Fuji Xerox
ApeosPort-II 7000/6000 Series
Controller Software for Asia Pacific

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:	Fuji Xerox ApeosPort-II 7000/6000 Series Controller Software for Asia Pacific Security Target
ST Version:	1.0.9
Publication Date:	September 26, 2008
Author:	Fuji Xerox Co., Ltd.

1.2. TOE Reference

This section provides information needed to identify this TOE.

The TOE of Fuji Xerox ApeosPort-II 7000 and that of Fuji Xerox ApeosPort-II 6000 are identified as Fuji Xerox ApeosPort-II 7000/6000 Series Controller Software for Asia Pacific and use the same ROM version:

TOE Identification:	Fuji Xerox ApeosPort-II 7000/6000 Series Controller Software for Asia Pacific
Version:	Controller ROM Ver 1.180.7
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 controller software for MFP and has copy, print, and scan functions.

The TOE is provided as the firmware product which controls the whole MFP and protects the used document data and the TOE setting data against threats. The TOE is stored on the controller ROM which is on the controller board.

1.3.1.2. Function Types

Table 1 shows the types of functions provided by the TOE.

Table 1: Function Types and Capabilities

Function types (Standard /Option)	Function capabilities
Basic Function	- CWIS - System Administrator's Security Management - Copy function - Print function - Scan function - Network Scan function
Optional Function (Data Security Kit)	- Hard Disk Data Overwrite - Hard Disk Data Encryption - Customer Engineer Operation Restriction
Optional Function (FAX Board not to be evaluated)	- FAX function - iFAX, D-FAX functions - FAX Flow Security

- To use print, scan, and D-FAX functions, the following items shall be installed to the external client for general user and that for system administrator: print driver, scan driver, Network Scan Utility, and FAX driver.

- The Data Security Kit, an option, must be used to obtain the security features.

1.3.1.3. Usage and Major Security Features of TOE

The TOE is mainly used to perform the following functions:

- 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. When more than one copy is ordered for one original, the data read from IIT is first stored into the MFP 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 MFP from Mailbox.
  It also enables a system administrator to refer to and rewrite TOE setting data via Web browser.

- Scan function is to read the original data from IIT and store it into Mailbox within the MFP 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 is 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 MFP. This function is operated according to the general user's instruction from the control panel.

- FAX function is to send and receive FAX data. According to the general user's instruction from the control panel to send a FAX, the original data is read from IIT and then sent to the destination via public telephone line. The document data is received from the sender's machine via public telephone line and then printed out from the recipient's IOT.

- The iFAX function is to send and receive FAX data via the Internet, not public telephone line.

- The D-FAX function is to send data from a user client to the destination via public telephone line. The data is first sent to MFP as a print job and then to the destination without being printed out.

The TOE provides the following security features:

- Hard Disk Data Overwrite (TSF_IOW)
  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 (TSF_CIPHER)
  The document data is encrypted before being stored into the internal HDD when any function of copy, print, scan, etc. is operated.

- System Administrator's Security Management (TSF_FMT)
  This function allows only the authenticated system administrator to refer to and change the TOE security settings by identifying and authorizing the system administrator from the control panel or system administrator client.

- Customer Engineer Operation Restriction (TSF_CE_LIMIT)
  A system administrator can inhibit CE from changing the TOE security settings.

- FAX Flow Security (TSF_FAX_FLOW)
  This function prevents unauthorized access to the TOE or the internal network via FAX board from public telephone line.

1.3.2. Environment Assumptions

This TOE is assumed to be used as an IT product at general office and to be linked to the internal network, public telephone line, and user clients.

Figure 1 shows the intended environment for TOE operation.

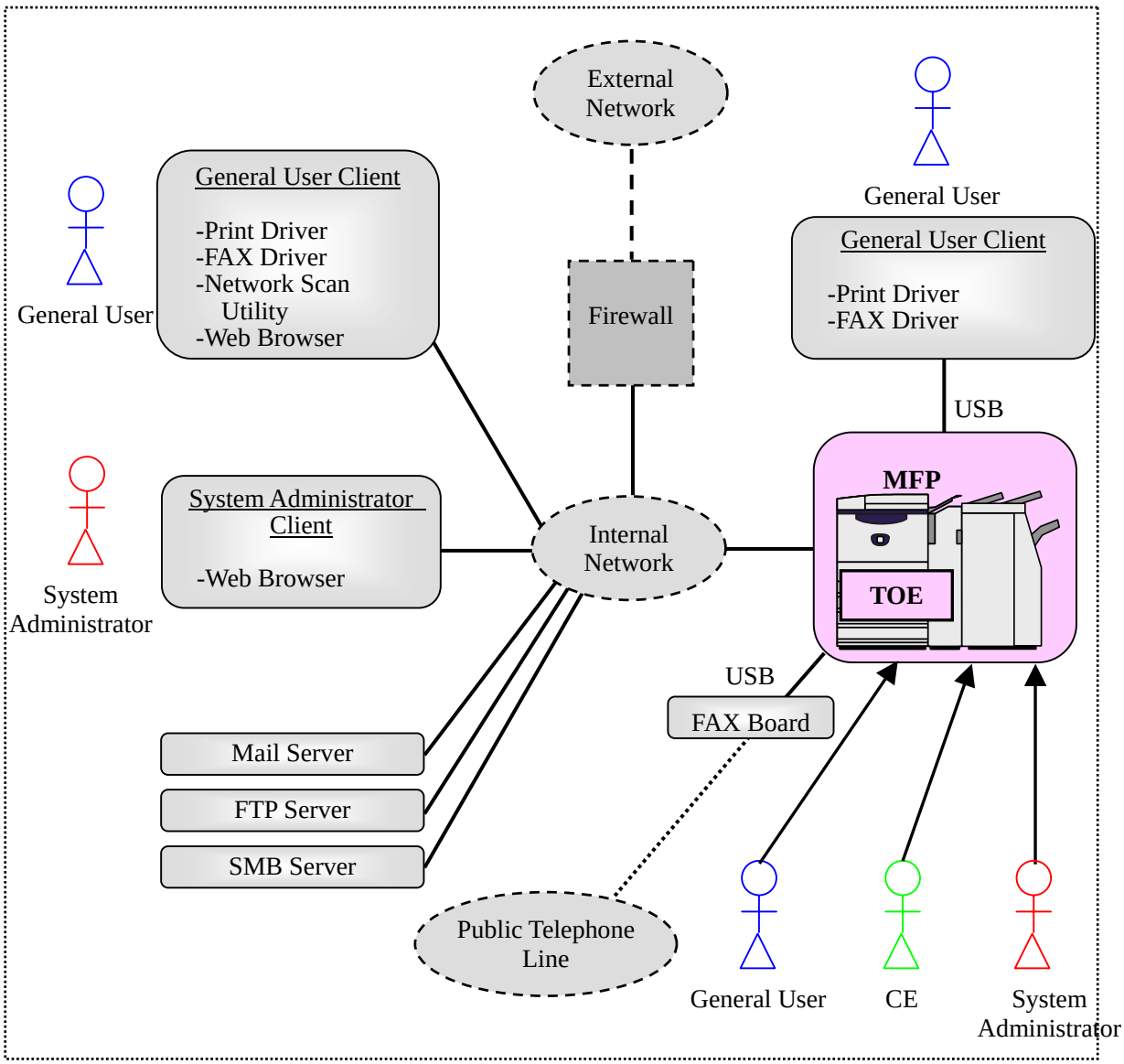

Figure 1: Intended Operational Environment

1.3.3. Required Non-TOE Hardware and Software

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

(1) MFP

The MFP (ApeosPort-II 7000/6000 Series) is a user interface to provide MFP functions and the hardware for scan/print/copy functions. It includes the control panel, ADF, IIT, IOT, controller board,

and FAX board (option).

(2) General user client:

The hardware is a general-purpose PC. When a client is linked to the MFP via the internal network and the print driver, Network Scan Utility, and FAX driver are installed to the client, the general user can request the MFP to print, FAX, and retrieve the document data.

The user can also request the MFP to retrieve the scanned document data via Web browser.

Additionally, the user can change the settings which he/she registered to the MFP: Mailbox name, password, access control, and automatic deletion of document.

When the client is linked to the MFP directly via USB and print/FAX driver is installed to the client, the user can request the MFP to print/FAX the document data.

(3) System administrator client:

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

(4) Mail server:

The hardware/OS is a general-purpose PC or server. The MFP sends/receives document data to/from Mail server via mail protocol.

(5) FTP server:

The hardware/OS is a general-purpose PC or server. The MFP sends document data to FTP server via FTP.

(6) SMB server:

The hardware/OS is a general-purpose PC or server. The MFP sends document data to SMB server via SMB.

(7) FAX board:

The FAX board is connected to external public telephone line and supports G3/G4 protocols. The FAX board is connected to the MFP via USB interface to enable FAX communication.

The OS's of general user client (2) and system administrator client (3) are assumed to be Windows 2000, Windows XP, and Windows Vista.

To protect the devices within the internal network from unauthorized access, each device needs to be linked to the external network via Firewall.

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 and FAX.
System administrator	A user who is authorized to manage the device using the tool mode. The system administrator can refer to and rewrite the TOE setting for device operation and that for security functions via Web browser.
Customer engineer (CE)	A user who can configure the TOE operational settings using the interface for CE from the control panel.

1.4.2. Logical Scope and Boundary

The logical scope of this TOE consists of each function of the programs recorded on the controller ROM.

Figure 2 shows the logical architecture of the MFP.

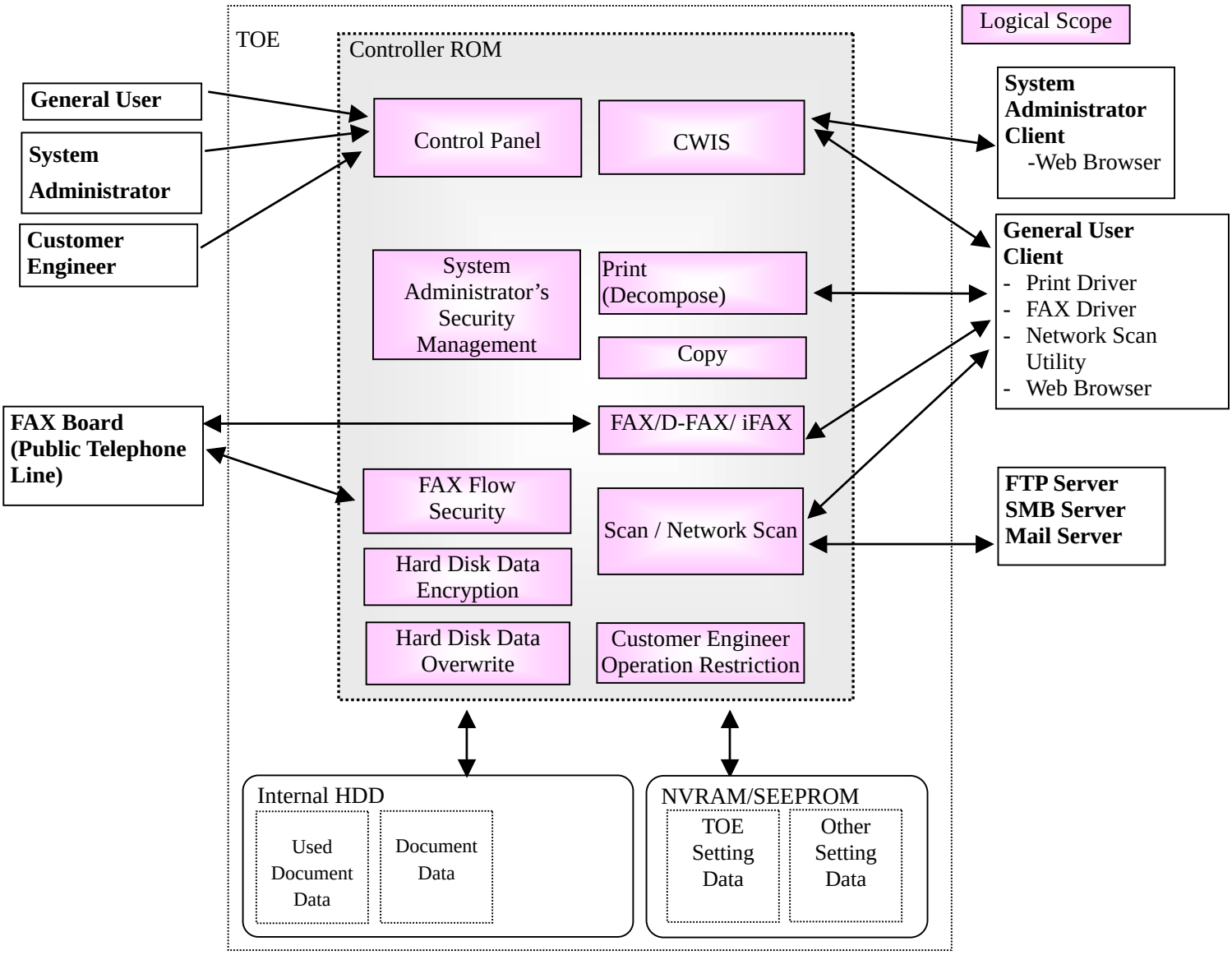

Figure 2: MFP Units and TOE Logical Scope

1.4.2.1. Basic Functions

The TOE provides the functions of control panel, copy, print, scan, FAX, iFAX / D-FAX, 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 MFP 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 When more than one copy is ordered for one original, the data read from IIT is first stored into the MFP 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 the general user client. The print data created via print driver is sent to the MFP 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 the 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 the general user client, FTP server, Mail server, or SMB server according to the information set in the MFP. A general user can request this function from the control panel.
FAX Function	FAX function is to send and receive FAX data. According to the general user's instruction from the control panel to send a FAX, the original data is read from IIT and sent to the destination via public telephone line. The document data is received from the sender's machine via public telephone line and printed out from the recipient's IOT.
D-FAX Function , iFAX Function	D-FAX function is to directly FAX document data to the destination. According to the instruction from the general user client to send a FAX, the print data created via FAX driver is sent to the MFP, analyzed, and decomposed. Then, the data is converted to the format for FAX sending and sent to the destination via public telephone line. iFAX function is to send and receive FAX data as in the normal FAX function. According to the general user's instruction from the control panel to send a FAX, the original data is read from IIT and sent to the destination via the Internet. The

	document data is received from the sender's machine via the Internet and printed out from the recipient's IOT.
CWIS Function	CWIS is to retrieve, from the internal HDD, the scanned document data and the received FAX data according to the instruction from Web browser of the 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 the system administrator client.

1.4.2.2. Security Functions

The security functions provided by the TOE are the following.

(1) Hard Disk Data Overwrite (TSF_IOW)

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, FAX, iFAX, or D-FAX) is completed. Without this function, the used document data remains and only its management data is deleted.

(2) Hard Disk Data Encryption (TSF_CIPHER)

The document data is encrypted before stored into the internal HDD when any of copy, print, scan, Network Scan, FAX, iFAX, or D-FAX function is operated. (The data is stored in the internal HDD while being used.) This encryption function is provided to solve the problem that, after the data is used, only its management data is deleted but the stored document data itself remains.

(3) System Administrator's Security Management (TSF_FMT)

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 configure the following security functions from the control panel:

- Enable or disable Hard Disk Data Overwrite;
- Enable or disable Hard Disk Data Encryption;
- Enable or disable use of password entered from MFP control panel in user authentication;
- Change the ID and password of system administrator;
- Enable or disable access denial due to authentication failure of system administrator ID, and set the allowable number of the failures before access denial;
- Enable or disable Customer Engineer Operation Restriction.

Additionally, with CWIS, this TOE allows only the authenticated system administrator to configure the following security functions via Web browser:

- Change the ID and password of system administrator;

- Enable or disable access denial due to authentication failure of system administrator ID, and set the allowable number of the failures before access denial.

(4) Customer Engineer Operation Restriction (TSF_CE_LIMIT)

This TOE allows only the authenticated system administrator to refer to or enable/disable the Customer Engineer Operation Restriction setting from the control panel. For this, CE cannot change the setting of each function described in (3) System Administrator's Security Management.

(5) FAX Flow Security (TSF_FAX_FLOW)

A FAX board is an option and is connected to TOE controller board via USB interface. An attacker cannot access the TOE or the internal network from public telephone line via the FAX board.

1.4.3. Physical Scope and Boundary

The physical scope of this TOE is the controller board. Figure 3 shows configuration of each unit and TOE physical scope.

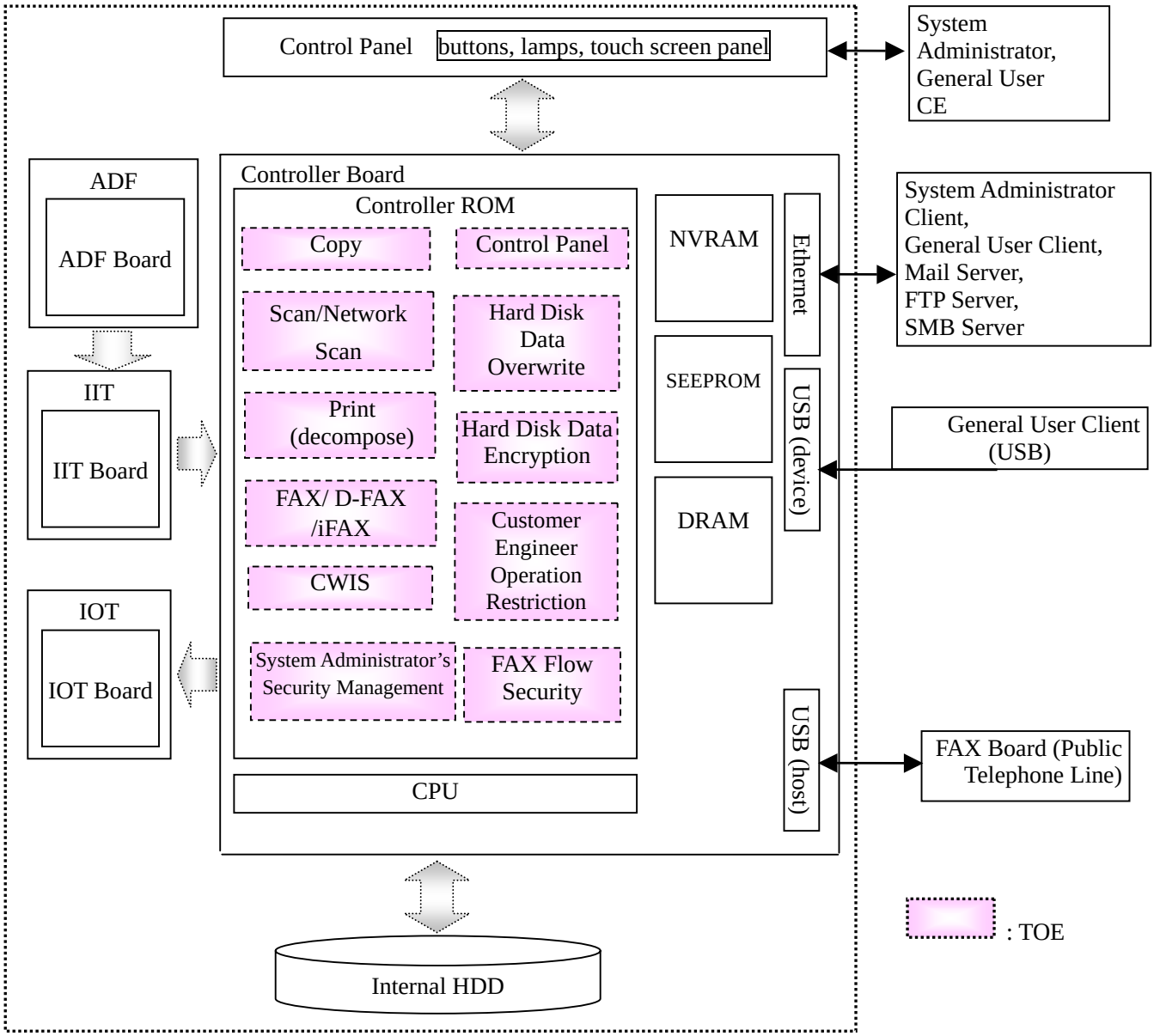

Figure 3: MFP Units and TOE Physical Scope

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

board.

The control panel is a panel on which buttons, lamps, and a touch screen panel are mounted to enable MFP functions of copy, scan, and FAX.

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

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

1.4.4. Guidance

The following are the guidance documents for this TOE.

ApeosPort-II 7000/6000 DocuCentre-II 7000/6000 Administrator Guide

ApeosPort-II 7000/6000 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 4):

(1) Used document data

When a general user uses any MFP function of copy, FAX, scan, etc., the document data is temporarily stored in the internal HDD for image processing, transmission, and Store Print. When the job is completed or canceled, only the management data is deleted but the document data itself remains. The residual data includes general user's confidential information. Therefore, it is assumed as an asset to be protected.

(2) TOE setting data

A system administrator can configure TOE security functions from the MFP control panel or system administrator client by 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. Therefore, it is assumed as an asset to be protected.

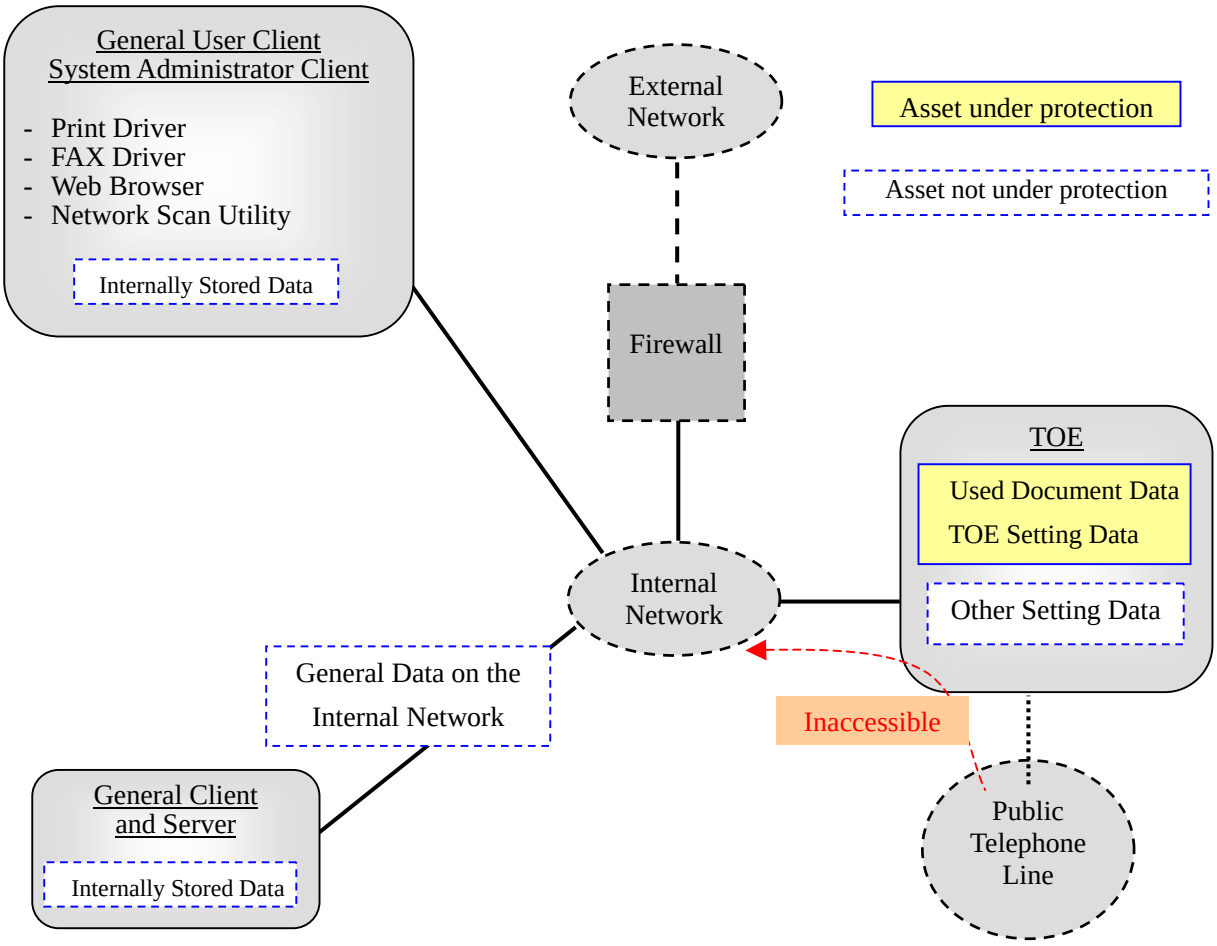

Figure 4: Assets under and not under Protection

Note) The data stored in the general client and server within the internal network and the general data on the internal network are not assumed as assets to be protected. However, TOE functions prevent the access to the internal network from public telephone line via TOE. Therefore, the access to the assets not under protection is not assumed as a threat.

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 use of password entered from MFP control panel in user authentication
Data on ID and password of system administrator
Data on access denial due to authentication failures of system administrator ID
Data on Hard Disk Data Overwrite
Data on Hard Disk Data Encryption
Data on Customer Engineer Operation Restriction

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
Unauthorized reproduction of the document data stored in the internal HDD	
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 used document data inside.
Unauthorized access to TOE setting data	
T.CONFDATA	An attacker may access, read, or alter, from control panel or Web browser, the TOE setting data which only a system administrator is allowed to access.

3.2. Organizational Security Policies

Table 6 below describes the organizational security policy the TOE must comply with.

Table 6: Organizational Security Policy

Organizational Policy (Identifier)	Description
P.FAX_OPT	At the behest of the Australian agency, it must be ensured that the internal network cannot be accessed via public telephone line.

3.3. Assumptions

Table 7 shows the assumptions for the operation and use of this TOE.

Table 7: 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 it viciously.
Protection Mode	
A.SECMODE	A system administrator shall configure the TOE as follows. • Use of password entered from MFP control panel in user authentication: enabled • Length of system administrator password: 7 characters or more

Assumption (Identifier)	Description
	• Access denial due to authentication failure of system administrator ID: enabled • Allowable number of system administrator's authentication failures before access denial: 5 • Customer Engineer Operation Restriction: enabled • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters
Network Connection Assumption	
A.NET	• Interception on the internal network of the MFP with the TOE installed shall be disabled. • When the internal network of the MFP with the TOE installed is linked to the external network, access to the MFP from the external network shall be disabled.

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

Table 8: Security Objectives for the TOE

Security Objectives (Identifier)	Description
O.CIPHER	The TOE encrypts the used document data to be stored into the HDD so that it cannot be analyzed even if retrieved.
O.FAX_SEC	The TOE must prevent the unauthorized access to the internal network via FAX modem from public telephone line.
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 prevent the used document data in the internal HDD from being reproduced or recovered.

4.2. Security Objectives for the Operational Environment

Table 9 defines the security objectives for the Operational Environment.

Table 9: Security Objectives for the Operational Environment

Security Objectives (Identifier)	Description
OE.ADMIN	An organization administrator shall assign an appropriate and reliable person for TOE management as a system administrator and train him/her.
OE.AUTH	A system administrator shall configure the TOE security functions as follows. • Use of password entered from MFP control panel in user authentication: enabled • Length of system administrator password: 7 characters or more • Access denial due to authentication failure of system administrator ID: enabled • Allowable number of system administrator's authentication failures before access denial: 5 • Customer Engineer Operation Restriction: enabled
OE.FUNCTION	A system administrator shall configure the TOE security functions as follows. • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled

Security Objectives (Identifier)	Description
	• Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters
OE.NET	An organization person in charge shall have a user install a device (client) and configure it properly to prevent interception on the internal network of the MFP with the TOE installed. An organization person in charge shall have a system administrator install a device (Firewall) and configure it properly to block the access from the external network to the MFP with the TOE installed.

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 10 shows the correspondences between the security objectives and the assumptions / threats / organizational security policies. Moreover, Table 11 shows that each defined TOE security problem is covered by the security objectives.

Table 10: Correspondences between Security Objectives and Assumptions / Threats / Organizational Security Policies

Security Problems / Security objectives	A.ADMIN	A.SECMODE	A.NET	T.RECOVER	T.CONFDATA	P.FAX_OPT
O.CIPHER				✓		
O.FAX_SEC						✓
O.MANAGE					✓	
O.RESIDUAL				✓		
OE.ADMIN	✓					
OE.AUTH		✓			✓	
OE.FUNCTION		✓		✓		
OE.NET			✓			

Table 11: Security Objectives Rationale for Security Problem

Security problem	Security Objectives Rationale
A.ADMIN	By satisfying the following objective, A.ADMIN can be realized: - OE.ADMIN By OE.ADMIN, an organization person in charge selects a suitable member for system administrator and provides management and education.
A.SECMODE	By satisfying the following objectives, A.SECMODE can be realized: - OE.AUTH By OE.AUTH, a system administrator sets an appropriate ID and password and enables Customer Engineer Operation Restriction. - OE.FUNCTION By OE.FUNCTION, Hard Disk Data Overwrite and Hard Disk Data Encryption are enabled, which disables the recovery of the used document data in the internal HDD.
A.NET	A.NET is an intended environment in which interception on the internal network of MFP and attack by general public from the external network are inhibited. By satisfying the following objective, A.NET can be realized: - OE.NET By OE.NET, interception on the internal network and the access to the MFP from the external network are disabled. To prevent interception, a device (client) is installed and properly configured. For example, it is configured to encrypt the data transmitted between MFP and the client. To block the access to the MFP from the external network, a device (Firewall) is installed and properly configured.
T.RECOVER	By satisfying the following objective, T.RECOVER can be countered: - OE.FUNCTION 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 recovery of the used document data in the internal HDD. To be specific, this threat can be countered by the following security objectives: O.CIPHER and O.RESIDUAL. - O.CIPHER By O.CIPHER, the document data to be stored into the internal HDD is encrypted. - O.RESIDUAL By O.RESIDUAL, the used document data is overwritten and deleted to disable the reproduction of the used document data stored in the internal

Security problem	Security Objectives Rationale
	HDD.
T.CONFDATA	By satisfying the following objective, T.CONFDATA can be countered: - OE.AUTH By OE.AUTH, it is necessary to enable the security functions (i.e. User Authentication with Password, System Administrator Password, Allowable Number of System Administrator's Authentication Failures before Access Denial, and Customer Engineer Operation Restriction) 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 objective: - O.MANAGE 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.
P.FAX_OPT	By satisfying the following objectives, P.FAX_OPT can be observed. - O.FAX_SEC By O.FAX_SEC, the access to the internal network via public telephone line is disabled. This realizes P.FAX_OPT. Since the data received from public telephone line is not sent to the internal network, the internal network cannot be accessed

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
Receiving information from public telephone line	To receive the document data from the sender's machine via public telephone line, as receiving FAX data.
Sending information to public telephone line	To send the document data to the destination via public telephone line according to the general user's instruction from the control panel or client PC, as sending FAX data.
Sending information to the internal network	To send the Network Scan data or the data received by iFAX to the destination, a client PC, within the internal network.
Receiving information from the internal network	To receive the print data or the D-FAX/iFAX data from the sender, a client PC, within the internal network.

- Object

Term/phrase	Definition
Used document data stored in the internal HDD	The remaining data in the MFP internal HDD even after deletion., the document data is first stored into the internal HDD, used, and then only its file is deleted.

- Operation

Term/phrase	Definition
Delivery	MFP receives the data from public telephone line for FAX function.
Modify	To change the settings of the following information: - Use of password entered from MFP control panel in user authentication; - ID and password of system administrator; - Access denial due to authentication failure of system administrator ID; - Hard Disk Data Overwrite; - Hard Disk Data Encryption; - Customer Engineer Operation Restriction.

- Data

Term/phrase	Definition
Data on public telephone line	The data which flows on public telephone line for FAX communication

- Security attributes

None

- Entity outside TOE

Term/phrase	Definition
System Administrator	An authorized user who manages MFP maintenance and configures TOE security functions.

- 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 MFP 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 MFP main unit is powered off/on.
Data on use of password entered from MFP control panel in user authentication	The data on whether to enable/disable the use of password to be entered from MFP control panel in user authentication. Included in the TOE setting data.
Data on ID of system administrator	The ID data used to authenticate system administrators. Included in the TOE setting data.
Data on password of system administrator	The password data used to authenticate system administrators. Included in the TOE setting data.
Data on access denial due to authentication failures of system administrator ID	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 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.
Public telephone line	The line/network on which the data flows for FAX communication.
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 MFP functions.

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 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 he 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]
・*bits*

(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 to be stored into the internal HDD and decryption of the document data retrieved from the internal HDD*

6.1.2. Class FDP: User data protection

(1) FDP_IFC.1	Subset information flow control
Hierarchical to:	No other components
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1	The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]
・*subjects, information, and operations to cause the information flow, listed in Table 12.*

Table 12: Subjects, Information, and Operations Covered by FAX Information Flow Control SFP

Subject	Information	Operation
Receiving information from public telephone line *Sending information to the internal network*	*Data on public telephone line*	*Delivery*

	[assignment: information flow control SFP] ・*FAX information flow control SFP*
(2) FDP_IFF.1	Simple security attributes
Hierarchical to:	No other components
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
FDP_IFF.1.1	The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].
	[assignment: information flow control SFP] ・*FAX information flow control SFP* [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes] ・*none. (Sending information to public telephone line, receiving information from the internal network, and the corresponding data on the public telephone line are not controlled under the FAX information flow control SFP).*
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].
	[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes] ・*the data received from public telephone line must not be sent to the internal network at any case*
FDP_IFF.1.3	The TSF shall enforce the [assignment: additional information flow control SFP rules].
	[assignment: additional information flow control SFP rules] ・*none.*

FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. [assignment: rules, based on security attributes, that explicitly authorize information flows] ・*none.*
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. [assignment: rules, based on security attributes, that explicitly deny information flows]. ・*none.*
(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*

6.1.3. Class FIA: Identification and authentication

(1) FIA_AFL.1	Authentication failure handling
Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of

	authentication events]. [assignment: list of authentication events] ・*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	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_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.
(3) 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

(4) 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.

6.1.4. Class FMT：Security management

(1) FMT_MOF.1	Management of security functions behaviour
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 behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

[assignment: list of functions]
・*for security listed in Table 13*
[selection: determine the behaviour of, disable, enable, modify the behaviour of]
・*determine the behaviour of, disable, enable, modify the behaviour of*
[assignment: the authorized identified roles]
・*system administrator*

Table 13: List of Security Functions

Security Functions	behaviour
Use of password entered from MFP control panel in user authentication	*Enable, disable*
Access denial due to authentication failure of system administrator ID	*Enable, disable, Modify*
Customer Engineer Operation Restriction	*Enable, disable*
Hard Disk Data Encryption	*Enable, disable*
Hard Disk Data Overwrite	*Enable, disable, Modify*

(2) 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].

[assignment: list of TSF data]
・*TSF data listed in Table 14*

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

[assignment: the authorized identified roles]
・*system administrator*

Table 14: Operation of TSF Data

TSF Data	Operation
Data on use of password entered from MFP control panel in user authentication	*query, modify*
Data on system administrator ID	*query, modify*
Data on system administrator password	*modify*
Data on Access denial due to authentication failure of system administrator ID	*query, modify*
Data on Customer Engineer Operation Restriction	*query, modify*
Data on Hard Disk Data Encryption	*query, modify*
Data on Hard Disk Data Overwrite	*query, modify*

(3) FMT_SMF.1	Specification of Management Functions
Hierarchical to:	No other components
Dependencies:	No dependencies
FMT_SMF.1.1	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]

・S*ecurity Management Functions listed in Table 15*

Table 15: Security Management Functions Provided by TSF

Functional requirements	Management items defined by CC	Management functions of TOE
FCS_CKM.1	None	-
FCS_COP.1	None	*Management of Information on Hard Disk Data Encryption*
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 Information 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_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 use of password entered from MFP control panel* *Management of information on system administrator (ID and password)*
FIA_UAU.7	None	-
FIA_UID.2	a) The management of the user identities.	*Management of information on system administrator (ID and password)*
FMT_MOF.1	a) Managing the group of roles that can interact with the functions in the TSF;	*Management of Information on Customer Engineer Operation Restriction*
FMT_MTD.1.	a) Managing the group of roles that can interact with the TSF data.	*Management of Information 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.*

(4) 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*
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2. Security Assurance Requirements

The requirements for the TOE security assurance are described in Table 16.
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 16: EAL3 Assurance Requirements

Assurance Requirements	Assurance Component Name	Dependencies
Class ADV: Development		
ADV_ARC.1	Security architecture description	ADV_FSP.1, ADV_TDS.1
ADV_FSP.3	Functional specification with complete summary	ADV_TDS.1
ADV_TDS.2	Architectural design	ADV_FSP.3
Class AGD:	Guidance documents	
AGD_OPE.1	Operational user guidance	ADV_FSP.1,
AGD_PRE.1	Preparative procedures	None
Class ALC:	Life-cycle support	
ALC_CMC.3	Authorization controls	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	Implementation representation CM coverage	None
ALC_DEL.1	Delivery procedures	None
ALC_DVS.1	Identification of security measures	None
ALC_LCD.1	Developer defined life-cycle model	None
Class ASE:	Security Target evaluation	
ASE_CCL.1	Conformance claims	ASE_INT.1, ASE_ECD.1, ASE_REQ.1
ASE_ECD.1	Extended components definition	None
ASE_INT.1	ST introduction	None
ASE_OBJ.2	Security objectives	ASE_SPD.1
ASE_REQ.2	Derived security requirements	ASE_OBJ.2, ASE_ECD.1
ASE_SPD.1	Security problem definition	None

Assurance Requirements	Assurance Component Name	Dependencies
ASE_TSS.1	TOE summary specification	ASE_INT.1, ASE_REQ.1, ADV_FSP.1
Class ATE:	Tests	
ATE_COV.2	Analysis of coverage	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	Testing: basic design	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
ATE_FUN.1	Functional testing	ATE_COV.1
ATE_IND.2	Independent testing - sample	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1
Class AVA:	Vulnerability assessment	
AVA_VAN.2	Vulnerability analysis	ADV_ARC.1,ADV_FSP.1, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

6.3. Security Requirement Rationale

6.3.1. Security Functional Requirements Rationale

Table 17 lists the correspondences between security functional requirements and security objectives. Table 18 shows the rationale demonstrating that each security objective is assured by TOE security functional requirements.

Table 17: Correspondences between Security Functional Requirements and Security Objectives

Security Objectives / Security Functional Requirements	O.CIPHER	O.FAX_SEC	O.MANAGE	O.RESIDUAL
FCS_CKM.1	✓			
FCS_COP.1	✓			
FDP_IFC.1		✓		
FDP_IFF.1		✓		
FDP_RIP.1				✓
FIA_AFL.1			✓	
FIA_UAU.2			✓	

Security Objectives / Security Functional Requirements	O.CIPHER	O.FAX_SEC	O.MANAGE	O.RESIDUAL
FIA_UAU.7			✓	
FIA_UID.2			✓	
FMT_MOF.1			✓	
FMT_MTD.1			✓	
FMT_SMF.1			✓	
FMT_SMR.1			✓	

Table 18: Security Objectives to SFR Rationale

Security Objectives	Security Functional Requirement Rationale
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. - FCS_CKM.1 By FCS_CKM.1, the cryptographic key is generated in accordance with the specified cryptographic key size (128 bits). - FCS_COP.1 By FCS_COP.1, the document 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.FAX_SEC	O.FAX_SEC is an objective that prevents the unauthorized access to the internal network via public telephone line. By satisfying the following security objectives, O.FAX_SEC can be realized: - FDP_IFC.1 and FDP_IFF.1 By FDP_IFC.1 and FDP_IFF.1, the internal network to which the TOE is connected is prevented from being accessed via public telephone line from the communication path of TOE FAX modem.
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

Security Objectives	Security Functional Requirement Rationale
	realized: - FIA_AFL.1 By FIA_AFL.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. - FIA_UAU.2 By FIA_UAU.2, user authentication is performed to identify a proper system administrator. - FIA_UAU.7 By FIA_UAU.7, illicit leakage of the information of system administrator authentication (password) is prevented because the authentication feedback is protected. - FIA_UID2 By FIA_UID2, user authentication is performed to identify a proper system administrator or individual. - FMT_MOF.1 By FMT_MOF.1, the person who enables/disables TOE security functions and makes functional settings is limited to system administrator. - FMT_MTD.1 By FMT_MTD.1, the person who modifies settings of TOE security functions is limited to system administrator. Thus, only system administrators can query and modify TSF data. - FMT_SMF.1 By FMT_SMF.1, TOE security management functions are provided for system administrator. - FMT_SMR.1 By FMT_SMR.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.
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: - FDP_RIP.1 By FDP_RIP.1, the previous information of the used document data file stored in the internal HDD is made unavailable.

6.3.2. Dependencies of Security Functional Requirements

Table 19 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 19: 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
FCS_CKM.1 Cryptographic key generation	FCS_COP.1	FCS_CKM.4: A cryptographic key is generated when MFP is booted, and stored on DRAM (volatile memory). A cryptographic key does not need to be destructed because this key is lost when the MFP 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 MFP is booted, and stored on DRAM (volatile memory). The cryptographic key does not need to be destructed because this key is lost when the MFP main unit is powered off. Therefore, the dependency on FCS_CKM.4 does not need to be satisfied.
FDP_IFC.1 Subset information flow control	FDP_IFF.1	-
FDP_IFF.1 Simple security attributes	FDP_IFC.1	FMT_MSA.3: A static attribute initialization is not required because FAX information flow has no security attribute.
FDP_RIP.1 Subset residual information protection	None	
FIA_AFL.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_UAU.2 User authentication before	-	FIA_UID.1: The dependency on FIA_UID.1 is satisfied because

Functional Requirement	Dependencies of Functional Requirements	
Requirement and its name	Requirement that is dependent on	Requirement that is not dependent on and its rationale
any action		FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1.
FIA_UAU.7 Protected authentication feedback	-	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	
FMT_MOF.1 Management of security functions behavior	FMT_SMF.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.

6.3.3. Security Assurance Requirements Rationale

This TOE is for a MFP, a commercial product. The threats are assumed to be caused by a low-level attacker and to include: attack via a MFP external interface from control panel or 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. TOE Security Functions

Table 20 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 20: Correspondences between Security Functional Requirements and TOE Security Functions

Security Functions / Security Functional Requirements	TSF_IOW	TSF_CIPHER	TSF_FMT	TSF_CE_LIMIT	TSF_FAX_FLOW
FCS_CKM.1		✓			
FCS_COP.1		✓			
FDP_IFC.1					✓
FDP_IFF.1					✓
FDP_RIP.1	✓				
FIA_AFL.1			✓		
FIA_UAU.2			✓		
FIA_UAU.7			✓		
FIA_UID.2			✓		
FMT_MOF.1			✓	✓	
FMT_MTD.1			✓	✓	
FMT_SMF.1			✓	✓	
FMT_SMR.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 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, FAX, iFAX, or D-FAX is completed.

This is because whether to prioritize efficiency or security depends on the usage environment of the MFP.

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 which is configured by a system administrator with the system administrator mode, the document data is encrypted before stored into the internal HDD when any of copy, print, scan, Network Scan, FAX, iFAX, or D-FAX function is operated.

(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 through FXOSENC algorithm, a secure algorithm with sufficient complexity, at the time of booting. (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 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 document 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. 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 following security functions from the control panel or system administrator client.

(1) FIA_AFL.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 MFP main unit is powered off/on.

(2) FIA_UAU.2 User authentication before any action

TOE requests a user to enter the password before permitting a system administrator to operate at the control panel or to operate CWIS function via Web browser of a system administrator client. The entered password is verified against the password registered on the TOE. 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.

(3) 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 or the Web browser in order to hide the password at the time of user authentication.

(4) FIA_UID.2 User identification before any action

TOE requests a user to enter the user ID before permitting a system administrator to operate at the control panel or to operate the CWIS function via Web browser of a system administrator client. The entered ID is verified against the ID registered on the TOE.

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.

(5) 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 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.
- Configure the cryptographic seed key for Hard Disk Data Encryption.
- Refer to the setting on the use of password entered from MFP control panel in user authentication, and enable/disable it.
- Refer to the setting of system administrator ID and change the ID and password.
- 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.

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

- Refer to the setting of system administrator ID and change the ID and password.
- Refer to the setting of access denial due to authentication failures of system administrator ID, enable/disable it, and set the allowable number of the failures before access denial.

(6) FMT_SMR.1 Security roles

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

7.1.4. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

A system administrator can restrict CE's operation in the system administrator mode to inhibit CE from 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.

With these functions, the required security management functions are provided.

7.1.5. FAX Flow Security (TSF_FAX_FLOW)

This function inhibits unauthorized access to the TOE via the FAX board, which is connected to the controller board via USB interface, at any case. Namely, the data on public telephone line is not delivered to the internal network.

(1) FDP_IFC.1 Subset information flow control
FDP_IFF.1 Simple security attributes

The data on public telephone line is not delivered to the internal network.

8. ACRONYMS AND TERMINOLOGY

8.1. Acronyms

The following acronyms are used in this ST:

Acronym	Definition
ADF	Auto Document Feeder
CC	Common Criteria for Information Technology Security Evaluation
CE	Customer Engineer / Customer Service Engineer
CWIS	CentreWare Internet Service
DC	Digital Copier
D-FAX	Direct FAX
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
iFAX	Internet FAX
IIT	Image Input Terminal
IOT	Image Output Terminal
MFP	Multi Function Peripheral
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
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface

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 engineer, and CE.
Customer Engineer (CE)	Customer service engineer, an engineer who maintains and repairs MFP.
Attacker	A malicious user of TOE
Control Panel	A panel of MFP on which buttons, lamps, and a touch screen panel are mounted to operate the MFP
General User Client	A client for general user to operate the MFP.
System Administrator Client	A client for system administrator. An administrator can refer to and rewrite TOE setting data of MFP 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 MFP functions.
FAX Driver	Software for Direct FAX function, which enables a general user to FAX data to the destination directly from a general user client through MFP. The user can send the FAX data just as printing
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFP.
Print Driver	Software for a general user to convert the data on a general user client into print data written in page description language (PDL), a readable format for MFP.
Print Data	The data written in PDL, a readable format for MFP, 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 MFP hardware units.
Bitmap Data	The decomposed data of the data read by copy function and the print data transmitted from a user client to MFP. 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.
Store Print	A print function in which bitmap data (decomposed print data) is temporarily stored in the MFP internal HDD and then printed out according to the general user's instruction from the control panel. There are three ways

Term	Definition
	for the Store Print: • Security Print Print operation is enabled when a user enters, from the control panel, the password which was registered on the print driver of general user client. • Sample Print When printing several copies, only one copy is printed out first as a sample document. A user can check its quality and send an instruction from the control panel to print out the remaining copies. • Mailbox Print Decomposed bitmap data is stored in Mailbox and then printed out according to the general user's instruction from the control panel.
Original	Texts, images and photos to be read from IIT in copy function.
Mailbox	A logical box created in the MFP internal HDD. Mailbox stores the scanned document data or the data to be printed later.
Document Data	Document data means all the image data transmitted across the MFP when any of copy, print, scan or FAX functions 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), • Bitmap data read from IIT and sent to the FAX destination and the bitmap data faxed from the sender's machine and printed out from the recipient's IOT (FAX function).
Used Document Data	The remaining data in the MFP internal HDD even after deletion. The document data is first stored into the internal HDD, used, and then only its file is deleted.
Internally Stored Data	The data which is stored in the 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, Customer Engineer Operation Restriction, Use of password entered from MFP control panel in user authentication, ID and password of system administrator, and access denial due to authentication failure of system administrator ID.
General Client and Server	Client and server which do not directly engage in TOE operations

Term	Definition
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 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 MFP 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.

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)

