RICOH IM C530F/C530FB,

SAVIN IM C530FB,

LANIER IM C530FB,

nashuatec IM C530F/C530FB,

Rex Rotary IM C530F/C530FB,

Gestetner IM C530F/C530FB

Security Target

Author: RICOH COMPANY, LTD.
Date: 2022-07-15
Version: 1.00

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This section describes ST Reference, TOE Reference, TOE Overview, and TOE Description.

1.1 ST Reference

The following is the identification information of the ST.

Title: RICOH IM C530F/C530FB,
SAVIN IM C530FB,
LANIER IM C530FB,
nashuatec IM C530F/C530FB,
Rex Rotary IM C530F/C530FB,
Gestetner IM C530F/C530FB Security Target

Version: 1.00

Date: 2022-07-15

Author: RICOH COMPANY, LTD.

1.2 TOE Reference

The following is the identification information of the TOE.

TOE Names: RICOH IM C530F/C530FB,
SAVIN IM C530FB,
LANIER IM C530FB,
nashuatec IM C530F/C530FB,
Rex Rotary IM C530F/C530FB,
Gestetner IM C530F/C530FB

Version: E-1.00

TOE Type: Multifunction product (hereinafter "MFP")

The target MFPs are products for overseas countries listed in Table 1, which are identified by product name and model code.

Table 1: Product Name and Model Code of the Target MFPs

No.	Product Name	Model Code
1	IM C530F	D0CT-27
2	IM C530FB	D0CS-17
3	IM C530FB	D0CS-27

Table 2 describes the identification information of software and hardware installed in these MFPs. Software is identified by name, version, and part number. However, Keymicon, GraphicData, and LegacyUIData are identified by name and version. Hardware is identified by name and version.

Table 2: Version and Part Number of Software and Hardware for Version E-1.00

Name of Software and Hardware for the MFPs		Version	Part Number
Software	CTL System	1.05	D0CS5260F
	CheetahSystem	1.05	D0CS5100F
	appsite	3.03.37	D0CS5176
	bleservice	1.00.02	D0CS5127A
	camelsl	1.11	D0CS5132A
	cispluginble	4.0.4	D0CS5109A
	cispluginkeystr	3.03.02	D0CS5117A
	cispluginnfc	3.03.02	D0CS5116A
	faxinfo	1.00	D0CS5125A
	helpservice	1.00	D0CS5111A
	iccd	3.08.02	D0CS5130A
	introductionset	1.01	D0CS5112A
	iwnnimelanguage	2.8.2	D0BQ1456A
	iwnnimelanguage	2.8.2	D0BQ1454A
	iwnnimelanguage	2.8.2	D0BQ1455A
	iwnnimeml	2.8.201	D0BQ1453C
	kerberos	1.07.04	D0CS5131B
	langswitcher	1.00	D0CS5102A
	mediaappappui	1.00	D0CS5107A
	mlpsmartdevicec	4.1.2	D0CS5101A
	multidevicehub	1.00	D0CS5133A
	optimorurcmf	1.1	D0BQ1499B
	programinfoserv	1.00	D0CS5128A
	remotesupport	1.00	D0CS5110

Name of Software and Hardware for the MFPs		Version	Part Number
	simpleauth	3.05.03	D0CS5123A
	simpledirectcon	1.18	D0CS5118
	simpleprinter	1.00	D0CS5103A
	smartcopy	1.00	D0CS5104A
	smartfax	1.01	D0CS5106B
	smartprtstoredj	1.01	D0CS5108B
	smartscanner	1.00	D0CS5105A
	smartscannerex	2.05	D0CS5113B
	stopwidget	1.00	D0CS5126A
	tonerstate	1.00	D0CS5124A
	traywidget	1.00	D0CS5135A
	Engine	011000:01	D0CS5160A
	ADF	2D1000:01	D0CS5161
	Engine(IPU)	1.03:04	D0CS5150D
Hardware	Ic Key	12714	No display

Software for the Operation Panel Unit		Version	Part Number
Software	Firmware	1.05	D0CS5100F
	Keymicon	9.10	No display
	Application Site	3.03.37	D0CS5176
	Bluetooth Authentication Plugin	4.0.4	D0CS5109A
	BluetoothService	1.00.02	D0CS5127A
	Change Languages	1.00	D0CS5102A
	Copy	1.00	D0CS5104A
	Direct Connection	1.18	D0CS5118
	Fax	1.01	D0CS5106B
	Fax RX File	1.00	D0CS5125A
	GraphicData	0.28	DXXXXXXX
	ICCardDispatcher	3.08.02	D0CS5130A
	Installation Settings	1.01	D0CS5112A

Software for the Operation Panel Unit		Version	Part Number
	iWnn IME	2.8.201	D0BQ1453C
	iWnn IME Korean Pack	2.8.2	D0BQ1456A
	iWnn IME Simplified Chinese Pack	2.8.2	D0BQ1454A
	iWnn IME Traditional Chinese Pack	2.8.2	D0BQ1455A
	KerberosService	1.07.04	D0CS5131B
	LegacyUIData	0.22	DXXXXXXX
	Multi Device Hub	1.00	D0CS5133A
	Print/Scan (Memory Storage Device)	1.00	D0CS5107A
	Printer	1.00	D0CS5103A
	ProgramInfoService	1.00	D0CS5128A
	Proximity Card Reader Support Plugin	3.03.02	D0CS5117A
	Quick Card Authentication Config.	3.05.03	D0CS5123A
	Quick Print Release	1.01	D0CS5108B
	Remote Panel Operation	1.11	D0CS5132A
	RemoteConnect Support	1.1	D0BQ1499B
	RemoteSupportService	1.00	D0CS5110
	RicohScanGUIService	2.05	D0CS5113B
	Scanner	1.00	D0CS5105A
	Smart Device Connector	4.1.2	D0CS5101A
	Standard IC Card Plugin	3.03.02	D0CS5116A
	Stop	1.00	D0CS5126A
	Supply Information	1.00	D0CS5124A
	Support Settings	1.00	D0CS5111A
	Tray/Remaining Paper	1.00	D0CS5135A

Make clear to the sales representative that you purchase the MFP as CC-certified product.

1.3 TOE Overview

This section describes TOE Type, TOE Usage, and Major Security Features of the TOE.

1.3.1 TOE Type

This TOE is an MFP, which is an IT device that has Copy Function, Printer Function, Scanner Function, and Fax Function.

1.3.2 TOE Usage and Major Security Features of the TOE

The TOE is an MFP which is assumed that it will be installed in an office and used in an environment where it is connected with a telephone line and the LAN as shown in Figure 1. The user uses each function (Copy Function, Printer Function, Scanner Function, and Fax Function) by operating from the Operation Panel Unit of the MFP (hereinafter "the Operation Panel") or from the client computer connected by the LAN.

Identification and authentication, access control, eMMC encryption, and a security function for TLS encrypted communication are provided to prevent disclosure or alteration of assets, including documents handled by the TOE and setting information related to security functions, through unauthorized access to the TOE or communication data on the network. The TOE also provides a function to prevent unauthorised intrusion from telephone lines to the LAN. Events occurred on the TOE can be confirmed by the MFP administrator as audit log data, and the MFP administrator can use the management functions from the Operation Panel or the client computer. In addition, the TOE verifies whether the software configuration is valid. Since the TOE is not equipped with an HDD and handles user data with an eMMC, the Residual Data Overwrite Function is not included in the evaluation target Security Functions.

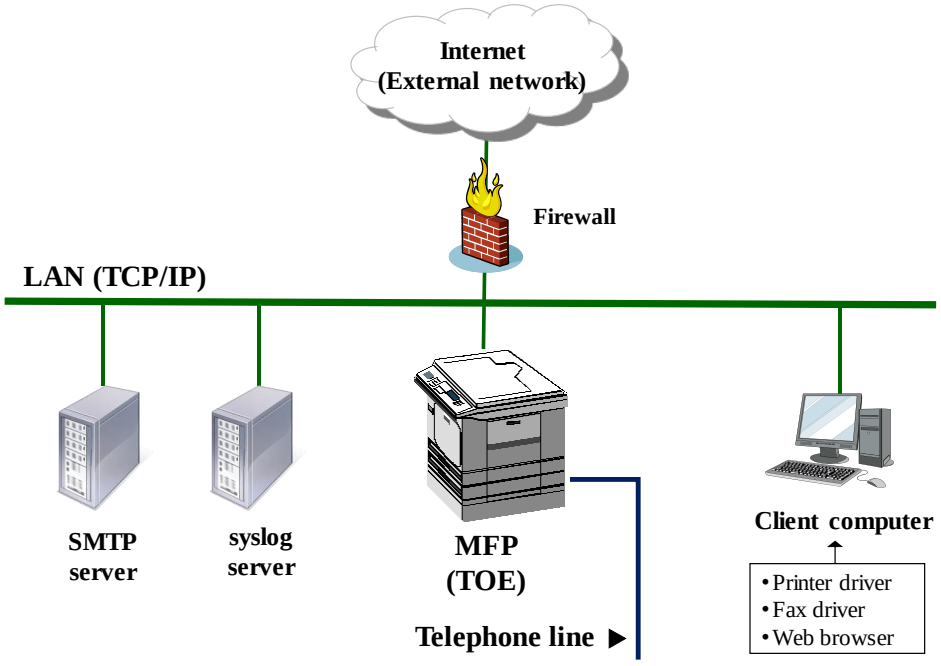


Figure 1: Example of TOE Environment

1.3.3 Hardware and Software Other than TOE That Is Necessary for the TOE

The following describes components other than TOE in the operational environment illustrated in Figure 1.

- Client computer
  - A computer that performs as a client of the TOE when it is connected to the LAN, and users can remotely operate the MFP from the client computer. It is necessary to use a Web browser to

operate various MFP settings and stored documents from the client computer. In order to store documents from the client computer, it is necessary to install the printer driver called PCL6 Driver (Version 1.1.0.0 or later version) provided by RICOH, which has a function that supports TLS (IPP over SSL). In addition, in order to transmit a fax from the client computer, it is necessary to install the fax driver called LAN Fax Driver (Version 9.5.0.0 or later version) provided by RICOH, which has a function that supports TLS (IPP over SSL).

- SMTP server
  - A server that is used when the TOE sends e-mail. The server uses the SMTP protocol and has a TLS-enabled service installed. It is necessary to use the Scanner Function (E-mail transmission of attachments).
- syslog server
  - A server that can receive audit log data recorded by the TOE. The server uses the syslog protocol and has a TLS-enabled service installed. Audit log data can be transferred to the syslog server as well. If the transfer setting is enabled, this server is used as a destination of audit log data.

The TOE is connected to the LAN to use the network, and connected to the telephone line to send and receive data to and from external faxes. In order to connect the TOE to an external network, it is necessary to set up a firewall to protect the TOE from unauthorized access from the external network.

Hardware and software other than TOE used in the TOE evaluation are shown below.

- Client computer
  - OS: Windows 10 and Windows 8.1
  - Printer driver: PCL6 Driver 1.1.0.0
  - Fax driver: LAN Fax Driver 9.5.0.0
  - Web browser: Internet Explorer 11 and Microsoft Edge 44
- SMTP server: Linux (Ubuntu 18.04.3 LTS) postfix 3.3.0
- syslog server: Linux (Ubuntu18.04.2 LTS) rsyslogd 8.32.0

1.4 TOE Description

This section describes Physical Boundary of the TOE and Logical Boundary of the TOE.

1.4.1 Physical Boundary of the TOE

The TOE consists of the MFP products in

Table 3 and guidance documents in Table 4 and Table 5. The target MFP product is the one equipped with software and hardware of a TOE version listed in Table 2. A delivery company delivers the MFP product to users. Some guidance documents are included in the MFP product, and others are delivered through the Web. Guidance documents are in English, and either guidance set of [English Version 1] for North America or [English Version 2] for Europe will be delivered.

Guidance documents will be delivered to users in the combinations described below.

Table 3: Combination to Be Delivered

No.	MFP		Guidance Document
	Product Name	Model Code	
1	IM C530F	D0CT-27	[English Version 2]
2	IM C530FB	D0CS-17	[English Version 1]
3	IM C530FB	D0CS-27	[English Version 2]

Table 4 and Table 5 show guidance documents included in [English Version 1] and [English Version 2] guidance sets, format, and delivery method.

Table 4: Guidance Documents for English Version 1

No.	Guidance Documents for the Product			
	Part Number	Guidance Document Name	Format	Delivery Method
1	D0BW-7035	Product Warranty Registration	Brochure	Included in the product
2	D0BW-7050A	For Users of This Product	Brochure	Included in the product
3	D0CS-7015	IM C530FB / IM C530F MULTIFUNCTION PRINTER LIMITED WARRANTY - FOR U.S. ONLY	Brochure	Included in the product
4	D0CS-7017	Notes for Users	Brochure	Included in the product
5	D0CS-7118	Notes for Users	Brochure	Included in the product
6	D256-7819A	Notes for Using This Machine Safely	Brochure	Included in the product
7	D256-7840A	SOFTWARE LICENSE AGREEMENT	Brochure	Included in the product
8	D0CS-7307	Safety Information	PDF	Through the Web
9	D0CS-7303	User Guide Selected Version	PDF	Through the Web
10	D0CS7305	Security Reference	HTML	Through the Web
11	D0CS7291	Setup	HTML	Through the Web
12	D0CS7292	Introduction and Basic Operations	HTML	Through the Web
13	D0CS7293	Copy	HTML	Through the Web
14	D0CS7294	Fax	HTML	Through the Web
15	D0CS7295	Scan	HTML	Through the Web

No.	Guidance Documents for the Product			
	Part Number	Guidance Document Name	Format	Delivery Method
16	D0CS7296	Printer	HTML	Through the Web
17	D0CS7297	Maintenance	HTML	Through the Web
18	D0CS7298	Troubleshooting	HTML	Through the Web
19	D0CS7299	Settings	HTML	Through the Web
20	D0CS7300	Specifications	HTML	Through the Web
21	D0CS7301	Security	HTML	Through the Web
22	D0CS7302	Driver Installation Guide	HTML	Through the Web
23	D0CS-7027 2022.03.02	Notes on Security Functions	PDF	Through the Web
24	D0CS-7025 2022.07.14	Notes for Administrators: Using This Machine in a Network Environment Compliant with Common Criteria	PDF	Through the Web
25	83NHENENZ 1.10 v228	Help	HTML	Through the Web

Guidance documents to be delivered through the Web can be downloaded from the following URL.

https://support.ricoh.com/services/device/ccmanual/IM_C530/en/Guidance_na.zip

Hash value (SHA256): 7d81777137c3e1a870b981a3bfd1d7fb420c50792510057fcc9ac500ab5bed9b

Table 5: Guidance Documents for English Version 2

No.	Guidance Documents for the Product			
	Part Number	Guidance Document Name	Format	Delivery Method
1	D0BW-7050A	For Users of This Product	Brochure	Included in the product
2	D0CS-7017	Notes for Users	Brochure	Included in the product
3	D0CS-7116	Notes for Users	Brochure	Included in the product
4	D0CS-7117	Notes for Users	Brochure	Included in the product
5	D0CS-7290	Notes for Users	Brochure	Included in the product
6	D256-7819A	Notes for Using This Machine Safely	Brochure	Included in the product
7	D256-7840A	SOFTWARE LICENSE AGREEMENT	Brochure	Included in the product
8	D0CS-7306	Safety Information	PDF	Through the Web

No.	Guidance Documents for the Product			
	Part Number	Guidance Document Name	Format	Delivery Method
9	D0CS-7303	User Guide Selected Version	PDF	Through the Web
10	D0CS7305	Security Reference	HTML	Through the Web
11	D0CS7291	Setup	HTML	Through the Web
12	D0CS7292	Introduction and Basic Operations	HTML	Through the Web
13	D0CS7293	Copy	HTML	Through the Web
14	D0CS7294	Fax	HTML	Through the Web
15	D0CS7295	Scan	HTML	Through the Web
16	D0CS7296	Printer	HTML	Through the Web
17	D0CS7297	Maintenance	HTML	Through the Web
18	D0CS7298	Troubleshooting	HTML	Through the Web
19	D0CS7299	Settings	HTML	Through the Web
20	D0CS7300	Specifications	HTML	Through the Web
21	D0CS7301	Security	HTML	Through the Web
22	D0CS7302	Driver Installation Guide	HTML	Through the Web
23	D0CS-7027 2022.03.02	Notes on Security Functions	PDF	Through the Web
24	D0CS-7025 2022.07.14	Notes for Administrators: Using This Machine in a Network Environment Compliant with Common Criteria	PDF	Through the Web
25	83NHENENZ 1.10 v228	Help	HTML	Through the Web

Guidance documents to be delivered through the Web can be downloaded from the following URL.

https://support.ricoh.com/services/device/ccmanual/IM_C530/en/Guidance_eu.zip

Hash value (SHA256): 105f0cd68c7499c4676191e7e92408b0b47dae246126dca2bc15b75cce91fe5e

1.4.2 Logical Boundary of the TOE

The logical boundary of the TOE is described below.

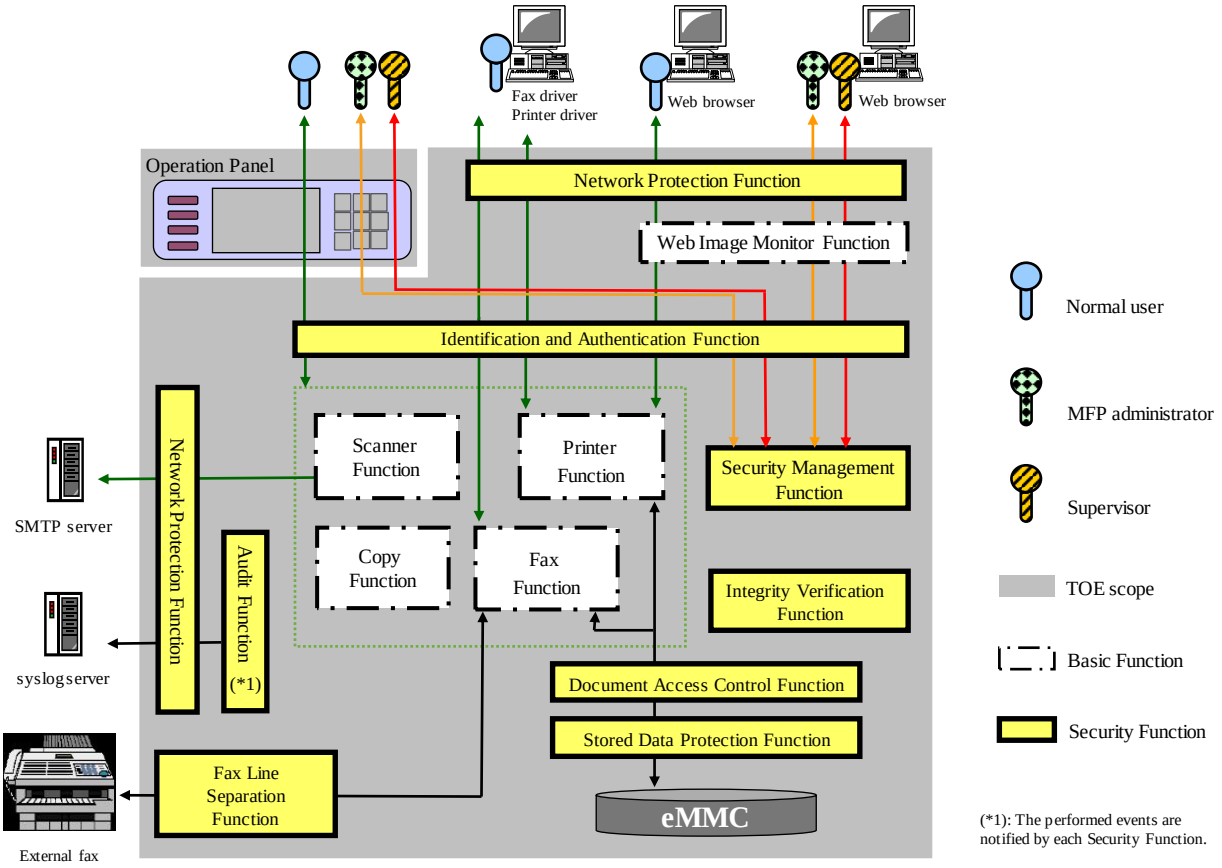


Figure 2: Logical Boundary of the TOE

As shown in Figure 2, the TOE has Basic Functions and Security Functions, which of each are described below.

1.4.2.1. Basic Functions

The overview of the Basic Functions is described below.

Web Image Monitor Function

The Web Image Monitor Function (hereinafter "WIM") is for the TOE user to remotely control the TOE. This function can be used from the Web browser on the client computer connected to the TOE via LAN.

Copy Function

The Copy Function is to scan paper documents and copy the scanned documents (image data) by user operation from the Operation Panel. The user can magnify or edit the copied image data.

Printer Function

The Printer Function is to store the document data received by the TOE from the printer driver of the client computer in eMMC as locked print document data, and is for the user to delete the document data from WIM or print/delete it from the Operation Panel.

Scanner Function

The Scanner Function is to scan paper documents and send the scanned documents to the SMB server by user operation from the Operation Panel.

Document data is transmitted by means of E-mail transmission of attachments. E-mail transmission of attachments is possible only with the mail server and e-mail addresses that are pre-registered in the TOE by the MFP administrator and with which secure communication can be ensured.

Fax Function

The Fax Function consists of Fax Transmission Function and Fax Reception Function using the G3 fax protocol, which uses a telephone line.

Fax Transmission Function is to send images of scanned paper documents or images of electronic documents to external faxes as document data. When sending images of electronic documents via fax, a fax driver is used. The telephone numbers that are pre-registered in the TOE are only allowed as a fax destination.

Fax Reception Function is to store documents, which are received from external faxes via a telephone line, in the eMMC. Stored document data can be printed from the Operation Panel.

1.4.2.2. Security Functions

The Security Functions are described below.

Audit Function

The Audit Function is to generate a log of TOE's security-relevant events (hereinafter, "audit events") associated with the user's identity in the eMMC as audit log data. This function provides the recorded audit log data in a legible fashion for users to audit. The recorded audit log data can be downloaded/deleted only by the MFP administrator.

The date and time to be recorded in the audit log data are retrieved from the system clock of the TOE. The TOE writes the newest audit log data over the oldest audit log data when there is insufficient space in the audit log data files to append the newest audit log data. The TOE can transfer the audit log data to the syslog server.

Identification and Authentication Function

The Identification and Authentication Function is to verify whether the person who is going to use the TOE is an authorised user, so that the TOE can allow only the authenticated users to operate the management functions and the MFP application and reject them when the authentication fails. The TOE verifies a user by receiving the login user name and login password of the user. This function includes the following functionality:

- Authentication feedback area protection function that displays the password using dummy letters when entering the login password

- Lockout function that prohibits users from logging in when the number of consecutive authentication failures reaches the threshold
- A function for protection of the quality of login passwords that registers only passwords satisfying the conditions of the minimum character number of passwords defined in advance by the MFP administrator and the required character type.
- A function for automatic user logout when no operation is performed for a certain period of time from the logged-in state.

Document Access Control Function

The Document Access Control Function is to permit the authorised user of the TOE authenticated by the Identification and Authentication Function to operate the user document data and the user job data based on the user privileges or the login user name.

Network Protection Function

The Network Protection Function is to prevent information leakage due to network monitoring by providing encrypted communication and detect alteration of communication details when communicating with trusted IT products (client computer, syslog server, SMTP server). The TOE implements this function with TLS.

Fax Line Separation Function

The Fax Line Separation Function is to prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol, in order to prevent intrusion from the telephone line into the LAN.

Stored Data Protection Function

The Stored Data Protection Function is to encrypt data to be written to the eMMC in order to protect data recorded in the eMMC from data leakage.

Security Management Function

The Security Management Function is to control the operation of TSF data and the behaviour of the Security Functions based on the user privileges or the login user name. In order to enable control, this function includes a function to maintain the role of operating the Security Management Function and associate the role with the authorised user of the TOE authenticated by the Identification and Authentication Function, and a function to set appropriate default values for the security attributes.

Integrity Verification Function

The Integrity Verification Function is a self-test function that verifies the integrity of executable code in the TSF.

2 Conformance Claim

This section describes 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 the TOE claim conformance

  Part 1:

  Introduction and general model April 2017 Version 3.1 Revision 5 (Japanese translation ver.1.0) CCMB-2017-04-001

  Part 2:

  Security functional components April 2017 Version 3.1 Revision 5 (Japanese translation ver.1.0) CCMB-2017-04-002

  Part 3:

  Security assurance components April 2017 Version 3.1 Revision 5 (Japanese translation ver.1.0) CCMB-2017-04-003

- Functional requirements: Part 2 extended
- Assurance requirements: Part 3 conformance

2.2 PP Claims

There is no PP that this ST and TOE conform to.

2.3 Package Claims

This ST and TOE claim conformity to package: EAL2.

There are no assurance components to be added.

2.4 Conformance Claim Rationale

This ST and TOE do not claim PP conformity.

3 Security Problem Definitions

This section describes Users, Assets, Threats, Organisational Security Policies, and Assumptions.

3.1 Definition of Users

This section defines the users related to the TOE.

The users consist of normal users and administrators, and the administrators are divided into MFP administrators and supervisors.

As described in Table 6, the users are classified according to their respective roles, and have user privileges based on the roles of normal users, MFP administrators, and supervisors.

Table 6: Definition of Users

Definition of Users		Explanation
Normal user		A user who is allowed to use the TOE. A normal user is provided with a login user name and can use Copy Function, Fax Function, Scanner Function, and Printer Function.
Administrator	MFP administrator	Has the privilege to manage the TOE, including: • Operation of configuration of normal user settings • Operation of setting information related to MFP device behaviour • Operation of audit log data • Operation of configuration of network settings • Access management of fax reception documents data
	Supervisor	Has the privilege to manage the TOE, including: • Change login password of MFP administrators • Unlock locked-out MFP administrators

3.2 Assets

In this section, the assets are categorised into the following two groups:

Table 7: Asset Categories

Asset Category	Definition
User data	Data created by the user, for the user, that does not affect the operation of the TSF.
TSF data	Data created by the TOE, for the TOE, that may affect the operation of the TSF.

The user data can be divided into the following two categories.

Table 8: User Data

User data	Definition
User document data	Information contained in the user's document in electronic or hard-copy format. In particular, the user document data stored and saved in the eMMC is called stored document data. Further, the data stored by means of locked print from the printer driver is called locked print document data, and the data stored from an external fax via a telephone line is called fax reception document data.
User job data	Information related to the user's document or document processing job.

3.2.1 TSF Data

The TSF data is divided into the following two categories.

Table 9: TSF Data Categories

TSF Data Category	Definition
TSF confidential data	Confidential TSF data that must be protected so that it cannot be viewed or modified by anyone other than authorised users.
TSF protected data	Protected TSF data that does not pose a security threat when published, but must be protected from unauthorised alteration.

The TSF data handled by this TOE for each category are shown below.

Table 10: TSF Data

Category	TSF data	Description
TSF confidential data	Login password	A password associated with each login user name.
	Audit log data	Audit log data in which events occurred are recorded.
	eMMC cryptographic key	Cryptographic key used to encrypt data in the eMMC.
TSF protected data	Login user name	User identifier associated with any of the normal user, MFP administrator, and supervisor. The TOE identifies users by this identifier.
	Stored reception file user	This is a list of login user names of normal users who are permitted to access the fax reception document data. There is one list for all fax reception document data.
	Lockout settings	Settings related to lockout policies and lockout status.
	Date/time settings	Settings related to date/time.
	Password quality settings	Settings of the minimum character number and the combination of characters to be registered for user authentication regarding the password policy.

Category	TSF data	Description
	Auto logout settings	Auto logout settings for the Operation Panel and auto logout settings for the WIM.
	Audit log data settings	Settings related to the transfer of audit log data.
	Cryptographic communication settings	Settings related to TLS communication with clients and servers.

3.3 Threats

This section defines and describes the assumed threats related to the use and operational environment of this TOE. The threats defined in this section are unauthorised persons with knowledge of published information about the TOE operations and such attackers are capable of Basic level of attack potential.

T.DOCUMENT_DATA_DIS Disclosure of user document data

User document data under the TOE management may be disclosed by persons without a login user name, or by persons with a login user name but without an access permission to the document.

T.DOCUMENT_DATA_ALT Alteration of user document data

User document data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the document.

T. JOB_ALT Alteration of user job data

User job data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the user job data.

T.PROTECT_DATA_ALT Alteration of TSF protected data

TSF protected data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

T.CONFIDENTIAL_DATA_DIS Disclosure of TSF confidential data

TSF confidential data under the TOE management may be disclosed by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONFIDENTIAL_DATA_ALT Alteration of TSF confidential data

TSF confidential data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

3.4 Organisational Security Policies

The following organisational security policies are taken as matters to be complied by TOE: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 created by the National Institute of Standards and Technology is considered.

P.AUTHORIZATION User identification and authentication

Only users with operation permission of the TOE shall be authorised to use the TOE.

P.VALIDATION Software verification

The TOE shall have procedures to self-verify executable code in the TSF.

P.AUDIT Management of audit log data records

To maintain operational accountability and security, records that provide an audit trail of TOE security-relevant events shall be created, maintained, protected from disclosure and alteration by unauthorised persons, and confirmed by authorised persons.

P.FAX Management of external interfaces

For provision of the Fax Function over the telephone line by the TOE, the separation between the telephone line and the LAN shall be ensured.

P.ENCRYPTION eMMC encryption

The data recorded in the TOE's eMMC shall be encrypted.

3.5 Assumptions

This section identifies and describes the assumptions related to the operational environment of this TOE.

A.PHYSICAL_PROTECTION Access management

The MFP administrator shall install the TOE in a secure and monitored area in accordance with the guidance documents and restrict a chance of physical access by unspecified number of persons.

A.NETWORK_PROTECTION **Network management**

The MFP administrator shall install the TOE in an operational environment protected from any external attempt to directly access the TOE's LAN interfaces.

A.USER **User training**

The MFP administrator shall train normal users according to the guidance documents and ensure that normal users are aware of the security policies and procedures of their organisation and have the competence to follow those policies and procedures.

A.ADMIN **Administrator training**

The MFP administrator shall be aware of the security policies and procedures of their organisation and have the competence to correctly configure and operate the TOE in accordance with the guidance documents following those policies and procedures.

A.TRUSTED_ADMIN **Trusted administrator**

Persons who do not use their privileged access rights for malicious purposes according to the guidance documents shall be appointed as administrators.

4 Security Objectives

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

4.1 Security Objectives for TOE

This section describes the security objectives for the TOE.

O.DOCUMENT_DATA_DIS **Protection of user document data disclosure**

The TOE shall protect user document data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the user document data.

O.DOCUMENT_DATA_ALT **Protection of user document data alteration**

The TOE shall protect user document data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user document data.

O.JOB_ALT **Protection of user job data alteration**

The TOE shall protect user job data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job data.

O.PROTECT_DATA_ALT **Protection of TSF protected data alteration**

The TOE shall protect TSF protected data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

O.CONFIDENTIAL_DATA_DIS **Protection of TSF confidential data disclosure**

The TOE shall protect TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

O.CONFIDENTIAL_DATA_ALT **Protection of TSF confidential data alteration**

The TOE shall protect TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

O.AUTHORIZATION **User identification and authentication**

The TOE shall require identification and authentication of users and shall ensure that users are authorised in accordance with security policies before allowing them to use the TOE.

O.FAX **Management of external interfaces by TOE**

For provision of the Fax Function over the telephone line by the TOE, the TOE shall ensure the separation between the telephone line and the LAN.

O.VALIDATION **Software verification**

The TOE shall provide procedures to self-verify executable code in the TSF.

O.AUDIT **Management of audit log data records**

The TOE shall ensure that logs of TOE security-relevant events are created and maintained as audit log data, and protected from disclosure or alteration by unauthorised persons. It shall also provide audit log data in a format that can be verified by authorised persons.

O.EMMC_ENCRYPTION **eMMC encryption**

The TOE shall ensure that the function to encrypt data first and then store it in the eMMC is provided.

4.2 Security Objectives for Operational Environment

This section describes the security objectives for the operational environment.

OE.AUDIT **Audit log data protection in trusted IT products**

The MFP administrator shall ensure that audit log data that is exported to a trusted IT product are protected from unauthorised access and modifications.

OE.PHYSICAL_PROTECTION **Physical management**

The MFP administrator shall ensure that the TOE is installed in a secure and monitored area in accordance with the guidance documents and a chance of physical access by unspecified number of persons is restricted.

OE.NETWORK_PROTECTION **Network management**

The MFP administrator shall ensure that the TOE is installed in an operational environment protected from any external attempt to directly access the TOE's LAN interfaces.

OE.AUTHORIZED_USER Assignment of user authority

The MFP administrator shall give users the authority to use the TOE in accordance with the security policies and procedures of their organisation.

OE.TRAINED_USER User training

The MFP administrator shall train users according to the guidance documents and ensure that users are aware of the security policies and procedures of their organisation and have the competence to follow those policies and procedures.

OE.TRAINED_ADMIN Administrator training

The responsible manager of MFP shall ensure that MFP administrators are trained to correctly configure and operate the TOE in accordance with the guidance documents following the security policies and procedures of their organisation and they have the competence to follow those policies and procedures.

OE.TRUSTED_ADMIN Trusted administrator

The responsible manager of MFP shall appoint administrators who will not use their privileged access rights for malicious purposes according to the guidance documents.

OE.AUDIT_MANAGE Log audit

The MFP administrator shall ensure that audit log data is reviewed at appropriate intervals for detecting security violations or unusual patterns of activity.

4.3 Security Objectives Rationale

This section describes the rationale for security objectives. The security objectives are for upholding the assumptions, countering the threats, and enforcing the organisational security policies, which are defined.

4.3.1 Correspondence Table of Security Objectives

Table 11 describes the correspondence between the assumptions, threats and organisational security policies, and each security objective.

Table 11: Rationale for Security Objectives

Security Objectives / Security Problem Definitions	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	OE.AUTHORIZED_USER	O.VALIDATION	O.AUDIT	OE.AUDIT	OE.AUDIT_MANAGE	O.FAX	OE.PHYSICAL_PROTECTION	OE.NETWORK_PROTECTION	O.EMMC_ENCRYPTION	OE.TRAINED_ADMIN	OE.TRUSTED_ADMIN	OE.TRAINED_USER
T.DOCUMENT_DATA_DIS	X						X	X											
T.DOCUMENT_DATA_ALT		X					X	X											
T.JOB_ALT			X				X	X											
T.PROTECT_DATA_ALT				X			X	X											
T.CONFIDENTIAL_DATA_DIS					X		X	X											
T.CONFIDENTIAL_DATA_ALT						X	X	X											
P.AUTHORIZATION							X	X											
P.VALIDATION									X										
P.AUDIT										X	X	X							
P.FAX													X						
P.ENCRYPTION																X			
A.PHYSICAL_PROTECTION														X					
A.NETWORK_PROTECTION															X				
A.ADMIN																	X		
A.TRUSTED_ADMIN																		X	
A.USER																			X

4.3.2 Security Objectives Descriptions

The following describes the rationale for each security objective being appropriate to satisfy the threats, assumptions and organisational security policies.

T.DOCUMENT_DATA_DIS

T.DOCUMENT_DATA_DIS is countered by O.DOCUMENT_DATA_DIS, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.DOCUMENT_DATA_DIS, the TOE protects the user document data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the user document data.

T.DOCUMENT_DATA_DIS is countered by these objectives.

T.DOCUMENT_DATA_ALT

T.DOCUMENT_DATA_ALT is countered by O.DOCUMENT_DATA_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.DOCUMENT_DATA_ALT, the TOE protects user document data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user document data.

T.DOCUMENT_DATA_ALT is countered by these objectives.

T.JOB_ALT

T.JOB_ALT is countered by O.JOB_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.JOB_ALT, the TOE protects the user job data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job data.

T.APPLICATIONS_ALT is countered by these objectives.

T.PROTECT_DATA_ALT

T.PROTECT_DATA_ALT is countered by O.PROTECT_DATA_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.PROTECT_DATA_ALT, the TOE protects the TSF protected data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

T.PROTECT_DATA_ALT is countered by these objectives.

T.CONFIDENTIAL_DATA_DIS

T.CONFIDENTIAL_DATA_DIS is countered by O.CONFIDENTIAL_DATA_DIS, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.CONFIDENTIAL_DATA_DIS, the TOE protects the TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONFIDENTIAL_DATA_DIS is countered by these objectives.

T.CONFIDENTIAL_DATA_ALT

T.CONFIDENTIAL_DATA_ALT is countered by O.CONFIDENTIAL_DATA_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.CONFIDENTIAL_DATA_ALT, the TOE protects the TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONFIDENTIAL_DATA_ALT is countered by these objectives.

P.AUTHORIZATION

P.AUTHORIZATION is countered by O.AUTHORIZATION and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE.

P.AUTHORIZATION is enforced by these objectives.

P.VALIDATION

P.VALIDATION is countered by O.VALIDATION.

By O.VALIDATION, the TOE provides measures for self-verifying the executable code of the TSF.

P.VALIDATION is enforced by this objective.

P.AUDIT

P.AUDIT is countered by O.AUDIT, OE.AUDIT, OE.AUDIT_MANAGE.

By O.AUDIT, the TOE creates and maintains logs of TOE security-relevant events as audit log data and protects them from disclosure or alteration by unauthorised persons. It also provides audit log data in a format that can be verified by unauthorised persons.

On the other hand, by OE.AUDIT, the MFP administrator ensures that audit log data that is exported to a trusted IT product is protected from being accessed and altered by unauthorised persons. In addition, by OE.AUDIT_MANAGE, the MFP administrator reviews audit log data at appropriate intervals for detecting security violations or unusual patterns of activity.

P.AUDIT is enforced by these objectives.

P.FAX

P.FAX is countered by O.FAX.

By O.FAX, for provision of the Fax Function over the telephone line by the TOE, the TOE ensures the separation between the telephone line and the LAN.

P.FAX is enforced by this objective.

P.ENCRYPTION

P.ENCRYPTION is countered by O.EMMC_ENCRYPTION.

By O.EMMC_ENCRYPTION, the TOE provides the function to encrypt data first and then store it in the eMMC.

P.ENCRYPTION is enforced by this objective.

A.PHYSICAL_PROTECTION

A.PHYSICAL_PROTECTION is operated under OE.PHYSICAL_PROTECTION.

By OE.PHYSICAL_PROTECTION, the TOE is installed in a secure and monitored area in accordance with the guidance documents and a chance of physical access by unspecified number of persons is restricted.

A.PHYSICAL_PROTECTION is fulfilled by this objective.

A.NETWORK_PROTECTION

A.NETWORK_PROTECTION is operated under OE.NETWORK_PROTECTION.

By OE.NETWORK_PROTECTION, the MFP administrator ensures that the TOE is installed in an operational environment protected from any external attempt to directly access the TOE's LAN interfaces.

A.NETWORK_PROTECTION is fulfilled by this objective.

A.ADMIN

A.ADMIN is operated under OE.TRAINED_ADMIN.

By OE.TRAINED_ADMIN, the responsible manager of MFP ensures that MFP administrators are trained to correctly configure and operate the TOE in accordance with the guidance documents following the security policies and procedures of their organisation and they have the competence to follow those policies and procedures.

A.ADMIN is fulfilled by this objective.

A.TRUSTED_ADMIN

A.TRUSTED_ADMIN is operated under OE.TRUSTED_ADMIN.

By OE.TRUSTED_ADMIN, the responsible manager of MFP appoints administrators who will not use their privileged access rights for malicious purposes according to the guidance documents.

A.TRUSTED_ADMIN is fulfilled by this objective.

A.USER

A.USER is operated under OE.TRAINED_USER.

By OE.TRAINED_USER, the MFP administrator instructs the users in accordance with the guidance documents to make them aware of the security policies and procedures of their organisation, and the users follow those policies and procedures.

A.USER is fulfilled by this objective.

5 Extended Components Definition

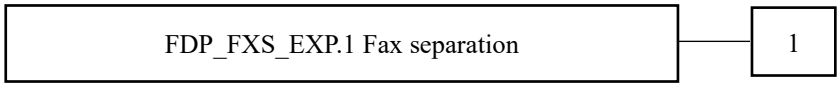
This section describes Extended Components Definition.

5.1 Fax separation (FDP_FXS_EXP)

Family behaviour

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

Component levelling



FDP_FXS_EXP.1 Fax separation requires that the fax interface is not available to create a network bridge between the telephone line and the LAN to which the TOE is connected.

Management: FDP_FXS_EXP.1

- There are no management actions foreseen.

Audit: FDP_FXS_EXP.1

There are no auditable events foreseen.

FDP_FXS_EXP.1 Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_FXS_EXP.1.1 **The TSF shall prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol.**

Rationale:

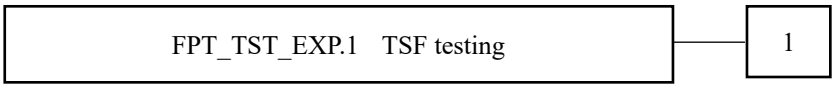
The fax separation protects the LAN against attacks from the telephone lines. Common Criteria does not provide suitable SFRs for protecting TSF or user data. Since this extended component protects TSF data or user data, it is considered as a component of the FDP class.

5.2 TSF testing (FPT_TST_EXP)

Family behaviour

This family addresses TSF's self-testing requirements for verifying the integrity of executable code in the TSF.

Component levelling



FPT_TST_EXP.1 TSF testing requires a suite of self-tests that runs at initial startup to verify the integrity of executable code in the TSF.

Management: FPT_TST_EXP.1

- There are no management actions foreseen.

Audit: FPT_TST_EXP.1

There are no auditable events foreseen.

FPT_TST_EXP.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXP.1.1 **The TSF shall run a suite of self-tests at initial startup (and power-on) to verify the integrity of executable code in the TSF.**

Rationale:

The TSF testing ensures that the integrity of executable code in the TSF is verified. The target of integrity verification is different from that of the SFRs provided by Common Criteria. Since this extended component protects the TOE, it is considered as a component of the FPT class.

6 Security Requirements

This section describes Security Functional Requirements, Security Assurance Requirements, and Security Requirements Rationale.

The terms used in this section are defined in Table 12.

Table 12: Terms in Section 6

Classification of Term	Name of Term	Description of Term
Subject	Normal user process	A process that acts on behalf of a normal user when the authentication of the normal user is successful.
	MFP administrator process	A process that acts on behalf of an MFP administrator when the authentication of the MFP administrator is successful.
	Supervisor process	A process that acts on behalf of a supervisor when the authentication of the supervisor is successful.
Object	Locked print document data	Document data stored in the TOE by means of locked print from the printer driver of the client computer instructed by a normal user.
	Fax reception document data	Document data stored in the TOE by means of fax reception from an external fax via a telephone line instructed by the TOE.
	User job data	Information related to the user's document or document processing job. Information regarding a sequence of operations of each TOE function (Copy Function, Scanner Function, Printer Function, Fax Transmission Function, and Fax Reception Function) from beginning to end.
Operation	Print	To print stored document data.
	Delete	To delete security attributes, TSF data, or objects.
	Modify	To modify security attributes and TSF data.
	Query	To refer security attributes and TSF data.
	Newly create	To newly create security attributes and TSF data.
	Generate	To generate TSF data

Classification of Term	Name of Term	Description of Term
Security attribute	Login user name	User identifier associated with any of the normal user, MFP administrator, and supervisor. The TOE identifies users by this identifier.
	Stored reception file user	This is a list of login user names of normal users who are permitted to access the fax reception document data. There is one list for all fax reception document data.
	User privilege	Any role of normal user, MFP administrator, or supervisor who uses the TOE, and the privilege according to that role.
External entity	Normal user	A user who is allowed to use the TOE. A normal user is provided with a login user name and can operate the MFP application (that is, run and cancel Copy Function, Fax Function, Scanner Function, and Printer Function).
	MFP administrator	A user who is allowed to manage the TOE. An MFP administrator has the privilege to do the following: - Operation of configuration of normal user settings - Operation of setting information related to MFP device behaviour - Operation of audit log data - Operation of configuration of network settings - Access management of fax reception documents data
	Supervisor	A user who is allowed to manage the TOE. A supervisor is authorised to change the login password of the MFP administrator.

6.1 Security Functional Requirements

This section describes the TOE security functional requirements for fulfilling the security objectives defined in section 4.1.

6.1.1 Class FAU: Security audit

6.1.1.1. FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 **The TSF shall be able to generate an audit record of the following auditable events:**
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
c) [assignment: *other specifically defined auditable events*].

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

- ***not specified***

[assignment: *other specifically defined auditable events*]

- ***Auditable events of the TOE shown in Table 13***

FAU_GEN.1.2 **The TSF shall record within each audit record at least the following information:**
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

[assignment: *other audit relevant information*]

- ***All login user names that attempted the user identification for FIA_UID.1, log type, communicating devices with the trusted channel, lockout operation type, locked out user, and locked out user who is to be released***

The related SFRs and auditable events for the TOE are listed in Table 13.

Table 13: List of Auditable Events

Auditable Event	Related SFR
Download and deletion of audit log data	FAU_STG.1 FAU_SAR.1 FAU_SAR.2
Start and end of printing locked print document data Deletion of locked print document data Start and end of printing fax reception document data Deletion of user job data	FDP_ACF.1
Starting and releasing lockout	FIA_AFL.1
Success and failure of login operation	FIA_UAU.1 FIA_UID.1
Table 24 Use of the management functions	FMT_SMF.1

Auditable Event	Related SFR
Termination of session by auto logout	FTA_SSL.3
Failure of communication with trusted channel (Failure of E-mail transmission of attachments from the scanner, failure of syslog transfer, failure of LAN Fax via the network, failure of locked print via the network, failure of WIM communication)	FTP_ITC.1

6.1.1.2. FAU_GEN.2 User identity 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.**

6.1.1.3. 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 unauthorised 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***

6.1.1.4. 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*

6.1.1.5. 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*]

- ***MFP administrator***

[assignment: *the list of audit information*]

- ***All audit log data***

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

6.1.1.6. 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.**

6.1.2 Class FCS: Cryptographic support

6.1.2.1. FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

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

[assignment: *list of standards*]

- ***NIST SP 800-90A***

[assignment: *cryptographic key generation algorithm*]

- ***Hash_DRBG(SHA256)***

[assignment: *cryptographic key sizes*]

- ***256 bits***

6.1.2.2. FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**

[assignment: *list of standards*]

- ***None***

[assignment: *cryptographic key destruction method*]

- ***Overwrite with 0***

6.1.2.3. FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [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 standards*]

- ***FIPS197***

[assignment: *cryptographic algorithm*]

- ***AES***

[assignment: *cryptographic key sizes*]

- ***256 bits***

[assignment: *list of cryptographic operations*]

- ***Encryption of data to be written to the eMMC***

  Decryption of data to be read from the eMMC

6.1.3 Class FDP: User data protection

6.1.3.1. 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 by the SFP*].**

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

- ***List of subjects, objects, and operations among subjects and objects shown in Table 14***

[assignment: *access control SFP*]

- ***User data access control SFP***

Table 14: List of Subjects, Objects, and Operations among Subjects and Objects

Subjects	Objects	Operations
Normal user process MFP administrator process Supervisor process	Locked print document data	Print Delete Modify
	Fax reception document data	Print Delete Modify
Normal user process MFP administrator process Supervisor process	User job data	Delete Modify

6.1.3.2. 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: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or a named group of SFP-relevant security attributes*].**

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or a named group of SFP- relevant security attributes*]

- ***Subjects, objects, and for each, the security attributes shown in Table 15***

[assignment: ***access control SFP*****]**

- ***User data access control SFP***

Table 15: Subjects, Objects, and Security Attributes

Subjects or Objects	Security Attributes
Normal user process	Login user name
MFP administrator process	User privilege
Supervisor process	User privilege
Locked print document data	Login user name
Fax reception document data	Stored reception file user
User job data	Login user name

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 governing access among controlled subjects and controlled objects using controlled operations on controlled objects*****].**

[assignment: ***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*****]**

- ***Rules to control operations among subjects and objects shown in Table 16***

Table 16: Rules to Control Operations among Subjects and Objects

Subjects (Security Attributes)	Objects (Security Attributes)	Operations	Rules of User Data Access Control SFP
Normal user process (Login user name)	Locked print document data (Login user name)	Print Delete	The print and delete operations are permitted only when the login user name for the normal user process and the login user name of the user who created the locked print document data match.
Normal user process (Login user name)	Fax reception document data (Stored reception file user)	Print	The print operation is permitted only when the login user name for the normal user process and the login user name registered for a stored reception file user match.
Normal user process (Login user name)	User job data (Login user name)	Delete	The delete operation is permitted only when the login user name for the normal user process and the login user name for the user job data match.

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*****]**

- ***Rules that explicitly authorise access shown in Table 17***

Table 17: Rules That Explicitly Authorise Access

Subjects (Security Attributes)	Objects (Security Attributes)	Operations	Rules of User Data Access Control SFP
MFP administrator process (User privilege)	Locked print document data (Login user name)	Delete	Allows the MFP administrator process, which has the user privilege of the MFP administrator, to delete locked print document data.
MFP administrator process (User privilege)	User job data (Login user name)	Delete	Allows the MFP administrator process, which has the user privilege of the MFP administrator, to delete user job data.

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [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*****]**

- ***Rules that explicitly deny access shown in Table 18***

Table 18: Rules That Explicitly Deny Access

Subjects (Security Attributes)	Objects (Security Attributes)	Operations	Rules of User Data Access Control SFP
MFP administrator process (User privilege)	Locked print document data (Login user name)	Print	Refuses the MFP administrator process, which has the user privilege of the MFP administrator, to print locked print document data.
MFP administrator process (User privilege)	Fax reception document data (Fax reception document user)	Print	Refuses the MFP administrator process, which has the user privilege of the MFP administrator, to print fax reception document data.
Supervisor process (User privilege)	Locked print document data (Login user name)	Print Delete	Refuses the supervisor process, which has the user privilege of the supervisor, to print and delete locked print document data.
Supervisor process (User privilege)	Fax reception document data (Fax reception document user)	Print	Refuses the supervisor process, which has the user privilege of the supervisor, to print fax reception document data.
Supervisor process (User privilege)	User job data (Login user name)	Delete	Refuses the supervisor process, which has the user privilege of the supervisor, to delete user job data.
Normal user process (Login user name)	Locked print document data (Login user name)	Modify	Refuses operations to change locked print document data for any subject. (*1)
MFP administrator process (User privilege)			
Supervisor process (User privilege)			
Normal user process (Login user name)	Fax reception document data (Fax reception document user)	Delete Modify	Refuses operations to delete and change fax reception document data for any subject. (*2)
MFP administrator process (User privilege)			
Supervisor process (User privilege)			

Subjects (Security Attributes)	Objects (Security Attributes)	Operations	Rules of User Data Access Control SFP
Normal user process (Login user name)	User job data (Login user name)	Modify	Refuses operations to change user job data for any subject. (*3)
MFP administrator process (User privilege)			
Supervisor process (User privilege)			

(*1) This TOE does not have an interface for making changes to locked print document data.

(*2) This TOE does not have an interface for making changes to or deleting fax reception document data.

(*3) This TOE does not have an interface for making changes to user job data.

6.1.3.3. FDP_FXS_EXP.1 Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_FXS_EXP.1.1 **The TSF shall prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol.**

6.1.4 Class FIA: Identification and authentication

6.1.4.1. FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when [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].**

[assignment: *list of authentication events*]

- ***Authentication events shown in Table 19***

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

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

[assignment: range of acceptable values]

- ***1 to 10***

Table 19: List of Authentication Events

Authentication Events
User authentication using the Operation Panel
User authentication using WIM
User authentication when printing locked print documents from the printer driver
User authentication when sending a fax from the fax driver

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: *the list of actions*]

- ***Actions shown in Table 20***

Table 20: List of Actions for Authentication Failure

Unsuccessfully Authenticated Users	Actions for Authentication Failure
Normal user	The normal user is locked out during the lockout time set by the MFP administrator, or until the MFP administrator performs the release operation.
Supervisor	The supervisor is locked out during the lockout time set by the MFP administrator, until the MFP administrator performs the release operation, or until a given time elapses after the TOE restarts.
MFP administrator	The MFP administrator is locked out during the lockout time set by the MFP administrator, until the supervisor performs the release operation, or until a given time elapses after the TOE restarts.

6.1.4.2. 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 privilege***

6.1.4.3. 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*]

- ***Quality metrics are as follows:***

(1) ***To use multiple character types of upper-case letters, lower-case letters, digits, and symbols (The required number of types is set by the MFP administrator as the password complexity setting.)***

(2) Passwords must be single-byte alphanumeric letters and symbols with minimum character number of password (8-32 characters set by the MFP administrator) or more, and

- ***Must be 128 characters or less for normal users***
- ***Must be 32 characters or less for MFP administrators and supervisors***

6.1.4.4. 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*] on behalf of the user to be performed before the user is authenticated.**

[assignment: *list of TSF mediated actions*]

- ***Viewing of user job data lists, WIM Help, system status, counter and information of inquiries, and execution of fax reception***

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.

6.1.4.5. 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 letters***

6.1.4.6. 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*] on behalf of the user to be performed before the user is identified.**

[assignment: *list of TSF-mediated actions*]

- ***Viewing of user job data lists, WIM Help, system status, counter and information of inquiries, and execution of fax reception***

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.

6.1.4.7. 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 privilege***

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 changing of attributes*]**

[assignment: *rules for changing of attributes*]

- ***None***

6.1.5 Class FMT: Security management

6.1.5.1. FMT_MOF.1 Control of the behaviour of the Security Functions

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Function

FMT_MOF.1.1 **The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: the *authorised and identified roles*].**

[assignment: *list of functions*]

- ***syslog transfer function***

[selection: *determine the behaviour of, disable, enable, modify the behaviour of]*

- ***disable, enable***

[assignment: *the authorised and identified roles*]

- ***MFP administrator***

6.1.5.2. FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Function

FMT_MSA.1.1 **The TSF shall enforce the [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 and identified roles*].**

[assignment: *list of security attributes*]

- ***Security attributes in*** *Table 21*

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

- ***delete, [assignment: other operations]***

[assignment: other operations]

- ***Newly create, modify***

[assignment: the *authorised and identified roles*]

- ***Roles (user privileges) for which operations in*** *Table 21* ***are allowed***

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

- ***User data access control SFP(s)***

Table 21: User Privilege by Security Attribute

Security Attributes	Operations	Roles (User Privileges) for Which Operations are Allowed
Login user name [When associated with a normal user]	Modify Delete Newly create	MFP administrator
Login user name [When associated with a supervisor]	Modify	Supervisor
Login user name [When associated with an MFP administrator]	Modify	MFP administrator
Stored reception file user	Modify	MFP administrator

6.1.5.3. FMT_MSA.3 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 **The TSF shall enforce the [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.**

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

- ***restrictive***

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

- ***User data access control SFP***

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

[assignment: the *authorised identified roles*]

- ***No authorised and identified roles***

6.1.5.4. 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 Function

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 authorised identified roles*].**

[assignment: *list of TSF data*]

- ***TSF data in Table 22***

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

- ***query, delete, [assignment: other operations]***

[assignment: other operations]

- ***Newly create, modify, generate***

[assignment: *the authorised identified roles*]

- ***Roles (user privileges) for which operations in Table 22 are allowed***

Table 22: List of TSF Data

Category	TSF data	Operations	Roles (User Privileges) for Which Operations are Allowed
TSF confidential data	Login password [When associated with a normal user]	Newly create Modify	MFP administrator
	Login password [When associated with the normal user who owns the login password]	Modify	Normal user who owns the login password
	Login password [When associated with a supervisor]	Modify	Supervisor
	Login password [When associated with an MFP administrator]	Modify	Supervisor MFP administrator
	eMMC cryptographic key	Query Delete Generate	MFP administrator
TSF protected data	Lockout settings	Modify	MFP administrator Supervisor (*1)
	Date/time settings	Modify	MFP administrator
	Password quality settings	Modify	MFP administrator
	Auto logout settings	Modify	MFP administrator
	Audit log data settings	Modify	MFP administrator
	Cryptographic communication settings	Modify	MFP administrator

(*1): Of the lockout settings, the supervisor can only perform the lockout release operation for the MFP administrator. Other lockout settings are made by the MFP administrator.

6.1.5.5. 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 Function

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 *authorised identified roles*].**

[assignment: *list of TSF data*]

- ***TSF data in*** Table 23

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

- ***Query***

[assignment: the *authorised identified roles*]

- ***Roles (user privileges) for which operations in*** Table 23 ***are allowed***

Table 23: List of TSF Data

Category	TSF data	Operations	Roles (User Privileges) for Which Operations are Allowed
TSF confidential data	Login password	Query	No roles for which operations are allowed

6.1.5.6. FMT_SMF.1 Specification of Management Function

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*]

- ***Management functions listed in Table 24***

Table 24: List of Specification of Management Functions

Management Functions
Stop/activate syslog transfer function
Newly create/modify login passwords
Query, delete, and generate eMMC cryptographic keys
Newly create/modify/delete login user names
Modify stored reception file user
Modify lockout settings
Modify date/time settings
Modify password quality settings
Modify auto logout settings
Modify audit log data settings
Modify cryptographic communication settings

6.1.5.7. FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

[assignment: *the authorised identified roles*]

- ***Normal user, supervisor, and MFP administrator***

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

6.1.6 Class FPT: Protection of the TSF

6.1.6.1. 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.

6.1.6.2. FPT_TST_EXP.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXP.1.1 **The TSF shall run a suite of self-tests at initial startup (and power-on) to verify the integrity of executable code in the TSF.**

6.1.7 Class FTA: TOE access

6.1.7.1. 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 [assignment: *time interval of user inactivity*]**

[assignment: *time interval of user inactivity*]

- ***Auto logout time for the Operation Panel elapsed, auto logout time for the WIM elapsed***

6.1.8 Class FTP: Trusted paths/channels

6.1.8.1. 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 channel 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*]

- ***The TSF, another trusted IT product***

FTP_ITC.1.3 **The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].**

[assignment: *list of functions for which a trusted channel is required*]

- ***E-mail transmission of attachments from the scanner***
- ***syslog transfer function***
- ***Fax Function***
- ***Printer Function***
- ***WIM Function***

6.2 Security Assurance Requirements

The evaluation assurance level of this TOE is EAL2. Table 25 lists the assurance components of the TOE.

Table 25: TOE Security Assurance Requirements (EAL2)

Assurance Classes	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
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	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 Requirements Rationale

This section describes the rationale for security requirements.

If all security functional requirements are satisfied as below, the security objectives defined in "4 Security Objectives" are fulfilled.

6.3.1 Tracing

Table 26 shows the relationship between the TOE security functional requirements and TOE security objectives. Items in **bold** provide the primal (**P**) fulfillment of the objectives, and items in standard typeface

support (S) its fulfillment. Table 26 shows that each TOE security functional requirement fulfils at least one TOE security objective.

Table 26: Relationship between Security Objectives and Functional Requirements

	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	O.FAX	O.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
FAU_GEN.1										**P**	
FAU_GEN.2										**P**	
FAU_STG.1						**P**				**P**	
FAU_STG.4										S	
FAU_SAR.1					**P**					**P**	
FAU_SAR.2					**P**					**P**	
FCS_CKM.1											S
FCS_CKM.4											S
FCS_COP.1											**P**
FDP_ACC.1	**P**	**P**	**P**								
FDP_ACF.1	**P**	**P**	**P**								
FDP_FXS_EXP.1								**P**			
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_SOS.1							S				
FIA_UAU.1							**P**				
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**			S	
FIA_USB.1							**P**				
FMT_MOF.1				**P**							
FMT_MSA.1	S	S	S	**P**							
FMT_MSA.3	S	S	S								
FMT_MTD.1(a)				**P**	**P**	**P**					
FMT_MTD.1(b)					**P**	**P**					

	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	O.FAX	O.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
FMT_SMF.1	S	S	S	S	S	S					
FMT_SMR.1	S	S	S	S	S	S					
FPT_STM.1										S	
FPT_TST_EXP.1									**P**		
FTA_SSL.3							S				
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

6.3.2 Justification of Traceability

This section describes how the TOE security objectives are fulfilled by the TOE security functional requirements corresponding to the TOE security objectives.

O.DOCUMENT_DATA_DIS Protection of user document data disclosure

O.DOCUMENT_DATA_DIS is the security objective to prevent the user document data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the user document data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 ensure that an access control policy for user document data is defined and access control functions are provided in accordance with the access control policy.

FDP_ACC.1 and FDP_ACF.1 are major SFRs to fulfill O.DOCUMENT_DATA_DIS.

(2) FTP_ITC.1

FTP_ITC.1 ensures that user document data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.DOCUMENT_DATA_DIS.

(3) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(4) FMT_MSA.3

FMT_MSA.3 ensures that security attributes are always set to restrictive values when user document data is generated.

FMT_MSA.3 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(5) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(6) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(7) FIA_UID.1

FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

O.DOCUMENT_DATA_DIS can be fulfilled by implementing these security functional requirements.

O.DOCUMENT_DATA_ALT Protection of user document data alteration

O.DOCUMENT_DATA_ALT is the security objective to prevent the user document data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user document data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 ensure that an access control policy for user document data is defined and access control functions are provided in accordance with the access control policy.

FDP_ACC.1 and FDP_ACF.1 are major SFRs to fulfill O.DOCUMENT_DATA_ALT.

(2) FTP_ITC.1

FTP_ITC.1 ensures that user document data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.DOCUMENT_DATA_ALT.

(3) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(4) FMT_MSA.3

FMT_MSA.3 ensures that security attributes are always set to restrictive values when user document data is generated.

FMT_MSA.3 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(5) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(6) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(7) FIA_UID.1

FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

O.DOCUMENT_DATA_ALT can be fulfilled by implementing these security functional requirements.

O.JOB_ALT Protection of user job data alteration

O.JOB_ALT is the security objective to prevent the user job data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 ensure that an access control policy for user job data is defined and access control functions are provided in accordance with the access control policy.

FDP_ACC.1 and FDP_ACF.1 are major SFRs to fulfill O.JOB_ALT.

(2) FTP_ITC.1

FTP_ITC.1 ensures that user job data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.JOB_ALT.

(3) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is an SFR that supports the fulfillment of O.JOB_ALT.

(4) FMT_MSA.3

FMT_MSA.3 ensures that security attributes of the user job data (object) are set to restrictive values when the user job data is generated.

FMT_MSA.3 is an SFR that supports the fulfillment of O.JOB_ALT.

(5) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.JOB_ALT.

(6) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.JOB_ALT.

(7) FIA_UID.1

FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.JOB_ALT.

O.JOB_ALT can be fulfilled by implementing these security functional requirements.

O.PROTECT_DATA_ALT Protection of TSF protected data alteration

O.PROTECT_DATA_ALT is the security objective to prevent the TSF protected data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access

permission to the TSF protected data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a)
FMT_MTD.1(a) ensures that the operation of TSF protected data is restricted to authorised users.
FMT_MTD.1(a) is a major SFR to fulfill O.PROTECT_DATA_ALT.

(2) FMT_SMF.1
FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.
FMT_SMF.1 is an SFR that supports the fulfillment of O.PROTECT_DATA_ALT.

(3) FMT_SMR.1
FMT_SMR.1 ensures that the authorised user roles are maintained.
FMT_SMR.1 is an SFR that supports the fulfillment of O.PROTECT_DATA_ALT.

(4) FTP_ITC.1
FTP_ITC.1 ensures that TSF protected data sent and received by the TOE via the LAN is protected.
FTP_ITC.1 is a major SFR to fulfill O.PROTECT_DATA_ALT.

(5) FMT_MOF.1
FMT_MOF.1 ensures that only MFP administrators are allowed to manage security functions.
FMT_MOF.1 is a major SFR to fulfill O.PROTECT_DATA_ALT.

(6) FMT_MSA.1
FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.
FMT_MSA.1 is a major SFR to fulfill O.PROTECT_DATA_ALT.

(7) FIA_UID.1
FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.
FIA_UID.1 is an SFR that supports the fulfillment of O.PROTECT_DATA_ALT.

O.PROTECT_DATA_ALT can be fulfilled by implementing these security functional requirements.

O.CONFIDENTIAL_DATA_DIS Protection of TSF confidential data disclosure

O.CONFIDENTIAL_DATA_DIS is the security objective to prevent the TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a), FMT_MTD.1(b)
FMT_MTD.1(a) and FMT_MTD.1(b) ensure that the operation of TSF confidential data is restricted to authorised users.
FMT_MTD.1(a) and FMT_MTD.1(b) are major SFRs to fulfill O.CONFIDENTIAL_DATA_DIS.

(2) FMT_SMF.1
FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.
FMT_SMF.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_DIS.

(3) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_DIS.

(4) FTP_ITC.1

FTP_ITC.1 ensures that TSF confidential data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.CONFIDENTIAL_DATA_DIS.

(5) FIA_UID.1

FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_DIS.

(6) FAU_SAR.1, FAU_SAR.2

FAU_SAR.1 ensures that the audit log data can be read in a format that can be verified by the MFP administrator. FAU_SAR.2 ensures that anyone other than the MFP administrator is prohibited to read the audit log data.

FAU_SAR.1 and FAU_SAR.2 are major SFRs to fulfill O.CONFIDENTIAL_DATA_DIS.

O.CONFIDENTIAL_DATA_DIS can be fulfilled by implementing these security functional requirements.

O.CONFIDENTIAL_DATA_ALT Protection of TSF confidential data alteration

O.CONFIDENTIAL_DATA_ALT is the security objective to prevent the TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a), FMT_MTD.1(b)

FMT_MTD.1(a) and FMT_MTD.1(b) ensure that the operation of TSF confidential data is restricted to authorised users.

FMT_MTD.1(a) and FMT_MTD.1(b) are major SFRs to fulfill O.CONFIDENTIAL_DATA_ALT.

(2) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_ALT.

(3) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_ALT.

(4) FTP_ITC.1

FTP_ITC.1 ensures that TSF confidential data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.CONFIDENTIAL_DATA_ALT.

(5) FIA_UID.1

FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_ALT.

(6) FAU_STG.1

FAU_STG.1 ensures that audit log data is protected from alteration.

FAU_STG.1 is a major SFR to fulfill O.CONFIDENTIAL_DATA_ALT.

O.CONFIDENTIAL_DATA_ALT can be fulfilled by implementing these security functional requirements.

O.AUTHORIZATION User identification and authentication

O.AUTHORIZATION is the security objective where the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. To fulfil this security objective, it is required to implement the following SFRs.

(1) FIA_UID.1, FIA_UAU.1

FIA_UID.1 and FIA_UAU.1 ensure that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified and authenticated.

FIA_UID.1 and FIA_UAU.1 are major SFRs to fulfill O.AUTHORIZATION.

(2) FIA_ATD.1, FIA_USB.1

FIA_ATD.1 and FIA_USB.1 ensure that the means of access to the predefined assets of the user is managed and associated with the user who succeeded in the identification and authentication.

FIA_USB.1 is a major SFR to fulfill O.AUTHORIZATION, and FIA_ATD.1 is an SFR to support the fulfillment of O.AUTHORIZATION.

(3) FIA_UAU.7

FIA_UAU.7 ensures that the disclosure of login passwords is prevented by displaying dummy letters as authentication feedback.

FIA_UAU.7 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(4) FIA_SOS.1

FIA_SOS.1 accepts only passwords that satisfy the minimum character number and password character combination specified by the MFP administrator, and makes it difficult to guess the password.

FIA_SOS.1 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(5) FIA_AFL.1

FIA_AFL.1 ensures that users who have repeatedly failed authentication a certain number of times are not allowed to access the TOE for a certain period of time.

FIA_AFL.1 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(6) FTA_SSL.3

FTA_SSL.3 ensures that a user automatically logs out from the TOE when the logged-in user does not operate the Operation Panel or WIM for a certain period of time, and the logged-in state is cancelled. Therefore, the user's sessions are managed, and the sessions that remain inactive are terminated.

FTA_SSL.3 is an SFR that supports the fulfillment of O.AUTHORIZATION.

O.AUTHORIZATION can be fulfilled by implementing these security functional requirements.

Among the cases where the TOE performs identification and authentication, when the identification and authentication is performed for a request from the printer driver and the fax driver, the logged-in state

terminates upon reception completion of the document data. Since there is no interactive session that continues at this point, it is not necessary to indicate this case in FTA_SSL.3.

O.FAX Management of external interfaces by TOE

O.FAX is the security objective to, for provision of the Fax Function over the telephone line by the TOE, ensure the separation between the telephone line and the LAN. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_FXS_EXP.1

FDP_FXS_EXP.1 ensures that communication via a fax interface is prohibited, except for transmission or reception of user data using a fax protocol.

FDP_FXS_EXP.1 is a major SFR to fulfill O.FAX.

O.FAX can be fulfilled by implementing this security functional requirement.

O.VALIDATION Software verification

O.VALIDATION is the security objective to ensure that the TOE provides procedures to self-verify executable code in the TSF. To fulfil this security objective, it is required to implement the following SFRs.

(1) FPT_TST_EXP.1

FPT_TST_EXP.1 ensures that a suite of self-tests is run at initial startup (and power-on) to verify the integrity of executable code in the TSF.

FPT_TST_EXP.1 is a major SFR to fulfill O.VALIDATION.

O.VALIDATION can be fulfilled by implementing this security functional requirement.

O.AUDIT Management of audit log data records

O.AUDIT is the security objective to ensure that the TOE creates and maintains logs of TOE security-related events as audit log data and protects them from disclosure or alteration by unauthorised persons, as well as provides audit log data in a format that can be verified by authorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FAU_GEN.1, FAU_GEN.2

FAU_GEN.1 and FAU_GEN.2 ensure that the events that should be audited are recorded together with the identification information of the cause of events that should be audited.

FAU_GEN.1 and FAU_GEN.2 are major SFRs to fulfill O.AUDIT.

(2) FAU_STG.1

FAU_STG.1 ensures that audit log data is protected from alteration.

FAU_STG.1 is a major SFR to fulfill O.AUDIT.

(3) FAU_STG.4

FAU_STG.4 ensures that the audit log data with the oldest time stamp is deleted and new audit log data is recorded if an auditable event occurs while the audit log data file is full.

FAU_STG.4 is an SFR that supports the fulfillment of O.AUDIT.

(4) FAU_SAR.1, FAU_SAR.2

FAU_SAR.1 ensures that the audit log data can be read in a format that can be verified by the MFP administrator. FAU_SAR.2 ensures that anyone other than the MFP administrator is prohibited to read the audit log data.

FAU_SAR.1 and FAU_SAR.2 are major SFRs to fulfill O.AUDIT.

(5) FPT_STM.1

FPT_STM.1 ensures that reliable time stamps are provided and the exact time when the audit event occurred is recorded to the audit log data.

FPT_STM.1 is an SFR that supports the fulfillment of O.AUDIT.

(6) FIA_UID.1

FIA_UID.1 ensures that the person who intends to use the TOE from the Operation Panel or the client computer on the network is identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.AUDIT.

O.AUDIT can be fulfilled by implementing these security functional requirements.

O.EMMC_ENCRYPTION eMMC encryption

O.EMMC_ENCRYPTION is the security objective to ensure that data to be written to the eMMC is encrypted. To fulfil this security objective, it is required to implement the following SFRs.

(1) FCS_CKM.1

FCS_CKM.1 ensure that cryptographic keys are generated in accordance with a specified algorithm.

FCS_CKM.1 is an SFR that supports the fulfillment of O.EMMC_ENCRYPTION.

(2) FCS_CKM.4

FCS_CKM.4 ensures that cryptographic keys are deleted in accordance with a specified method.

FCS_CKM.4 is an SFR that supports the fulfillment of O.EMMC_ENCRYPTION.

(3) FCS_COP.1

FCS_COP.1 ensures that data to be written to the eMMC is encrypted in accordance with the specified algorithm and key sizes, and data read from the eMMC is decrypted.

FCS_COP.1 is a major SFR to fulfill O.EMMC_ENCRYPTION.

O.EMMC_ENCRYPTION can be fulfilled by implementing these security functional requirements.

6.3.3 Dependency Analysis

Table 27 shows the result of dependency analysis in this ST for the TOE security functional requirements.

Table 27: Results of Dependency Analysis of TOE Security Functional Requirements

TOE Security Functional Requirements	Claimed Dependencies	Dependencies Satisfied in ST	Dependencies Not Satisfied in ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None

TOE Security Functional Requirements	Claimed Dependencies	Dependencies Satisfied in ST	Dependencies Not Satisfied in ST
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.1	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4	None
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1	None
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	None
FDP_FXS_EXP.1	None	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	None
FIA_ATD.1	None	None	None
FIA_SOS.1	None	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	None
FIA_UID.1	None	None	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	None
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	None
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	None
FMT_MTD.1(a)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	None

TOE Security Functional Requirements	Claimed Dependencies	Dependencies Satisfied in ST	Dependencies Not Satisfied in ST
FMT_MTD.1(b)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1	FMT_SMF.1
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1	None
FPT_STM.1	None	None	None
FPT_TST_EXP.1	None	None	None
FTA_SSL.3	None	None	None
FTP_ITC.1	None	None	None

The following explains the rationale for acceptability in all cases where a dependency is not satisfied.

Rationale for Removing Dependencies on FMT_SMF.1

There is no interface to make a query for login passwords, which are TSF confidential data of this TOE. Since no interface is provided, no management function is required.

6.3.4 Security Assurance Requirements Rationale

This TOE is the MFP which is a commercially available product. The MFP is assumed that it will be used in a general office and this TOE does not assume the attackers with Enhanced-Basic or higher level of attack potential.

The evaluation of the TOE design (ADV_TDS.1) is adequate to show the validity of commercially available products. A high attack potential is required for the attacks that circumvent or tamper with the TSF, which is not covered in this evaluation. Dealing with attacks performed by an attacker possessing Basic attack potential (AVA_VAN.2) is therefore adequate for general needs.

Based on the terms and costs of the evaluation, the evaluation assurance level of EAL2 is appropriate for this TOE.

7 TOE Summary Specification

This section describes the TOE summary specification for each security function. The security functions are described for each corresponding security functional requirement.

7.1 Audit Function

The Audit Function is to generate a log of TOE's audit events in the eMMC as audit log data, and provide the recorded audit log data in a legible fashion for users to audit. Only the MFP administrators can read and delete audit log data. This function also includes a function to provide reliable time stamps and a control function used when audit log data is full. Audit log data can also be transferred to and stored on the syslog server.

FAU_GEN.1 (Audit data generation)

The TOE records the audit log data items, shown in Table 29, in the eMMC when audit events shown in Table 28 occur. Audit log data items include basic log items and expanded log items. Basic log items are recorded whenever audit log data is recorded, and expanded log items are recorded only when audit events that record the audit log data items shown in Table 29 occur.

Table 28: List of Audit Events

Audit Events
Start-up of the Audit Function
Shutdown of the Audit Function
Download and deletion of audit log data
Start and end of printing locked print document data
Deletion of locked print document data
Start and end of printing fax reception document data
Deletion of user job data
Starting and releasing lockout
Success and failure of login operation
Table 24 Use of the management functions
Termination of session by auto logout
Failure of E-mail transmission of attachments from the scanner
Failure of syslog transfer
Failure of LAN Fax via the network
Failure of locked print via the network
Failure of WIM communication

Table 29: List of Audit Log Data Items

	Audit Log Data Items	Setting Values of Audit Log Data Items	Audit Events to Record Audit Log Data
Basic Log Items	Starting date/time of an event	Values of the TOE system clock at an event occurrence	• All auditable events shown in Table 28
	Ending date/time of an event	Values of the TOE system clock at an event termination	
	Event types	Audit event identity	
	Subject identity	Login user name of the user who caused the audit event	
	Outcome	Audit event outcome (*1)	
Expanded Log Items	Log type	Information for identifying the operation of document data (print/delete) and the type of job	• Start and end of printing locked print document data • Start and end of printing fax reception document data • Deletion of locked print document data • Deletion of user job data
	Login user name	All login user names that attempted the user identification	• Login success and failure
	Communicating devices	Communicating IP address	• Failure of syslog transfer • Failure of LAN Fax via the network • Failure of locked print via the network • Failure of WIM communication
		Communicating e-mail address for E-mail transmission of attachments	• Failure of E-mail transmission of attachments from the scanner
	Lockout operation type	Information to identify starting lockout and releasing lockout	• Starting and releasing lockout
	Locked out user	Login user name of a user who is locked out	• Starting and releasing lockout
	Locked out user who is to be released	Login user name of a user who is released from lockout	• Starting and releasing lockout

(*1): Record either "success" or "failure". Record only successes for the results of "Deletion of locked print document data".

For the following audit events, record as “failure”.

- Failure of E-mail transmission of attachments from the scanner
- Failure of syslog transfer
- Failure of LAN Fax via the network
- Failure of locked print via the network
- Failure of WIM communication

FAU_GEN.2 (User identity association)

The TOE records the login user name in the audit log data so that it can identify who caused the audit event.

FPT_STM.1 (Reliable time stamps)

The TOE retrieves the date (year/month/day) and time (hour/minute/second) to be recorded in the audit log data from the system clock of the TOE.

FAU_SAR.1 (Audit review)

The TOE provides the MFP administrators with all audit log data in a text format. The TOE allows the MFP administrator to download audit log data with the WIM only when the MFP administrator accesses it.

FAU_SAR.2 (Restricted audit review)

The TOE does not provide an interface for downloading audit log data to all users except the MFP administrators.

FAU_STG.1 (Protected audit trail storage)

The TOE allows only the MFP administrators to delete audit log data. To delete audit log data, the WIM or the Operation Panel will be used. The TOE does not provide an interface for making partial changes to audit log data.

FAU_STG.4 (Prevention of audit data loss)

The TOE writes the newest audit log data over the oldest audit log data when there is insufficient space in the audit log data files to append the newest audit log data.

7.2 Identification and Authentication Function

The Identification and Authentication Function is to verify whether the person who is going to use the TOE is an authorised user based on the login user name and login password entered by the user, so that the TOE can allow only the authenticated users to use the TOE and reject them when the authentication fails. The lockout function, password protection function, and automatic logout function are also included in this function.

FIA_UAU.1 and FIA_UID.1 (User authentication and identification)

The TOE identifies and authenticates a user with the login user name and login password.

Before the Operation Panel or the WIM is used, the TOE displays the login screen and prompts the user to enter the login user name and login password. In addition, when the TOE receives a request from the printer driver or fax driver, the TOE receives the login user name and login password entered by a user at the same time as the request. The TOE performs identification and authentication by checking whether the login user name and login password entered by the user match the login user name and login password registered in the TOE in advance.

If the identification and authentication is successful, the user is allowed to use the TOE. If it fails, the user is not allowed to use it. However, regarding the viewing of user job data lists, WIM Help, system status, counter and information of inquiries, and execution of fax reception, the users are allowed to use the TOE before performing identification and authentication.

FIA_USB.1 (User-subject binding)

Based on the result of FIA_UAU.1 and FIA_UID.1, the TOE assigns the login user name and user privilege to processes performed by the authorised user.

FIA_ATD.1 (User attribute definition)

The TOE retains the login user name and user privilege based on settings for each user. User privilege is set for each user according to the role to which the user is classified at the time of registration. The login user name assigned to the user can be changed for each user.

FTA_SSL.3 (TSF-initiated termination)

The TOE automatically logs out the user when they are logged in and do not operate the TOE for a certain period of time.

The TOE works as follows depending on the interface to which the user is logged-in.

- For the Operation Panel, the user is logged out of the TOE automatically when the time that elapses since their final operation reaches Operation Panel auto logout time (10 to 999 seconds).
- For the WIM, the user is logged out of the TOE automatically when the time that elapses since their final operation reaches WIM auto logout time (3 to 60 minutes).

FIA_UAU.7 (Protected authentication feedback)

Regarding login passwords entered by a person who intends to use the Operation Panel or the WIM, the TOE does not display the entered letters, instead, it displays a sequence of dummy letters with same number of characters as the entered password on the login screen.

FIA_AFL.1 (Authentication failure handling)

If the user enters the wrong password in succession when logging in, the lockout function will work and the TOE will prohibit the user from logging in with that login user name. With the locked-out login user name, authentication will fail even if the user enters the correct password. The user cannot use the TOE until the

lockout is released after a certain period of time elapses or the MFP administrator or supervisor unlocks the lockout.

The number of authentication failures is added up even if the login destination (Operation Panel, WIM, printer driver, and fax driver) varies. The user is locked out when the number of attempts before lockout for the password (1-10 times) set by the administrator is reached.
If a user name is locked out, the user with that user name is not allowed to log in unless any of the following conditions is fulfilled:

- For normal users, the lockout time set by the MFP administrator elapses
- For MFP administrators and supervisors, 60 seconds elapse since the MFP becomes executable after its power is turned on
- For locked out users listed in Table 30, until an unlocking administrator releases the lockout

Table 30 : Relationships regarding Lockout Release

Locked Out User	Unlocking Administrator
Normal user	MFP administrator
Supervisor	MFP administrator
MFP administrator	Supervisor

FIA_SOS.1 (Verification of secrets)

Login passwords for users can be registered only if these passwords meet the given conditions. Passwords cannot be registered if they do not satisfy the conditions.

Usable characters and types are as follows. The password complexity for which the conditions of combination of characters (two or more types, or three or more types) are determined is set by the MFP administrator.

- Upper-case letters: [A-Z] (26 letters)
- Lower-case letters: [a-z] (26 letters)
- Numbers: [0-9] (10 digits)
- Symbols: SP (spaces) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ (33 symbols)

The conditions for registrable password length differ depending on normal users, MFP administrators, and supervisors, as shown below. The minimum character number of login password (i.e. minimum login password length) is set by the MFP administrator in the range of 8 to 32 characters.

- For normal users: Equal to or longer than the minimum character number, and 128 characters or less
- For MFP administrators and supervisors: Equal to or longer than the minimum character number, and 32 characters or less

7.3 Document Access Control Function

The Document Access Control Function is to permit the authorised user of the TOE to operate the user document data and the user job data based on the user privileges or the login user name.

FDP_ACC.1, FDP.ACF (Subset access control and Security attribute based access control)

The TOE controls user operations for stored document data and user job data in accordance with (1) access control rule on locked print document data, (2) access control rule on fax reception document data, and (3) access control rule on user job data.

(1) **Access control rule on locked print document data**

The TOE provides users with the interface for printing and deleting locked print document data. An interface for making changes to locked print document data will not be provided.

The TOE allows the normal user who has the same login user name as the normal user who created the locked print document data to operate the locked print document data. That is, the user can operate the locked print document data created by themselves.

After the normal user logs in with the Operation Panel, the TOE displays a list of locked print document data for which the user is authorised to operate and the menu for the authorised operations (print, deletion). When the printing of locked print document data is completed, the TOE deletes the locked print document data. In addition, after the normal user logs in with the WIM, the TOE displays a list of locked print document data for which the user is authorised to operate, and permits the operation (deletion) of the displayed locked print document data. Locked print document data for which operations are not authorised is not displayed in the list.

After a person with the user privilege of the MFP administrator logs in with the Operation Panel or WIM, the TOE displays a list of all locked print document data and the operation menu for deleting data. The MFP administrator can select documents to delete from a list of locked print document data and delete the documents.

Users with user privilege for supervisor processes are not allowed to operate locked print document data.

(2) **Access control rule on fax reception document data**

The TOE provides users with the interface for printing fax reception document data.

The TOE allows the normal user who has the login user name registered as the stored reception file user to operate the fax reception document data. The stored reception file users are registered in one list for all fax reception document data.

After the normal user logs in with the Operation Panel, the TOE displays the menu for the authorised operations (print). The user can confirm the contents of the fax reception document data only by printing it. There is no interface for making changes to or deleting data. When the printing of fax reception document data is completed, the TOE deletes the fax reception document data.

Users with user privilege of the MFP administrator and the supervisor are not allowed to operate fax reception document data.

The user privileges that allow users to edit the stored reception file users are shown in "7.6 Security Management Function".

(3) **Access control rule on user job data**

The TOE provides users with the interface for canceling user job data to delete it. An interface for making changes to user job data will not be provided.

After the user logs in with the Operation Panel or WIM, the TOE displays a menu to cancel user job data only if the user who attempted to cancel (delete) the user job data is the owner of the user job data (normal

user who has the same login user name) or the MFP administrator. Other users are not allowed to operate user job data.

When the user job data is cancelled, any document data handled by the cancelled user job data will be deleted. However, if the document data handled by the cancelled user job data is the stored document data, the data will not be deleted and remain stored in the TOE.

7.4 Network Protection Function

The Network Protection Function is to prevent information leakage due to network monitoring by providing encrypted communication and detect alteration of communication details when communicating with trusted IT products (client computer, syslog server, SMTP server). The TOE implements this function with TLS.

FTP_ITC.1 (Inter-TSF trusted channel)

The TOE provides encrypted communication to protect user document data and TSF data on the communication path of the internal network when communicating with trusted IT products.

The TOE allows the client computer's Web browser, printer driver, or fax driver to initiate encrypted communication. The TOE can initiate encrypted communication with the SMTP server or the syslog server.

Table 31 shows the encrypted communications provided by the TOE.

When using the WIM, encrypted communication with the client computer is performed by specifying a URL for which encrypted communication is valid on a Web browser. When using the Printer Function, encrypted communication with the client computer (IPP over SSL) is performed if locked print document data is sent from the printer driver to the TOE. When using the Fax Function, encrypted communication with the client computer (IPP over SSL) is performed if fax transmission data is sent from the fax driver to the TOE. When using the E-mail transmission of attachments from the scanner, encrypted communication with the SMTP server (SMTP over SSL) is performed. When using the syslog transfer function, encrypted communication with the syslog server protected by TLS is performed by using the syslog protocol.

Table 31: Encrypted Communications Provided by the TOE

Communicating Devices	Encrypted Communications Provided by the TOE	
	Protocols	Cryptographic Algorithms
Client computer	TLS1.2	AES (128bits, 256bits)
SMTP server	TLS1.2	AES (128bits, 256bits)
syslog server	TLS1.2	AES (128bits, 256bits)

7.5 Stored Data Protection Function

The Stored Data Protection Function is to encrypt data to be written to the eMMC in order to protect data recorded in the eMMC from data leakage.

FCS_CKM.1 (Cryptographic key generation)

The TOE generates a 256-bit eMMC cryptographic key using the Hash_DRBG (SHA256) algorithm when encrypting the eMMC upon operation by the MFP administrator.

At this time, the TOE generates random numbers using an algorithm that is compliant with the standard NIST SP 800-90A.

FCS_CKM.4 (Cryptographic key destruction)

When decrypting the eMMC, the cryptographic key is overwritten with 0.

FCS_COP.1 (Cryptographic operation)

The TOE encrypts the data to be written to/read from the eMMC before writing it and decrypts the data after reading it. The TOE conforms to the standard FIPS197, and encrypts and decrypts data using the AES algorithm with a key of 256-bit cryptographic key size.

7.6 Security Management Function

The Security Management Function is to control the operation of TSF data and the behaviour of the Security Functions based on the user privileges or the login user name. This function includes a function to maintain the role of operating the Security Management Function and associate the role with the user, and a function to set appropriate default values for the security attributes.

FMT_SMR.1 (Security roles)

The TOE user has the role of normal user, MFP administrator, or supervisor. The role is associated with the login user name registered in the TOE. The TOE associates the logged-in user with the role corresponding to the login user name.

FMT_MSA.1, FMT_MTD.1(a), FMT_MTD.1(b), FMT_SMF.1, FMT_MOF.1 (Management of security attributes, Management of TSF data, Specification of Management Function, Control of the behaviour of the Security Functions)

The TOE performs the following management functions:

- TOE restricts operations on security attributes according to the role of the user. It allows users who have user privilege corresponding to the role for which operations are allowed to operate each security attribute. Among the TSF data shown in Table 32, the security attributes are the login user names and the stored reception file users.
- The TOE provides only the MFP administrators with an interface for setting the syslog transfer function to stop or operate.
- TOE restricts operations on the TSF data according to the role of the user. As shown in Table 32, it allows users who have user privilege corresponding to the role for which operations are allowed to operate the TSF Data. There is no interface to change the security attributes of locked print document data and user job data. In addition, there is no interface for making queries about the login passwords.

Table 32: Management of TSF Data

Category	**TSF Data**	**Operations**	**Roles (User Privileges) for Which Operations are Allowed**	Operation Interface
TSF confidential data	Login password [When associated with a normal user]	Newly create Modify	MFP administrator	Operation Panel WIM
		Query	No roles for which operations are allowed	None
	Login password [When associated with the normal user who owns the login password]	Modify	Normal user who owns the login password	Operation Panel WIM
		Query	No roles for which operations are allowed	None
	Login password [When associated with a supervisor]	Modify	Supervisor	Operation Panel WIM
		Query	No roles for which operations are allowed	None
	Login password [When associated with an MFP administrator]	Modify	Supervisor MFP administrator	Operation Panel WIM
		Query	No roles for which operations are allowed	None
	eMMC cryptographic key	Query Delete Generate	MFP administrator	Operation Panel
TSF protected data	Login user name [When associated with a normal user]	Modify Delete Newly create	MFP administrator	Operation Panel WIM
	Login user name [When associated with a supervisor]	Modify	Supervisor	Operation Panel WIM
	Login user name [When associated with an MFP administrator]	Modify	MFP administrator	Operation Panel WIM
	Stored reception file user	Modify	MFP administrator	Operation Panel WIM
	Lockout settings	Modify	MFP administrator	WIM
	Date/time settings	Modify	MFP administrator	Operation Panel WIM

Category	**TSF Data**	**Operations**	**Roles (User Privileges) for Which Operations are Allowed**	Operation Interface
	Password quality settings	Modify	MFP administrator	Operation Panel
	Auto logout settings	Modify	MFP administrator	WIM Operation Panel (*1)
	Audit log data settings	Modify	MFP administrator	WIM Operation Panel
	Cryptographic communication settings	Modify	MFP administrator	Operation Panel WIM

(*1): The operation interface for setting auto logout on the Operation Panel is the Operation Panel and WIM, and the operation interface for setting auto logout on the WIM is WIM only.

FMT_MSA.3 (Static attribute initialisation)

The security attributes in the user data access control SFP include the stored reception file user and the login user name.

- The stored reception file user is a security attribute for the fax reception document data. Since the login user name of the normal user registered as the stored reception file user is specified as the initial value, a restrictive default value is set.
- The login user name is a security attribute for locked print document data and user job data. Since the login user name of the normal user who created the locked print document data is set as the initial value for the locked print document data, and the login user name of the normal user who created the user job data is set as the initial value for the user job data, restrictive default values are set.

There is no interface to change these restrictive default values.

7.7 Integrity Verification Function

The Integrity Verification Function is a self-test function that verifies the integrity of execution code in the MFP Control Software and the Operation Panel control software.

FPT_TST_EXP.1 (TSF testing)

The TOE performs the integrity verification of control software during the initial start-up.

By comparing the hash value or verifying digital signature for the MFP Control Software and the Operation Panel control software, the TOE verifies the integrity of control software.

If the hash value for the integrity verification obtained at startup does not match the correct value, or if the digital signature is not verified, the TOE will display an error message on the Operation Panel and will not accept the operation. If the obtained hash value matches the correct value and the digital signature is verified, the TOE will become available.

7.8 Fax Line Separation Function

The Fax Line Separation Function is to prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol, in order to prevent intrusion from the telephone line into the LAN.

FDP_FXS_EXP.1 (Fax separation)

By communicating only with the G3 standard on the telephone line and not using other communications, the TOE prohibits communication via a fax interface, except for transmission or reception of user data using a fax protocol.

8 Glossary

In this section, the meanings of specific terms used in this ST are defined below.

Table 33: Specific Terms Related to This ST

Terms	Definitions
MFP Control Software	A software component installed in the TOE. This is stored in the eMMC of the main unit.
Operation Panel Control Software	A software component installed in the TOE. This is stored in the Operation Panel Control Board.
Lockout	A type of behaviour to deny login of particular users.
Auto logout	A function for automatic user logout if no access is attempted from the Operation Panel or the WIM for the predetermined period of time.
eMMC	Abbreviation for Embedded Multi Media Card. A storage device that is non-volatile memory. In this document, unless otherwise specified, "eMMC" indicates the eMMC installed on the TOE.
Job	A sequence of operations of each TOE function (Copy Function, Scanner Function, Printer Function, Fax Transmission Function, and Fax Reception Function) from beginning to end.
Document data	General term for paper documents and electronic documents used in the TOE.
Stored document data	Document data stored in the TOE by the Printer Function and Fax Function. It can be classified into locked print document data and fax reception document data.
MFP application	General term for functions provided by the TOE (Copy Function, Scanner Function, Printer Function, Fax Transmission Function, and Fax Reception Function).
Operation Panel	A panel that consists of a touch screen LCD and key switches. The Operation Panel is used by users to operate the TOE.
WIM	Web Image Monitor function. This is a function for TOE users to remotely operate the TOE from the client computer's Web browser.
E-mail transmission of attachments	A function to send user document data read by the Scanner Function from the MFP to the client computer via the SMTP server in e-mail format. TLS protects the communication for realising this function.
LAN Fax	One of Fax Functions. A function that transmits fax data using the fax driver on client computer. Sometimes referred to as "PC FAX".
SPDF	A type of Auto Document Feeder (ADF) that feeds the originals set on the device one by one to the exposure glass. When scanning both sides of the original, both sides are scanned simultaneously.
LAN	Abbreviation for local area network. Network used in the TOE installation environment.

Terms	Definitions
Telephone line	A public switched telephone network line for the TOE to communicate with external faxes.
Firewall	A device to prevent the office environment from network attacks via the Internet.
SMTP server	A server used by the TOE for e-mail transmission.
syslog server	A server that can receive audit log data recorded by the TOE using the syslog protocol.
Responsible manager of MFP	A person who is indirectly involved in the TOE and responsible for appointment of the TOE administrators in the organisation where the TOE is used.