Xerox 4112/4127 Copier/Printer

Security Target

Version 1.0.9

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

- 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 4112/4127 Copier/Printer Security Target
ST Version:	V 1.0.9
Publication Date:	January 27, 2010
Author:	Fuji Xerox Co., Ltd.

1.2. TOE Reference

This section provides information needed to identify this TOE.

The TOE of Xerox 4112 Copier/Printer and Xerox 4127 Copier/Printer are identical and identified as the following TOE name and ROM version:

TOE Identification:	Xerox 4112/4127 Copier/Printer	
Version:	・Controller+PS ROM	Ver. 1.211.8
	・IOT ROM	Ver. 46.18.0
	・IIT ROM	Ver. 15.6.1
	・IIT Option ROM	Ver. 14.0.4
	・ADF ROM	Ver. 12.2.7
Manufacturer:	Fuji Xerox Co., Ltd.	

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 Xerox 4112/4127 Copier/Printer (hereinafter referred to as “MFD”) which has copy, print, and scan functions.

The TOE is the product which controls the whole MFD and protects the data that is transmitted over the encryption communication protocols. These protocols protect the security of the TOE setting data, the security audit log data and the document data on the internal network between TOE and the remote.

The TOE also protects from unauthorized disclosure, the security audit log data, the document data and the used document data in the internal HDD.

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 - CWIS - Copy - Print - Scan - Network Scan
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

- The Data Security Kit, an option, must be used to obtain the security features of the TOE.
- To use print and scan functions, the following items shall be installed to the external client for general user and that for system administrator
  : print driver, scan driver, and Network Scan Utility.

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 it out from IOT according to the general user's instruction from the control panel. Also, as a function to store the copies, it is possible to concurrently print and save the reprint data to IOT, and also to save the data for reprint.When more than one copy is ordered for one original, the data read from IIT is first stored into the MFD internal HDD. Then, the stored data is read out from the HDD as needed 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.
- CWIS (CentreWare Internet Service) is to retrieve the document data scanned by MFD from Mailbox.
  It also enables a system administrator to refer to and rewrite TOE setting data via Web browser.
- Scan function Control Panel function are to read the original data from IIT and store it into Mailbox within the MFD internal HDD, according to the general user's instruction from the control panel.

The stored document data can be retrieved via standard Web browser by CWIS or Network Scan Utility.

- Network Scan function and Control Panel function are to read the original data from IIT and transmit the document data to FTP server, SMB 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.

The TOE provides the following security features:

- Hard Disk Data Overwrite
  To completely delete the used document data in the internal HDD, the data is overwritten with new data after any function of copy, print, scan, etc. is completed.
- Hard Disk Data Encryption
  The document data and the security audit log data are encrypted before being stored into the internal HDD when operating any function of copy, print, scan, etc. or configuring various security function settings.
- User Authentication
  Access to the TOE functions is restricted to the authorized user and this function identifies and authenticates users. A user needs to enter his/her ID and password from the print driver, Network Scan Utility, or CWIS of the general user client, or MFD control panel.
- 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.
- Customer Engineer Operation Restriction
  A system administrator can inhibit CE from referring to / changing the TOE security function settings.
- 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.
- Internal Network Data Protection
  This function protects the communication data on the internal network such as document data, security audit log data, and TOE setting data. (The following general encryption communication- protocols are supported: SSL/TLS, IPSec, SNMP v3, and S/MIME.)

1.3.2. Environment Assumptions

This TOE is assumed to be used as an IT product at general office and to be linked to user clients, and the internal network protected from threats on the external network by firewall etc.

Figure 1 shows the intended environment for TOE operation.

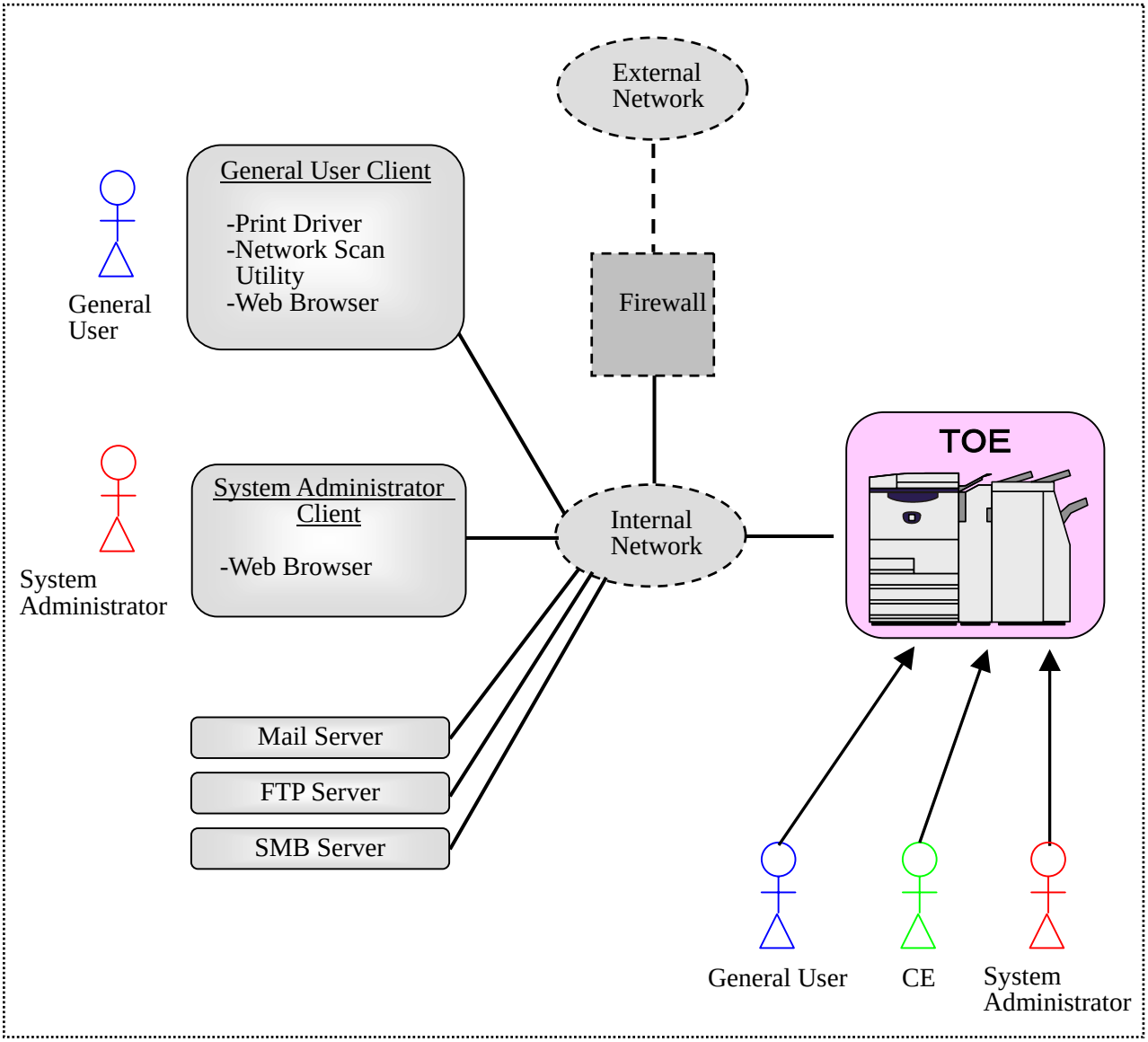

Figure 1: Intended Operational Environment

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 linked to the MFD via the internal network and the print driver and Network Scan Utility are installed to the client, the general user can request the MFD to print, and retrieve the document data.
The user can also request the MFD to retrieve the scanned document data via Web browser. Additionally, the user can change the settings which he/she registered to the MFD: Mailbox name, password, access control, and automatic deletion of document.
When the client is linked to the MFD directly via USB and print 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) SMB server:
The hardware/OS is a general-purpose PC or server. The MFD sends document data to SMB server via SMB.

The OS's of general user client (1) and system administrator client (2) are assumed to be Windows 2000, Windows XP, and Windows Vista.

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

User	Role Description
Administrator of the organization	An administrator or responsible official of the organization which owns and uses TOE.
General user	A user of TOE functions such as copy, print.
System administrator (Key operator + System Administrator Privilege [SA])	A user who is authorized to manage the device using the system administrator mode. A system administrator can refer to and rewrite the TOE setting for device operation and that for security functions via TOE control panel, and Web browser.
Customer engineer (CE)	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 consists of each function of the programs.

Figure 2 shows the logical architecture of the MFD.

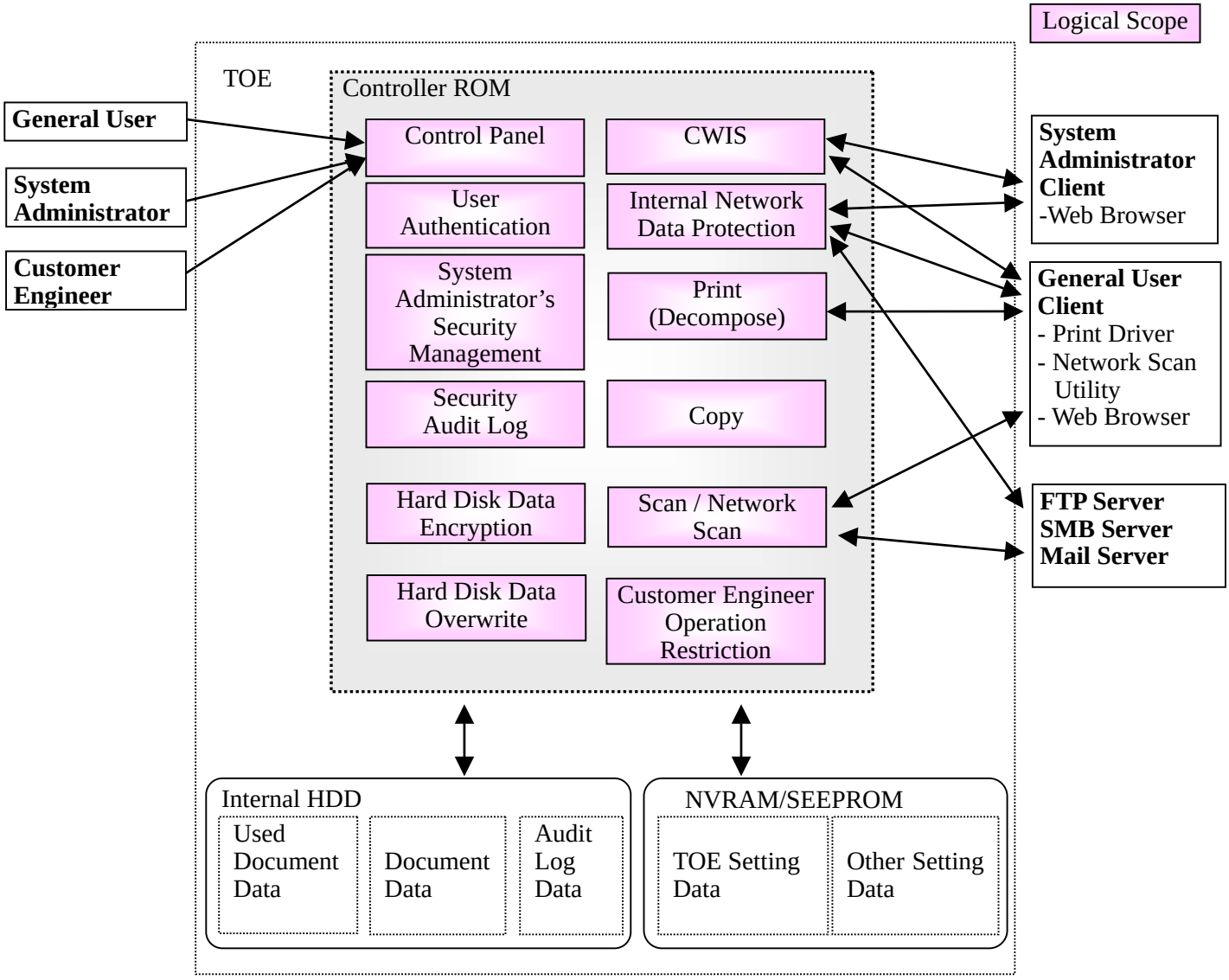

Figure 2: MFD Units and TOE Logical Scope

1.4.2.1. Basic Functions

The TOE provides the functions of control panel, copy, print, scan, network scan, and CWIS to general user.

Table 3: TOE Basic Functions

Function	Description
Control Panel Function	Control panel function is a user interface function for general user, CE, and system administrator to operate MFD functions.
Copy Function	Copy function is to read the original data from IIT and print it out from IOT according to the general user's instruction from the control panel. Also, as a function to store the copies, it is possible to concurrently print and save the reprint data to IOT, and also to save the data for reprint. When more than one copy is ordered for one original, the data read from IIT is first stored into the MFD internal HDD. Then, the stored data is read out from the HDD as needed 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 print driver is 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 is printed out from IOT directly after decomposed and the Store Print in which the bitmap data is temporarily stored in the internal HDD and then printed out from IOT according to the general user's instruction from the control panel.
Scan Function, Network Scan Function	Scan function is to read the original data from IIT and then store it into the internal HDD according to the general user's instruction from the control panel. A general user can retrieve the stored document data from a general user client via CWIS or Network Scan Utility. Network scan function is to read the original data from IIT and automatically transmit it to a general user client, FTP server, Mail server, or SMB server according to the information set in the MFD. A general user can request this function from the control panel.
CWIS Function	CWIS is to retrieve, from the internal HDD, the scanned document data according to the instruction from Web browser of a general user client. CWIS also 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 is overwritten with new data after each job (copy, print, scan, Network Scan) is completed. Without this function, the used document data remains and only its management data is deleted.

Additionally, Scheduled Image 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 security audit log data and the document data in Mail Box remain in the internal HDD even if the machine is powered off. To solve this problem, the document data and security audit log data are encrypted before being stored into the internal HDD when operating any function of copy, print, scan, network scan, or configuring various security function settings.

(3) User Authentication

Access to the MFD functions is restricted to the authorized user. A general user needs to enter his/her ID and password from MFD control panel, print driver, Network Scan Utility, or CWIS of the user client.

Only the authenticated general user can use the following functions:

a) Functions controlled by the MFD control panel:
Copy, scan, network scan, Mailbox, and print (This print function requires user ID and password preset from print driver. A user must be authenticated from the control panel for print job.)

b) Functions controlled by Network Scan Utility of user client:
Function to retrieve document data from Mailbox

c) Functions controlled by CWIS:
Display of device condition, display of job status and its log, function to retrieve document data from Mailbox, and print function by file designation

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 a legitimate user:
The print function (Private Print function) and the Mailbox function, which require user authentication from the control panel,
The function to retrieve document data from Mailbox which requires user authentication from CWIS or Network Scan Utility (Mailbox function), and the Store Print function by file designation from CWIS (Private Print function).

Figure 3 shows the authentication flow of the above functions.

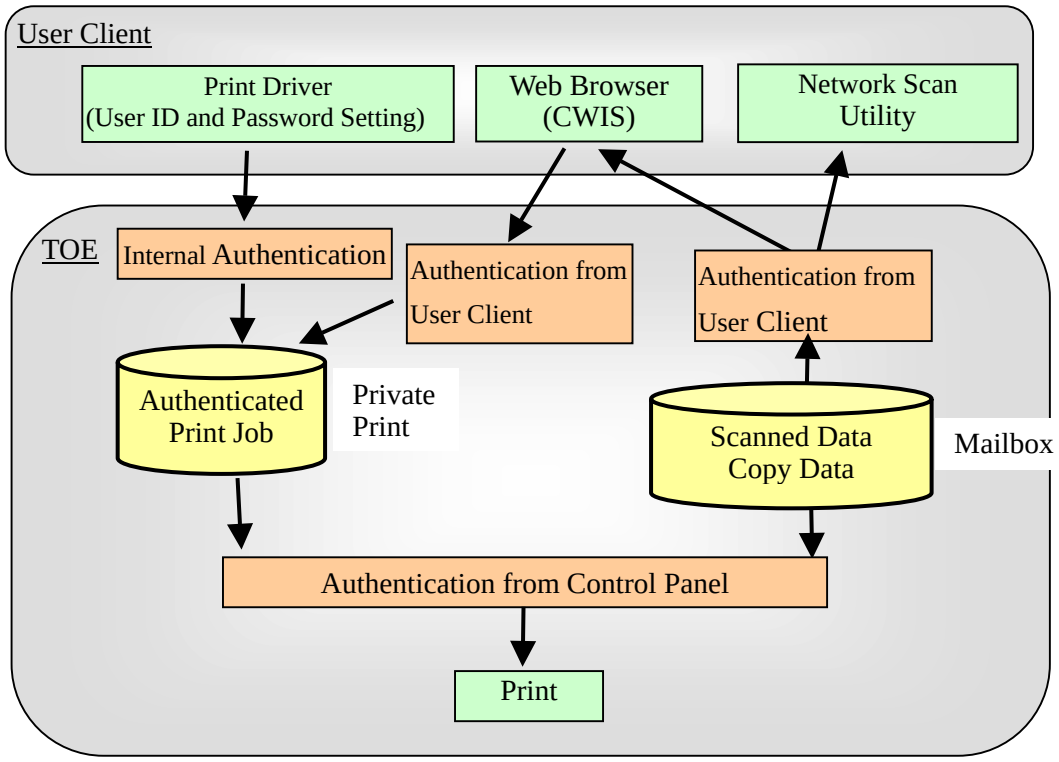

Figure 3: Authentication Flow for Private Print and Mailbox

- Store Print Function (Private Print Function)

To enable this function, the user needs to configure the MFD to "store an authenticated job to Private Print area*" and also needs to preset his/her ID and password from print driver of a user client. When a user sends a print request from print driver, the MFD compares the user ID and password against those preset in the MFD. Only when the user is authenticated, the print data is decomposed into bitmap data. Then, the data is classified according to the user ID and temporarily stored in the corresponding Private Print area within the internal HDD. (*Private Print area means the storage area of data for Private Print.)

The user can also enable this function by entering his/her ID and password from CWIS for authentication and by sending a print request with designating the files within a user client.

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

- Mailbox Function

The copy data and scanned data can be stored into Mailbox from IIT which is not shown in Figure 3.

To store the copy data and scanned data into Mailbox, a user needs to enter his/her ID and password from the control panel and needs to be authenticated to use copy and scan functions. Then, the document data can be scanned from IIT and stored into the internal HDD according to the user's instruction to store copies or scan from the control panel.

To refer to, retrieve, print, or delete the stored data in the Personal Mailbox corresponding to the each registered user's ID, user authentication is required; the MFD compares the user ID and password preset in the device against those entered by a user from the control panel, CWIS, or Network Scan Utility.

(4) System Administrator's Security Management

To accord 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 Hard Disk Data Overwrite;
- Refer to and set Hard Disk Data Encryption;
- Set the cryptographic seed key for Hard Disk Data Encryption;
- Refer to and set use the password entered from MFD control panel in user authentication;
- Set the ID and password of key operator (only a key operator is privileged);
- Refer to and set the ID of SA / general user and set the password;
- Refer to and set the set of access denial due to system administrator's authentication failures;
- Refer to and set the limit of user password length (for general user and SA);
- Refer to and set the SSL/TLS communication;
- Refer to and set the IPSec communication;
- Refer to and set the S/MIME communication
- Refer to and set the Scheduled Image Overwrite;
- Refer to and set the User Authentication;
- Refer to and set the Store Print;
- Refer to and set the date and time;

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

- Set the ID 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;
- Refer to the setting of access denial due to system administrator's authentication failures;
- Refer to and set the limit of user password length (for general user and SA);
- Refer to and set Audit Log;
- Refer to and set the SSL/TLS communication;
- Refer to and set the IPSec communication;
- Refer to and set the SNMPv3 communication;
- Refer to and set the SNMPv3 authentication password.
- Refer to and set the S/MIME communication;
- Create/upload/download an X.509 certificate;
- Refer to and set the Scheduled Image Overwrite;
- Refer to and set the User Authentication;

(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 the control panel and CWIS. 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 it in the form of tab-delimited text file via Web browser using CWIS. To download the log data, SSL/TLS communication needs to be enabled.

(7) Internal Network Data Protection

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

- SSL/TLS
- IPSec
- SNMP v3
- S/MIME

1.4.3. Physical Scope and Boundary

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

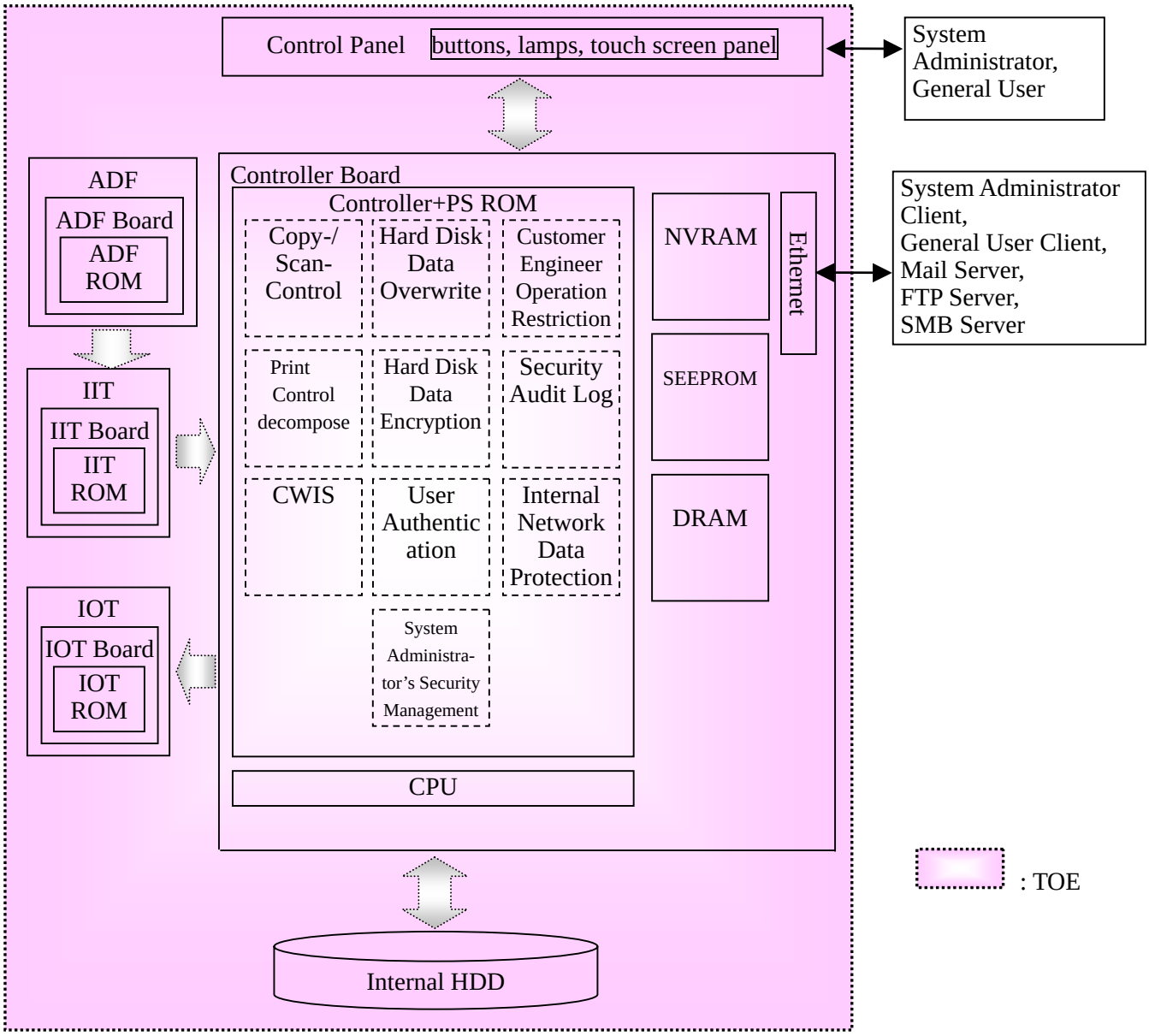

Figure 4: MFD Units and TOE Physical Scope

The MFD consists of the PWB units of controller board and control panel, IIT, and IOT, ADF.
The controller board is connected to the control panel via the internal interfaces which transmit control data, to the IIT board and IOT board via the internal interfaces which transmit document data and control data, and to
The controller board is a PWB which controls MFD functions of copy, print, scan.
The board has a network interface (Ethernet) and local interfaces (USB) and is connected to the IIT

board and IOT board.
The control panel is a panel on which buttons, lamps, and a touch screen panel are mounted to enable MFD functions of copy, scan
The IIT (Image Input Terminal) is a device to scan an original and send its data to the controller board for copy, print, scan,
The IOT (Image Output Terminal) is a device to output image data which was sent from the controller board.
The ADF(Auto Document Feeder) is a device to transfer original documents to IIT.

1.4.4. Guidance

The following are the guidance documents for this TOE.
Xerox 4112/4127 Copier/Printer System Administration Guide
Xerox 4112/4127 Copier/Printer User Guide
Xerox 4112/4127 Copier/Printer Security Function Supplementary Guide

2. CONFORMANCE CLAIMS

2.1. CC Conformance Claims

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

Part 1: Introduction and general model, Version 3.1 Translation revision 1.2, dated March 2007,
Part 2: Security functional requirements, Version 3.1 Translation revision 2.0, dated March 2008
Part 3: Security assurance requirements, Version 3.1 Translation revision 2.0, dated March 2008

The security functional requirements of this ST conform to CC Part 2.
The security assurance requirements of this ST conform to CC Part 3.

2.2. PP Claims, Package Claims

2.2.1. PP Claims

There is no applicable Protection Profile.

2.2.2. Package Claims

This ST conforms to EAL3.

2.2.3. Conformance Rationale

There is no applicable PP rationale since this ST does not conform 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 (Figure 5):

(1) Right to use MFD functions

The general user's right to use each function of TOE is assumed as an asset to be protected.

(2) Document data stored for job processing

When a general user uses MFD functions of copy, print, and scan, the document data is temporarily stored in the internal HDD for image processing, transmission, and Store Print. The user can retrieve the stored document data in the MFD from a general user client by CWIS function and Network Scan Utility. The stored data includes general user's confidential information and is assumed as an asset to be protected.

(3) Used document data

When a general user uses MFD functions of copy, print, and scan, the document data is 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. The residual data includes general user's confidential information and is assumed as an asset to be protected.

(4) Security audit log data

In the function of Security Audit Log, the important events such as device failure, configuration change and user operation are recorded based on when and who operated what function. For preventive maintenance and response to the events and detection of unauthorized access, only a system administrator can retrieve the log data stored in MFD by CWIS function. The log data is assumed as an asset to be protected.

(5) TOE setting data

A system administrator can set TOE security functions from the MFD control panel or system administrator client by the function of System Administrator's Security Management. The setting data stored in the TOE (see Table 4) can be a threat to other assets if used without authorization and is assumed as an asset to be protected.

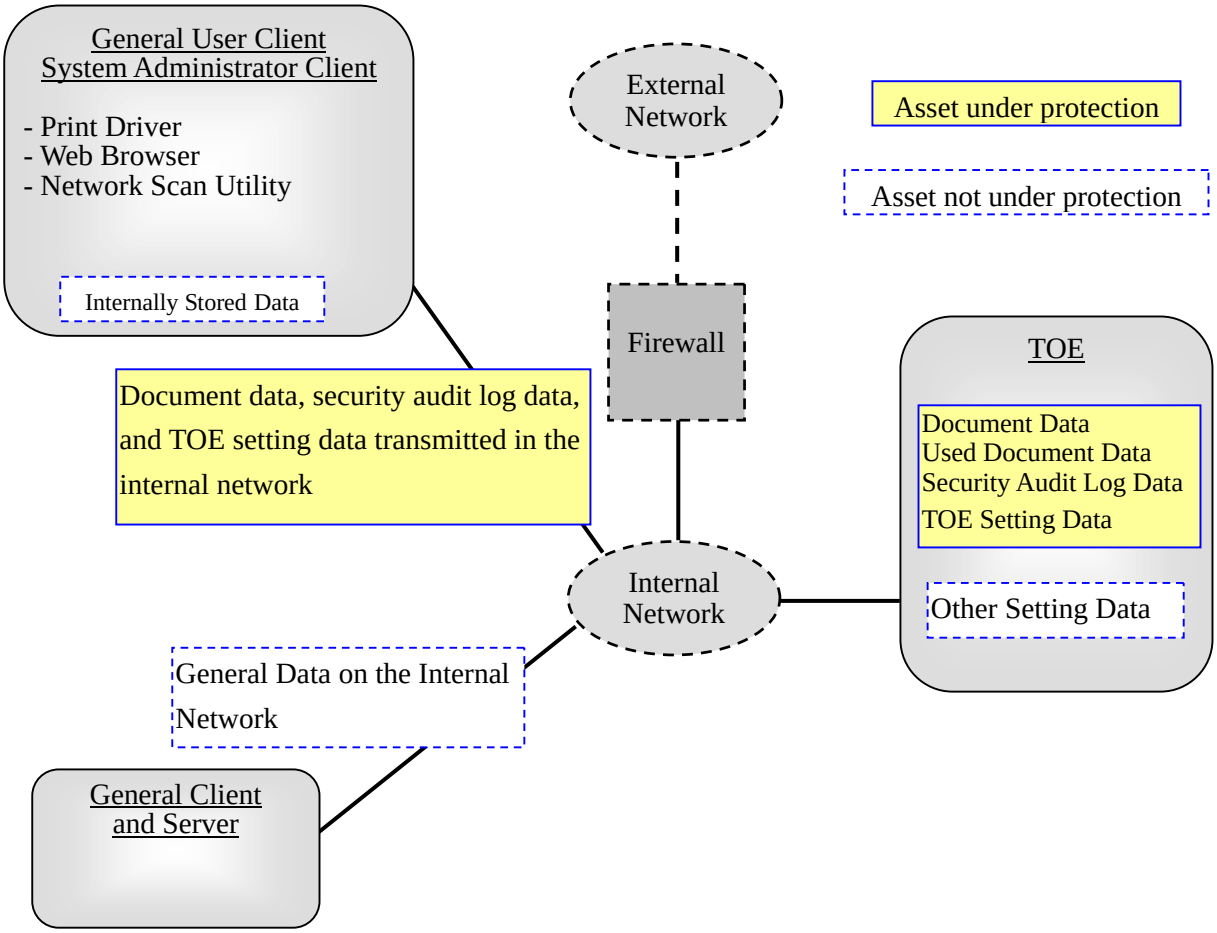

Figure 5: Assets under and not under Protection

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.

Table 4 categorizes the TOE setting data recorded on NVRAM and SEEPROM of the controller board.

Table 4: Categories of TOE Setting Data

Categories of TOE Setting Data (Note)
Data on Hard Disk Data Overwrite
Data on Hard Disk Data Encryption
Data on use of password entered from MFD control panel in user authentication
Data on minimum password length of user password
Data on ID and password of system administrator
Data on access denial due to authentication failures of system administrator
Data on Customer Engineer Operation Restriction
Data on Internal Network Data Protection

Categories of TOE Setting Data (Note)
Data on Security Audit Log
Data on Mailbox
Data on User Authentication
Data on Store print
Data on date and time

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

3.1.2. Threats

Table 5 identifies the threats addressed by the TOE. An attacker is considered to have public knowledge of how the TOE operates and low-level attack capability.

Table 5: Threats Addressed by the TOE

Threat (Identifier)	Description
T.RECOVER	An attacker may remove the internal HDD and connect it to commercial tools so that he/she can read out and leak the document data, used document data, security audit log data from the HDD without authorization.
T.CONFDATA	An attacker may access, read, or alter, from control panel or system administrator client, the TOE setting data which only a system administrator is allowed to access.
T.DATA_SEC	An attacker may read document data and security audit log data from control panel or Web browser without authorization.
T.COMM_TAP	An attacker may intercept or alter document data, security audit log data, and TOE setting data on the internal network.
T.CONSUME	An attacker may access TOE and use TOE functions without authorization.

3.2. Organizational Security Policies

There is no organizational security policy the TOE must comply with.

3.3. Assumptions

Table 6 shows the assumptions for the operation and use of this TOE.

Table 6: Assumptions

Assumption (Identifier)	Description
Personnel Confidence	
A.ADMIN	A system administrator shall have the necessary knowledge of TOE security functions to perform the given role of managing the TOE and shall not operate the TOE with malicious intent.
Protection Mode	
A.SECMODE	A system administrator shall configure the TOE as follows. ・ Use of password entered from MFD control panel in user authentication: enabled. ・ Length of system administrator password: 9 characters or more ・ Access denial due to authentication failure of system administrator: enabled ・ Allowable number of system administrator's authentication failures before access denial: 5 ・ Customer Engineer Operation Restriction: enabled ・ User authentication setting: enabled (select Local Authentication) ・ Length of user password (for general user and SA): 9 characters or more ・ Private Print setting: store authenticated jobs to Private Print area ・ Audit Log setting: enabled ・ SNMP v3 communication: enabled ・ SNMP v1/v2c communication: disabled ・ Length of authentication password for SNMP v3 communication: 8 characters or more ・ SSL/TLS communication: enabled ・ IPSec communication: enabled ・ S/MIME communication: enabled ・ SMB communication: NetBEUI disabled ・ Hard Disk Data Overwrite: enabled ・ Hard Disk Data Encryption: enabled ・ Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters

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 7 defines the security objectives to be accomplished by the TOE.

Table 7: Security Objectives for the TOE

Security Objectives(Identifier)	Description
O.AUDITS	The TOE must provide Security Audit Log and its log data which are necessary to monitor unauthorized access.
O.CIPHER	The TOE must encrypt the document data, used document data, and security audit log data to be stored into the HDD so that they cannot be analyzed even if retrieved.
O.COMM_SEC	The TOE must provide encryption communication function to protect the document data, security audit log data, and TOE setting data on the internal network between TOE and the remote from interception and alteration.
O.MANAGE	The TOE must inhibit a general user from accessing TOE setting data. The TOE allows only the authenticated system administrator to access the system administrator mode which enables him/her to configure the security functions.
O.RESIDUAL	The TOE must provide overwrite function to prevent the used document data in the internal HDD from being reproduced or recovered.
O.USER	The TOE must provide the function to identify TOE user and allow only the legitimate user to store, retrieve, and delete the document data and to change the password.
O.RESTRICT	The TOE must inhibit an unauthorized user from using the TOE.

4.2. Security Objectives for the Environment

Table 8 defines the security objectives for the TOE environment.

Table 8: Security Objectives for the Environment

Security Objectives(Identifier)	Description
OE.ADMIN	A system administrator who is assigned by an organization administrator as an appropriate and reliable person for this TOE management, and who receives necessary training to manage the TOE and performs the TOE management according to the guidance.
OE.AUTH	A system administrator shall configure the TOE security functions as follows. ・ Use of password entered from MFD control panel in user authentication: enabled ・ Length of system administrator password: 9 characters or more ・ Access denial due to authentication failure of system administrator: enabled ・ Allowable number of system administrator's authentication failures before access denial: 5 ・ Customer Engineer Operation Restriction: enabled ・ User authentication setting: enabled (select Local Authentication) ・ Length of user password (for general user and SA): 9 characters or more ・ Private Print setting: store authenticated jobs to Private Print area
OE.COMMS_SEC	A system administrator needs to configure the TOE as follows so that the document data, security audit log data, and TOE setting data are protected from interception. ・ SNMP v3 communication: enabled ・ SNMP v1/v2c communication: disabled ・ Length of authentication password for SNMP v3 communication: 8 characters or more ・ SSL/TLS communication: enabled ・ IPSec communication: enabled ・ S/MIME communication: enabled ・ SMB communication: NetBEUI disabled
OE.FUNCTION	A system administrator shall configure the TOE security functions as follows. ・ Hard Disk Data Overwrite: enabled ・ Hard Disk Data Encryption: enabled ・ Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters

Security Objectives(Identifier)	Description
	・ Audit Log: enabled

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 9 shows the correspondences between the security objectives and the assumptions / threats / organizational security policies. Moreover, Table 10 shows that each defined security problem is covered by the security objectives.

Table 9: Correspondences between Security Objectives and Assumptions / Threats / Organizational Security Policies

Security Problems / Security Objectives	A.ADMIN	A.SECMODE	T.RECOVER	T.CONFDATA	T.COMM_TAP	T.DATA_SEC	T.CONSUME
O.AUDITS				✓		✓	
O.CIPHER			✓				
O.COMM_SEC					✓		
O.MANAGE				✓		✓	
O.RESIDUAL			✓				
O.USER				✓		✓	
O.RESTRICT							✓
OE.ADMIN	✓						
OE.AUTH		✓		✓		✓	
OE.COMM_SEC		✓			✓		
OE.FUNCTION		✓	✓	✓		✓	

Table 10: Security Objectives Rationale for Security Problem

Security Problem	Security Objectives Rationale
A.ADMIN	By satisfying the following objective, A.ADMIN can be realized: By OE.ADMIN, a system administrator is assigned by an organization administrator as an appropriate and reliable person for this TOE management, and receives necessary training to manage the TOE to perform the TOE management according to the guidance.

Security Problem	Security Objectives Rationale
A.SECMODE	By satisfying the following objectives, A.SECMODE can be realized: By OE.AUTH, a system administrator sets an appropriate ID and password and enables user authentication and Customer Engineer Operation Restriction. By OE.COMMS_SEC, the internal network data (incl. document data, security audit log data, and TOE setting data) are protected from interception. By OE.FUNCTION, Hard Disk Data Overwrite, Hard Disk Data Encryption, and Security Audit Log are enabled, which disables the recovery of the used document data in the internal HDD.
T.RECOVER	By satisfying the following objective, T.RECOVER can be countered: By OE.FUNCTION, it is necessary to enable the TOE security functions (i.e. Hard Disk Data Overwrite and Hard Disk Data Encryption) and disable the reading-out of the document data and security audit log data in the internal HDD as well as the recovery of the used document data. To be specific, this threat can be countered by the following security objectives: O.CIPHER and O.RESIDUAL. By O.CIPHER, the document data and security audit log data in the internal HDD are encrypted to disable the reference and reading-out of the document data, used document data, and security audit log data. By O.RESIDUAL, the used document data is overwritten and deleted to disable the recovery and reproduction of the used document data stored in the internal HDD.
T.CONFDATA	By satisfying the following objective, T.CONFDATA can be countered: By OE.AUTH and OE.FUNCTION, it is necessary to enable the security functions (i.e. User Authentication with Password, System Administrator Password, Access Denial due to System Administrator's Authentication Failures, Customer Engineer Operation Restriction, and Audit Log) and permits only the authenticated system administrator to change the TOE setting data. To be specific, this threat can be countered by the following security objectives, O.MANAGE, O.USER, and O.AUDITS: By O.MANAGE, only the authenticated system administrator is allowed to enable/disable the TOE security functions and to refer to / update the TOE setting data. By O.USER, only the legitimate user is allowed to change the password. By O.AUDITS, the audit log function necessary to monitor unauthorized access and the security audit log data are provided.

Security Problem	Security Objectives Rationale
T.CONSUME	By satisfying the following objective, T.CONSUME can be countered. By O.RESTRICT, the access to the TOE can be controlled.
T.COMM_TAP	By satisfying the following objectives, T.COMM_TAP can be countered. By O.COMM_SEC, the client/server authentication function of encryption communication protocol allows only the legitimate user to send/receive the communication data. Encrypting communication data with encryption function also disables the interception and alteration of the internal network data (incl. document data, security audit log data, and TOE setting data). By OE.COMMS_SEC, the document data, security audit log data, and TOE setting data on the internal network can be protected from interception.
T.DATA_SEC	By satisfying the following objectives, T.DATA_SEC can be countered. By OE.AUTH and OE.FUNCTION, it is necessary to enable the following passwords, user authentication function, and security audit log function: User Password, System Administrator Password, Local Authentication, Security Audit Log. Then, only the authenticated user is allowed to access the security audit log data and document data. By O.USER, only the authenticated user is allowed to read out the document data and security audit log data stored in the internal HDD. By O.MANAGE, only the authenticated system administrator is allowed to configure the TOE security functions. By O.AUDITS, the audit log function necessary to monitor unauthorized access and the security audit log data are provided.

5. EXTENDED COMPONENTS DEFINITION

5.1. Extended Components

This ST conforms to CC Part 2 and CC Part 3, and there are no extended components which shall be defined.

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 Process	Operation at using Mailbox and Store Print with the user authentication of key operator succeeded.
SA Process	Operation at using Mailbox and Store Print with the user authentication of SA succeeded.
General User Process	Operation at using Mailbox and Store Print with the user authentication of general user succeeded.

- Object

Term/phrase	Definition
Mailbox	A logical box created in the MFD internal HDD. Mailbox can store the scanned document data categorizing by users and senders. Mailbox is categorized into Personal Mailbox and Shared Mailbox.
Personal Mailbox	The Mailbox privately used by a general user. Each user can create his/her own Personal Mailbox.
Shared Mailbox	The Mailbox shared by any general user. Key operator can create the Shared Mailbox.
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 general 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 is first stored into the internal HDD, used, and then only its file is deleted.
Document data	Document data means all the image data transmitted across the MFD when any of copy, print, scan functions is operated by a general user.
Security Audit Log	The chronologically recorded data of important events of 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
Modify of behavior	To change the settings of the following information: ・ User Authentication(Local, Remote) ・ Store Print(Save or Deletion of login failure job)) ・ Internal Network Data Protection(Certificate and encryption type) ・ Hard Disk Data Overwrite(number of overwrite, data of overwrite)
Modify	Changes of TSF data and security attributes.

- Security attributes

Term/phrase	Definition
General User Role	Indicates the authority required for general user to use TOE.
SA Role	Indicates the authority required for SA to use TOE.
Key Operator Role	Indicates the authority required for key operator to use TOE.
General User identity	User ID and password used to authenticate and identify general user.
SA identity	User ID and password used to authenticate and identify SA.
Key Operator identity	User ID and password used to authenticate and identify key operator.
Owner identity of Personal Mailbox (Personal, Shared)	Data on each Mailbox, incl. permitted user, box name, password, conditions for deleting documents, etc.
Owner identity of Store Print area	Data on Private Print, incl. user ID, password, measures to be taken at authentication failure, etc.

- Entity outside TOE

Term/phrase	Definition
System Administrator	This term covers both key operator and SA.
Key Operator	An authorized user who manages MFD maintenance and makes TOE security function settings.
System Administrator Privilege (SA)	The user(s) 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.
General User	Any person who uses copy, scan, and print functions of

	MFD.

- Other terminology

Term/phrase	Definition
The Fuji Xerox's standard method, FXOSENC	The Fuji Xerox's standard algorithm to generate a cryptographic key. This is used when MFD is booted.
AES	The FIPS-standard encryption algorithm used for encryption/decryption of Hard Disk data.
Access denial due to authentication failure of system administrator ID	When the defined number of unsuccessful authentication attempts with system administrator ID has been met, the control panel does not accept any operation except power cycle, and the web browser does not accept authentication operation until the MFD main unit is powered off/on.
Data on use of password entered from MFD control panel in user authentication	The data on whether to enable/disable the use of password to be entered from MFD control panel in user authentication. Included in the TOE setting data.
Data on ID of key operator	ID data for key operator authentication. Included in the TOE setting data.
Data on password of key operator	Password data for key operator authentication. Included in the TOE setting data.
Data on ID of SA	ID data for SA authentication. Included in the TOE setting data.
Data on password of SA	Password data for SA authentication. Included in the TOE setting data.
Data on ID of General User	ID data for general user authentication. Included in the TOE setting data.
Data on password of General User	Password data for general user 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. It also incorporates 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 TOE such as device failure, configuration change, and user operation, based on when and who operated what function.

Data on User Authentication	The data on whether to enable/disable the authentication function using the data on user authentication for using copy, scan and print functions of MFD. It also incorporates the data on the authentication method.
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, security audit log data, and TOE setting data. It also incorporates the data on the setting.
Data on Customer Engineer Operation Restriction-	The data on whether to enable/disable Customer Engineer Operation Restriction. Included in the TOE setting data.
Data on Hard Disk Data Encryption	The data on whether to enable/disable the functions related to Hard Disk Data Encryption. It also incorporates the data on the encryption seed key. 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. It also incorporates the data on the number of pass (overwrite procedure). Included in the TOE setting data.
Data on date and time	The horologe information to manage log. Included in the TOE setting data.
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.
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.
Print 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.
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFD.

6.1. Security Functional Requirements

Security functional requirements which the TOE offers are described below. The security functional requirements are based on the class and component which are specified by the [CC part 2].

6.1.1. Class FAU: Security audit

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

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

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

[selection, choose one of: minimum, basic, detailed, not specified]
- not specified
[assignment: other specifically defined auditable events]
- the actions to be audited (defined by CC) and the corresponding auditable events (events to be recorded as execution log) of TOE. Showing Table 11

Table 11: Auditable Events of TOE and Individually Defined Auditable Events

Functional Requirements	Actions to be audited (defined by CC)	Auditable events of TOE
FAU_GEN.1	None	-
FAU_SAR.1	a) Basic: Reading of information from the audit records.	*Basic: Successful download of audit log data.*
FAU_SAR.2	a) Basic: Unsuccessful attempts to read information from the audit records.	*Basic: Unsuccessful download of audit log data.*
FAU_STG.1	None	-
FAU_STG.4	a) Basic: Actions taken due to the audit storage failure.	*None*
FCS_CKM.1	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).	*None*

FCS_COP.1	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.	*None*
FDP_ACC.1	None	-
FDP_ACF.1	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.	*Basic: Creation/deletion of Mailbox.* *User name, job information, and success/failure regarding access to Mailbox and execution of Store Print.*
FDP_IFC.1	None	-
FDP_IFF.1	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	*None*
FDP_RIP.1	None	-
FIA_AFL.1	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).	*<Minimal>* *Continuous authentication failures.*
FIA_ATD.1	None	-
FIA_UAU.2	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	*<Minimal>* *Continuous authentication failures.*
FIA_UAU.7	None	-
FIA_UID.2	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.	*<Minimal>* *Continuous authentication failures.*
FIA_USB.1	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).	*<Minimal>* *Continuous*

	b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	*authentication failures.*
FMT_MOF.1	a) Basic: All modifications in the behavior of the functions in the TSF.	*<Basic>* *Changes in security function configuration.*
FMT_MSA.1	a) Basic: All modifications of the values of security attributes.	*<Basic>* *Creation/deletion of Mailbox.* *User name, job information, and success/failure regarding access to Mailbox and execution of Store Print.*
FMT_MSA.3	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	*<Individually defined auditable events>* *Successful/unsuccessful authentication of system administrator.*
FMT_MTD.1.	a) Basic: All modifications to the values of TSF data.	*<Individually defined auditable events>* *Changes in security function configuration.*
FMT_SMF.1	a) Minimal: Use of the management functions.	*<Individually defined auditable events>* *Successful/unsuccessful authentication of system administrator.*
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	*<Individually defined auditable events>* *Successful/unsuccessful authentication of system administrator.*
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	*<Minimal>* *Changes in time setting.*
FTP_TRP.1	a) Minimal: Failures of the trusted path functions. b) Minimal: Identification of the user associated with all trusted path failures, if available. c) Basic: All attempted uses of the trusted path functions.	*<Individually defined auditable events>* *Creation/deletion of certificates.*

	d) Basic: Identification of the user associated with all trusted path invocations, if available.	

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

[assignment: other audit relevant information].

- *none*

(2) 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.

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

[assignment: authorized users]

- *system 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.

(3) 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.

(4) 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*

(5) 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

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

FCS_CKM.1.1 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]
- *none*
[assignment: cryptographic key generation algorithm]
- *the Fuji Xerox's standard method, FXOSENC*
[assignment: cryptographic key sizes]
- *128bits*

(2) 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]
- *128bits*
[assignment: list of cryptographic operations]
- *encryption of the document data and security audit log data to be stored in the internal HDD and decryption of the document data and security audit log data retrieved from the internal HDD.*

6.1.3. Class FDP: User data protection

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

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]

- MFD access control SFP
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- subjects, objects, and operations between subjects and objects listed in Table 12

Table 12: Operations between Subjects and Objects Covered by MFD Access Control SFP

Subject	Object	Operation
Key operator process	*Mailbox*	*Creation of Personal Mailbox* *Deletion of Personal Mailbox* *Creation of Shared Mailbox* *Deletion of Shared Mailbox* *Storage of document data* *Deletion of all document data* *Retrieval of all document data*
	Store Print	*Storage of document data* *Deletion of all document data* *Retrieval of all document data*
SA process	*Mailbox*	*Creation of Personal Mailbox* *Deletion of Personal Mailbox* *Storage of document data* *Deletion of all document data* *Retrieval of all document data*
	Store Print	*Storage of document data* *Deletion of all document data* *Retrieval of all document data*
General user process	*Mailbox*	*Creation of Personal Mailbox* *Deletion of Personal Mailbox* *Storage of document data* *Deletion of all document data* *Retrieval of all document data*
	Store Print	*Storage of document data* *Deletion of document data* *Retrieval of document data*

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

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects

based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- MFD access control SFP
[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].
- general user identity corresponding to the general user process, SA identity corresponding to the SA process, Key operator identity corresponding to the Key operator process,
- owner identity corresponding to each Mailbox, owner identity corresponding to each Store Print area

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- the rules, shown in Table 13, for controlling the access of the controlled subjects to the controlled objects for the controlled operations

Table 13: Rules for Access Control

Rules for Mailbox Operation in the General User Process and SA Process
- Creation of Personal Mailbox *In the general user process and SA process to create Personal Mailbox, the Personal Mailbox in which general user identity and SA identity are set as its owner is created.* *- Deletion of Personal Mailbox* *When the general user identity and SA identity of the general user process and SA process match the owner identity of Personal Mailbox, deletion of the corresponding Personal Mailbox is allowed.* *- Storage, retrieval, and deletion of document data in Personal Mailbox* *When the general user identity and SA identity of the general user process and SA process match the owner identity of Mailbox, storage, retrieval, and deletion of the document data inside are allowed.* *- Storage, retrieval, and deletion of document data in Shared Mailbox*

Storage, retrieval, and deletion of document data in Shared Mailbox are allowed.
Rules for Store Print Operation in the General User Process and SA Process
- Storage of document data *In the general user process and SA process to store document data, the Store Print area in which general user identity and SA identity is set as its owner is created. The document data is then stored inside.* *- Deletion and retrieval of document data* *When the general user identity and SA identity of the general user process and SA process match the owner identity of Store Print area, retrieval and deletion of the document data inside are allowed. When the document data is deleted, the corresponding Store Print area is also deleted.*
Mailbox Operation in the Key Operator Process
- Creation and Deletion of Shared Mailbox *In the key operator process, creation and deletion of Shared Mailbox are allowed.*

FDP_ACF.1.3 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 rules, shown in Table 14 for explicitly authorizing access of the subject to an object based on security attributes.

Table 14: Rules for Explicit Access Authorization

Rule for Mailbox Operation in the Key Operator Process
- In the key operator process, deletion of Personal and Shared Mailbox, storage, deletion, and retrieval of the document data inside are allowed.
Rule for Store Print Operation in the Key Operator Process and SA Process
*- In the key operator process and SA process, all operations regarding Store Print (*i.e. *storage, deletion, and retrieval of the document data inside) are allowed.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
- no rules to explicitly deny the access

(3) 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: [assignment: list of objects].

[assignment: list of objects]
- *used document data stored in the internal HDD*
[selection: allocation of the resource to, deallocation of the resource from]
- *deallocation of the resource from*

6.1.4. Class FIA: Identification and authentication

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

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

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

FIA_AFL.1.2 (1) 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]
- *never allow the control panel to accept any operation except power cycle. Web browser is also inhibited from accepting authentication operation until the main unit is cycled.*

(2) FIA_AFL.1 (2) Authentication failure handling
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 (2) 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]
- *general user authentication*
[selection: [assignment: positive integer number] , an administrator configurable positive integer within [assignment: range of acceptable values]
- *[assignment: positive integer number]*
[assignment: positive integer number]
- *1*

FIA_AFL.1.2 (2) When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].

[selection: met, surpassed]
- *met*
[assignment: list of actions]
- *have the control panel to display the message of "authentication was failed" and to require reentry of the user information. The TSF shall also have Web browser, and Network Scan Utility to reenter the user information*

(3) 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*
- *General User* Role

(4) FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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

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

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

(6) FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

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

[assignment: list of user security attributes].
- *Key Operator Role*
- *SA Role*
- *General User Role*

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

[assignment: rules for the initial association of attributes].
- none

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

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

6.1.5. Class FMT: Security management

(1) 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]
- enable, disable, or modify the behavior of
[assignment: list of functions]
- for security listed in Table 15
[assignment: the authorized identified roles]
- the roles listed in Table 15

Table 15: List of Security Functions

Security Functions	enable, disable, or modify the behavior of	Role
Use of password entered from MFD control panel in user authentication	*Enable, disable*	*Key operator, SA*
Access denial due to authentication failure of system administrator ID	*Enable, disable*	*Key operator, SA*

User Authentication	*Enable, disable, modify*	*Key operator, SA*
Security Audit Log	*Enable, disable*	*Key operator, SA*
Store Print	*Enable, disable, modify*	*Key operator, SA*
Internal Network Data Protection	*Enable, disable, modify*	*Key operator, SA*
Customer Engineer Operation Restriction	*Enable, disable*	*Key operator, SA*
Hard Disk Data Encryption	*Enable, disable*	*Key operator, SA*
Hard Disk Data Overwrite	*Enable, disable, modify*	*Key operator, SA*

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

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

[assignment: access control SFP(s), information flow control SFP(s)]
- *MFD access control SFP to*
[selection: change default, query, modify, delete, [assignment: other operations]]
- *query, modify, delete,[assignment: other operations]*
[assignment: other operations]
- *create*
[assignment: list of security attributes]
- *user identity, Mailbox owner identity, and Store Print owner identity*
[assignment: the authorized identified roles].
- *the operations and roles listed in Table 16*

Table 16: Security Attributes and Authorized Roles

Security Attribute	query, delete, modify, create	Role
Key operator identity	*Modify*	*Key operator*

SA identity	*Query, modify delete, create*	*Key operator, SA*
General user identity	*Query, modify delete, create*	*Key operator, SA*
Mailbox owner identity (Personal Mailbox)	*Query, delete, create*	*General user , SA*
All Mailbox owner identity (All of Personal Mailbox)	*Query, delete, create*	*Key operator*
Mailbox owner identity (Shared Mailbox)	*Query, delete, create*	*Key operator*
Store Print owner identity	*Query, delete*	*Key operator, SA , General user*
All Store Print owner identity	*Query, delete*	*Key operator, SA*

(3) FMT_MSA.3 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 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]
- *MFD access control SFP*
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- *choose one of: permissive, [assignment: other property]*
[assignment: other property]]
-*none*

FMT_MSA.3.2 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*

(4) FMT_MTD.1 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 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]]
- *create*
[assignment: list of TSF data]
- *TSF data listed in Table 17*

[assignment: the authorized identified roles].
- *the operations and roles listed in Table 18*

Table 17: Operation of TSF Data

TSF Data	*query, modify, delete, create*	Role
Data on key operator ID	*modify*	*Key operator*
Data on key operator Password	*modify*	*Key operator*
Data on SA ID	*Query, modify , delete,create*	*Key operator, SA*
Data on SA Password	*modify*	*Key operator, SA*
Data on General user ID	*Query, modify, delete,create*	*Key operator, SA*
Data on General user Password	*modify*	*Key operator, SA ,General user*
Data on User Authentication	*Query, modify*	*Key operator, SA*
Data on use of password entered from MFD control panel in user authentication	*Query, modify*	*Key operator, SA*
Data on minimum password length of user password	*Query, modify*	*Key operator, SA*
Data on store print	*Query, modify*	*Key operator, SA*
Data on Access denial due to authentication failure of system administrator	*Query, modify*	*Key operator, SA*

Data on Security Audit Log	*Query, modify*	*Key operator, SA*
Data on Internal Network Data Protection	*Query, modify, delete*	*Key operator, SA*
Data on Customer Engineer Operation Restriction	*Query, modify*	*Key operator, SA*
Data on Hard Disk Data Encryption	*Query, modify*	*Key operator, SA*
Data on Hard Disk Data Overwrite	*Query, modify*	*Key operator, SA*
Data on date and time	*Query, modify*	*Key operator, SA*

(5) 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 18*

Table 18: Security Management Functions Provided by TSF

Functional requirements	Management items defined by CC	Management functions of TOE
FAU_GEN.1	There are no management activities foreseen.	*Management of data on Security Audit Log*
FAU_SAR.1	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	*Management of data on system administrator (ID and password)*
FAU_SAR.2	None	-
FAU_STG.1	None	-
FAU_STG.4	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	*None* *Reason: The control parameter of audit log is fixed and is not managed.*
FCS_CKM.1	None	-
FCS_COP.1	None	*Management of data on Hard Disk Data Encryption*
FDP_ACC.1	None	-
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.	*None* *Reason: Access is managed using user authentication information (ID and password).*
FDP_IFC.1	None	-
FDP_IFF.1	a) Managing the attributes used to make explicit access based decisions.	*None* *Reason: Access is restricted*

		and does not need to be managed.
FDP_RIP.1	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.	*Management of data on Hard Disk Data Overwrite*
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure.	*Management of allowable number of system administrator's authentication failures* *Management of Denial of machine operation*
FIA_ATD.1	a) if so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.	*None* *Reason: there are no additional security attributes and is not managed.*
FIA_UAU.2	a) Management of the authentication data by an administrator; b) Management of the authentication data by the user associated with this data.	*Management of Data on use of password entered from MFD control panel in user authentication* *Management of data on key operator, SA, and general user (ID and password)*
FIA_UAU.7	None	-
FIA_UID.2	a) The management of the user identities.	*Management of data on key operator, SA, and general user (ID and password)*
FIA_USB.1	a) an authorized administrator can define default subject security attributes. b) an authorized administrator can change subject security attributes.	*None* *Reason: action and security attributes is fixed and is not managed.*
FMT_MOF.1	a) Managing the group of roles that can interact with the functions in the TSF;	*Management of data on Customer Engineer Operation Restriction*
FMT_MSA.1	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.	*None* *Reason: The role group is fixed and is not managed.*
FMT_MSA.3	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.	*None* *Reason: The role group is only a system administrator and is not managed.*
FMT_MTD.1.	a) Managing the group of roles that can interact with the TSF data.	*Management of data on Customer Engineer Operation Restriction*

FMT_SMF.1	None	-
FMT_SMR.1	a) Managing the group of users that are part of a role.	*None* *Reason: The role group is fixed and is not managed*
FPT_STM.1	a) management of the time.	*Management of time and data.*
FTP_TRP.1	a) Configuring the actions that require trusted path, if supported.	*Management of Internal Network Data Protection.*

(6) 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]
- *system administrator ,SA, normal user*

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

6.1.6. Class FPT: Protection of the TSF

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

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

6.1.7. Class FTP: Trusted path/channels

(1) FTP_TRP.1 Trusted path
Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].

[selection: remote, local]
- *remote*

[selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].
- *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*.
[assignment: other types of integrity or confidentiality violation]
- *none*

FTP_TRP.1.2 The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.

[selection: the TSF, local users, remote users]
- *remote users*

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].

[selection: initial user authentication, [assignment: other services for which trusted path is required]].
- *TOE communication service via Web, communication service for print driver, communication service for communication service for network utility, communication service for other services which require trusted path.*

6.2. Security Assurance Requirements

The requirements for the TOE security assurance are described in Table 20.

The evaluation assurance level of TOE is EAL3. All the requirement components for assurance have quoted directly the component of EAL3 specified by [the CC part 3].

Table 19: EAL3 Assurance Requirements

Assurance Requirements	Assurance Component Name
Class ADV: Development	
ADV_ARC.1	Security architecture description
ADV_FSP.3	Functional specification with complete summary
ADV_TDS.2	Architectural design
Class AGD: Guidance documents	
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
Class ALC: Life-cycle support	
ALC_CMC.3	Authorization controls
ALC_CMS.3	Implementation representation CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
Class 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
Class ATE: Tests	
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
Class AVA: Vulnerability assessment	
AVA_VAN.2	Vulnerability analysis

6.3. Security Requirement Rationale

6.3.1. Security Functional Requirements Rationale

Table 20 lists the correspondences between security functional requirements and security objectives. As shown in this table, each security objective supports at least one TOE security functional requirement. Table 21 shows the rationale demonstrating that each security objective is assured by TOE security functional requirements.

Table 20: Correspondences between Security Functional Requirements and Security Objectives

Security Objectives / Security Functional Requirements	O.AUDITS	O.CIPHER	O.COMM_SEC	O.MANAGE	O.RESIDUAL	O.RESTRICT	O.USER
FAU_GEN.1	✓						
FAU_SAR.1	✓						
FAU_SAR.2	✓						
FAU_STG.1	✓						
FAU_STG.4	✓						
FCS_CKM.1		✓					
FCS_COP.1		✓					
FDP_ACC.1							✓
FDP_ACF.1							✓
FDP_RIP.1					✓		
FIA_AFL.1 (1)				✓		✓	✓
FIA_AFL.1 (2)						✓	✓
FIA_ATD.1							✓
FIA_UAU.2				✓		✓	✓
FIA_UAU.7				✓		✓	✓
FIA_UID.2				✓		✓	✓
FIA_USB.1							✓
FMT_MOF.1				✓			
FMT_MSA.1							✓
FMT_MSA.3							✓
FMT_MTD.1				✓			✓
FMT_SMF.1				✓			
FMT_SMR.1				✓			✓
FPT_STM.1	✓						
FTP_TRP.1			✓				

Table 21: Security Objectives to SFR Rationale

Security Objectives	Security Functional Requirements Rationale
O.AUDITS	O. AUDITS is an objective that provides Security Audit Log and its log data. By satisfying the following security objectives, O.AUDITS can be realized. By FAU_GEN.1, the security audit log data is generated for the auditable events: (However, audit is unnecessary for the following functional requirements for each reason.) - FAU_STG.4: The total number of audit log data events is fixed. The data are stored and updated automatically. - FCS_CKM.1, FSC_COP.1: An encryption failure is monitored as job status. 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. 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. By FPT_STM.1, the auditable events are recorded with time stamp in the audit log, using highly reliable clock of TOE. Thus, the functional requirements related to this objective are surely conducted.
O.CIPHER	O. CIPHER is an objective that encrypts the used document data in the internal HDD so that they cannot be analyzed even if retrieved. By satisfying the following security objectives, O.CIPHER can be realized. By FCS_CKM.1, the cryptographic key is generated in accordance with the specified cryptographic key size (128 bits). By FCS_COP.1, the document data and security audit log data to be stored into the internal HDD is encrypted and then decrypted when the data is read, in accordance with the determined cryptographic algorithm and cryptographic key size.
O.COMM_SEC	O.COMM_SEC is an objective that protects the document data, security audit log data, and TOE setting data on the internal network from interception and alteration. By satisfying the following security objectives, O.COMM_SEC can be realized:

Security Objectives	Security Functional Requirements Rationale
	By FTP_TRP.1, a highly reliable communication path is provided through communication data encryption protocol so that the document data, security audit log data, and TOE setting data on the internal network between TOE and the remote can be protected from threats. Thus, the functional requirements related to this objective are surely conducted.
O.MANAGE	O. MANAGE is an objective that allows only an authenticated system administrator to access the system administrator mode for security function setting and inhibits a general user from accessing the TOE setting data. By satisfying the following security objectives, O.MANAGE can be realized: By FIA_AFL.1 (1), successive attacks are prevented because the power needs to be cycled when the number of system-administrator authentication failures reaches the defined number of times. By FIA_UAU.2 and FIA_UID2, user authentication is performed to identify a proper system administrator or individual. By FIA_UAU.7, illicit leakage of the authentication information (password) is prevented because the authentication feedback is protected. By FMT_MOF.1, the person who enables/disables TOE security functions and makes functional settings is limited to system administrator. By FMT_MTD.1, the person who can make settings of TOE security functions is limited to system administrator. Thus, only system administrators can query and modify TSF data. By FMT_SMF.1, TOE security management functions are provided for system administrator. By FMT_SMR.1 (1), the role related to the security is limited to system administrator by maintaining the role of system administrator as a user who has special authority. Thus, the functional requirements related to this objective are surely conducted.
O.RESIDUAL	O.RESIDUAL is an objective that disables the reproduction and recovery of the used document data in the internal HDD. By satisfying the following security objective, O.RESIDUAL can be realized: By FDP_RIP.1, the previous information of the used document data stored in the internal HDD is made unavailable.
O.RESTRICT	O.RESTRICT is an objective that offers the function to inhibit an unauthorized person from using the TOE. By satisfying the following security objectives, O.RESTRICT can be

Security Objectives	Security Functional Requirements Rationale
	realized: By FIA_AFL.1 (1), successive attacks are prevented because the power needs to be cycled when the number of system-administrator authentication failures reaches the defined number of times. By FIA_AFL.1 (2), when user authentication fails, “incorrect password” message is displayed, requesting password re-entry. By FIA_UIA.2 and FIA_UID.2, user authentication is performed to identify a proper general user and system administrator. By FIA_UAU.7, illicit leakage of the authentication information (password) is prevented because the authentication feedback is protected. Thus, the functional requirements related to this objective are surely conducted.
O.USER	O.USER is an objective that identifies the TOE user and allows only the authorized user to store, retrieve, and delete the document data and to change password. By satisfying the following security objectives, O.USER can be realized: By FDP_ACC.1 and FDP_ACF.1, user authentication is performed. Only authorized user is allowed to operate the objects. By FIA_AFL.1 (1), successive attacks are prevented because the power needs to be cycled when the number of system-administrator authentication failures reaches the defined number of times. By FIA_AFL.1 (2), when user authentication fails, “incorrect password” message is displayed, requesting password re-entry. 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.2 and FIA_UID.2, user authentication is performed to identify a proper general user and system administrator. By FIA_UAU.7, illicit leakage of the authentication information (password) is prevented because the authentication feedback is protected. By FMT_MSA.1, the query, deletion, and creation of security attributes are managed. By FMT_MSA.3, the suitable default values are managed. By FMT_MTD.1, 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). By FMT_SMR.1 , the role of general user and system administrator is maintained and associated with the general user and system administrator.

Security Objectives	Security Functional Requirements Rationale
	Thus, the functional requirements related to this objective are surely conducted.

6.3.2. Dependencies of Security Functional Requirements

Table 22 describes the functional requirements that are depended on by security functional requirements and those that are not and the reason why it is not problematic even if dependencies are not satisfied.

Table 22: 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_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	-
FCS_CKM.1 Cryptographic key generation	FCS_COP.1	FCS_CKM.4: A cryptographic key is generated when MFD is booted, and stored on DRAM (volatile memory). A cryptographic key does not need to be destructed because this key is lost when the MFD main unit is powered off. Therefore, the dependency on FCS_CKM.4 does not need to be satisfied.
FCS_COP.1 Cryptographic operation	FCS_CKM.1	FCS_CKM.4: A cryptographic key is generated when MFD is booted, and stored on DRAM (volatile memory). A cryptographic key does not need to be destructed because this key is lost when the MFD main unit is powered off.

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_ACC.1 Subset access control	FDP_ACF.1	-
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 FMT_MSA.3	-
FDP_RIP.1 Subset residual information protection	None	
FIA_AFL.1(1) Authentication failure handling	FIA_UAU.2	FIA_UAU.1: The dependency on FIA_ UAU.1 is satisfied because FIA_UAU.2 is the functional security requirement that is an upper hierarchy of FIA_ UAU.1.
FIA_AFL.1(2) Authentication failure handling	FIA_UAU.2	FIA_UAU.1: The dependency on FIA_ UAU.1 is satisfied because FIA_UAU.2 is the functional security requirement that is an upper hierarchy of FIA_ UAU.1.
FIA_ATD.1 User attribute definition	None	
FIA_UAU.2 User authentication before any action	FIA_UID.2	FIA_UID.1: The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1.
FIA_UAU.7 Protected authentication feedback	FIA_UID.2	FIA_UAU.1: The dependency on FIA_ UAU.1 is satisfied because FIA_UAU.2 is the functional security requirement that is an upper hierarchy of FIA_ UAU.1.
FIA_UID.2 User identification before any action	None	
FIA_USB.1 User-subject binding	FIA_ATD.1	-
FMT_MOF.1 Management of security functions behavior	FMT_SMF.1 FMT_SMR.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
FMT_MSA.1 Management of security attributes	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 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.2	FIA_UID.1: The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1.
FPT_STM.1 Reliable time stamp	None	
FTP_TRP.1 Trusted Path	None	

6.3.3. Security Assurance Requirements Rationale

This TOE is for a MFD, a commercial product. The threats are assumed to be caused by a low-level attacker and to include: attack or interception/alteration of data on internal network via a MFD external interface from control panel, Web browser of system administrator's client; and reading-out of information by removing the internal HDD and connecting it to a commercial tool.

To counter these threats, this TOE is required to provide the security functions which assure security. The evaluation assurance level of TOE is EAL3 which includes the following analyses:

Analysis of the security measures of TOE at development phase

(Performing/analyzing systematic tests and evaluating the management of the development environment and the developed products.)

Analysis of whether the sufficient guidance information is included so that the security functions can be used safely. Therefore, EAL 3 is the reasonable evaluation level for 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 23 shows the correspondences between security functional requirements and 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 23: Correspondences between Security Functional Requirements and 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
FAU_GEN.1						✓	
FAU_SAR.1						✓	
FAU_SAR.2						✓	
FAU_STG.1						✓	
FAU_STG.4						✓	
FCS_CKM.1		✓					
FCS_COP.1		✓					
FDP_ACC.1			✓				
FDP_ACF.1			✓				
FDP_RIP.1	✓						
FIA_AFL.1 (1)			✓				
FIA_AFL.1 (2)			✓				
FIA_ATD.1			✓				
FIA_UAU.2			✓				
FIA_UAU.7			✓				
FIA_UID.2			✓				
FIA_USB.1			✓				
FMT_MOF.1				✓	✓		
FMT_MSA.1			✓	✓			
FMT_MSA.3				✓			
FMT_MTD.1			✓	✓	✓		
FMT_SMF.1				✓	✓		

Security Functions / Security Functional Requirements	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT
FMT_SMR.1			✓	✓	✓		
FPT_STM.1						✓	
FTP_TRP.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 is deleted by either one- or three-pass overwrite procedure on the document data area when each job of copy, print, scan, Network Scan is completed.
This is because whether to prioritize efficiency or security depends on the usage environment of the MFD.
When efficiency is prioritized, one pass overwrite procedure is applied. When security is prioritized, three pass overwrite procedure is applied. Three pass overwrite has lower processing speed than one pass but can provide more solid overwrite function. Therefore, three pass is an appropriate number of times to overwrite.

(1) FDP_RIP.1 Subset Residual Information Protection

To control the overwrite function conducted after each job, two options are available: one pass (zero) overwrite procedure and three pass (random number / random number / zero) overwrite procedure.
List of the used document data which is to be overwritten and deleted is on the internal HDD. When the existence of the used document data is 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)

According to Hard Disk Data Encryption setting which is configured by a system administrator with the system administrator mode, the document data and security audit log data are encrypted before stored into the internal HDD when operating any function of copy, print, scan, etc. or configuring various security function settings.

(1) FCS_CKM.1 Cryptographic key generation

TOE uses the “hard disk data encryption seed key” configured by a system administrator and generates a 128-bit encryption key at the time of booting through FXOSENC algorithm, which is Fuji Xerox’s standard method and a secure algorithm with sufficient complexity. (When the "hard disk data encryption seed key" is the same, the same cryptographic key is generated.)

(2) FCS_COP.1 Cryptographic operation

Before storing the document data and security audit log data into the internal HDD, TOE encrypts the data using the 128-bit cryptographic key generated at the time of booting (FCS_CKM.1) and the AES algorithm based on FIPS PUBS 197. When reading out the stored data, the TOE decrypts the data also using the 128-bit cryptographic key generated at the time of booting 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 print driver / Network Scan Utility / CWIS of the user client, or MFD control panel.

Only the authenticated user can use the following functions:

a) Functions controlled by the MFD control panel

Copy, scan, network scan, Mailbox operation, and print (This print function requires the user ID and password preset from print driver. A user must be authenticated from the control panel for print job.)

b) Functions controlled by Network Scan Utility of user client

Function to retrieve document data from Mailbox.

c) Functions controlled by CWIS

Display of device condition, display of job status and its log, function to retrieve document data from Mailbox, and print function by file designation

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 (1) Authentication failure handling

The function 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 administrator ID reaches 5 times, the control panel does not accept any operation except power cycle, and the web browser does not accept authentication operation until the MFD main unit is powered off/on.

(2) FIA_AFL.1 (2) Authentication failure handling

The function to handle the authentication failures is provided for the general user authentication which is performed before using the MFD functions. When the entered password does not match the one set by a legitimate user, the message saying “authentication was failed” is displayed, requesting re-entry of the user information.

Re-entry of user information is also required at Web browser, Network Scan Utility

(3) FIA_ATD.1 User attribute definition

The function to define and retain the roles of key operator, SA, and general user.

(4) FIA_UAU.2 User authentication before any action

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

This authentication and the identification (FIA_UID.2) are simultaneously performed, and the operation is allowed only when both of the identification and authentication succeed.

(5) FIA_UAU.7 Protected authentication feedback

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

(6) FIA_UID.2 User identification before any action

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

This identification and the authentication (FIA_UAU.2) are simultaneously performed, and the operation is allowed only when both of the identification and authentication succeed.

(7) FIA_USB.1 User-subject binding

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

(8) FMT_MSA.1 Management of security attributes

With the user authentication function, TOE permits the authenticated user to operate the identities related to each Mailbox and Store Print as shown in Table 24.

Table 24: Management of security attributes

Security Attribute	Query, modify ,delete, create	Role
Key operator identity	Modify	Key operator,
SA identity	Query, modify ,delete, create	Key operator, SA
General user identity	Query, Modify ,delete, create	Key operator, SA
Mailbox owner identity (Personal Mailbox)	Query, delete, create	General user, SA
All Mailbox owner identity (All of Personal Mailbo*x*)	Query, delete, create	Key operator
Mailbox owner identity (Shared Mailbox)	Query, delete, create	Key operator
Store Print owner identity	Query, delete	Key operator, SA, General user
All Store Print owner identity	Query, delete	Key operator, SA

(9) FMT_MTD.1 Management of TSF data

The TOE provides the user interface for setting password only to the authenticated legitimate 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).

(10) FMT_SMR.1 Security role

TOE maintains the roles of system administrator and general user and associates these roles to the legitimate users.

(11) FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute based access control

With the user authentication function, TOE permits the authenticated user to operate Mailbox and Store Print (Private Print) as shown in Table 25.

Table 25: Access Control

	Personal Mailbox	Shared Mailbox	Store Print
Creation of Mailbox	Available for general user, SA and key operator	Available for key operator	-

Deletion of Mailbox	Available for registered general user ,SA and key operator	Available for key operator	-
Storage, Retrieval and Deletion of document data	Available for registered general user ,SA and key operator	Available for general user, SA and key operator	Available for general user, SA and key operator
Retrieval and Deletion of all document data	Available for key operator	Available for key operator	Available for SA and key operator

User authentication is performed before accessing Mailbox or Store Print.

a) Private Print Function

To enable this function, the user needs to configure the MFD to "store an authenticated job to Private Print area*" and also needs to preset his/her ID and password from print driver of the user client. When a user sends a print request from print driver, the MFD compares the user ID and password against those preset in the MFD. Only when the user is authenticated, the print data is decomposed into bitmap data. Then, the data is classified according to the user ID and temporarily stored in the corresponding Private 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. Then, the data on the waiting list corresponding to the user ID is displayed. The user can request print or deletion of the data on the list.

b) Mailbox Function

The scanned data can be stored into Mailbox from IIT which is not shown in Figure 3.

To store the scanned data into Mailbox, a user needs to enter his/her ID and password from the control panel. Then, the document data can be scanned from IIT and stored into the internal HDD according to the user's instruction from the control panel.

To refer to, retrieve, print, or delete the stored data in the Personal Mailbox corresponding to each registered user ID, user authentication is required; the MFD compares the user ID and password preset in the MFD against those entered by a general user from the control panel, CWIS, or Network Scan Utility.

- Mailbox Operation by a General User / SA

- Creation of Personal Mailbox

  When a general user / SA operates to create Personal Mailbox, the Personal Mailbox in which general user identity / SA identity is set as its owner is created.

- Deletion of Personal Mailbox

  When the general user identity / SA identity matches the owner identity of Personal Mailbox, deletion of the corresponding Personal Mailbox is allowed.

- Storage, retrieval, and deletion of document data in Personal Mailbox
  When the general user identity / SA identity matches the owner identity of Personal Mailbox, storage, retrieval, and deletion of the document data inside are allowed.
- Storage, retrieval, and deletion of document data in Shared Mailbox
  Storage, retrieval, and deletion of document data in Shared Mailbox are allowed.

- Store Print Operation by a General User / SA

- Storage of document data
  When a general user / SA operates to store document data, the Store Print area in which general user identity / SA identity is set as its owner is created. The document data is then stored inside.
- Deletion and retrieval of document data
  When the general user identity / SA identity matches the owner identity of Store Print area, retrieval and deletion of the document data inside are allowed. When the document data is deleted, the corresponding Store Print area is also deleted.

- Mailbox Operation by the Key Operator

- Creation and deletion of Shared Mailbox, creation and deletion of Personal Mailbox
  Creation and deletion of Shared Mailbox are allowed.

- Mailbox Operation by the Key Operator
  For all Mailboxes, the key operator's operations to delete Mailbox, and to store, retrieve, and delete the document data inside are allowed.

- Store Print Operation by the Key Operator / SA
  For all the Store Print areas, the key operator's / SA's operations to retrieve and delete the document data inside are allowed.

7.1.4. System Administrator’s Security Management (TSF_FMT)

To accord 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 behavior
FMT_MTD.1 Management of TSF data
FMT_SMF.1 Specification of management functions

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 the setting of Hard Disk Data Overwrite, enable/disable it, and set the number of pass (overwrite procedure);
- Refer to the setting of Hard Disk Data Encryption and enable/disable it;
- Set the cryptographic seed key for Hard Disk Data Encryption;
- Refer to the setting on the use of password entered from MFD control panel in user authentication, and enable/disable it;
- Refer to the setting of access denial due to authentication failure of system administrator identification, enable/disable it, and set the allowable number of the failures before access denial;
- Change the key operator ID and password (only a key operator is privileged);
- Refer to the setting of ID of SA and general user and change the ID and password;
- Refer to the setting of access denial due to authentication failure of system administrator, enable/disable it, and set the allowable number of failures;
- Refer to and set the minimum password length (for general user and SA);
- Refer to the setting of SSL/TLS communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of IPSec communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of S/MIME communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of User Authentication and enable/disable Local Authentication;
- Refer to the setting of Store print and set the store/print;
- Refer to and set date and time;

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

- Change the key operator ID and password (only a key operator is privileged);
- Refer to the setting of ID of SA and general user and change the ID and password;
- Refer to the setting of access denial due to authentication failures of system administrator, enable/disable it, and set the allowable number of the failures before access denial;
- Refer to and set the minimum password length (for general user and SA);
- Refer to the setting of Security Audit Log and enable/disable it,
  (When Security Audit Log is enabled, security audit log data can be downloaded in the form of tab-delimited text to a system administrator client.);
- Refer to the setting of SSL/TLS communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of IPSec communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of SNMP v3 communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Set the authentication password for SNMPv3 communication;

- Refer to the setting of S/MIME communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Download/upload and create an X.509 certificate;
- Refer to the setting of User Authentication and enable/disable Local Authentication;

(2) FMT_MSA.1 Management of security attributes

TOE restricts the operation of the general user identifier only to a system administrator.

(3) FMT_MSA.3 Static attribute initialization

TOE provides the suitable default value.

(4) FMT_SMR.1 Security roles

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

7.1.5. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

A system administrator can restrict CE’s operation in the system administrator mode to inhibit CE from referring to / changing the settings related to System Administrator’s Security Management (TSF_FMT). This function can prevent setting change by an attacker who is impersonating CE.

(1) FMT_MOF.1 Management of security functions behavior
FMT_MTD.1 Management of TSF data
FMT_SMF.1 Specification of management functions

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 control panel and CWIS.

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 TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function. All of 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 26 shows the details of the audit log data.

Table 26: Details of Security Audit Log Data

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
  (except common record items)

Logged Events	Description	Status
Change in Device Status		
System Status	Started normally(cold boot)	-
	Started normally (warm boot)	
	Shutdown requested	
	User operation (Local)	Start/End
	Scheduled Image Overwriting started	Successful/Failed
	Scheduled Image Overwriting finished	Successful/Failed
User Authentication		
Login/Logout	Login (Local Access)	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	
	Mailbox	
	Print Reports	
	Job Flow Service	
Change in Device Settings		

Logged Events	Description	Status
Device Settings	Adjust Time	Successful/Failed
	Create Mailbox	
	Delete Mailbox	
	Switch Authentication Mode	Successful (Setting items recorded)
	Change Security Setting	
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	

(2) FAU_SAR.1 Audit review

It is assured that all the information recorded in the audit log can be read.

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, SSL/TLS communication needs to be enabled before using Web browser.

(3) FAU_SAR.2 Restricted audit review

The person who reads the audit log is limited to the authenticated system administrator. A system administrator can access the audit log 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 audit log.

(4) FAU_STG.1 Protected audit trail storage

There is no function to delete the audit log, and the audit log data is protected from untrusted alteration and modification.

(5) FAU_STG.4 Prevention of audit data loss

When audit trail file is full, the oldest stored audit record is overwritten with the new data so that the new data is 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.

(6) 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 with the following four protocols which are configured by a system administrator using the system administrator mode:

(1) FTP_TRP.1 Trusted Path

The document data, security audit log data, and TOE setting data are protected by the encryption communication protocol that ensures secure data communication between TOE and the remote (communication service via Web, communication service for print driver, communication service for network utility, communication service for other services which require trusted path). This trusted path is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communication data from modification or disclosure.

a) SSL/TLS

According to the SSL/TLS communication which is configured by a system administrator using the system administrator mode, SSL/TLS ensuring secure data transmission is supported. This protects the security of document data, security audit log data, and TOE setting data on the internal network.
By supporting SSL/TLS, TOE can act as SSL/TLS server or SSL/TLS client. Moreover, SSL/TLS can protect data transmission between 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 booting a session and lost at the time of ending the session or powering off the MFD main unit.

Cryptographic key generated as SSLv3/TLSv1 at every session
Specifically, one of the cryptographic suites below is adopted:

Cryptographic Suites of SSL/TLS	Cryptographic Method and Size of Secret Key	Hash Method
SSL_RSA_WITH_RC4_128_SHA	RC4 / 128 bits	SHA-1
SSL_RSA_WITH_3DES_EDE_CBC_SHA	3-Key Triple-DES / 168 bits	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA	AES / 128 bits	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	AES / 256 bits	SHA-1

Protection from the alteration is realized by HMAC (Hashed Message Authentication Code - IETF RFC 2104) of SSL/TLS.
When SSL/TLS communication is enabled on the Web client, requests from the client must be received via HTTPS. The SSL/TLS communication needs to be enabled before IPSec, SNMPv3,

or S/MIME is enabled or before security audit log data is 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, security audit log data, and 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 TOE and the remote. After the association is established, all transmission data among the specified IP addresses is encrypted by the transport mode of IPSec until the TOE is powered off or reset. A cryptographic key is generated at the time of booting 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
3-Key Triple-DES /168 bits	SHA-1

c) SNMPv3

According to the SNMP v3 communication which is configured by a system administrator using the system administrator mode, SNMP v3 is supported. This is one of the security solutions for the network management protocol, SNMP. As defined in IETF RFC3414, SNMP v3 is used for not only data encryption but also authentication of each SNMP message.

To enable this function, both authentication password and privacy password need to be set up in both TOE and the remote server. Length of both passwords must be 8 characters or more. Authentication of SNMP v3 uses SHA-1 hash function; encryption of the protocol uses CBC-DES. A cryptographic key is generated at the time of booting a session and lost at the time of ending the session or powering off the MFD main unit.

Cryptographic key generated as SNMP v3 at every session:

Cryptographic Method and Size of Secret Key	Hash Method
DES / 56 bits	SHA-1

d) 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/from the outside by e-mail is protected from interception. By S/MIME signature mail function, the document data is protected from interception and alteration.

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.

Cryptographic key generated as S/MIME for every mail

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
RC2 / 128 bits	SHA-1
3-Key Triple-DES / 168 bits	SHA-1

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
CWIS	Centre Ware Internet Service
DC	Digital Copier
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
User	Any entity outside TOE who interacts with the TOE: *i.e.* general user, system administrator, and CE.
System Administrator Privilege (SA)	A user authorized by key operator to manage MFD maintenance and configure TOE security functions.
System Administrator	An authorized user who manages MFD maintenance and configures TOE security functions. This term covers both key operator and SA.
Customer Engineer (CE)	Customer service engineer, an engineer who maintains and repairs MFD.
Attacker	A malicious user of TOE
Control Panel	A panel of MFD on which buttons, lamps, and a touch screen panel are mounted to operate the MFD
General User Client	A client for general user.
System Administrator Client	A client for system administrator. An administrator can refer to and rewrite TOE setting data of MFD via Web.
CentreWare Internet Service (CWIS)	A service to retrieve the document data scanned by MFD from Mailbox. It also enables a system administrator to refer to and rewrite TOE setting data via Web browser.
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.
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFD.
Print 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 is to be converted into bitmap data by TOE decompose function.
Control Data	The data that is transmitted by command and response interactions. This is one type of data transmitted between MFD hardware units.
Bitmap Data	The decomposed data of the data read by copy function and the print data transmitted from a user client to MFD. Bitmap data is stored into the internal HDD after being compressed in the unique process.
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.

Term	Definition
Print Function	A function to decompose and print out the print data transmitted by a user client.
Original	Texts, images and photos to be read from IIT in copy function.
Document Data	Document data means all the image data transmitted across the MFD when any of copy, print, scan is operated 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), ・ Bitmap data read from IIT and then stored into the internal HDD (scan function), ・
Used Document Data	The remaining data in the MFD internal HDD even after deletion. The document data is first stored into the internal HDD, used, and then only its file is deleted.
Security Audit Log Data	The chronologically recorded data of important events of 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 is stored in a general user client or in the general client and server, but does not include data regarding TOE functions.
General Data	The data on the internal network. The general data does not include data regarding TOE functions.
TOE Setting Data	The data which is created by TOE or for TOE and may affect TOE operations. Specifically, it includes the information regarding the functions of Hard Disk Data Overwrite, Hard Disk Data Encryption, System Administrator's Security Management, Customer Engineer Operation Restriction, Use of password entered from MFD control panel in user authentication, ID and password of system administrator, access denial due to authentication failure of system administrator, Internal Network Data Protection, Security Audit Log, Mailbox, and User Authentication.
General Client and Server	Client and server which do not directly engage in TOE operations
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 is deleted. Therefore, user cannot access the document data which was logically deleted. However, the document data itself is not deleted but remains as the used document data until new data is written in the same storage area.
Overwrite	To write over the area of the document data stored in the internal HDD

Term	Definition
	when deleting the data.
Cryptographic Seed Key	The 12 alphanumeric characters to be entered by a user. When data in the internal HDD can be encrypted, a cryptographic key is generated based on the cryptographic seed key.
Cryptographic Key	The 128-bit data which is automatically generated based on the cryptographic seed key. Before the data is 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 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 TOE, and are protected from the security risks coming from the external network.
User Authentication	A function to limit the accessible TOE functions by identifying the user before he/she uses each TOE function.
Local Authentication	A mode to manage user authentication of TOE using the user information registered in the MFD.

9. REFERENCES

The following documentation was used to prepare this ST.

Short Name	Document Title
[CC Part 1]	Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 1: Introduction and general model, dated September 2006, CCMB-2006-09-001 (Translation version 1.2, dated March 2007, translated by Information-Technology Promotion Agency, Japan)
[CC Part 2]	Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 2: Security functional requirements, dated September 2007, CCMB-2007-09-002 (Translation version 2.0, dated March 2008, translated by Information-Technology Promotion Agency, Japan)
[CC Part 3]	Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 3: Security assurance requirements, dated September 2007, CCMB-2007-09-003 (Translation version 2.0, dated March 2008, translated by Information-Technology Promotion Agency, Japan)
[CEM]	Common Methodology for Information Technology Security Evaluation - Version 3.1 Evaluation Methodology, dated September 2007, CCMB-2007-09-004 (Translation version 2.0, dated March 2008, translated by Information-Technology Promotion Agency, Japan)