Xerox VersaLink C505/C605 Color Multifunction Printer models with Hard Disk, Fax Security Target

Version 1.1.8

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

July 2018

- Table of Contents -

- List of Figures and Tables -

1. ST INTRODUCTION

This chapter describes Security Target (ST) Reference, TOE Reference, TOE Overview, and TOE Description.

1.1. ST Reference

This section provides information needed to identify this ST.

ST Title:	Xerox VersaLink C505/C605 Color Multifunction Printer models with Hard Disk, Fax Security Target
ST Version:	V 1.1.8
Publication Date:	July 23, 2018
Author:	Fuji Xerox Co., Ltd.

1.2. TOE Reference

This section provides information needed to identify this TOE.

The TOE is VersaLink C505X and VersaLink C605X.

The TOE name is integrated as below.

TOE Identification:	Xerox VersaLink C505/C605 Color Multifunction Printer models with Hard Disk, Fax
Version:	Controller ROM Ver. 1.12.32
Developer:	Fuji Xerox Co., Ltd.

The followings are the target products.

Xerox VersaLink C505X :
Controller ROM Ver. 1.12.32

Xerox VersaLink C605X :
Controller ROM Ver. 1.12.32

“X” included in a product name indicates that the machine has a FAX function. Hard disks are equipped on the X model of C505/C605. Whether a machine is the TOE can be distinguished by the product name included X that is displayed on the controle panel when the machine is turned on. If “X” does not follow “C505”, “C605” in the product name, the machine is not the TOE.

1.3. TOE Overview

1.3.1. TOE Type and Major Security Features

1.3.1.1. TOE Type

This TOE, categorized as an IT product, is the VersaLink C505/C605 (hereinafter referred to as "MFD") which has the copy, print, network scan, and fax functions.
The TOE is the product which controls the whole MFD and protects the data that are transmitted over the encryption communication protocols.
These protocols protect the security of the TOE setting data, job information, the security audit log data and the document data on the internal network between the TOE and the remote.
The TOE also prevents the document data and the used document data in the internal HDD from being disclosed by unauthorized person.

1.3.1.2. Function Types

Table 1 shows the Function types and functions provided by the TOE.

Table 1 Function Types and Functions provided by the TOE

Function types	Functions provided by the TOE
Basic Function	- Control Panel - Copy - Print - Network Scan - Fax - Embedded Web Server
Security Function	- Hard Disk Data Overwrite - Hard Disk Data Encryption System - User Authentication - Administrator's Security Management - Customer Engineer Operation Restriction - Security Audit Log - Internal Network Data Protection - Information Flow Security - Self Test

- To use print function, the printer driver shall be installed to the external client for general user and that for system administrator.
- There are two types of user authentication, local authentication and remote authentication, and the TOE behaves with either one of the authentication types depending on the setting.
  In this ST, the difference of the TOE behavior is described if the TOE behaves differently

depending on the type of authentication being used. Unless specified, the behavior of the TOE is the same for both authentication types.
There are two types of remote authentication, LDAP authentication and Kerberos authentication.

Note:

- Since the TOE’s functions to print from USB and store to USB are set to disabled, they are not included in the target of evaluation. Therefore, the [Store to USB] and [Media Print] buttons do not appear on the control panel.

1.3.1.3. Usage and Major Security Features of TOE

The TOE is mainly used to perform the following functions:

- Copy function and Control Panel function are to read the original data from IIT and print them out from IOT according to the general user’s instruction from the control panel. When more than one copy of original data are ordered, the data read from IIT are first stored into the MFD internal HDD. Then, the stored data are read out from the internal HDD for the required number of times so that the required number of copies can be made.
- Print function is to decompose and print out the print data transmitted by a general user client.
- Embedded Web Server enables a system administrator to refer to and rewrite TOE setting data via Web browser.
- Network Scan function and Control Panel function are to read the original data from IIT and transmit the document data to FTP server, or Mail server, according to the information set in the MFD. This function is operated according to the general user’s instruction from the control panel.
- Fax function and Control Panel function are to send and receive fax data. According to the general user’s instruction from the control panel to send a fax, the original data are read from IIT and then sent to the destination via public telephone line. The document data are received from the sender’s machine via public telephone line and then stored in Faxbox. Then, a system administrator prints the document data from the control panel.

The TOE provides the following security features:

(1) Hard Disk Data Overwrite

To completely delete the used document data in the internal HDD, the data are overwritten with new data after any job of copy, print, scan, etc. is completed.

(2) Hard Disk Data Encryption

The document data are encrypted before being stored into the internal HDD when using any function of copy, print, scan, etc. or configuring various security function settings.

(3) User Authentication

Access to the TOE functions is restricted to the authorized user and this function identifies and authenticates users. This function identifies and authenticates a user using his/her ID and password entered from the control panel or Embedded Web Server of a general user client, and enables access control over use of the TOE.
When a print job is received from a user client, the TOE identifies a registered user ID and stores the print job, without authenticating the user.

(4) System Administrator's Security Management
This function allows only the system administrator identified and authorized from the control panel or system administrator client to refer to and change the TOE security function settings.

(5) Customer Engineer Operation Restriction
A system administrator can prohibit CE from referring to, and changing the TOE security function settings.

(6) Security Audit Log
The important events of TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who used what function.

(7) Internal Network Data Protection
This function protects the communication data on the internal network such as document data, security audit log data, job information, and TOE setting data.
The following general encryption communication- protocols are supported:
TLS, IPSec, and S/MIME.

(8) Information Flow Security
This function restricts the unpermitted communication between external interfaces and internal network.

(9) Self Test
This function verifies the integrity of TSF executable code and TSF data.

1.3.2. Environment Assumptions

This TOE is assumed to be used as an IT product at general office and to be connected to public telephone line, user clients, and the internal network protected from threats on the external network by firewall etc.
Figure 1 shows the general environment for TOE operation.

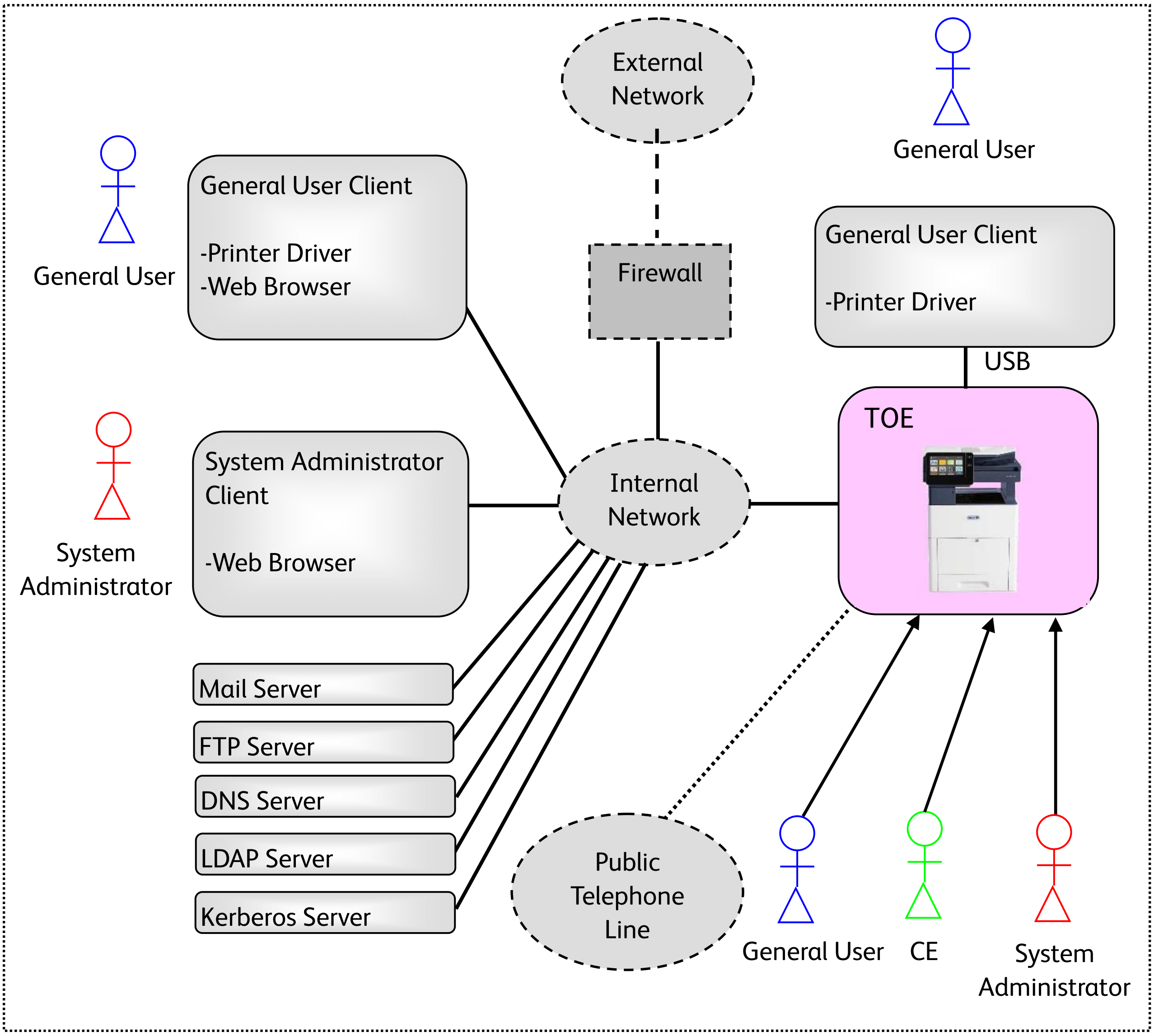

Figure 1 General Operational Environment

1.3.3. Required Non-TOE Hardware and Software

In the operational environment shown in Figure 1, the TOE (MFD) and the following non-TOE hardware/software exist.

(1) General user client:

The hardware is a general-purpose PC. When a client is connected to the MFD via the internal network and when the printer driver is installed to the client, the general user can request the MFD to print.

When the client is connected to the MFD directly via USB and printer driver is installed to the client, the user can request the MFD to print the document data.

(2) System administrator client:

The hardware is a general-purpose PC. A system administrator can refer to and change TOE setting data via Web browser.

(3) Mail server:
The hardware/OS is a general-purpose PC or server. The MFD sends/receives document data to/from Mail server via mail protocol.

(4) FTP server:
The hardware/OS is a general-purpose PC or server. The MFD sends document data to FTP server via FTP.

(5) DNS server
The hardware/OS is a general-purpose PC or server. The MFD retrieves an IP address from the DNS server using the DNS protocol.

(6) LDAP server:
The hardware/OS is a general-purpose PC or server. The MFD acquires identification and authentication information from LDAP server via LDAP. In addition, it acquires SA information of user role assumptions.

(7) Kerberos server:
The hardware/OS is a general-purpose PC or server. The MFD acquires identification and authentication information from Kerberos server via Kerberos.

The OS of (1) general user client and (2) system administrator client are assumed to be Windows 7, and Windows 8.1.
The (1) General user client uses ”PCL6 Driver – Xerox User Interface – Microsoft Certified” as a printer driver.
The (6) LDAP server and (7) Kerberos server are assumed to be Windows Active Directory.

1.4. TOE Description

This section describes user assumptions and logical/physical scope of this TOE.

1.4.1. User Assumptions

Table 2 specifies the roles of TOE users assumed in this ST.

Table 2 User Role Assumptions

Designation		PP Definition	Description
U.USER		Any authorized User.	User:
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE.	General user: A user of TOE functions such as copy, print, and fax.
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.	System administrator (key operator and SA): A user who is authorized to manage the device using the system administrator mode. A system administrator can only refer to and change the TOE setting for device operation and that for security functions via TOE control panel and Web browser.
TOE Owner		A person or organizational entity responsible for protecting TOE assets and establishing related security policies.	Administrator of the organization: An administrator or responsible official of the organization which owns and uses TOE.
Customer Engineer		-	A user who can configure the TOE operational settings using the interface for CE.

1.4.2. Logical Scope and Boundary

The logical scope of this TOE is each function of the programs.
Figure 2 shows the logical architecture of the MFD.

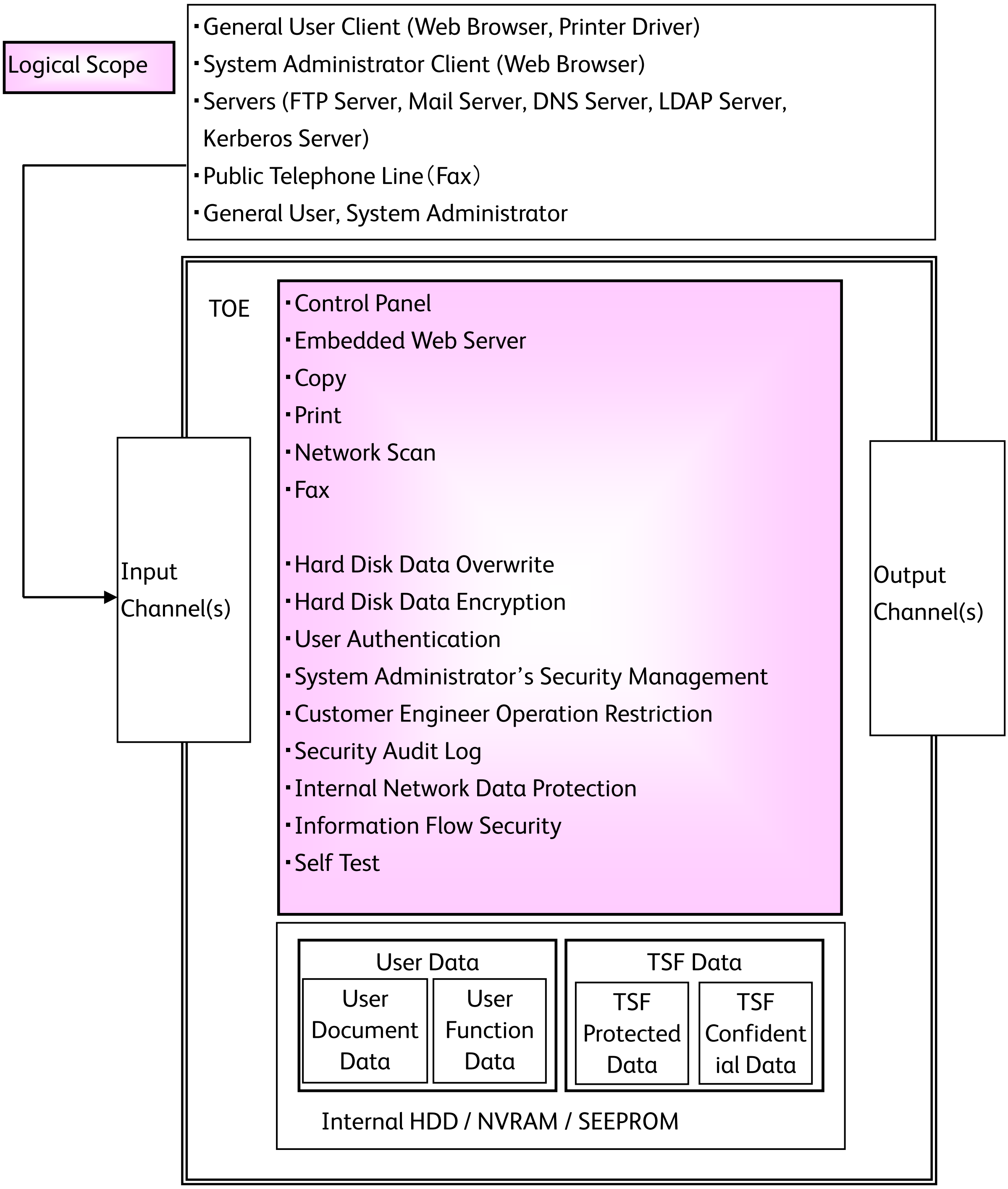
Logical Scope
･General User Client (Web Browser, Printer Driver)
･System Administrator Client (Web Browser)
･Servers (FTP Server, Mail Server, DNS Server, LDAP Server, Kerberos Server)
･Public Telephone Line（Fax）
･General User, System Administrator
TOE
･Control Panel
･Embedded Web Server
･Copy
･Print
･Network Scan
･Fax
･Hard Disk Data Overwrite
･Hard Disk Data Encryption
･User Authentication
･System Administrator's Security Management
･Customer Engineer Operation Restriction
･Security Audit Log
･Internal Network Data Protection
･Information Flow Security
･Self Test
Input Channel(s)
Output Channel(s)
User Data
User Document Data
User Function Data
TSF Data
TSF Protected Data
TSF Confidential Data
Internal HDD / NVRAM / SEEPROM

Figure 2 MFD Units and TOE Logical Scope

There are the following 4 types for Channel.

a) Private Medium Interface

   Control panel and local interface that cannot be accessed by multiple simultaneous Users.

b) Shared Medium Interface

   Mechanisms for exchanging information that can be simultaneously accessed by multiple Users; such as network interface.

c) Original Document Handler

   Mechanisms for transferring User Document Data into the TOE in hardcopy form.

d) HardCopy Output Handler
Mechanisms for transferring User Document Data out of the TOE in hardcopy form.

1.4.2.1. Basic Functions

The TOE provides the functions of control panel, copy, print, network scan, fax, and Embedded Web Server to general user.

Table 3 TOE Basic Functions

Function	Description
Copy Function	Copy function is to read the original data from IIT and print them out from IOT according to the general user's instruction from the control panel. When more than one copy of an original is ordered, the data read from IIT are first stored into the MFD internal HDD. Then, the stored data are read out from the internal HDD for the required number of times so that the required number of copies can be made.
Print Function	Print function is to print out the data according to the instruction from a general user client. The print data created via printer driver are sent to the MFD to be analyzed, decomposed, and printed out from IOT. The print function is of two types: the normal print in which the data are printed out from IOT directly after decomposed and the Store Print in which the bitmap data are temporarily stored in the internal HDD and then printed out from IOT according to the general user's instruction from the control panel.
Network Scan Function	Network scan function is to read the original data from IIT and automatically transmit them to a general user client, FTP server, or Mail server according to the information set in the MFD. A general user can request this function from the control panel.
Fax Function	Fax function is to send and receive fax data. According to the general user's instruction from the control panel to send a fax, the original data are read from IIT and sent to the destination via public telephone line. The document data are received from the sender's machine via public telephone line and then stored in a Faxbox. Then, a system administrator prints the document data from the control panel.
Control Panel Function	Control panel function is a user interface function for general user, CE, and system administrator to operate MFD functions.
Embedded Web Server Function	Embedded Web Server function is to operate from Web browser of a general user client for general users. Embedded Web Server enables System Administrator's Security Management by which a system administrator can access and rewrite TOE setting data. For this, a system administrator must be authenticated by

	his/her ID and password entered from Web browser of a system administrator client.

1.4.2.2. Security Functions

The security functions provided by the TOE are the following.

(1) Hard Disk Data Overwrite

To completely delete the used document data in the internal HDD, the data are overwritten with new data after each job (copy, print, network scan, or fax) is completed. Without this function, the used document data remain and only the management data are deleted. Additionally, On Demand Overwrite function is provided to delete the stored data at the specific time scheduled by a system administrator.

(2) Hard Disk Data Encryption

Some data such as the document data in Faxbox remain in the internal HDD even if the machine is powered off. To solve this problem, the document data are encrypted before being stored into the internal HDD when operating any function of copy, print, network scan, and fax or configuring various security function settings.

(3) User Authentication

Access to the MFD functions is restricted to the authorized user. To be identified and authenticated, a user needs to enter his/her ID and password from MFD control panel, or the Embedded Web Server of the user client.

Only the authenticated user can use the following functions:

a) Functions controlled by the MFD control panel:
Copy, fax (send), network scan, Faxbox, and print (This print function requires the Store Print preset from printer driver. A user must be authenticated from the control panel for print job.)

b) Functions controlled by Embedded Web Server:
Display of device condition, display of job status and its log,

Among the above functions which require user authentication, some particularly act as security functions. The following are the security functions which prevent the unauthorized reading of document data in the internal HDD by an attacker who is impersonating an authorized user:
- The Store Print function and the Faxbox function, which require user authentication from the control panel.

Figure 3 shows the authentication flow of Store Print Function and Faxbox Function.

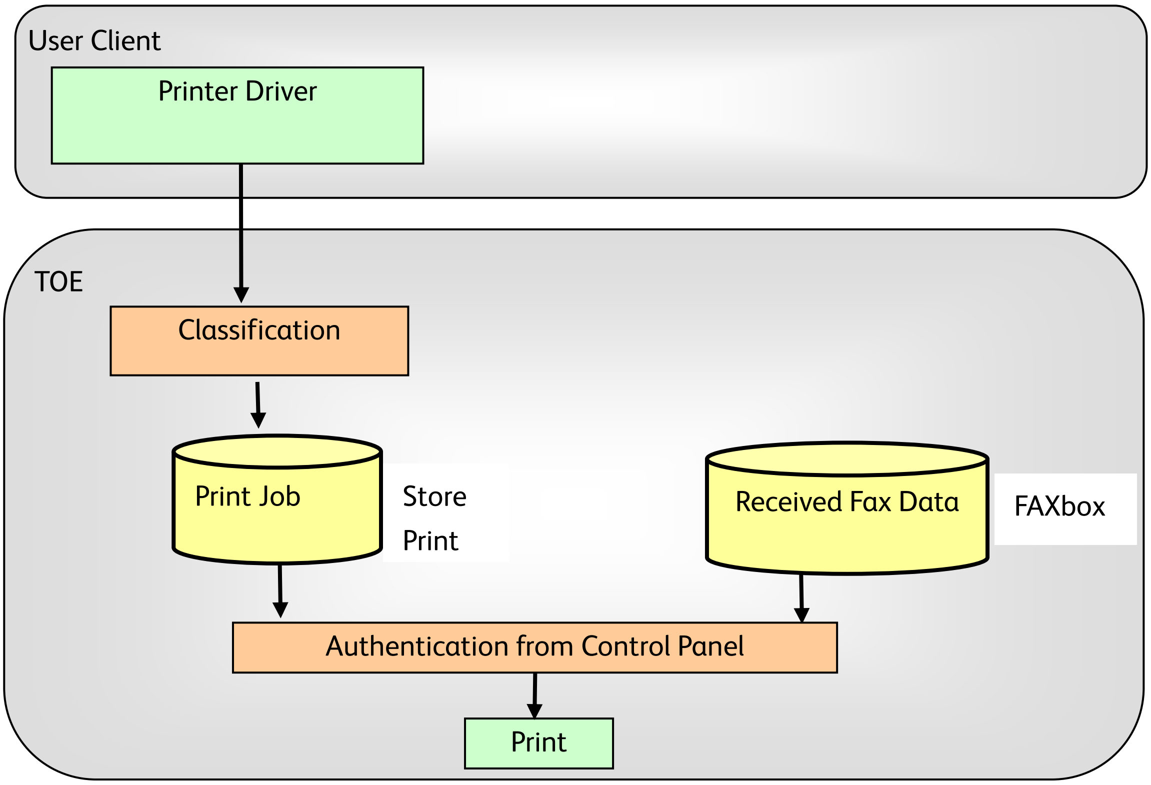

Figure 3 Authentication Flow for Store Print and Faxbox

- Store Print Function

  When a user sends a print request from the printer driver in which the Store Print is preset, the print data are decomposed into bitmap data, classified according to the user ID, and temporarily stored in the corresponding Store Print area within the internal HDD.

  To refer to the stored print data, a user needs to enter his/her ID and password from the control panel. When the user is authenticated, the data on the waiting list corresponding to the user ID are displayed. The user can request printing or deletion of the data on the list.

- Faxbox Function

  The received fax data can be stored into Faxbox from Public Telephone Line (Fax card) which are not shown in Figure 3.

  To store the received fax data into Faxbox, user authentication is not required. The received fax data transmitted over public telephone line are automatically stored into the Faxbox.

  To print the stored data in the Faxbox , user authentication is required; the MFD compares the user ID and password preset in the device against those entered by a System administrator from the control panel.

(4) System Administrator’s Security Management

To grant a privilege to a specific user, this TOE allows only the authenticated system administrator to access the System Administrator mode which enables him/her to refer to and set the following security functions from the control panel:

- Refer to and set the Time/Date;
- Refer to and set the TLS communication;

Additionally, this TOE allows only the system administrator, who is authenticated from the system administrator client via Web browser using Embedded Web Server, to refer to and set the following security functions via Embedded Web Server:

- Refer to and set the Hard Disk Data Overwrite;
- Refer to and set the On Demand Overwrite;
- Refer to and set the access denial when system administrator's authentication fails;
- Refer to and set the Time/Date;
- Refer to and set the Self Test;
- Set the password of key operator (only a key operator is privileged);
- Refer to and set the ID of SA / general user and set the password (with local authentication only);
- Refer to and set the limit of user password length (for general user and SA, with local authentication only);
- Refer to and set the Security Audit Log;
- Refer to and set the TLS communication;
- Refer to and set the IPSec communication;
- Refer to and set the S/MIME communication;
- Create/upload/download an X.509 certificate;
- Refer to and set the User Authentication;
- Refer to and set the general user permission
- Refer to and set the Auto Clear (Control Panel and Embedded Web Server);
- Refer to and set the Customer Engineer Operation Restriction;

(5) Customer Engineer Operation Restriction

This TOE allows only the authenticated system administrator to refer to or enable/disable the Customer Engineer Operation Restriction setting from Embedded Web Server. For this, CE cannot refer to or change the setting of each function described in (4) System Administrator's Security Management.

(6) Security Audit Log

The important events of TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function. Only a system administrator can supervise or analyze the log data by downloading them in the form of tab-delimited text file via Web browser using Embedded Web Server. To download the log data, TLS communication needs to be enabled.

(7) Internal Network Data Protection

The communication data on the internal network such as document data, Job information, security audit log data, and TOE setting data are protected by the following general encryption communication-protocols:

- TLS
- IPSec
- S/MIME

(8) Information Flow Security

This TOE has the function of restricting the unpermitted communication between external interfaces and internal network.

Fax card of TOE device is connected to a controller board via the internal interface, but theunauthorized access from a public telephone line to the inside TOE or internal network via fax card cannot be made.

(9) Self Test

This TOE can execute the self test function to verify the integrity of TSF executable code and TSF data.

1.4.2.3. Settings for the Secure Operation

System administrator shall set the following to enable security functions in 1.4.2.2.

- Hard Disk Data Overwrite
  Set to [Enabled]
- Access denial when system administrator’s authentication fails
  Default [5] Times
- User Passcode Minimum Length
  Set to [9] characters
- TLS
  Set to [Enabled]
- IPSec
  Set to [Enabled]
- S/MIME
  Set to [Enabled]
- User Authentication
  Set to [Login to Local Authentication] or [Remote Authentication]
- Store Print
  Set to [authority of user to only Store Print]
- Auto Clear
  Set to [Enabled]
- Security Audit Log
  Set to [Enabled]

- Customer Engineer Operation Restriction
  Set to [Enabled]
- Self Test
  Set to [Enabled]

1.4.3. Physical Scope and Boundary

The physical scope of this TOE is the MFD. Figure 4 shows configuration of each unit and TOE physical scope.

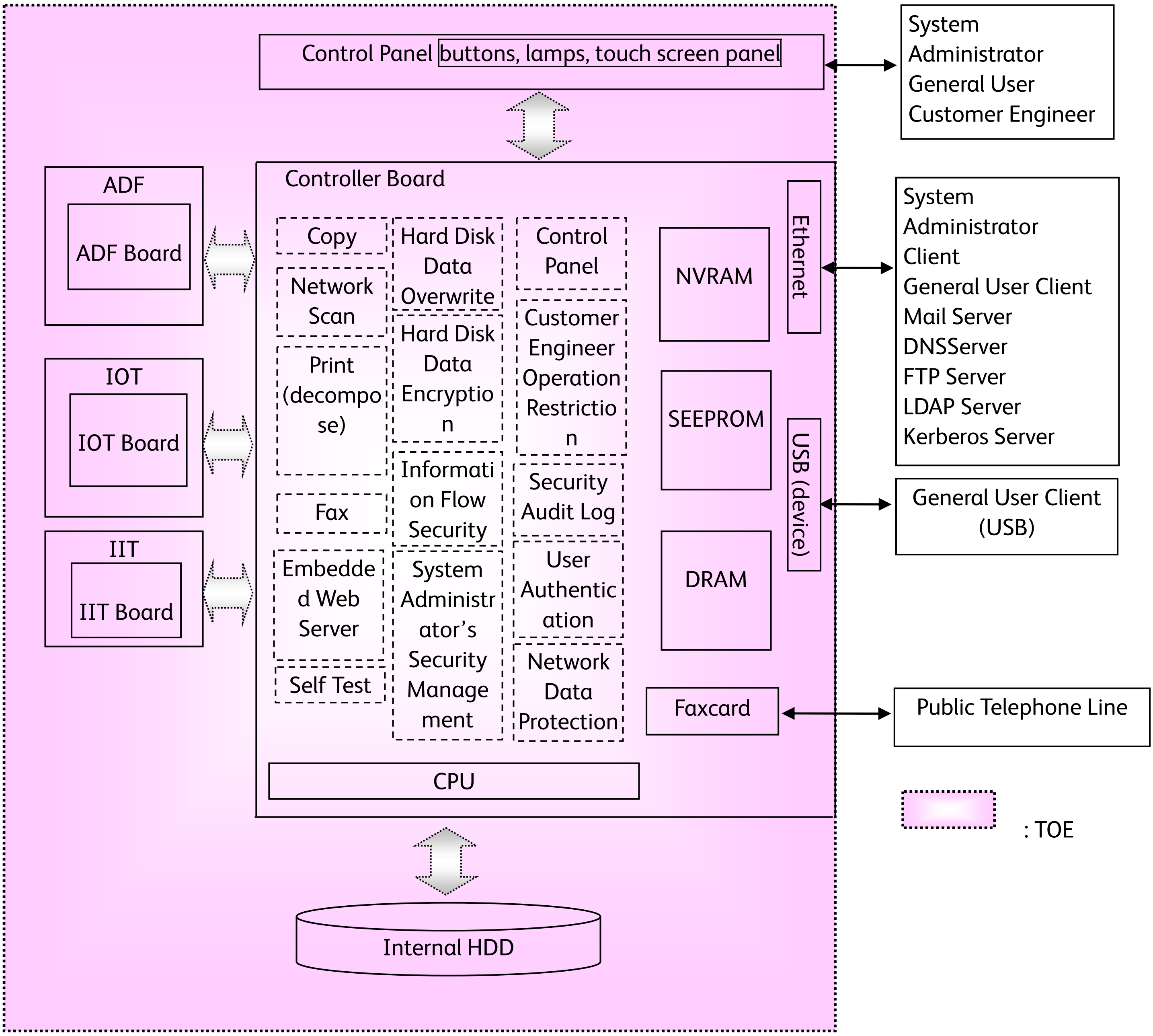

Figure 4 MFD Units and TOE Physical Scope

The MFD consists of the controller board, Internal HDD, control panel, IIT, ADF and IOT.
The controller board is connected to the control panel via the internal interfaces which transmit control data, to the ADF board, IIT board, and IOT board via the internal interfaces which transmit document data and control data.

The controller board is a PWB which controls MFD functions of copy, print, network scan, and fax. The board has a network interface (Ethernet) and local interfaces (USB) and is connected to the IIT board and IOT board. The program is installed in Controller ROM.

The IOT (Image Output Terminal) is a device to output image data which was sent from the controller board.

The IIT (Image Input Terminal) is a device to scan an original and send its data to the controller board for copy, scan, and Fax functions.

The ADF (Auto Document Feeder) is a device to automatically transfer original documents to IIT.

The control panel is a panel on which buttons, lamps, and a touch screen panel are mounted to use and configure MFD functions of copy, print, network scan, and fax.

NVRAM (Including eMMC Memory) and the internal HDD in TOE are not the removable memory media.

4 types of Channel correspond to the following in TOE.

- Private Medium Interface
  Control panel, USB
- Shared Medium Interface
  Ethernet
- Original Document Handler
  IIT
- HardCopy Output Handler
  IOT

1.4.4. Guidance

The following are the guidance documents for this TOE.

(1) Xerox VersaLink C505 Color Multifunction Printer User Guide：Version 2.0 January 2018
(SHA256 Hash value:
1aa645e5355730c38fa3b3a4b3ffea7702dac46fa4bd668ee061230d92fc310c)

(2) Xerox VersaLink C605 Color Multifunction Printer User Guide：Version 2.0 January 2018
(SHA256 Hash value:
905a2f9c51440316c7448c6ac5cb3482685b6d51bbcda0fd7435d29cb29c69d5)

(3) Xerox VersaLink Series Multifunction and Single Function Printers System Administrator Guide; Version 2.0 October 2017
(SHA256 Hash value:
55ec10501077ecf5434d2663b080caa91d3ad8b30b612d008afb7e3f79545b50)

(4) Xerox VersaLink C505/C605/B605/B615 Multifunction Printer　Security Function Supplementary Guide：　Version 1.0, July 2018
(SHA256 Hash value:
7c7c7bc3e548b404cd5672861fe75eb6213a183e1ecd088e408122630ed92464)

2. CONFORMANCE CLAIM

2.1. CC Conformance Claim

This ST and TOE conform to the following evaluation standards for information security (CC):
CC version which ST and TOE claim to conform to:

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model (September 2012 Version 3.1 Revision 4)
Part 2: Security functional components (September 2012 Version 3.1 Revision 4)
Part 3: Security assurance components (September 2012 Version 3.1 Revision 4)

CC Part2 extended [FPT_FDI_EXP.1]
CC Part3 conformant

2.2. PP claim, Package Claim

2.2.1. PP Claim

This Security Target claims demonstrable conformance to:
U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™ -2009)

2.2.2. Package Claim

This Security Target claims EAL2 augmented by ALC_FLR.2.

Also, it claims the following packages of the SFR Package that can select PP description as the package conformant.

Title: 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B
Package Version: 1.0

2.2.3. Conformance Rationale

This ST is written with the functions partially added, covering the following written inPP: Common HCD Functions, Print Functions, Scan Functions, Copy Functions, Fax Functions, and Shared-medium Interfaces Functions.

The type of TOE in this ST is the MFD (Multi Function Device) with copy, print, network scan, and fax functions, and is the same term as Hardcopy Device written in 4.1 Typical Products of PP, incorporating the required functions.

Also, as shown below, the Security Problem Definition, Security Objectives, and Security Functional Requirements are written covering the PP.

- P.CIPHER is added for OSP for the TOE in addition to Threats / OSP / Assumptions required in PP. P.CIPHER is the data encryption of the internal HDD, and is independent from other Problem Definition, causing no impact.
  There is no change in Assumptions. Therefore, the Threats / OSP / Assumptions are more restrictive than the statement of the Security Problem Definition of PP.

- Security Objectives are set by excluding OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED from the Security Objectives for the environment specified in PP. As other contents are quoted without any changes and there is no additional objective, the Security Objectives for the environment have the restrictions equivalent to or less than that in the statement of Security Objectives of PP.

- O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED are added for the Security Objectives for the TOE in addition to the Security Objectives required in PP.
  The Security Objectives for the TOE are more restrictive than the statement in the Security Objectives of PP.

- The relation between the SFR specified by PP and that used by ST is shown in Table 14.
  The detailed SFR description and the added SFR content for each SFR are described.
  The description of the operation of registering the document data of Common Access Control SFP is added. However, only the authorized user can register the document data, thus FDP_ACC.1 / FDP_ACF.1 is more restrictive than PP.
  The security attributes of +SMI is not defined, but as there is no operation to restrict the transfer of FPT_FDI_EXP.1, it is equivalent to the PP requirement.
  As it is defined in the access control SFP of D.DOC that some deletion processing is not

allowed for U.USER, FDP_ACC.1 is more restrictive than PP.
Other SFRs specified in PP are equivalent to the requirement, and TOE is set to be more restrictive by the additional SFR.
Therefore, the SFR of this ST is more restrictive than that of PP.

In this ST, the content quoted from the SFR of PP is written in italics, describing the content required by PP.
Also, the assigned part is similarly written in italics, including the part fixed in PP.

- Among the Security Objectives Rationale specified in PP, the objective of P.AUDIT.LOGGING replaces OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED with O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED.
  Also, O.CIPHER is added to the objectives of P.CIPHER. Others describe the content required by PP without any changes to show its assurance.

- Objectives are assured as the description is added for the added TOE objectives and SFR., The relationship between FMT_MSA.1 and the security objectives are different from PP, but this does not change the content of security requirements specified in PP. This is because, in order to protect user data, the requirements to prevent disclosure and alteration of security attributes are apllied to TSF data security objectives.
  As to other TOE objectives and SFR, the contents required by PP are described.

- The SAR specified in PP describes the content required by PP without any changes.

Therefore, this ST demonstrably conforms to PP

3. SECURITY PROBLEM DEFINITION

This chapter describes the threats, organizational security policies, and the assumptions for the use of this TOE.

3.1. Threats

3.1.1. Assets Protected by TOE

This TOE protects the following assets

Table 4 Assets for User Data

Designation	PP Definition	Asset under Protection	Description
D.DOC	User Document Data consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.	Document data stored for job processing	When a user uses MFD functions of copy, print, fax, and network scan, the document data are temporarily stored in the internal HDD for image processing, transmission, and Store Print.
		Used document data after job processing	When a user uses MFD functions of copy, print, fax, and network scan, the document data are temporarily stored in the internal HDD for image processing, transmission, and Store Print. When the jobs are completed or canceled, only the management information is deleted but the data itself remains.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.	User job infomation	A job received from a user or entity outside the TOE.

Table 5 Assets for TSF Data

Designation	PP Definition	Asset under Protection	Description
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.	Table 24, Table25,Table 26, Table 27, Table 28、Table 31/ Table 32, (excluding the following D.CONF)	Even though the contents of the TOE setting data and security attributes are disclosed, it will not be a security threat.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.	-Data on General user Password -Data on Security Audit Log (Table 15) - Data on Internal Network Data Protection	The system administrator can set security functions of TOE from the MFD's control panel or the system administrator client by using the System Administrator's Security Management function. The setting data are saved in TOE. General users can set their IDs and passwords from the MFD's control panel by using the User Authentication function. The setting data are saved in TOE. The system administrator can retrieve the security audit log data from the system administrator client. The security audit log data are saved in TOE.

Table 6 Other Assets

Designation	PP Definition	Asset under Protection	Description
Functions	Functions perform processing, storage, and transmission of data that may be present in HCD products. These functions are used by SFR packages.	MFD functions	Only the permitted user can use the copy, print, network scan, and Fax functions of TOE.

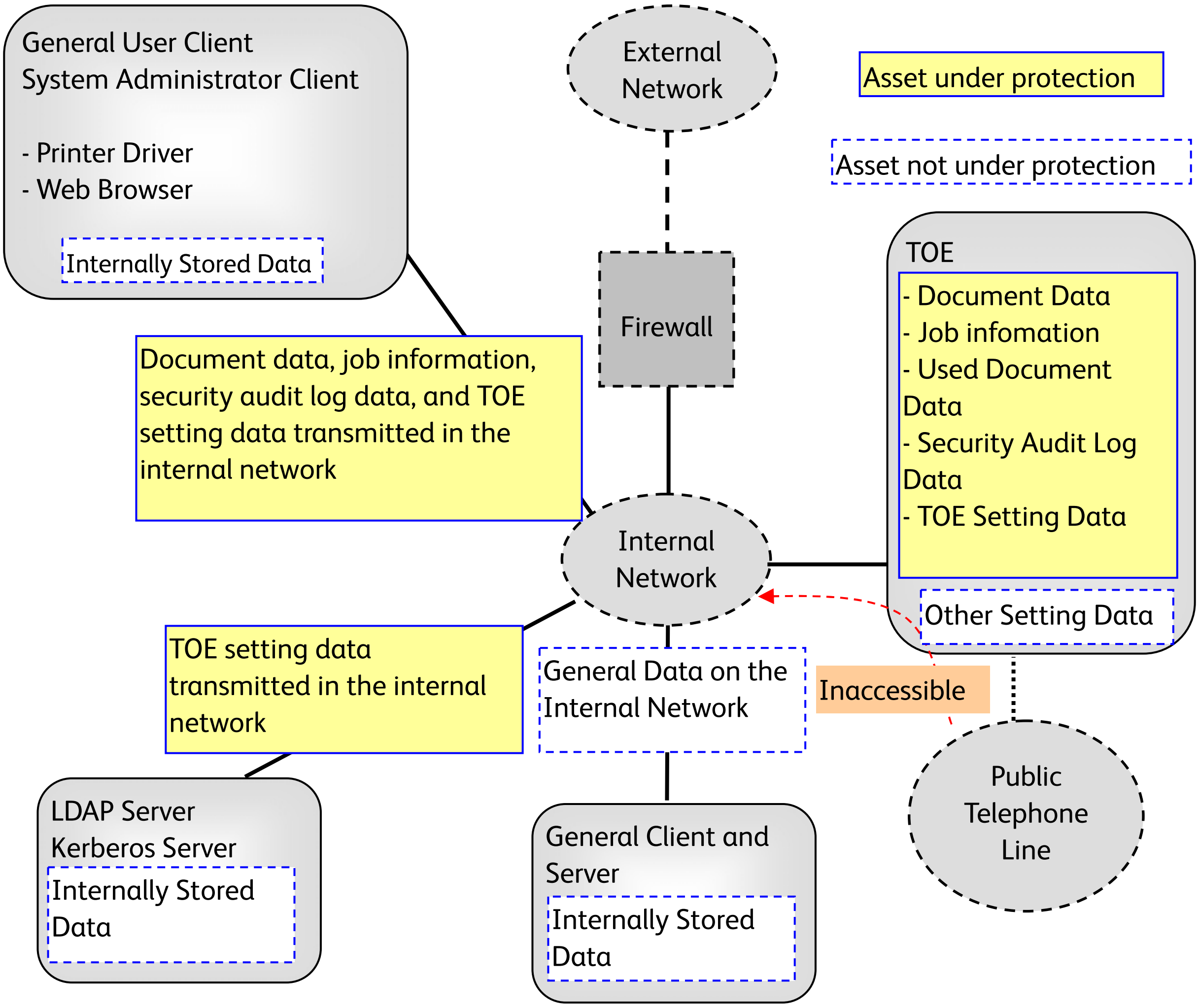

Figure 5 Assets under and not under Protection

Note) The data stored in a general client and server within the internal network and the general data on the internal network are not assumed as assets to be protected. This is because TOE functions prevent the access to the internal network from public telephone line and it cannot be a threat.

TSF data in Table 5 are stored in the internal HDD, NVRAM (Including eMMC Memory) and SEEPROM of the controller board.
However, the present time data are not included.

The setting data other than TOE setting data are also stored on NVRAM (Including eMMC Memory) and SEEPROM. Those setting data, however, are not assumed as assets to be protected because they do not engage in TOE security functions.

Security Audit Log data are temporarily stored in NVRAM, but stored in the internal HDD as a file.

3.1.2. Threats agents

This ST assumes the following four categories of threats agents as Attacker, each having low-level attack capability and the disclosed information on TOE operations.

a) Persons who are not permitted to use the TOE who may attempt to use the TOE.

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

3.1.3. Threats

Table 7 identifies the threats addressed by the TOE. Unauthorized persons are assumed to be the threat agents described in 3.1.2.

Table 7 Threats to User Data and TSF Data

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.2. Organizational Security Policies

Table 8 below describes the organizational security policies the TOE must comply with.

Table 8 Organizational Security Policies

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of the interfaces will be controlled by the TOE and its IT environment.
P.CIPHER	To prevent unauthorized reading-out, the document data in the internal HDD will be encrypted by the TOE. (A cryptographic key does not need to be destructed.)

3.3. Assumptions

Table 9 shows the assumptions for the operation and use of this TOE.

Table 9 Assumptions

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4. Security Objectives

This chapter describes the security objectives for the TOE and for the environment and the rationale.

4.1. Security Objectives for the TOE

Table 10 defines the security objectives to be accomplished by the TOE.

Table 10 Security Objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that audit records are protected from unauthorized access, deletion, and modifications.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.
O.CIPHER	The TOE shall provide the function to encrypt the document data in the internal HDD so that they cannot be read out.

4.2. Security Objectives for the Environment

Table 11 defines the security objectives for the TOE environment.

Table 11 Security objectives for the environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization, and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization, have the training, competence, and time to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE interfaces.

4.3. Security Objectives Rationale

The security objectives are established to correspond to the assumptions specified in Security Problem Definition, to counter the threats, or to realize the organizational security policies. Table 12 shows assumptions / threats / organizational security policies and the corresponding security objectives.) Moreover, Table 13 shows that each defined security problem is covered by the security objectives.

Table 12 Assumptions / Threats / Organizational Security policies and the Corresponding Security Objectives

Objectives Threats, Policies, and Assumptions	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	OE.INTERFACE.MANAGED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	O.CIPHER
T.DOC.DIS	✓						✓	✓												
T.DOC.ALT		✓					✓	✓												
T.FUNC.ALT			✓				✓	✓												
T.PROT.ALT				✓			✓	✓												
T.CONF.DIS					✓		✓	✓												
T.CONF.ALT						✓	✓	✓												
P.USER.AUTHORIZATION							✓	✓												
P.SOFTWARE.VERIFICATION									✓											
P.AUDIT.LOGGING										✓	✓	✓	✓							
P.INTERFACE.MANAGEMENT														✓	✓					
P.CIPHER																				✓
A.ACCESS.MANAGED																✓				
A.ADMIN.TRAINING																	✓			
A.ADMIN.TRUST																		✓		
A.USER.TRAINING																			✓	

Table 13 Security Objectives Rationale for Security Problem

Threats, policies, and assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons.	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	User Document Data may be altered by unauthorized persons.	O.DOC.NO_ALT protects D.DOC from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons.	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.	O.PROT.NO_ALT protects D.PROT from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes

Threats, policies, and assumptions	Summary	Objectives and rationale
		responsibility of the TOE Owner to appropriately grant authorization
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons.	O.CONF.NO_ALT protects D.CONF from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE.	O.USER.AUTHORIZED establishes user authorization to use the TOE identification and authentication as the basis for OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events and prevents unauthorized disclosure or alteration. OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed. O.AUDIT_STORAGE.PROTECTED protects audit logs from unauthorized access, deletion, and alteration for the TOE. O.AUDIT_ACCESS.AUTHORIZED enables the analysis of audit logs only by authorized users to detect potential security violations for the TOE.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies. OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
P.CIPHER	User Data stored in the	O.CIPHER encrypts the document data in the

Threats, policies, and assumptions	Summary	Objectives and rationale
	HDD will be encrypted by the TOE.	internal HDD to disable unauthorized reading-out of them.
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures.	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5. EXTENDED COMPONENTS DEFINITION

This Protection Profile defines components that are extensions to Common Criteria 3.1 Release 2, Part 2. These extended components are defined in the Protection Profile but are used in SFR Packages, and therefore, are employed only in TOEs whose STs conform to those SFR Packages.

5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE’s external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces
1

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces, provides for the functionality to require TSF controlled processing of data received over defined external interfaces before this data is sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

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

a) Definition of the role(s) that are allowed to perform the management activities.

b) Management of the conditions under which direct forwarding can be allowed by an administrative role.

c) Revocation of such an allowance.

Audit: FPT_FDI_EXP.1

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

There are no auditable events foreseen.

Rationale:
Quite often a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data is allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i. e. without processing the data first) between different external interfaces is therefore a function that – if allowed at all – can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and could therefore be placed in either the FDP or FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this lead the authors to define a new family with just one member.

FPT_FDI_EXP.1 **Restricted forwarding of data to external interfaces**

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

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: list of external interfaces] from being forwarded without further processing by the TSF to [assignment: list of external interfaces].

6. SECURITY REQUIREMENTS

This chapter describes the security functional requirements, security assurance requirements, and security requirement rational.
The terms and phrases used in this chapter are defined below.

- Subject

Term/phrase	Definition
Key Operator	Operation upon using Faxbox and Store Print when the user authentication of key operator succeeded.
SA	Operation upon using Faxbox and Store Print when the user authentication of SA succeeded.
U.ADMINISTRATOR	Operation upon using Faxbox and Store Print when the user authentication of Key Operator/SA succeeded.
U.NORMAL	Operation upon using Store Print when the user authentication of U.NORMAL succeeded.
U.USER	Operation upon using Store Print when the user authentication of U.ADMINISTRATOR/ U.NORMAL succeeded.

- Object

Term/phrase	Definition
Faxbox	A logical box created in the MFD . Faxbox can store the document data received via fax.
Store Print	A print function in which bitmap data (decomposed print data) is temporarily stored in the MFD internal HDD and then printed out according to the authenticated user's instruction from the control panel.
Used document data stored in the internal HDD	The remaining data in the MFD internal HDD even after deletion. The document data are first stored into the internal HDD, used, and then only their files are deleted.
Document data	Document data means all the data including image data transmitted across the MFD when any of copy, print, network scan, or fax function is operated by a general user.
Security Audit Log	The chronologically recorded data of important events of the TOE. The events such as device failure, configuration change, and user operation are recorded based on when and who caused what event and its result.

- Operation

Term/phrase	Definition
send the document data	Distribute the scanned document data to user client, FTP server, Mail server, and Fax (public telephone line).
modify the behavior	Modify the behavior of the following: User Authentication (local, remote), Internal Network Data Protection (authentication/encryption method), Report Print (only system administrator) and Hard Disk Data Overwrite (overwrite procedure, On Demand Overwrite procedure).
modify	Modify settings of TOE setting data and security attributes (user identifier, user identifier for document data, functional authority of user)

- Security attributes

Term/phrase	Definition
U.NORMAL role	Indicates the authority required for general user (U.NORMAL) to use the TOE.
SA role	Indicates the authority required for SA to use the TOE.
Key Operator role	Indicates the authority required for key operator to use the TOE.
U.ADMINISTRATOR role	Indicates the authority required for system administrator (U.ADMINISTRATOR) to use the TOE.
U.USER identifier	This term covers U.NORMAL identifier, SA identifier, and Key Operator identifier.
U.NORMAL identifier	User ID used to authenticate and identify general user (U.NORMAL).
SA identifier	User ID used to authenticate and identify SA.
Key Operator identifier	User ID used to authenticate and identify Key Operator.
Functional authority of U.ADMINISTRATOR	Authority set for the system administrator (U.ADMINISTRATOR) role for the use of copy, print, network scan, fax and Faxbox functions.
Functional authority of U.NORMAL	Authority set for the general user (U.NORMAL) role for the use of copy, print, network scan and fax functions.
Owner identifier of D.DOC	Data on authorized users for the document data inside Faxbox and Store Print.
Owner identifier of D.FUNC	Data on authorized users for Jobs.

- Entity outside the TOE

Term/phrase	Definition
Key Operator	An authorized user who manages MFD maintenance and makes TOE security function settings.
SA(System Administrator Privilege)	The users who manage MFD maintenance and configure TOE security functions. SA can be created/registered by key operator or the other SA who is already registered.
U.ADMINISTRATOR (System Administrator)	This term covers both key operator and SA.
U.NORMAL (General User)	Any person who uses copy, network scan, fax, and print functions of MFD.

- Other terminology

Term/phrase	Definition
SHA-2 algorithm	The FIPS-standard cryptographic hash function used for generation of a cryptographic key of Hard Disk data
AES	The FIPS-standard encryption algorithm used for encryption/decryption of Hard Disk data.
Access denial due to authentication failure of system administrator	When the number of unsuccessful authentication attempts has exceeded the specified number of times, Identification and authentication of relevant user is inhibited until the TOE is cycled.
Data on minimum user password length	Minimum user password length to set the user password from MFD control panel. Included in the TOE setting data.
Data on key operator Password	Password data for Key Operator authentication. Included in the TOE setting data.
Data on SA ID	ID data for SA identification. Included in the TOE setting data.
Data on SA Password	Password data for SA authentication. Included in the TOE setting data.
Data on General user ID	ID data for General User (U.NORMAL) identification. Included in the TOE setting data.
Data on General user Password	Password data for General User (U.NORMAL) authentication. Included in the TOE setting data.
Data on access denial due to authentication failures of system administrator	The data on whether to enable/disable access denial due to authentication failure of system administrator ID. They also incorporate the data on the allowable number of the failures before access denial. Included in the TOE setting data.

Data on Security Audit Log	The data on whether to enable/disable the function to trace/ record the important events of the TOE such as device failure, configuration change, and user operation, based on when and who operated what function. Included in the TOE setting data.
Data on User Authentication	The data on whether to enable/disable the authentication function using the data on user authentication when copy, network scan, Fax, and print functions of MFD are used. It also incorporates the data on the authentication method. Included in the TOE setting data.
Data on user permission	The data on authority of U.NORMAL. Included in the TOE setting data.
Data on Internal Network Data Protection	The data on whether to enable/disable the general encryption communication protocols to protect the communication data on the internal network such as document data, job information, security audit log data, and TOE setting data. They also incorporate the data on the setting, certificate, authentication/encryption password, and common key password. Included in the TOE setting data.
Data on Customer Engineer Operation Restriction-	The data on whether to enable/disable the functions related to Customer Engineer Operation Restriction and the data on the maintenance password. Included in the TOE setting data.
Data on Hard Disk Data Overwrite	The data on whether to enable/disable the functions related to Hard Disk Data Overwrite. They also incorporate the data on the On Demand Overwrite function and the data on Date/Time. Included in the TOE setting data.
Data on date and time	The time zone / summer time information and the present time data. Included in the TOE setting data.
Data on Auto Clear	The data on whether to enable/disable the functions of Auto Clear on control panel/Embedded Web Server and the time to clear. Included in the TOE setting data.
Data on Self Test	The data on whether to enable/disable the functions related to Self Test. Included in the TOE setting data.
Data on Report Print	The data on whether to enable/disable the functions related to Report Print. Included in the TOE setting data.

6.1. Security Functional Requirements

Security functional requirements which the TOE offers are described below.

List of functional requirements to be used in this ST is shown in Table 14 below.

Table 14 Security functional Requirements

Security functional components		PP Required Component	Difference from PP
FAU_GEN.1	Audit data generation	Yes	Auditable Event is described and added in detail for each TOE.
FAU_GEN.2	User identity association	Yes	No change from PP.
FAU_SAR.1	Audit review	No	The function of retrieving audit log data are provided to system administrator only by the addition of this SFR.
FAU_SAR.2	Restricted audit review	No	
FAU_STG.1	Protected audit trail storage	No	Audit log data are protected from unauthorized deletion or alteration by the addition of this SFR.
FAU_STG.4	Prevention of audit data loss	No	The oldest stored audit record is overwritten by a new audit event when the audit trail file is full, by the addition of this SFR.
FCS_CKM.1	Cryptographic key generation	No	The data of internal HDD is encrypted by the addition of this SFR.
FCS_COP.1	Cryptographic operation	No	
FDP_ACC.1(a)	Subset access control	Yes	PP description is quoted for Attributes, Operations, and Access Control rule, and also the operations of Delete and Modify are detailed and added for each TOE.
FDP_ACC.1(b)	Subset access control	Yes	Access Control SFP is described for each TOE.

Security functional components		PP Required Component	Difference from PP

FDP_ACC.1(c)
(PRT SFR Package)
FDP_ACC.1(d)
(SCN SFR Package)
FDP_ACC.1(e)
(CPY SFR Package)
FDP_ACC.1(f)
(FAX SFR Package)
	Subset access control	Yes	PP description is quoted for Attributes, Operations, and Access Control rule, and also the operation of Read is detailed for each TOE.

FDP_ACF.1(a)	Security attribute based access control	Yes	PP description is quoted for Attributes, Operations, and Access Control rule, and also the operations of Delete and Modify are detailed and added for each TOE.

FDP_ACF.1(b)
FDP_ACF.1(c)
(PRT SFR Package)
FDP_ACF.1(d)
(SCN SFR Package)
FDP_ACF.1(e)
(CPY SFR Package)
FDP_ACF.1(f)
(FAX SFR Package)
	Security attribute based access control	Yes	PP description is quoted for Attributes, Operations, and Access Control rule, and also the operation of Read is detailed for each TOE.

FDP_RIP.1	Subset residual information protection	Yes	Described in accordance with TOE.
FIA_AFL.1 (a) FIA_AFL.1 (b)	Authentication failure handling	No	Access denial function for authentication failure in the system administrator authentication is provided by the addition of this SFR.
FIA_ATD.1	User attribute definition	Yes	Described in accordance with TOE.
FIA_SOS.1	Verification of secrets	No	Described in accordance with TOE.
FIA_UAU.1	Timing of authentication	Yes	Described in accordance with TOE.
FIA_UAU.7	Protected	No	Authentication feedback is protected

Security functional components		PP Required Component	Difference from PP
	authentication feedback		by the addition of this SFR.
FIA_UID.1	Timing of identification	Yes	Described in accordance with TOE.
FIA_USB.1	User-subject binding	Yes	Described in accordance with TOE.
FMT_MOF.1	Management of security functions behaviour	No	Setting of security functions is restricted to system administrator only by the addition of this SFR.

FMT_MSA.1(a)
FMT_MSA.1(b)
	Management of security attributes	Yes	Management role of security attributes is described in accordance with TOE.

FMT_MSA.1(c)
FMT_MSA.1(d)
FMT_MSA.1(e)
FMT_MSA.1(f)
	Management of security attributes	No	Management of security attributes is described for the TOE.

FMT_MSA.3(a)
FMT_MSA.3(b)
	Static attribute initialisation	Yes	Described in accordance with TOE.

FMT_MSA.3(c)
FMT_MSA.3(d)
FMT_MSA.3(e)
FMT_MSA.3(f)
	Static attribute initialisation	No	Described for the TOE.

FMT_MTD.1(a)
FMT_MTD.1(b)
	Management of TSF data	Yes	Operation list of TSF data are described for the TOE.
			Note that FMT_MTD.1(b) is for D.CONF only.

FMT_SMF.1	Specification of Management Functions	Yes	List of security management functions is described for the TOE.
FMT_SMR.1	Security roles	Yes	Described in accordance with TOE.
FPT_FDI_EXP.1 (SMI SFR Package)	Restricted forwarding of data to external interfaces	Yes	No change from PP.
FPT_STM.1	Reliable time stamps	Yes	No change from PP.
FPT_TST.1	TSF testing	Yes	Described in accordance with TOE.
FTA_SSL.3	TSF-initiated termination	Yes	Described in accordance with TOE.
FTP_ITC.1 (SMI SFR Package)	Inter-TSF trusted channel	Yes	No change from PP.

6.1.1. Class FAU: Security Audit

FAU_GEN.1 Audit data generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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

[selection, choose one of: minimum, basic, detailed, not specified]
- not specified
[assignment: other specifically defined auditable events]
- all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table15;

Table 15 Auditable Events of TOE and Individually Defined Auditable Events

Relevant SFR	Auditable event	Audit level	Additional information	Actions to be audited (defined by CC)
FAU_GEN.1	-	-	-	There are no auditable events foreseen.
FAU_GEN.2	-	-	-	There are no auditable events foreseen.
FAU_SAR.1	*Successful download of audit log data.*	*<Basic>*	*None*	a) Basic: Reading of information from the audit records.
FAU_SAR.2	*Unsuccessful download of audit log data.*	*<Basic>*	*None*	a) Basic: Unsuccessful attempts to read information from the audit records.
FAU_STG.1	-	-	-	There are no auditable events foreseen.
FAU_STG.4	*None*	-	-	a) Basic: Actions taken due to the audit storage failure.
FCS_CKM.1	*None*	-	-	a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object

				value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_COP.1	*None*	-	-	a) Minimal: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FDP_ACC.1	-	-	-	There are no auditable events foreseen.
FDP_ACF.1(a)	-	*<not specified>*	*Type of job*	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.

FDP_ACF.1(b)
FDP_ACF.1(c)
FDP_ACF.1(d)
FDP_ACF.1(f)
	Job completion and cancellation of Print, Copy, Scan, and Fax.			

FDP_RIP.1	-	-	-	There are no auditable events foreseen.

FIA_AFL.1(a)
FIA_AFL.1(b)
	Authentication lock of system administrator	*<Minimal>*	*None required*	a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).

FIA_ATD.1	-	-	-	There are no auditable events foreseen.
FIA_SOS.1	*Registration of user and changes in user registration data (password)*	*<not specified>*	-	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of

				any changes to the defined quality metrics
FIA_UAU.1	*Success/failure of authentication*	*<Basic>*	*None required*	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism. c) Detailed: All TSF mediated actions performed before authentication of the user.
FIA_UAU.7	-	-	-	There are no auditable events foreseen.
FIA_UID.1	*Success/failure of identification and authentication*	*<Basic>*	*Attempted user identity*	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.
FIA_USB.1	*Registration of system administrator, and changes in user registration data (role)*	*<not specified>*	*None*	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).
FMT_MOF.1	*Changes in security function configuration*	*<Basic>*	*None*	a) Basic: All modifications in the behavior of the functions in the TSF.

FMT_MSA.1(a)
FMT_MSA.1(b)
FMT_MSA.1(c)
FMT_MSA.1(d)
FMT_MSA.1(e)
FMT_MSA.1(f)
	Registration of system administrator, changes in registration data (password, access right) of system administrator, and deletion of system	*<not specified>*	*None*	a) Basic: All modifications of the values of security attributes.

	administrator			
FMT_MSA.3 (a) FMT_MSA.3 (b) FMT_MSA.3 (c) FMT_MSA.3 (d) FMT_MSA.3 (e) FMT_MSA.3 (f)	*None*	*<Basic>*	*None*	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
FMT_MTD.1(a)	*Changes in registration data (password) of system administrator, and in the setting of security functions*	*<not specified>*	*None*	a) Basic: All modifications to the values of TSF data.
FMT_MTD.1(b)	*Changes in registration data (password) of system administrator*			
FMT_SMF.1	*Access to system administrator mode*	*<Minimal>*	*None required*	a) Minimal: Use of the management functions.
FMT_SMR.1	*Registration of system administrator, changes in user registration data (role), and deletion of system administrator*	*<Minimal>*	*None required*	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.
FPT_STM.1	*Changes in time setting*	*<Minimal>*	*None required*	a) Minimal: changes to the time; b) Detailed: providing a timestamp.
FPT_TST.1	*Execution of Self Test and the test result*	*<Basic>*	*None*	Basic: Execution of the TSF self tests and the results of the tests.
FTA_SSL.3	*Log-in timeout from remote.*	*<Minimal>*	*None required*	a) Minimal: Termination of an interactive session by the

	Log-in timeout from control panel.			session locking mechanism.
FTP_ITC.1	*Failure of the trusted Communication within a specified period of time, and client host data (host name or IP address)*	*<Minimal>*	*None required*	a) Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.
FPT_FDI_EXP.1	-	-	-	There are no auditable events foreseen.

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

[assignment: other audit relevant information]
- for each Relevant SFR - listed in Table15: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);

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.

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: authorized users] with the capability to read [assignment: list of audit information] from the audit records.

[assignment: authorized users]
- *U.ADMINISTRATOR*
[assignment: list of audit information]
- *all log information*

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

FAU_SAR.2 Restricted audit review
Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

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

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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

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

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

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorized 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 authorized 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]
- no other actions to be taken

6.1.2. Class FCS: Cryptographic Support

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 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]
- FIPS PUB 180-2
[assignment: cryptographic key generation algorithm]
- SHA-2 algorithm
[assignment: cryptographic key sizes]
- 256bits

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]
- FIPS PUB 197
[assignment: cryptographic algorithm]
- AES
[assignment: cryptographic key sizes]
- 256bits
[assignment: list of cryptographic operations]
- encryption of the document data to be stored in the internal HDD and decryption of the document data retrieved from the internal HDD.

6.1.3. Class FDP: User Data Protection

The Security Function Policy (SFP) described in Table16 is referenced by the Class FDP SFRs in this clause.

Table 16 Common Access Control SFP

Object	Attribute	Operation(s)	Subject	*Access control rule
D.DOC	*attributes from Table 17*	*Delete* *- Delete the document data in Store Print*	*U.USER*	*Denied, except for his/her own documents* *When the owner identifier of D.DOC matches the user identifier, operation to delete the document in Store Print is permitted.*
		Delete *- Delete the document data except for Store Print*	*U.USER*	*Denied*

Object	Attribute	Operation(s)	Subject	*Access control rule
D.FUNC	*attributes from Table 17*	*Modify; Delete* *- Modify and delete the Job data*	*U. USER*	*Denied, except for his/her own function data* *- When the owner identifier of D.FUNC matches the user identifier, operation to modify and delete the Job data is permitted.*

Table 17 SFR Package attributes

Designation	Definition
+PRT	*Indicates data that is associated with a print job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+SCN	*Indicates data that is associated with a scan job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+CPY	*Indicates data that is associated with a copy job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+FAXIN	*Indicates data that is associated with an inbound (received) fax job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+FAXOUT	*Indicates data that is associated with an outbound (sent) fax job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*

+SMI	*Indicates data that is transmitted or received over a shared-medium interface.* *- none*

FDP_ACC.1 (a) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (a) 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: access control SFP]
- Common Access Control SFP in Table16
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table16

FDP_ACC.1 (b) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (b) 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: access control SFP]
- TOE Function Access Control SFP in Table 18
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- users as subjects, TOE functions as objects, and the right to use the functions as operations in Table 18.

Table 18 Function Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
Copy (F.CPY)	*Functional authority of U.Normal*	*- Copy operation from control panel*	*U.USER*	*When the Functional*

Object	Attribute(s)	Operation	Subject	Access control rule
Network Scan (F.SCN, F.SMI)	*Functional authority of U.Normal*	*- Send the scanned data from control panel to user client, FTP server, and Mail server*	*U.USER*	*authority of U.Normal includes each function, operation of the function is permitted.* **U.Administrator is always permitted the operation of the functions*
Fax (F.FAX)	*Functional authority of U.Normal*	*- Send the scanned data to remote fax from control panel*	*U.USER*	
Print (F.PRT, F.SMI)	*Functional authority of U.Normal*	*- Print the document data in Store Print from control panel*	*U.USER*	
Faxbox Operation (F.FAX)	*Functional authority of U.Administrator*	*Print the document data in Faxbox from control panel*	*U.USER*	*Only the Functional authority of U.ADMINISTRATOR includes this function and operation of the function is permitted.*

FDP_ACC.1(c) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(c) 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: access control SFP]
- PRT Access Control SFP in Table19
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the PRT Access Control SFP in Table19.

Table 19 PRT Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+PRT*	*Read* *Print the document data in Store Print*	*U.USER*	*Denied, except for his/her own documents* *When the owner identifier of D.DOC matches the user identifier, print operation is permitted.*

FDP_ACC.1 (d) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (d) 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: access control SFP]
- SCN Access Control SFP in Table20
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the SCN Access Control SFP in Table 20

Table 20 SCN Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+SCN*	*Read* *- Send the document data to server*	*U.USER*	*Denied, except for his/her own documents*

FDP_ACC.1 (e) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (e) 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: access control SFP]
- CPY Access Control SFP in Table21
[assignment: list of subjects, objects, and operations among subjects

and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the CPY Access Control SFP in Table 21

Table 21 CPY Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+CPY*	*Read*	*This package does not specify any access control restriction*	

FDP_ACC.1 (f) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (f) 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: access control SFP]
- FAX Access Control SFP in Table22
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the FAX Access Control SFP in Table 22

Table 22 FAX Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+FAXIN*	*Read* *- Print the document data in Faxbox*	*U.USER*	*Denied, except for his/her own documents* *- Only U.ADMINISTRATOR print operation is permitted.*
	+FAXOUT	*Read* *- Send the document data to fax*	*U.USER*	*Denied, except for his/her own documents*

FDP_ACF.1 (a) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (a) 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 named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- Common Access Control SFP in Table 16
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of users as subjects and objects controlled under the Common Access Control SFP in Table 16, and for each, the indicated security attributes in Table 17

FDP_ACF.1.2 (a) 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 specified in the Common Access Control SFP in Table 16 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects

FDP_ACF.1.3 (a) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- In the U.ADMINISTRATOR process, operation to delete the incomplete document data at Copy, Scan, Fax, Print job is permitted by Job Deletion function.

FDP_ACF.1.4 (a) 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].

- none

FDP_ACF.1 (b) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (b) 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 named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- TOE Function Access Control SFP *in Table 18*
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- users and *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP in Table 19*

FDP_ACF.1.2 (b) 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].
- [selection: the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions [assignment: list of functions], [assignment: other conditions]]
- [assignment: other conditions]
- rules specified in the TOE Function Access Control SFP in Table 18

FDP_ACF.1.3(b) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

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

- the user acts in the role U.ADMINISTRATOR,
[assignment: other rules, based on security attributes, that explicitly authorise access of subjects to objects].
[assignment: other rules, based on security attributes, that explicitly authorise access of subjects to objects]
-none

FDP_ACF.1.4 (b) 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].
-none

FDP_ACF.1(c) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1(c) 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 named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- PRT Access Control SFP in Table 19
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of subjects and objects controlled under the PRT Access Control SFP in Table 19, and for each, the indicated security attributes in Table 19.

FDP_ACF.1.2(c) 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 specified in the PRT Access Control SFP in Table 19 governing access among Users and controlled objects using controlled operations on controlled objects.

FDP_ACF.1.3(c)	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]. [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. *-none*
FDP_ACF.1.4(c)	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]. *- none*
FDP_ACF.1 (d)	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1 (d)	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 named groups of SFP-relevant security attributes]. [assignment: access control SFP] ***- SCN Access Control SFP in Table 20*** [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]. *- the list of subjects and objects controlled under the SCN Access Control SFP in Table 20, and for each, the indicated security attributes in Table 20.*
FDP_ACF.1.2 (d)	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 specified in the SCN Access Control SFP in Table 20 governing access among Users and controlled objects using controlled operations on controlled objects.

FDP_ACF.1.3 (d) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- *none*

FDP_ACF.1.4 (d) 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].
- *none*

FDP_ACF.1 (e) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (e) 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 named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- CPY Access Control SFP in Table 21
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or

named groups of SFP-relevant security attributes].
- the list of subjects and objects controlled under the CPY Access Control SFP in Table 21, and for each, the indicated security attributes in Table 21.

FDP_ACF.1.2 (e) 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 specified in the CPY Access Control SFP in Table 21 governing access among Users and controlled objects using controlled operations on controlled objects.

FDP_ACF.1.3 (e) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- none

FDP_ACF.1.4 (e) 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].
- none

FDP_ACF.1 (f) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (f) 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 named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- FAX Access Control SFP in Table 22
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of subjects and objects controlled under the FAX Access Control SFP in Table 22, and for each, the indicated security attributes in Table 22.

FDP_ACF.1.2 (f) 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 specified in the FAX Access Control SFP in Table 22 governing access among Users and controlled objects using controlled operations on controlled objects.

FDP_ACF.1.3 (f) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- none

FDP_ACF.1.4 (f) 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].
- none

FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
Dependencies:	No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: **D.DOC**, [assignment: list of objects].

[selection: allocation of the resource to, deallocation of the resource from]
- *deallocation of the resource from*
[assignment: list of objects]
- *none*

6.1.4. Class FIA: Identification and Authentication

FIA_AFL.1(a)	Authentication failure handling
Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(a) 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]
- *key operator authentication*
[selection: [assignment: positive integer number] , an administrator configurable positive integer within [assignment: range of acceptable values]
- *[assignment: positive integer number]*
- *5*

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

[selection: met, surpassed]
- *met*
[assignment: list of actions]
- *Identification and authentication of key operator is inhibited until TOE is cycled*

FIA_AFL.1 (b)	Authentication failure handling
Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 (b) 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]
- *SA authentication (with local authentication)*

[selection: [assignment: positive integer number] , an administrator configurable positive integer within [assignment: range of acceptable values]
- *[assignment: positive integer number]*
- *5*

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

[selection: met, surpassed]
- *met*

[assignment: list of actions]
- *Identification and authentication of relevant user is inhibited until TOE is cycled.*

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].
- *Key Operator role*
- *SA role*
- *U.NORMAL role*

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 (U.USER password when local authentication is used) meet [assignment: a defined quality metric].

[assignment: a defined quality metric].
- Password length is restricted to 9 or more characters

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

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

[assignment: list of TSF mediated actions]
- storing the fax data received from public telephone line
- storing the print job delivered from user client

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

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

[assignment: list of feedback]
- display of asterisks ("") to hide the entered password characters*

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]

- storing the fax data received from public telephone line

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding
Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

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

[assignment: list of user security attributes]
- Key Operator role
- SA role
- U.NORMAL role

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

[assignment: rules for the changing of attributes]
- none

6.1.5. Class FMT: Security Management

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

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

[selection: determine the behavior of, disable, enable, modify the behavior of]
- disable, enable, modify the behavior of
[assignment: list of functions]
-List of security functions in Table 23
[assignment: the authorized identified roles]
- the roles listed in Table 23

Table 23 List of Security Functions

Security Functions	Operation	Roles
Access denial due to authentication failure of system administrator ID	*enable, disable*	*U.ADMINISTRATOR*
User Authentication	*enable, disable, modify the behavior*	*U.ADMINISTRATOR*
Security Audit Log	*enable, disable*	*U.ADMINISTRATOR*
Internal Network Data Protection	*enable, disable, modify the behavior*	*U.ADMINISTRATOR*
Customer Engineer Operation Restriction	*enable, disable*	*U.ADMINISTRATOR*
Hard Disk Data Overwrite	*enable, disable*	*U.ADMINISTRATOR*
Auto Clear	*enable, disable*	*U.ADMINISTRATOR*
Self Test	*enable, disable*	*U.ADMINISTRATOR*

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

FMT_MSA.1.1 (a) The TSF shall enforce 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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- Common Access Control SFP in Table 16

[selection: change default, query, modify, delete, [assignment: other operations]]
- query, modify, delete, [assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 24

Table 24 Security Attributes and Authorized Roles

Security attributes	Operation	Roles
Key operator identifier	*query*	*U.ADMINISTRATOR*
SA identifier	*query,* *delete, creation*	*U.ADMINISTRATOR*
U.NORMAL identifier	*query,* *delete, creation*	*U.ADMINISTRATOR*
Owner identifier of D.DOC (own document data in Store Print)	*query, delete, creation*	*U.USER*
Owner identifier of D.DOC (document data in Faxbox)	*query*	*U.ADMINISTRATOR*
Owner identifier of D.FUNC	*query, delete, creation*	*U.USER*

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

FMT_MSA.1.1 (b) The TSF shall enforce 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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- TOE Function Access Control SFP in Table 18,
[selection: change default, query, modify, delete, [assignment: other operations]]
- query, modify ,delete ,[assignment: other operations]

[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 18
[assignment: the authorized identified roles].
- the roles listed in Table 25

Table 25 Security Attributes and Authorized Roles (Function Access)

Security Attributes	Operation	Roles
Key operator identifier	*query*	*U.ADMINISTRATOR*
SA identifier	*query, delete, creation*	*U.ADMINISTRATOR*
U.NORMAL identifier	*query, delete, creation*	*U.ADMINISTRATOR*
Functional authority of U.NORMAL	*query, modify*	*U.ADMINISTRATOR*

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

FMT_MSA.1.1 (c) 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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- PRT Access Control SFP in Table 19
[selection: change default, query, modify, delete, [assignment: other operations]]
- query, modify, delete, [assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 26

Table 26 Security Attributes and Authorized Roles(PRT)

Security Attributes	Operation	Roles
Key operator identifier	*query*	*U.ADMINISTRATOR*
SA identifier	*query, delete, creation*	*U.ADMINISTRATOR*
U.USER identifier	*query, delete, creation*	*U.ADMINISTRATOR*
Owner identifier of D.DOC (own document data in Store Print)	*query, delete, creation*	*U.USER*

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

FMT_MSA.1.1 (d) 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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- SCN Access Control SFP in Table 20
[selection: change default, query, modify, delete, [assignment: other operations]]
- query, modify, delete, [assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 27

Table 27 Security Attributes and Authorized Roles (SCN)

Security Attributes	Operation	Roles
Key operator identifier	*query*	*U.ADMINISTRATOR*
SA identifier	*Query, delete, creation*	*U.ADMINISTRATOR*

U.NORMAL identifier	*Query, delete, creation*	*U.ADMINISTRATOR*

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

FMT_MSA.1.1 (e) 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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- *CPY Access Control SFP in Table 21*
[selection: change default, query, modify, delete, [assignment: other operations]]
- *none*
[assignment: other operations]
- *none*
[assignment: list of security attributes]
- *none*
[assignment: the authorized identified roles].
- *none*

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

FMT_MSA.1.1 (f) 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 authorized identified roles].

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

- FAX Access Control SFP in Table 22

[selection: change default, query, modify, delete, [assignment: other operations]]

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

[assignment: other operations]

- creation

[assignment: list of security attributes]

- the security attributes listed in Table 17

[assignment: the authorized identified roles].

- the roles listed in Table 28

Table 28 Security Attributes and Authorized Roles (FAX)

Security Attributes	Operation	Roles
Key operator identifier	*query*	*U.ADMINISTRATOR*
SA identifier	*query, delete, creation*	*U.ADMINISTRATOR*
U.NORMAL identifier	*query, delete, creation*	*U.ADMINISTRATOR*
Owner identifier of D.DOC (document data in Faxbox)	*query*	*U.ADMINISTRATOR*

FMT_MSA.3 (a) Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (a) 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.

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

- Common Access Control SFP in Table16

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

- [assignment: other property]

- Initialization property in Table 29

Table 29 Initialization property

Object	Security Attributes	Default
D.DOC	*Owner identifier of D.DOC*	*Creator's user identifier and*

D.FUNC	*Owner identifier of D.FUNC*	*available user identifier*

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

[assignment: the authorized identified roles]
- *none*

FMT_MSA.3 (b) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (b) 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.

[assignment: access control SFP, information flow control SFP]
- *TOE Function Access control SFP in Table 18*
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- [assignment: other property]
- *permissive initialization property for basic functions such as copy, print, scan, and fax as the default of security attribute.*

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

[assignment: the authorized identified roles]
- *none*

FMT_MSA.3 (c) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (c) 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.

[assignment: access control SFP, information flow control SFP]
- PRT Access Control SFP in Table 19
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- [assignment: other property]
- Initialization property in Table 30

Table 30 Initialization property

Object	Security Attributes	Default
D.DOC	*Owner identifier of D.DOC*	*Creator's user identifier and available user identifier*

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

[assignment: the authorized identified roles]
- none

FMT_MSA.3 (d) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (d) 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.

[assignment: access control SFP, information flow control SFP]
- SCN Access Control SFP in Table 20
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- [assignment: other property]
- Initialization property in Table 30

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

[assignment: the authorized identified roles]
- none

FMT_MSA.3 (e) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (e) 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.

[assignment: access control SFP, information flow control SFP]
- CPY Access Control SFP in Table 21
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- permissive

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

[assignment: the authorized identified roles]
- none

FMT_MSA.3 (f) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (f) 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.

[assignment: access control SFP, information flow control SFP]
- FAX Access Control SFP in Table 22
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- [assignment: other property]
- Owner identifier of Faxbox which receives the fax data from public

telephone line

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

[assignment: the authorized identified roles]
- *none*

FMT_MTD.1 (a) Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

[selection: change default, query, modify, delete, clear, [assignment: other operations]]
- *query, modify, delete*
[assignment: other operations]
- *creation*
[assignment: list of TSF data]
- *TSF data listed in Table 31*
[assignment: the authorized identified roles].
- *selection, choose one of: Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]*
- *U.ADMINISTRATOR, Key Operator*

Table 31 Operation of TSF Data

TSF Data	Operation	Roles
Data on key operator Password	*modify*	*Key Operator*
Data on SA ID	*query, delete, creation*	*U.ADMINISTRATOR*
Data on SA Password	*modify*	*U.ADMINISTRATOR*
Data on User Authentication	*query, modify*	*U.ADMINISTRATOR*
Data on minimum user password length	*query, modify*	*U.ADMINISTRATOR*
Data on user permission	*query, modify*	*U.ADMINISTRATOR*

Data on Access denial due to authentication failure of system administrator	*query, modify*	*U.ADMINISTRATOR*
Data on Security Audit Log	*query, modify*	*U.ADMINISTRATOR*
Data on Internal Network Data Protection	*query, modify, delete*	*U.ADMINISTRATOR*
Data on Customer Engineer Operation Restriction	*query, modify*	*U.ADMINISTRATOR*
Data on Hard Disk Data Overwrite	*query, modify*	*U.ADMINISTRATOR*
Data on date and time	*query, modify*	*U.ADMINISTRATOR*
Data on Auto Clear	*query, modify*	*U.ADMINISTRATOR*
Data on Self Test	*query, modify*	*U.ADMINISTRATOR*
Data on Report Print	*query, modify*	*U.ADMINISTRATOR*

FMT_MTD.1 (b) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

[selection: change default, query, modify, delete, clear, [assignment: other operations]]
- query, modify, delete
[assignment: other operations]
- creation
[assignment: list of TSF data]
- list of TSF data associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL in Table 32
[assignment: the authorized identified roles].
- selection, choose one of: Nobody, [selection: U.ADMINISTRATOR, U.NORMAL to whom such TSF data is associated].
- U.ADMINISTRATOR, U.NORMAL to whom such TSF data is associated

Table 32 Operation of TSF Data

TSF Data	Operation	Roles
Data on General user ID	*query, delete, creation*	*U.ADMINISTRATOR*
Data on General user Password	*modify*	*U.ADMINISTRATOR , U.NORMAL*

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No dependencies.

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

[assignment: list of management functions to be provided by the TSF]
- Security Management Functions listed in Table 33

Table 33 Security Management Functions Provided by TSF

Relevant SFR	Management Function	Management items defined by CC
FAU_GEN.1	*Management of data on Security Audit Log settings*	There are no management activities foreseen.
FAU_GEN.2	-	There are no management activities foreseen.
FAU_SAR.1	*Management of data on key operator password,* *Management of data on SA ID and SA password*	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SAR.2	-	There are no management activities foreseen.
FAU_STG.1	-	There are no management activities foreseen.
FAU_STG.4	*none* *Reason: The control parameter of audit log is fixed and is not managed*	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FCS_CKM.1	-	There are no management activities foreseen.
FCS_COP.1	-	There are no management activities foreseen.

FDP_ACC.1(a)
FDP_ACC.1(b)
FDP_ACC.1(c)
FDP_ACC.1(d)
FDP_ACC.1(e)
FDP_ACC.1(f)
	-	There are no management activities foreseen.

FDP_ACF.1(a)	*- Management of user identifier* *- Management of owner identifier of D.DOC* *- Management of owner identifier of D.FUNC* *- Management of user permission*	a)Managing the attributes used to make explicit access or denial based decisions.
FDP_ACF.1(b)	*- Management of user identifier* *- Management of Functional authority of U.NORMAL*	
FDP_ACF.1(c)	*- Management of user identifier* *- Management of owner identifier of D.DOC*	

FDP_ACF.1(d)
FDP_ACF.1(f)
	- Management of user identifier
	- Management of owner identifier of D.DOC	

FDP_ACF.1(e)	*none* *Reason: there are no additional security attributes and is not managed.*	
FDP_RIP.1	*Management of data on Hard Disk Data Overwrite*	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.

FIA_AFL.1(a)
FIA_AFL.1(b)
	Management of data on access denial due to authentication failure of system administrator	a) Management of the threshold for unsuccessful authentication attempts;
		b) Management of actions to be taken in the event of an authentication failure.

FIA_ATD.1	*none* *Reason: there are no additional security attributes and there are no additional security attributes to be managed.*	a) If so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.
FIA_SOS.1	*- Management of Data on minimum user password length*	a) the management of the metric used to verify the secrets.

FIA_UAU.1	*- Management of data on key operator, SA, and general user password* *- Management of data on user authentication.* *- Management of data on minimum user password length*	a) Management of the authentication data by an administrator; b) Management of the authentication data by the associated user; c) Managing the list of actions that can be taken before the user is authenticated.
FIA_UAU.7	-	There are no management activities foreseen.
FIA_UID.1	*- Management of data on SA, and general user ID* *- Management of data on user authentication.*	a) The management of the user identities. b) If an authorised administrator can change the actions allowed before identification, the managing of the action lists.
FIA_USB.1	*none* *Reason: action and security attributes are fixed and are not managed.*	a) an authorized administrator can define default subject security attributes. b) an authorized administrator can change subject security attributes.
FMT_MOF.1	*Management of data on Customer Engineer Operation Restriction*	a) Managing the group of roles that can interact with the functions in the TSF;

FMT_MSA.1(a)
FMT_MSA.1(b)
FMT_MSA.1(c)
FMT_MSA.1(d)
FMT_MSA.1(e)
FMT_MSA.1(f)
	none
	Reason: The role group is fixed and is not managed
		a) managing the group of roles that can interact with the security attributes;
		b) management of rules by which security attributes inherit specified values.

FMT_MSA.3(a)
FMT_MSA.3(b)
FMT_MSA.3(c)
FMT_MSA.3(d)
FMT_MSA.3(e)
FMT_MSA.3(f)
	none
	Reason: The role group is only a system administrator and is not managed.
		a) managing the group of roles that can specify initial values;
		b) managing the permissive or restrictive setting of default values for a given access control SFP;
		c) management of rules by which security attributes inherit specified values.

FMT_MTD.1(a)	*- Management of data on Customer Engineer Operation Restriction* *- Management of data on Report Print*	a) Managing the group of roles that can interact with the TSF data.
FMT_MTD.1(b)	*none* *Reason: The role group is fixed and is not managed*	
FMT_SMF.1	-	There are no management activities foreseen.
FMT_SMR.1	*none* *Reason: The role group is fixed and is not managed*	a) Managing the group of users that are part of a role.
FPT_STM.1	*- Management of time and data.*	a) management of the time.
FPT_TST.1	*- Management of data on Self Test.*	a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) management of the time interval if appropriate.
FTA_SSL.3	*- Management of data on Auto Clear.*	a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user; b) specification of the default time of user inactivity after which termination of the interactive session occurs.
FTP_ITC.1	*- Management of data on Internal Network Data Protection.*	a) Configuring the actions that require trusted channel, if supported.
FPT_FDI_EXP.1	*none* *Reason: The role and transfer conditions are fixed and are not managed.*	a) Definition of the role(s) that are allowed to perform the management activities; b) Management of the conditions under which direct forwarding can be allowed by an administrative role; c) Revocation of such an allowance.

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 authorized identified roles].

[assignment: the authorized identified roles]
- U.ADMINISTRATOR, U.NORMAL, key operator, SA

FMT_SMR.1.2 The TSF shall be able to associate users with roles, except for the role "Nobody" to which no user shall be associated.

6.1.6. Class FPT: Protection of the TSF

FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles.

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: list of external interfaces] from being forwarded without further processing by the TSF to [assignment: list of external interfaces].

[assignment: list of external interfaces]
- any external interfaces
[assignment: list of external interfaces]
- any Shared-medium interfaces

FPT_STM.1	Reliable time stamps
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

[selection: during initial start-up, periodically during normal

operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]
- at the conditions [assignment: conditions under which self test should occur]
[assignment: conditions under which self test should occur]
- at initiation under which self test is set
[selection: [assignment: parts of TSF], the TSF].
- [assignment: parts of TSF]
- TSF executable code

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

[selection: [assignment: parts of TSF data], TSF data]
- [assignment: parts of TSF data]
- TSF data (excluding audit log data and present time data)

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

[selection: [assignment: parts of TSF], TSF]
- [assignment: parts of TSF]
- TSF executable code

6.1.7. Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies.
FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity].

[assignment: time interval of user inactivity]
- Auto clear time for the control panel can be set to 10 to 900 seconds.
- Login timeout for the Embedded Web Server can be set to 5 to 60 minutes.
- There is no inactive time with printer/fax driver.

6.1.8. Class FTP: Trusted Path/Channels

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].
- communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface

6.2. Security Assurance Requirements

The requirements for the TOE security assurance are described in Table 34.

The evaluation assurance level of the TOE is EAL2. The added security assurance component is ALC_FLR.2.

Table 34 Security Assurance Requirements

Assurance Class	Assurance Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
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 Requirement Rationale

6.3.1. Security Functional Requirements Rationale

Table 35 lists security functional requirements and the corresponding security objectives.
As shown in this table, each security functional requirement corresponds to at least one security objective of the TOE. Table 36 shows the rationale demonstrating that each security objective is assured by TOE security functional requirements.

Table 35 Security Functional Requirements and the Corresponding Security Objectives

Objectives SFRs	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.CIPHER
FAU_GEN.1										✓			
FAU_GEN.2										✓			
FAU_SAR.1												✓	
FAU_SAR.2												✓	
FAU_STG.1											✓		
FAU_STG.4											✓		
FCS_CKM.1													✓
FCS_COP.1													✓
FDP_ACC.1 (a)	✓	✓	✓										
FDP_ACC.1 (b)							✓						
FDP_ACC.1 (c)	✓												
FDP_ACC.1 (d)	✓												
FDP_ACC.1 (e)	✓												
FDP_ACC.1 (f)	✓												
FDP_ACF.1 (a)	✓	✓	✓										
FDP_ACF.1 (b)							✓						
FDP_ACF.1 (c)	✓												
FDP_ACF.1 (d)	✓												
FDP_ACF.1 (e)	✓												
FDP_ACF.1 (f)	✓												

Objectives SFRs	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.CIPHER
FDP_RIP.1	✓												
FIA_AFL.1 (a)							✓	✓					
FIA_AFL.1 (b)							✓	✓					
FIA_ATD.1							✓						
FIA_SOS.1							✓	✓					
FIA_UAU.1							✓	✓					
FIA_UAU.7							✓	✓					
FIA_UID.1	✓	✓	✓	✓	✓	✓	✓	✓		✓			
FIA_USB.1							✓						
FMT_MOF.1				✓	✓	✓							
FMT_MSA.1 (a)	✓	✓	✓	✓									
FMT_MSA.1 (b)				✓			✓						
FMT_MSA.1 (c)	✓			✓									
FMT_MSA.1 (d)	✓			✓									
FMT_MSA.1 (e)	✓			✓									
FMT_MSA.1 (f)	✓			✓									
FMT_MSA.3 (a)	✓	✓	✓										
FMT_MSA.3 (b)							✓						
FMT_MSA.3 (c)	✓												
FMT_MSA.3 (d)	✓												
FMT_MSA.3 (e)	✓												
FMT_MSA.3 (f)	✓												
FMT_MTD.1 (a)				✓	✓	✓							
FMT_MTD.1 (b)				✓	✓	✓							
FMT_SMF.1	✓	✓	✓	✓	✓	✓							
FMT_SMR.1	✓	✓	✓	✓	✓	✓	✓						
FPT_FDI_EXP.1								✓					
FPT_STM.1										✓			

Objectives SFRs	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.CIPHER
FPT_TST.1									✓				
FTA_SSL.3							✓	✓					
FTP_ITC.1	✓	✓	✓	✓	✓	✓							

Table 36 Security Objectives to SFR Rationale

Security Objectives	Security Functional Requirements Rationale
O.AUDIT.LOGGED (Logging and authorized access to audit events)	O.AUDIT.LOGGED is the objective to prevent unauthorized disclosure and alteration by creating and maintaining the event logs related to the TOE usage and security. This security objective can be realized by satisfying the following security functional requirement: By FAU_GEN.1, the security audit log data are generated for the auditable events: (However, audit is unnecessary for the following functional requirements for each reason described below.) - FAU_STG.4: The total number of security audit log data events is fixed. The data are stored and updated automatically. - FCS_CKM.1: When cryptographic key generation fails, a system error occurs at the time of booting of the MFD. - FCS_COP.1: An encryption failure is monitored as job status. - FMT_MSA.3: No change in default and rules. By FAU_GEN.2 and FIA_UID.1, each auditable event is associated with the identity of user who caused the event. By FPT_STM.1, the auditable events are recorded with time stamp in the security audit log data, using highly reliable clock of TOE. Thus, the functional requirements related to this objective are surely fulfilled.
O.SOFTWARE.VERIFIED (Verification of software integrity)	O.SOFTWARE.VERIFIED is the objective to provide the procedure of self verification on the executable code of TOE. This security objective can be realized by satisfying the following security functional requirement:

Security Objectives	Security Functional Requirements Rationale
	By FPT_TST.1, self test function can be set to be executed upon initialization. This function verifies the integrity of TSF executable code and TSF data. Thus, the functional requirements related to this objective are surely fulfilled.
O.INTERFACE.MANAGED (Management of external interfaces)	O.INTERFACE.MANAGED is the objective to manage the operations related to the external interfaces such as Embedded Web Server, the control panel, and the printer driver according to the security policy. This security objective can be realized by satisfying the following security functional requirement: In order to prevent attackers from using privileges given to system administrators and accessing protected assets, the power needs to be cycled when the system-administrator authentication fails (FIA_AFL.1 (a)), and the number of system-administrator authentication failures reaches the defined number of times (FIA_AFL.1 (b)). By FIA_UAU.1 and FIA_UID.1, user identification and authentication is conducted upon access to Embedded Web Server and control panel to identify authorized user and system administrator. By FIA_UAU.7, unauthorized disclosure of the authentication information (password) is prevented because the authentication feedback is protected. By FTA_SSL.3, when there is no access to Embedded Web Server and control panel for a specified period of time, login is cleared and re-authentication is required. The session is ended immediately after the required processing ends, without retaining the session with printer. By FIA_SOS1, the minimum length of password for user is limited. By FPT_FDI_EXP.1, unpermitted transfer of the data received from external interfaces to the internal network is restricted. Thus, the functional requirements related to this objective are surely fulfilled.
O.USER.AUTHORIZED (Authorization of Normal Users and Administrators to use the TOE)	O.USER.AUTHORIZED is the objective to request the authentication and identification of the user with authority given according to the security policy before the use of TOE is permitted. This objective can be realized by satisfying the following security functional requirements: By FDP_ACC.1(b) and FDP_ACF.1(b), user authentication is performed and only authorized user is allowed to operate the objects. In order to prevent attackers from using privileges given to system administrators and accessing protected assets, the power needs to be cycled when the system-administrator authentication fails (FIA_AFL.1 (a)),

Security Objectives	Security Functional Requirements Rationale
	and the number of system-administrator authentication failures reaches the defined number of times (FIA_AFL.1 (b)). By FIA_ATD.1 and FIA_USB.1, each role of key operator, SA, and general user is maintained and only the authorized users are associated with the subjects. By FIA_UAU.1 and FIA_UID.1, user identification and authentication is conducted upon access from Embedded Web Server and control panel to identify authorized user and system administrator. By FIA_SOS1, the minimum length of password for user is limited. By FIA_UAU.7, unauthorized disclosure of the authentication information (password) is prevented because the authentication feedback is protected. By FMT_MSA.1(b), the query, modification, deletion, and creation of security attributes are managed. By FMT_MSA.3 (b), the suitable default values are managed. By FMT_SMR.1, the role of key operator, SA, system administrator and general user is maintained and associated with the key operator, SA, system administrator and general user. By FTA_SSL.3, when there is no access to Embedded Web Server and control panel for a specified period of time, settings on the control panel are cleared and re-authentication is required. Thus, the functional requirements related to this objective are surely fulfilled.
O.DOC.NO_DIS (Protection of User Document Data from unauthorized disclosure)	O.DOC.NO_DIS is the objective to protect User Document Data of TOE from unauthorized disclosure. This security objective can be realized by satisfying the following security functional requirements: By FDP_RIP.1, the previous information of the used document data stored in the internal HDD is made unavailable. Only the authorized user is permitted to operate User Document Data by conducting the user identification by the following: FDP_ACC.1(a), FDP_ACC.1(c), FDP_ACC.1(d), FDP_ACC.1(e), FDP_ACC.1(f) (Enforces protection by establishing an access control policy.), FDP_ACF.1(a), FDP_ACF.1(c), FDP_ACF.1(d), FDP_ACF.1(e), FDP_ACF.1(f), and FIA_UID.1. By FMT_MSA.1(a), FMT_MSA.1(c), FMT_MSA.1(d), FMT_MSA.1(e), FMT_MSA.1(f), the query, modification, deletion, and creation of security attributes are managed. By FMT_MSA.3 (a), FMT_MSA.3 (c), FMT_MSA.3 (d), FMT_MSA.3 (e),FMT_MSA.3 (f), the suitable default values are managed. By FMT_SMR.1, the role of key operator, SA, system administrator and

Security Objectives	Security Functional Requirements Rationale
	general user is maintained and associated with the key operator, SA, system administrator and general user. By FMT_SMF.1, TOE security management functions are provided for system administrator. By FTP_ITC.1, communication data encryption protocol is supported to protect User Document Data on the internal network between TOE and IT products from any threat. Thus, the functional requirements related to this objective are surely fulfilled.
O.DOC.NO_ALT, (Protection of User Document Data from unauthorized alteration)	O.DOC.NO_ALT is the objective to protect User Document Data of TOE from unauthorized alteration. This security objective can be realized by satisfying the following security functional requirements: Only the authorized user is permitted to operate User Document Data by conducting the user identification by the following: FDP_ACC.1(a), FDP_ACF.1(a), and FIA_UID.1. By FMT_MSA.1(a) , the query, modification, deletion, and creation of security attributes are managed. By FMT_MSA.3 (a), the suitable default values are managed. By FMT_SMR.1, the role of key operator, SA, system administrator and general user is maintained and associated with the key operator, SA, system administrator and general user. By FMT_SMF.1, TOE security management functions are provided for system administrator. By FTP_ITC.1, communication data encryption protocol is supported to protect User Document Data on the internal network between TOE and IT products from any threat. Thus, the functional requirements related to this objective are surely fulfilled.
O.FUNC.NO_ALT (Protection of User Function Data from unauthorized alteration)	O.FUNC.NO_ALT is the objective to protect User Document Data of TOE from unauthorized alternation. This security objective can be realized by satisfying the following security functional requirements: Only the authorized user is permitted to operate User Document Data by conducting the user identification by the following: FDP_ACC.1(a), FDP_ACF.1(a), and FIA_UID.1. By FMT_MSA.1(a), the query, modification, deletion, and creation of security attributes are managed. By FMT_MSA.3 (a), the suitable default values are managed. By FMT_SMR.1, the role of key operator, SA , system administrator and

Security Objectives	Security Functional Requirements Rationale
	general user is maintained and associated with the key operator, SA , system administrator and general user. By FMT_SMF.1, TOE security management functions are provided for system administrator. By FTP_ITC.1, communication data encryption protocol is supported to protect User Document Data on the internal network between TOE and IT products from any threat. Thus, the functional requirements related to this objective are surely fulfilled.
O.PROT.NO_ALT, (Protection of TSF Data from unauthorized alteration)	O.PROT.NO_ALT is the objective to protect TSF Data of TOE from unauthorized alternation. This security objective can be realized by satisfying the following security functional requirements: By FIA_UID.2, only the authorized system administrator is permitted to handle TSF Data by conducting the user identification. By FMT_MOF.1, the user who enables/disables TOE security functions and makes functional settings is limited to system administrator. By FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.1(d), FMT_MSA.1(e), FMT_MSA.1(f), modification, deletion, and creation of security attributes are managed. By FMT_MTD.1 (a), the person who can make settings of TOE security functions is limited to system administrator. Thus, only system administrators can query and modify TOE setting Data. By FMT_MTD.1 (b), the setting of ID for general users is restricted to system administrator and owner. By FMT_SMF.1, TOE security management functions are provided for system administrator. By FMT_SMR.1, the roles of key operator, SA, system administrator and general user are maintained and associated with the key operator, SA, system administrator and general user. By FTP_ITC.1, communication data encryption protocol is supported to protect D.CONF on the internal network between TOE and IT products from any threat. Thus, the functional requirements related to this objective are surely fulfilled.
O.CONF.NO_DIS, O.CONF.NO_ALT (Protection of TSF Data from unauthorized	O.CONF.NO_DIS and O.CONF.NO_ALT are the objectives to protect D.CONF of TOE from unauthorized disclosure or alteration. This security objective can be realized by satisfying the following security functional requirements: By FIA_UID.1, only the authorized user is permitted to handle D.CONF by

Security Objectives	Security Functional Requirements Rationale
disclosure or alteration)	conducting the user identification. By FMT_MOF.1, the user who enables/disables TOE security functions and makes functional settings is limited to system administrator. By FMT_MTD.1(a), the person who can make settings of TOE security functions is limited to system administrator. Thus, only system administrators can query and modify D.CONF. By FMT_MTD.1(b), the setting of ID and password for general users is restricted to system administrator and owner. By FMT_SMF.1, TOE security management functions are provided for system administrator. By FMT_SMR.1, the roles of key operator, SA, system administrator and general user are maintained and associated with the key operator, SA, system administrator and general user. By FTP_ITC.1, communication data encryption protocol is supported to protect the security audit log data and D.CONF on the internal network between TOE and IT products from any threat. Thus, the functional requirements related to this objective are surely fulfilled.
O.AUDIT_STORAGE.PROTECTED	O.AUDIT_STORAGE.PROTECTED is the objective that protects the audit logs from unauthorized access, deletion, and modification. This security objective can be realized by satisfying the following security functional requirements: By FAU_STG.1, the security audit log data stored in an audit log file is protected from unauthorized deletion and alteration. By FAU_STG.4, when the audit trail file is full, the oldest stored audit record is overwritten and a new audit event is stored into the audit log file. Thus, the functional requirements related to this objective are surely fulfilled.
O.AUDIT_ACCESS.AUTHORIZED	O.AUDIT_ACCESS.AUTHORIZED is the objective that enables the audit logs to be analyzed by the authorized user only to detect potential security violations. This security objective can be realized by satisfying the following security functional requirements: By FAU_SAR.1, the authorized system administrator can read the security audit log data from an audit log file. By FAU_SAR.2, only the authorized system administrator can access the audit log. Thus, the functional requirements related to this objective are surely fulfilled.
O.CIPHER	O. CIPHER is the objective that encrypts the document data in the internal

Security Objectives	Security Functional Requirements Rationale
	HDD so that they cannot be analyzed even if retrieved. This security objective can be realized by satisfying the following security functional requirements: By FCS_CKM.1, the cryptographic key is generated in accordance with the specified cryptographic key size (256 bits). By FCS_COP.1, the document data and used document data to be stored into the internal HDD is encrypted and then decrypted when the data are read, in accordance with the determined cryptographic algorithm and cryptographic key size. Thus, the functional requirements related to this objective are surely fulfilled.

6.3.2. Dependencies of Security Functional Requirements

Table 37 describes the functional requirements that security functional requirements depend on and those that do not and the reason why it is not problematic even if dependencies are not satisfied.

Table 37 Dependencies of Functional Security Requirements

Functional Requirement	Dependencies of Functional Requirements	
Requirement and its name	Requirement that is dependent on	Requirement that is not dependent on and its rationale
FAU_GEN.1 Audit data generation	FPT_STM.1	-
FAU_GEN.2 User identity association	FAU_GEN.1 FIA_UID.1	-
FAU_SAR.1 Audit review	FAU_GEN.1	-
FAU_SAR.2 Restricted audit review	FAU_SAR.1	-
FAU_STG.1 Protected audit trail storage	FAU_GEN.1	-
FAU_STG.4 Prevention of audit data loss	FAU_STG.1	-

Functional Requirement	Dependencies of Functional Requirements	
Requirement and its name	Requirement that is dependent on	Requirement that is not dependent on and its rationale
FCS_CKM.1 Cryptographic key generation	FCS_COP.1	FCS_CKM.4: As specified in the Organizational Security Policies, a cryptographic key does not need to be destructed.
FCS_COP.1 Cryptographic operation	FCS_CKM.1	FCS_CKM.4: As specified in the Organizational Security Policies, a cryptographic key does not need to be destructed.
FDP_ACC.1(a) Subset access control	FDP_ACF.1(a)	-
FDP_ACC.1(b) Subset access control	FDP_ACF.1(b)	-
FDP_ACC.1(c) Subset access control	FDP_ACF.1(c)	-
FDP_ACC.1(d) Subset access control	FDP_ACF.1(d)	-
FDP_ACC.1(e) Subset access control	FDP_ACF.1(e)	-
FDP_ACC.1(f) Subset access control	FDP_ACF.1(f)	-

FDP_ACF.1(a)
Security attribute based access control
	FDP_ACC.1(a)
	FMT_MSA.3(a)
		-

FDP_ACF.1 (b)
Security attribute based access control
	FDP_ACC.1(b)
	FMT_MSA.3(b)
		-

FDP_ACF.1 (c)
Security attribute based access control
	FDP_ACC.1(c)
	FMT_MSA.3(c)
		-

FDP_ACF.1 (d)
Security attribute based access control
	FDP_ACC.1(d)
	FMT_MSA.3(d)
		-

FDP_ACF.1 (e) Security attribute based access control	FDP_ACC.1e) FMT_MSA.3(e)	-

Functional Requirement	Dependencies of Functional Requirements	
Requirement and its name	Requirement that is dependent on	Requirement that is not dependent on and its rationale

FDP_ACF.1 (f)
Security attribute based access control
	FDP_ACC.1(f)
	FMT_MSA.3(f)
		-

FDP_RIP.1 Subset residual information protection	None	
FIA_AFL.1 Authentication failure handling	FIA_UAU.1	-
FIA_ATD.1 User attribute definition	None	
FIA_SOS.1 Verification of secrets	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1	-
FIA_UAU.7 Protected authentication feedback	FIA_UAU.1	-
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1	-
FMT_MOF.1 Management of security functions behavior	FMT_SMF.1 FMT_SMR.1	-
FMT_MSA.1(a) Management of security attributes	FDP_ACC.1(a) FMT_SMF.1 FMT_SMR.1	-
FMT_MSA.1(b) Management of security attributes	FDP_ACC.1(b) FMT_SMF.1 FMT_SMR.1	-
FMT_MSA.1(c) Management of security attributes	FDP_ACC.1(c) FMT_SMF.1 FMT_SMR.1	-
FMT_MSA.1(d) Management of security attributes	FDP_ACC.1(d) FMT_SMF.1 FMT_SMR.1	-
FMT_MSA.1(e)	FDP_ACC.1(e)	-

Functional Requirement	Dependencies of Functional Requirements	
Requirement and its name	Requirement that is dependent on	Requirement that is not dependent on and its rationale
Management of security attributes	FMT_SMF.1 FMT_SMR.1	
FMT_MSA.1(f) Management of security attributes	FDP_ACC.1(f) FMT_SMF.1 FMT_SMR.1	-
FMT_MSA.3(a) Static attribute initialization	FMT_MSA.1(a) FMT_SMR.1	-
FMT_MSA.3(b) Static attribute initialization	FMT_MSA.1(b) FMT_SMR.1	-
FMT_MSA.3(c) Static attribute initialization	FMT_MSA.1(c) FMT_SMR.1	-
FMT_MSA.3(d) Static attribute initialization	FMT_MSA.1(d) FMT_SMR.1	-
FMT_MSA.3(e) Static attribute initialization	FMT_MSA.1(e) FMT_SMR.1	-
FMT_MSA.3(f) Static attribute initialization	FMT_MSA.1(f) FMT_SMR.1	-
FMT_MTD.1 Management of TSF data	FMT_SMF.1 FMT_SMR.1	-
FMT_SMF.1 Specification of management functions	None	
FMT_SMR.1 Security roles	FIA_UID.1	-
FPT_STM.1 Reliable time stamp	None	
FPT_TST.1 TSF testing	None	
FTA_SSL.3 TSF-initiated termination	None	
FTP_ITC.1	None	

Functional Requirement	Dependencies of Functional Requirements	
Requirement and its name	Requirement that is dependent on	Requirement that is not dependent on and its rationale
Inter-TSF trusted channel		
FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces	FMT_SMF.1 FMT_SMR.1	-

6.3.3. Security Assurance Requirements Rationale

This TOE is Hardcopy Device used in restrictive commercial information processing environments that require a relatively high level of document security, operational accountability, and information assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces.

Agents have limited or no means of infiltrating the TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

EAL 2 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7. TOE SUMMARY SPECIFICATION

This chapter describes the summary specifications of the security functions provided by this TOE.

7.1. Security Functions

Table 38 shows security functional requirements and the corresponding TOE security functions. The security functions described in this section satisfy the TOE security functional requirements that are specified in section 6.1 of this ST.

Table 38 Security Functional Requirements and the Corresponding TOE Security Functions

Security Functions Security Functional Requirements	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT	TSF_INF_FLOW	TSF_S_TEST
FAU_GEN.1						✓			
FAU_GEN.2						✓			
FAU_SAR.1						✓			
FAU_SAR.2						✓			
FAU_STG.1						✓			
FAU_STG.4						✓			
FCS_CKM.1		✓							
FCS_COP.1		✓							
FDP_ACC.1(a)			✓						
FDP_ACC.1(b)			✓						
FDP_ACC.1(c)			✓						
FDP_ACC.1d)			✓						
FDP_ACC.1(e)			✓						
FDP_ACC.1(f)			✓						
FDP_ACF.1(a)			✓						
FDP_ACF.1(b)			✓						
FDP_ACF.1(c)			✓						
FDP_ACF.1(d)			✓						
FDP_ACF.1(e)			✓						
FDP_ACF.1(f)			✓						
FDP_RIP.1	✓								
FIA_AFL.1(a)			✓						

Security Functions Security Functional Requirements	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT	TSF_INF_FLOW	TSF_S_TEST
FIA_AFL.1(b)			✓						
FIA_ATD.1			✓						
FIA_SOS.1			✓						
FIA_UAU.1			✓						
FIA_UAU.7			✓						
FIA_UID.1			✓						
FIA_USB.1			✓						
FMT_MOF.1				✓	✓				
FMT_MSA.1(a)			✓						
FMT_MSA.1(b)			✓						
FMT_MSA.1(c)			✓						
FMT_MSA.1(d)			✓						
FMT_MSA.1(e)			✓						
FMT_MSA.1(f)			✓						
FMT_MSA.3(a)				✓					
FMT_MSA.3(b)				✓					
FMT_MSA.3(c)				✓					
FMT_MSA.3(d)				✓					
FMT_MSA.3(e)				✓					
FMT_MSA.3(f)				✓					
FMT_MTD.1(a)			✓	✓	✓				
FMT_MTD.1(b)			✓	✓					
FMT_SMF.1			✓	✓	✓				
FMT_SMR.1			✓	✓	✓				
FTA_SSL.3			✓						
FTP_ITC.1							✓		
FPT_FDI_EXP.1								✓	
FPT_STM.1						✓			
FPT_TST.1									✓

The summary of each TOE security function and the corresponding security functional requirements are described below.

7.1.1. Hard Disk Data Overwrite (TSF_IOW)

According to Hard Disk Data Overwrite setting which is configured by a system administrator with the system administrator mode, the used document data in the internal HDD are deleted by either three pass overwrite procedure on the document data area when each job of copy, print, network scan, or fax is completed.
Additionally, On Demand Overwrite function is provided to delete the stored data at the specific time scheduled by a system administrator.

(1) FDP_RIP.1 Subset residual information protection
When a job is completed, the TOE overwrites each job using three pass (zero / one / random number) overwrite and verification procedure.
List of the used document data which are to be overwritten and deleted is on the internal HDD. When the existence of the used document data are found in this list at the time of booting the TOE, the overwrite function is performed.

7.1.2. Hard Disk Data Encryption (TSF_CIPHER)

With Hard Disk Data Encryption, the document data are encrypted before stored into the internal HDD when operating any function of copy, print, network scan, and fax or configuring various security function settings.

(1) FCS_CKM.1 Cryptographic key generation
The TOE generates a 256-bit encryption key with SHA-2 algorithm based on FIPS PUB 180-2.

(2) FCS_COP.1 Cryptographic operation
Before storing the document data into the internal HDD, the TOE encrypts the data using the 256-bit cryptographic key generated (FCS_CKM.1) and the AES algorithm based on FIPS PUBS 197. When reading out the stored document data, the TOE decrypts the data also using the 256-bit cryptographic key and the AES algorithm.

7.1.3. User Authentication (TSF_USER_AUTH)

Access to the MFD functions is restricted to the authorized user. A user needs to enter his/her ID and password from the MFD control panel, or Embedded Web Server of the user client.
User authentication is conducted by using the user information registered in MFD or external server.

There are the following two types of authentication depending on how user information is registered.

a) Local Authentication

Authentication is managed by using the user information registered in TOE.

b) Remote Authentication

Authentication is conducted to the remote authentication server. User information is not registered in TOE.

Remote authentication is conducted using the user information managed by the remote authentication server (LDAP server and Kerberos server).

Only the authenticated user can use the following functions:

a) Functions controlled by the MFD control panel

Copy, fax (send), network scan, Faxbox operation, and print (This print function requires the Store Print preset from printer driver. A user must be authenticated from the control panel for print job.)

b) Functions controlled by Embedded Web Server

Display of device condition, display of job status and its log

In addition, access to and setting change of the TOE security functions are restricted to the authorized system administrator. A system administrator needs to enter his/her ID and password from MFD control panel or system administrator client.

(1) FIA_AFL.1(a), FIA_AFL.1(b) Authentication failure handling

The function of the TOE to handle the authentication failures is provided for the system administrator authentication which is performed before accessing the system administrator mode. When the number of unsuccessful authentication attempts with system administrators' IDs reaches 5 times, TOE does not accept login attempts by the user until the MFD main unit is powered off/on.

(2) FIA_ATD.1 User attribute definition

The function of the TOE to define and retain the roles of system administrator, and general user.

(3) FIA_SOS.1 Verification of secrets

When setting a password of a user, the TOE rejects settings if the password is less than the minimum number of characters.

(4) FIA_UAU.1 Timing of authentication
FIA_UID.1 Timing of identification

The TOE requests a user to enter his/her ID and password before permitting him/her to operate the MFD function via Web browser of a user client, or the control panel. The entered user ID and password are verified against the data registered in the TOE setting data.

This identification (FIA_UID.1) and the authentication (FIA_UAU.1) are simultaneously performed, and the operation is allowed only when both of the identification and authentication succeed.

When a print job is received from a user client, the TOE identifies a registered user ID and stores the job without authenticating the user.

When receiving fax data by the public telephone line, the TOE receives the fax data and stores them in Faxbox without user identification and authentication.

(5) FIA_UAU.7 Protected authentication feedback

The TOE offers the function to display the same number of asterisks (`*`) as the entered-password characters on the control panel or Web browser in order to hide the password at the time of user authentication.

(6) FIA_USB.1 User-subject binding

With the authenticated ID, TOE associates the roles of key operator, SA, and general user with the subjects.

(7) FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.1(d), FMT_MSA.1(e), FMT_MSA.1(f) Management of security attributes

As shown in Table 39, the TOE restricts the handling of security attributes to the user whose identity is authenticated by the user authentication function.

Table 39 Management of security attributes

Security Attribute	Operation	Roles
Key operator identifier	Query	system administrator
SA identifier	Query, delete, create	system administrator
General user identifier	Query, delete, create	system administrator,
Functional authority of user	Query, Change	system administrator
Owner identifier of D.DOC (own document data in Faxbox)	Query	system administrator
Owner identifier of D.DOC (own document data in Store Print)	Query, delete, create	system administrator, General user
Owner identifier of D.FUNC (Job data)	Query, delete, create	General user, system administrator

(8) FMT_MTD.1(a), FMT_MTD.1(b) Management of TSF data

FMT_SMF.1 Specification of Management Functions

The TOE provides the user interface for setting password only to the authenticated authorized user.
The setting of password for key operator is limited to key operator, that for SA is limited to key operator and SA, and that for general user is limited to system administrator and the general user (when it is his/her own).

(9) FMT_SMR.1 Security roles
The TOE maintains the roles of key operator, SA, system administrator and general user and associates these roles to the authorized users.

(10) FTA_SSL.3 TSF-initiated termination
The TOE clears the login (authentication session) and requests re-authentication if there is no access to Embedded Web Server from Web browser for a specified period of time (settable from 5 to 60 minutes).
In addition, when there is no operation from the control panel for a specified period of time (settable from 10 to 900 seconds), the setting on the control panel is cleared, returning to the authentication screen.
The session with printer is not retained, and the session ends immediately after processing the request of print.

(11) FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACC.1(c), FDP_ACC.1(d), FDP_ACC.1(e), FDP_ACC.1(f) Subset access control ,
FDP_ACF.1(a), FDP_ACF.1(b), FDP_ACF.1(c), FDP_ACF.1(d), FDP_ACF.1(e), FDP_ACF.1(f) Security attribute based access control
As shown in Table 40, the TOE restricts the operations of basic functions of MFD, copy, fax, scan, and print, to the authenticated user by user authentication function.

Table 40 Access Control for Basic Functions

Function	Permitted Operations and Rules	User
Copy	When Functional authority of user contains permission for the function, copy operation from the control panel is permitted.	system administrator General user
Network Scan	When Functional authority of user contains permission for the function, the following are permitted: Sending of the scanned data from the control panel to user client, FTP server, and Mail server.	
Fax send	When Functional authority of user contains permission for the function, sending of the scanned data from the control panel to remote fax is permitted.	

Function	Permitted Operations and Rules	User
Print Operation	When Functional authority of user contains permission for the function, the following operations are permitted. Storage of the print data from user client to Store Print, and printing of the document data in the print data from the control panel.	
Faxbox Operation	When functional authority of user contains permission for the function, printing of the document data in the Faxbox from the control panel is permitted.	System administrator

As shown in Table 41, TOE restricts the operation on User Data to the authorized user.

Table 41 Access Control for User Data

User Data	Permitted Operations and Rules	User
Copy Data	A copy job permitted by Access Control for Basic Functions is executed. There is no function for deleting D.DOC (Copy Data).	system administrator General user
Scan Data	When a scan job permitted by Access Control for Basic Functions is executed, sending of the scanned data to the FTP server and Mail server is permitted. There is no function for deleting D.DOC (Scan Data).	system administrator General user
Fax Send Data	When a fax job permitted by Access Control for Basic Functions is executed, sending of the fax data to the destination fax device is permitted. There is no function for deleting D.DOC (Fax Send Data).	system administrator General user
Received fax data	Only a system administrator is permitted to print D.DOC (Document data in Faxbox). There is no function for deleting D.DOC (Document data in Faxbox).	system administrator
Document Data in Store Print	When the owner identifier of D.DOC (own document data in Store Print) and the entered user identifier are matched, print and deletion of the own document data in Store Print are permitted.	system administrator General user
Data of a job that is being executed	When the owner identifier of D.FUNC and the entered user identifier are matched, modification or deletion of a copy, scan, fax, or print job that is being executed is permitted.	system administrator General user

With the user authentication function, TOE permits the authenticated user to operate Faxbox, and Store Print as shown in Table 41.

Print is restricted to system adminitrators by storing all received fax data in the Faxbox.

- Store Print Function

When a user sends a print request from the printer driver in which Store Print is preset, after the user has been successfully identified and authenticated, the print data are decomposed into bitmap data, classified according to the user ID, and temporarily stored in the corresponding Store Print area within the internal HDD.

To refer to the stored print data, a user needs to enter his/her ID and password from the control panel. When the user is authenticated, the data on the waiting list corresponding to the user ID are displayed. The user can request printing or deletion of the data on the list.

- Faxbox Function

The received fax data can be stored into Faxbox from public telephone line (Faxcard) which are not shown in Figure 3.

To store the received fax data into Faxbox, user authentication is not required. The received fax data transmitted from remote destination over public telephone line is stored in Faxbox . To refer to print the stored data in the Faxbox, user authentication is required; the MFD compares the user ID and password preset in the MFD against those entered by a system administrator from the control panel.

7.1.4. System Administrator’s Security Management (TSF_FMT)

To grant a privilege to a specific user, this function allows only the authorized system administrator to access the system administrator mode which enables him/her to refer to and configure the settings of the following TOE security functions from the control panel or system administrator client.

(1) FMT_MOF.1 Management of security functions behaviour
FMT_MTD.1(a), FMT_MTD.1(b) Management of TSF data
FMT_SMF.1 Specification of Management Functions

The TOE provides a user interface which allows only the authenticated system administrator to refer to / change the TOE setting data related to the following TOE security functions and to make setting whether to enable/disable each function.
With these functions, the required security management functions are provided.

The settings of the following TOE security functions can be referred to and changed from the control panel.

- Refer to and set the TLS communication;
- Refer to and set the date and time;

With Embedded Web Server function, the settings of the following TOE security functions can be referred to and changed from a system administrator client via Web browser.

- Refer to and set the Hard Disk Data Overwrite;
- Refer to and set the On Demand Overwrite
- Refer to and set the access denial due to authentication failures of system administrator,
- Refer to and set the date and time;
- Refer to and set the Self Test;
- Set the key operator password (only a key operator is privileged);
- Refer to and set the ID of SA and general user and set the password (with local authentication only);
- Refer to and set the minimum password length (with local authentication only);
- Refer to and set the Security Audit Log;
- Refer to and set the TLS communication;
- Refer to and set the IPSec communication;
- Refer to and set the S/MIME communication;
- Download/upload and create an X.509 certificate;
- Refer to and set the User Authentication ;
- Refer to and set the general user permission;
- Refer to and set the Customer Engineer Operation Restriction ;
- Refer to and set the Auto Clear (Control Panel and Embedded Web Server);

(2) FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), FMT_MSA.3(d), FMT_MSA.3(e), FMT_MSA.3(f) Static attribute initialization

The TOE sets to permit all basic functions such as copy, print, network scan, and fax as the default value of security attribute.

Also, the TOE sets the created user identifier and available user identifier for the owner identifier as the default value of security attribute for D.DOC.

Also, the TOE sets the created user identifier and available user identifier for the owner identifier as the default value of security attribute for D.FUNC(job information).

(3) FMT_SMR.1 Security roles

The role of key operator, SA, and system administrator is maintained and the role is associated with an authorized user.

7.1.5. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

A system administrator can restrict CE’s operation in the system administrator mode to prohibit CE from referring to / changing the settings related to System Administrator’s Security Management (TSF_FMT).

This function can prevent setting change by Customer Engineer.

(1) FMT_MOF.1 Management of security functions behaviour
FMT_MTD.1(a) Management of TSF data
FMT_SMF.1 Specification of Management Functions

The TOE provides a user interface which allows only the authenticated system administrator to refer to / change (enable/disable) the TOE settings related to Customer Engineer Operation Restriction from the Embedded Web Server.
With these functions, the required security management functions are provided.

(2) FMT_SMR.1 Security roles

The system administrator's role is maintained and the role is associated with a system administrator.

7.1.6. Security Audit Log (TSF_FAU)

According to Security Audit Log setting which is configured by a system administrator using the system administrator mode, the important events of the TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function. All the TOE users are the targets of this audit log.

(1) FAU_GEN.1 Audit data generation

It is assured that the defined auditable event is recorded in the audit log.
Table 42 shows the details of the audit log.

Table 42 Details of Security Audit Log

The auditable events are recorded with the following fixed size entries:
Log ID: consecutive numbers as an audit log identifier (1 - 60000)
Date: date data (yyyy/mm/dd, mm/dd/yyyy, or dd/mm/yyyy)
Time: time data (hh:mm:ss)
Logged Events: event name (arbitrary characters of up to 32 digits)
User Name: user name (arbitrary characters of up to 32 digits)
Description: description on events
(arbitrary characters of up to 32 digits, see below for details)
Status: status or result of event processing
(arbitrary characters of up to 32 digits, see below for details)
Optionally Logged Items: additional information recorded to audit log（subject identity, etc.）

Logged Events	Description	Status
Change in Device Status		
System Status	Started normally(cold boot)	-
	Started normally(warm boot)	

Logged Events	Description	Status
	Shutdown requested	
	User operation(Local)	Start/End
	Scheduled Image Overwriting started	Successful/Failed
	Scheduled Image Overwriting finished	Successful/Failed
	Self Test	Successful/Failed
User Authentication		
Login/Logout	Login	Successful, Failed(Invalid UserID), Failed(Invalid Password), Failed
	Logout	
	Locked System Administrator Authentication	- (Number of authentication failures recorded)
	Detected continuous Authentication Fail	
Change in Audit Policy		
Audit Policy	Audit Log	Enable/Disable
Job Status		
Job Status	Print	Completed, Completed with Warnings, Canceled by User, Canceled by Shutdown, Aborted, Unknown
	Copy	
	Scan	
	Fax	
	Print Reports	
Change in Device Settings		
Device Settings	Adjust Time	Successful/Failed
	Switch Authentication Mode	Successful (Setting items recorded)
	Change Security Setting	
	View Security Setting	Successful
Access to Data Stored in Device		
Device Data	Import Certificate	Successful/Failed
	Delete Certificate	
	Add Address Entry	
	Delete Address Entry	
	Edit Address Entry	
	Export Audit Log	
Communication Result		
Communication	Trusted Communication	Failed (Protocol and communication destination stored)

(2) FAU_GEN.2 User identity association

TOE records the defined auditable event in the audit log file by associating it with the identity of user who caused the event.

(3) FAU_SAR.1 Audit review

It is assured that all the information recorded in the audit log can be retrieved.
Security audit log data can be downloaded in the form of tab-delimited text by pressing the button "store as a text file." To download security audit log data, TLS communication needs to be enabled before using Web browser.

(4) FAU_SAR.2 Restricted audit review

The person who retrieves the audit log is limited to the authenticated system administrator. A system administrator can access the security audit log data only via Web browser and the access from the control panel is inhibited. Therefore, a system administrator needs to log in from Web browser to access the security audit log data.

(5) FAU_STG.1 Protected audit trail storage

The security audit log data are to be read only, and not to be deleted or modified, thus protected by unauthorized falsification and alternation.

(6) FAU_STG.4 Prevention of audit data loss

When security audit log data are full, the oldest stored audit record is overwritten with the new data so that the new data are not lost but surely recorded.
Auditable events are stored with time stamps into NVRAM. When the number of stored events reaches 50, the 50 logs on NVRAM is stored into one file ("audit log file") within the internal HDD. Up to 15,000 events can be stored. When the number of recorded events exceeds 15,000, the oldest audit log file is overwritten and a new audit event is stored.

(7) FPT_STM.1 Reliable time stamps

The time stamp of TOE's clock function is issued when the defined auditable event is recorded in the audit log file.
By TSF_FMT, only a system administrator is enabled to change the clock setting.

7.1.7. Internal Network Data Protection (TSF_NET_PROT)

Internal Network Data Protection is provided by the following three protocols which are configured by a system administrator using the system administrator mode:

(1) FTP_ITC.1 Inter-TSF trusted channel

The document data, job information, security audit log data, and TOE setting data are protected by the encryption communication protocol that ensures secure data communication between the TOE and the IT products. This trusted path is logically distinct from other communication channel and provides assured identification of its endpoints and protection of the communication data from modification or disclosure.

The followings are the encryption algorithms for network communication provided by the TOE.

Protocol	Target Products.	Encryption Algorithm
TLS	Client PC (Web Browser, Printer Driver) LDAP Server	AES/128 bit AES/256 bit
IPSec	Client PC (Web Browser, Printer Driver) LDAP Server Kerberos Server SMTP Server FTP Server DNS Server	AES/128 bit Triple-DES/168 bit
S/MIME	SMTP Server	Triple-DES/168 bit AES/128 bit AES/192 bit AES/256 bit

a) TLS

According to theTLS communication which is configured by a system administrator using the system administrator mode, TLS ensuring secure data transmission is supported. This protects the security of document data, job information, security audit log data, and TOE setting data on the internal network.

By supporting TLS, the TOE can act as TLS server or TLS client. Moreover, TLS can protect data transmission between the TOE and the remote from interception and alteration. Protection from interception is realized by encrypting transmission data with the following cryptographic keys. A cryptographic key is generated at the time of starting a session and lost at the time of ending the session or powering off the MFD main unit.

- Cryptographic key generated as TLSv1.0/TLSv1.1/TLSv1.2 upon every session
  Specifically, one of the cryptographic suites below is adopted:

Cryptographic Suites of TLS	Cryptographic Method and Size of Secret Key	Hash Method
TLS_RSA_WITH_AES_128_CBC_SHA	AES/128 bits	SHA1
TLS_RSA_WITH_AES_256_CBC_SHA	AES/256 bits	SHA1
TLS_RSA_WITH_AES_128_CBC_SHA256	AES/128 bits	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES/256 bits	SHA256

Protection from the alteration is realized by HMAC (Hashed Message Authentication Code - IETF RFC 2104) of TLS.
When TLS communication is enabled on the Web client, requests from the client must be received via HTTPS. The TLS communication needs to be enabled before IPSec, or S/MIME is enabled or before security audit log data are downloaded by a system administrator.

b) IPSec

According to the IPSec communication which is configured by a system administrator using the system administrator mode, IPSec ensuring secure data transmission is supported. This protects the security of document data, job information, security audit log data, and the TOE setting data on the internal network.
IPSec establishes the security association to determine the parameters (e.g. private key and cryptographic algorithm) to be used in the IPSec communication between the TOE and the remote. After the association is established, all transmission data among the specified IP addresses are encrypted by the transport mode of IPSec until the TOE is powered off or reset. A cryptographic key is generated at the time of starting a session and lost at the time of ending the session or powering off the MFD main unit.

- Cryptographic key generated as IPSec (ESP: Encapsulating Security Payload) at every session
  Specifically, one of the following combinations between secret-key cryptographic method and hash method is adopted:

Cryptographic Method and Size of Secret Key	Hash Method
AES / 128 bits	SHA-1, SHA256, SHA384, SHA512
3-Key Triple-DES /168 bits	SHA-1, SHA256, SHA384, SHA512

c) S/MIME

According to the S/MIME communication which is configured by a system administrator using the system administrator mode, S/MIME ensuring secure mail communication is supported. This protects the security of document data on the internal and external networks.
By S/MIME encrypting mail function, the document data being transmitted to the outside by E-mail are protected from interception.
A cryptographic key is generated at the time of starting mail encryption and lost at the time of completion of the encryption or powering off the MFD main unit.

Secret-key cryptographic method generated as S/MIME protocol for mail encryption

Cryptographic Method and Size of Secret Key
3Key Triple-DES/168 bits
AES / 128 bits
AES / 192 bits
AES / 256 bits

7.1.8. Information Flow Security (TSF_INF_FLOW)

Information Flow Security function restricts the unpermitted communication between external interfaces and shared-medium interfaces (internal network).

(1) FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

TOE provides the following capabilities to restrict the transfer of the received data from external interfaces to the internal network without processing.

External Interface	Restriction on Communication with SMI (Internal Network)
USB (Device)	Interface for receiving print data. Not permitted to transfer the data to other interfaces. (Note: The print job is stored in Store Print)
Public telephone line / Faxcard	Unable to access TOE via Faxcard that is connected with a controller board by an exclusive internal interface, and the data are not transmitted between public telephone line and internal network. Thus, the public telephone line data received by the public telephone line is not transmitted to the internal network.
Ethernet	Unpermitted to transfer the data to other interfaces upon receiving the print data. Unpermitted to receive other user data from the user client or server, and no data are transferred. (Note: The print job is stored in Store Print) When the identification and authentication data are received from user client and the user authentication function is set to remote authentication, TOE sends the identification and authentication data to LDAP server or Kerberos server.
Control Panel	Identification and authentication are required to use functions from the control panel. In addition, there is no function to transfer the data input from the control panel to other interfaces without any instruction.

	When the user authentication function is set to remote authentication, TOE sends the identification and authentication data to LDAP server or Kerberos server.

7.1.9. Self Test (TSF_S_TEST)

TOE can execute a self test function to verify the integrity of TSF executable code and TSF data.

(1) FPT_TST.1 TSF testing

TOE verifies the area of NVRAM and SEEPROM including TSF data upon initiation, and displays an error on the control panel if an error occurs.

However, an error is not detected for the data on security audit log data and time and date as these are not included in the target. Also, at the time of booting the TOE, the TOE calculates the checksum of Controller ROM and Fax ROM to confirm if it matches the specified value, and displays an error on the control panel if an error occurs.

8. ACRONYMS AND TERMINOLOGY

8.1. Acronyms

The following acronyms are used in this ST:

Acronym	Definition
ADF	Auto Document Feeder
CC	Common Criteria
CE	Customer Engineer / Customer Service Engineer
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standard publication
IIT	Image Input Terminal
IOT	Image Output Terminal
IT	Information Technology
IP	Internet Protocol
MFD	Multi Function Device
NVRAM	Non Volatile Random Access Memory
PDL	Page Description Language
PP	Protection Profile
SAR	Security Assurance Requirement
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2. Terminology

The following terms are used in this ST:

Term	Definition
Network Scan	A service to enable the instruction of directly transferring the data from the control panel of the TOE via network (FTP/SMTP protocol) to PC's shared folder, FTP server, and mail server. Also, it enables to designate the conversion to PDF, TIFF, and JPEG, etc.
Faxbox	A location to store the fax document in the TOE. It enables to print the document stored in Faxbox.
Store Print	A function to store the confidential output data temporarily in the TOE and start its output after identification and authentication. When this function is set to [authority of user to only Store Print], normal printing is disabled. It enables a highly-confidential document output without being mixed with other documents.
Embedded Web Server	Embedded Web Server is a service on a Web server in the TOE to confirm the status of the TOE, change settings, job deletion of the TOE via the Web browser of the user client. Embedded Web Server can be used with the Windows standard Web browser.
User Authentication	A function to limit the accessible TOE functions by identifying the user before he/she uses each TOE function. There are two modes, Local Authentication and Remote Authentication, and TOE operates with either one of these authentication modes.
Local Authentication	A mode to manage user authentication of the TOE using the user information registered in the MFD
Remote Authentication	A mode to manage user authentication of the TOE using the user information registered in the remote authentication server.
Hard Disk Data Overwrite	To write over the area of the document data stored in the internal HDD when deleting the data.
On Demand Overwrite	A function to delete and overwrite the document data stored in the internal HDD by manual or scheduled execution.
Decompose Function	A function to analyze and convert the print data written in PDL into bitmap data.
Decompose	To analyze and convert the data written in PDL into bitmap data by decompose function.
System administrator mode	An operation mode that enables a system administrator to refer to and rewrite TOE setting for device operation and that for security functions according to the operational environment. This mode is distinguished from the operation mode that enables a general user to use the MFD functions.

Term	Definition
Auto Clear	A function to automatically logout authentication after a specified period of time passes without any operations from the control panel and Embedded Web Server.
Customer Engineer	Customer service engineer, an engineer who maintains and repairs MFD.
Attacker	A person who accesses TOE or protected property by unauthorized means. It includes the approved user who attempts to access by hiding his/her identity.
Control Panel	A panel on which button, lamp, and touch-screen display necessary for MFD operations are arranged.
General User Client	A client for general user.
System Administrator Client	A client for system administrator. An administrator can refer to and change the TOE setting data of MFD via Web browser.
General Client and Server	Client and server which do not directly engage in the TOE operations
Printer driver	Software to convert the data on a general user client into print data written in page description language (PDL), a readable format for MFD. Used on the user client.
Print Data	The data written in PDL, a readable format for MFD, which are to be converted into bitmap data by the TOE decompose function.
Control Data	The data that are transmitted by command and response interactions. This is one type of the data transmitted between MFD hardware units.
Bitmap Data	The decomposed data of the data read by the copy function and the print data transmitted from a user client to MFD by the print function. Bitmap data are stored into the internal HDD after being compressed in the unique process.
Deletion from the Internal Hard Disk Drive (HDD)	Deletion from the internal HDD means deletion of the management information. When deletion of document data from the internal HDD is requested, only the management information corresponding to the data are deleted. Therefore, user cannot access the document data which were logically deleted. However, the document data themselves are not deleted but remain as the used document data until new data are written in the same storage area.
Original document	Texts, images and photos to be read from IIT in the copy function.
Document Data	Document data means all the data including images transmitted across the MFD when any of copy, print, network scan or fax functions is used by a general user. The document data includes: - Bitmap data read from IIT and printed out from IOT (copy function), - Print data sent by general user client and its decomposed bitmap data (print function),

Term	Definition
	- Bitmap data read from IIT and then stored into the internal HDD (network scan function), - Bitmap data read from IIT and sent to the fax destination and the bitmap data faxed from the sender's machine and printed out from the recipient's IOT (Fax function).
Used Document Data	The remaining data in the MFD internal HDD even after deletion. The document data are first stored into the internal HDD, used, and then only their files are deleted.
Security Audit Log Data	The chronologically recorded data of important events of the TOE. The events such as device failure, configuration change, and user operation are recorded based on when and who caused what event and its result.
Internally Stored Data	The data which are stored in a general user client or in the general client and server, but do not include data regarding TOE functions.
General Data	The data on the internal network. The general data do not include data regarding TOE functions.
TOE Setting Data	The data which are created by the TOE or for the TOE and may affect the TOE security functions. Included in the TSF data, specifically they include the information regarding the functions of Hard Disk Data Overwrite, System Administrator's Security Management, Customer Engineer Operation Restriction, ID and password of users, Access denial due to authentication failure of system administrator, Internal Network Data Protection, Security Audit Log, User Authentication, User permission, Report Print, Auto Clear, Data/Time, and Self Test.
Cryptographic Key	The 256-bit data which is automatically generated. Before the data are stored into the internal HDD, it is encrypted with the cryptographic key.
Network	A general term to indicate both external and internal networks.
External Network	The network which cannot be managed by the organization that manages the TOE. This does not include the internal network.
Internal Network	Channels between MFD and highly reliable remote server / client PC. The channels are located in the network of the organization, the owner of the TOE, and are protected from the security risks coming from the external network.
Public Telephone Line/Network	Line/network of transmitting/receiving fax data.
Public Telephone Line Data Fax data	Transmitted/received data over the public telephone line of fax.
Certificate	Defined in the X.509 which is recommended by ITU-T. The data for user authentication (name, identification name, organization where he/she belongs to, etc.), public key, expiry date, serial number, signature, etc.

9. REFERENCES

The following documentation was used to prepare this ST.

Short Name	Document Title
[CC Part 1]	Part 1: Introduction and general model (September 2012 Version 3.1 Revision 4) Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 1: Introduction and general model, dated September 2012, CCMB-2012-09-001 (Japanese version 1.0, dated November 2012, translated by Information-Technology Promotion Agency, Japan)
[CC Part 2]	Part 2: Security functional components (September 2012 Version 3.1 Revision 4) Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 2: Security functional components, dated September 2012, CCMB-2012-09-002 (Japanese version 1.0, dated November 2012, translated by Information-Technology Promotion Agency, Japan)
[CC Part 3]	Part 3: Security assurance components (September 2012 Version 3.1 Revision 4) Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 3: Security assurance components, dated September 2012, CCMB-2012-09-003 (Japanese version1.0, dated November 2012, translated by Information-Technology Promotion Agency, Japan)
[CEM]	Common Methodology for Information Technology Security Evaluation - Version 3.1 Evaluation Methodology, dated September 2012, CCMB-2012-09-004 (Japanese version 1.0, dated November, translated by Information-Technology Promotion Agency, Japan)
[PP]	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2 TM -2009)