryption key to be used in the AES algorithm by using the encryption key generation algorithm in accordance with NIST SP800-56C. This encryption key is generated from multiple information including the encryption code which users register and a unique value on a per device basis, every time each TOE is powered on, and this encryption key is stored in a volatile memory. Information for encryption key is set only at the start of operation, and is not changed during the operation.

(2) FCS_COP.1(a) Cryptographic operation (Storage Encryption)
When storing data on the SSD, the TOE encrypts the data, using the 256 bits encryption

key generated at the time of booting (FCS_CKM.1(a)) and the AES encryption algorithm based on FIPS PUB 197, and write into the SSD. When reading out the stored data from the SSD, the TOE decrypts the data, similarly using the 256 bits encryption key generated at the time of booting and the AES encryption algorithm.

7.5. Audit Log Function

TSF.AUDIT_LOGGED

The audit log function is a function that generates, records and manages audit logs when occurring auditable events.

(1) FAU_GEN.1 Audit data generation

The TOE records audit data as listed in Table 7-3, and generates audit logs when auditable events shown in Table 7-3 occur.

Table 7-3 Auditable Events and Audit Data

Auditable Events	Audit Data	Additional Audit Data
Power-on[*1]	Date and time of the event, Type of event, Identification information of the user (Including the identification information of the user who attempted to login), The outcome of the event (success or failure)	—
Power-off[*1]		—
Success and failure of the user identification and authentication		—
Execution of user lockout and release of lockout status by a device administrator when the number of consecutive unsuccessful authentication attempts since the last successful authentication, reaches the threshold.		—
Session termination by auto-logout		—
Operation of image data (read, delete)		Identification information of the event
Edit of user management information (Modify user authorization)		—
When registration of login user password is made, deny by quality check (create, edit)		
Use of security management function		—
Change of time		—
Communication failure of TLS or IPsec		Recipient's

communication		communication IP address

*1 Start-up and shutdown of the audit functions synchronize power-on and power-off of the TOE, and thus power-on and power-off of the TOE of the event can be substituted.

(2) FAU_GEN.2 User identity association
FIA_UID.1 The timing of identification
For each auditable event, the TOE associates the user identity information that is a cause, with the audit log.

(3) FAU_SAR.1 Audit review
FAU_SAR.2 Restricted audit review
The TOE provides device administrators only with the capability to read information from the audit records. Read-access to the audit records is sent (by email) to the email destination set by a device administrator.

(4) FAU_STG.1 Protected audit trail storage
The TOE provides device administrators only with capability to read and delete information from the audit records, and does not provide normal users other than device administrators with a function to access to the audit records.

(5) FAU_STG.4 Prevention of audit data loss
The TOE overwrites the oldest stored audit records and records new auditable events if the audit log files are full.

(6) FPT_STM.1 Reliable time stamps
The TOE has a system clock inside itself. The TOE records a date and time of the event with the system clock when auditable events occur. The TOE provides a highly reliable time stamp by recording the time stamps on audit records without delay when the time is recorded by the system clock inside the TOE.

7.6. Security Management Function

TSF.SECURITY_MANAGEMENT

Security management function is a function that allows authorized users only to edit user information, set the TOE security functions and manage. The Security management function can be performed from the Operation Panel and Client PCs. Web browser is used for operation from Client PCs.

(1) FMT_MSA.1(a) Management of security attributes

The TOE allows device administrators only to use box functions for all boxes as shown below.

- Modify a box owner
- Modify a box permission

Whereas, the TOE allows device administrators only to use box functions for documents as shown below.

- Modify document owner information

Normal users are allowed to perform the following operation on the self owner boxes.

- Read and modify a box permission

(2) FMT_MSA.1(b) Management of security attributes

The TOE allows only Device Administrator to perform following operation for Fax forward setting.

- Modify Fax forward setting.

(3) FMT_MTD.1(a) Management of TSF Data

The TOE provides device administrators only with the operation listed in Table 7-4 on TSF data listed in Table 7-4.

Table 7-4 Operation of TSF Data by Device Administrators

TSF Data	Authorized Operation
Register user information (Login user name, login user password, user authorization)	Edit, Delete, Newly create
User account lockout policy settings (number of retries until locked, lockout duration)	Modify
Lockout list	Modify
Auto logout time setting	Modify
Password policy settings	Modify
Date and time settings	Modify
Network Encryption Setting	Modify
Send destination information for audit log report	Modify

(4) FMT_MTD.1(b) Management of TSF Data

The TOE provides normal users with the operation listed in Table 7-5 on TSF data listed in

Table 7-5.

Table 7-5 Operation of TSF Data by Normal Users

TSF Data	Authorized Operation
Edit user information (Login user password associated to the users)	Edit

(5) FMT_SMR.1 Security roles
The TOE maintains the user authorizations of device administrators and normal users, and associates users to the user authorizations.

(6) FMT_SMF.1 Specification of management function
The TOE provides management function of security attributes for box functions as mentioned in (1), and security management function shown in Table 7-4 and Table 7-5 on TSF data shown in Table 7-4 and Table 7-5.

7.7. Self-Test Function

TSF.SELF_TEST

The self-test function is a function that performs the following self-test.

(1) FPT_TST.1 TSF test
The TOE performs the following self-test.

- Check if SSD encryption function is correctly performed.
- Check the integrity of the encryption key
- Check the integrity of executable module of the security function

At the TOE start-up, the TOE simultaneously checks if SSD encryption function is correctly performed and the integrity of the encryption key is verified by confirming encryption and decryption operations using the encryption key. Also, the TOE checks the integrity of executable module of the security functions when receiving an instruction from a device administrator.

In case abnormal operation is found by check at the TOE start-up, the users are notified of this abnormal status by displaying it on the Operation Panel of the TOE. If no abnormal item is found on the Operation Panel, the users assume the TOE correctly operates and so the users can use the TOE.

7.8. Network Protection Function

TSF.NETWORK_PROTECT

The network protection function is a function that encrypts all data in transit over the internal network and prevents unauthorized alteration and disclosure. It is protected by encrypted data flow on the internal network when a user uses Scan to Send function, Printer driver function, and Web browser function.

(1) FTP_ITC.1 Trusted channel between TSF

When the TOE communicates with each type of server or a Client PC that are trusted IT products, communication starts between them via a trusted channel. This communication can start from either of the TOE or the trusted IT product. The following functions are provided.

- Scan to send function
- Print function
- Box function (Send Function)
- Operation of a box function from a client PC (web browser)
- Operation of security management function from a client PC (web browser)

However, use of print function for a direct connection with the TOE is exception.

The TOE provides trusted channel communications listed below.

Table 7-6 Trusted channel communications provided by the TOE

Destination	Protocols	Encryption algorithm
Client PC	TLSv1.2, TLSv1.3	AES(128 bits, 256 bits), ChaCha20-Poly1305
Mail Server	IPsec with ESP	3DES(168 bits), AES(128 bits, 192 bits, 256 bits)
FTP Server	IPsec with ESP	3DES(168 bits), AES(128 bits, 192 bits, 256 bits)

(2) FCS_CKM.1(b) Cryptographic key generation (TLS)

Secure Communications requires generation of a certificate with an RSA public-private key pair.

The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL.

(3) FCS_CKM.1(c) Cryptographic key generation (IPSec)

ISAKMP and IKEv1 are used to establish the Security Association (SA) and keys for the IPSec exchanges.

(4) FCS_COP.1(b) Cryptographic operation (TLS)

TLS 1.2 (RFC5246) is used to establish secure channel between client PCs and TOE. The TOE sends the server certificate chain to the client. The client performs certificate path validation of the server certificate during the TLS handshake. If the certificate cannot be successfully validated (e.g. it has expired or has been revoked) the TLS session is not established.
The TOE only allows the establishment of a TLS secure channel using TLSv1.2 and TLSv1.3. The TOE denies any attempt by a TLS client to establish communication using the following versions of the SSL or TLS protocols: SSLv1.0, SSLv2.0, SSLv3.0, TLSv1.0 or TLSv1.1. The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL. This session key is held in memory and is only valid for that given session. Once the session is terminated the key cannot be used to decrypt subsequent sessions. The TOE supports the following cipher suites:

- TLS_AES_256_GCM_SHA384 (RFC8446)
- TLS_AES_128_GCM_SHA256 (RFC8446)
- TLS_CHACHA20_POLY1305_SHA256 (RFC8439)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (RFC5289)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (RFC5289)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (RFC5289)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (RFC5289)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305 (RFC7905)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (RFC5288)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (RFC5288)
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305 (RFC7905)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (RFC5288)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (RFC5288)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (RFC5246)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (RFC5246)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (RFC5246)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (RFC5246)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (RFC5246)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (RFC5246)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (RFC5246)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (RFC5246)
- TLS_RSA_WITH_AES_256_CBC_SHA (RFC5246)
- TLS_RSA_WITH_AES_128_CBC_SHA (RFC5246)

(5) FCS_COP.1(c) Cryptographic operation (IPSec)
IPSec with ESP is required for network datagram exchanges with Mail Server/FTP Server. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported

encryption options for ESP are 3DES and AES. HMAC-SHA256-128, HMAC-SHA384-192, and HMAC-SHA512-256 are supported for Data authentication.

ISAKMP and IKEv1 are used to establish the Security Association (SA) and keys for the IPSec exchanges. Diffie-Hellman is used for IKEv1 Key Derivation Function as specified in RFC2409, using Oakley Groups 14, 16, 17, 18, 19, 20, 21, 22, 23, or 24. In the ISAKMP exchange, a pre-shared keys is configured by administrators and validated between endpoints.

The key size specified in the SA exchange is 128, 192, or 256 bits and the encryption algorithm is 3DES or AES-CBC and the Hash Authentication Algorithm may be SHA-256, SHA-384, or SHA-512 (as configured by administrators).

Keys generated for the IKEv1 exchanges are performed per RFC2409. If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. All keys are held in memory and is only valid with the corresponding SA. Once the SA is terminated the key cannot be used.

7.9. Deviations From Allowed Cryptographic Standards

The following deviations from the Allowed Cryptographic Standards in 188 Scheme Crypto Policy are noted:

1. Hashing: SHA-1 is supported for backward compatibility with remote systems.
2. Block cipher: AES-XTS is supported for storage encryption.
3. Authenticated Encryption with Associated Data: ChaCha20-Poly1305 is supported for TLSv1.3 communication.

8. Acronyms and Terminology

8.1. Definition of terms

The definitions of the terms used in this ST are indicated in Table 8-1.

Table 8-1 Definitions of terms used in this ST

Terms	Definitions
FAX System 12	This is provided as an optional product of MFP to use faxfunction. FAX function can be used by installing FAX board separately on MFP.
TWAIN	This function is to read image from scanner and send the image to a client PC. The term, “TWAIN” indicates the API specification.
FAX Data Reception	It indicates an action that includes reception of incoming FAX data to TOE. (the process such as printing and forwarding of data is not included.)
Job	This is the operation processing unit to perform copy function, print function, scan to send function, fax function and document box function of TOE.
Job Information	It indicates information that job holds. It mainly indicates jobs in operation. However, it also indicates histories of execution results.
A list of Job Information	One that list job information.
Box Information	Information that is stored in an area, called “box” when using box function. For example, box name, box number, box size etc. Security attributes such as box owner and box permission are also included in this information.
Edit	An operation that modifies data registered by users, such as user information and box information.
Move	It is to move document stored in a box to another box.
Join	It is to join multiple documents stored in a box, and create a new joined document. Original documents remain.
Preview Send Image	This is one of scan to send function and FAX function operation. A function that displays image preview read from a scanner of TOE for sending on the operation panel.

Preview Copy Image	This is one of copy function operation. A function that displays image preview read from a scanner of TOE for copying on the operation panel.
Box Preview	This is one of box function operation. It is to display the preview of the document stored in a box on the operation screen.
Device Status	Information that shows TOE status. Remaining toner volume, papers and mechanical errors are displayed.
Counter Information	Information about counting jobs performed by TOE. When print function performs, print counter increases. When scan to send function performs, send counter increases.
Image Data	It indicates the image information that is processed inside the MFP when TOE normal users use copy function, scan to send function, print function, FAX function and box function.
Client PC	It indicates the computers that connect to the network, and utilize the TOE services (functions) of the TOEs that are connected to the network.
FIPS PUB 180-4	This is an algorithm about a hash function, which is standardized by the NIST, U.S.(National Institute of Standards and Technology).
FIPS PUB 197	This is an algorithm about the common cryptographic key, which is standardized by the NIST, U.S. (National Institute of Standards and Technology). Also, this is called “AES”.
Operation Panel	This is installed on the uppermost part of the MFP, and is constituted by a liquid crystal panel. It is an external interface, and users can utilize the TOE via this operation panel.
Task to be executed on behalf of user	This is an executed process on behalf of users(Normal User, Device Administrator).
Task to receive data from public line	This is a process received from public line.
Task to send data to an external interface	This is a process to send to an external interface.

8.2. Definition of acronyms

The definitions of the acronyms used in this ST are indicated in Table 8-2.

Table 8-2 Definitions of acronyms used in this ST

Acronyms	Definitions
A.	assumption (when used in hierarchical naming)
ADMIN.	administrator (when used in hierarchical naming)
AES	Advanced Encryption Standard
CC	Common Criteria
EAL	Evaluation Assurance Level
FAX	facsimile
IT	information technology
MFP	Multi Functional Printer
NCU	Network Control Unit
NAND	Not AND
O.	Security Objective (of the TOE) (when used in hierarchical naming)
OE.	Security Objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security target
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality
USB	Universal Serial Bus

(The final page)