Xerox WorkCentre 7346

Security Target

Version 1.0.3

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) identification information, an overview of the ST, the evaluation assurance level of Target of Evaluation (TOE), Common Criteria (CC) conformance, references, acronyms, and terminology.

1.1. ST Identification

This section provides information needed to identify this ST and its Target of Evaluation (TOE). This ST complies with ISO/IEC 15408 (2005).

(1) ST Identification

ST Title:	Xerox WorkCentre 7346 Security Target
ST Version:	Ver. 1.0.3
Author:	Fuji Xerox Co., Ltd.
Publication Date:	May 21, 2008
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3 ISO/IEC 15408 (2005)
Keywords:	Multifunction System, Multi Function Peripheral, Copy, Print, Scan, Fax, Internal Hard Disk Drive, Document Overwrite, Document Encryption, Internal Network Data Protection, SSL/TLS, IPSec, SNMPv3, S/MIME

(2) TOE Identification

TOE Identification:	Xerox WorkCentre 7346	
ROM Versions:	- Controller+PS ROM	Ver. 1.223.4
	- IOT ROM	Ver. 3.2.0
	- IIT ROM	Ver. 20.4.3
	- ADF ROM	Ver. 11.6.5
Manufacturer:	Fuji Xerox Co., Ltd.	

1.2. ST Overview

This ST provides the security specifications of Xerox WorkCentre 7346 (hereinafter referred to as "MFP"). MFP is the short name of Multi Function Peripheral which has copy, print, scan and fax functions.

This ST covers the security functions to protect, from unauthorized disclosure, the document data stored in the internal HDD after being processed by MFP and the used document data (*i.e.* the residual data after deleted). The ST also describes the protection of data transmitted over general encryption communication protocols. These protocols protect the security of data on the internal network between MFP and highly reliable remote server / client PC (hereinafter referred to as "between TOE and the remote") as well as the identification data used at user authentication. However, the function to protect the internal network data is not available when the data is communicated with the remote which does not support the encryption communication protocols.

Additionally, at the behest of the U.S. agency, the user data and TOE configuration data on the internal network are protected from unauthorized access via fax line using public telephone line.

This TOE provides the following security functions:

- Hard Disk Data Overwrite (TSF_IOW)
- Hard Disk Data Encryption (TSF_CIPHER)
- User Authentication (TSF_USER_AUTH)
- System Administrator’s Security Management (TSF_FMT)
- Customer Engineer Operation Restriction (TSF_CE_LIMIT)
- Security Audit Log (TSF_FAU)
- Internal Network Data Protection (TSF_NET_PROT)
- Fax Flow Security (TSF_FAX_FLOW)

1.3. Common Criteria Conformance Claim

This ST conforms to the following evaluation standards for information security (CC). It does not conform to a Protection Profile (PP).

- CC Part 2
- CC Part 3
- Evaluation Assurance Level: EAL 2

1.4. 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 2.3 Part 1: Introduction and general model, dated August 2005, CCMB-2005-08-001 (Translation version 1.0, dated December 2005, translated by Information-Technology Promotion Agency, Japan）
［CC Part 2］	Common Criteria for Information Technology Security Evaluation - Version 2.3 Part 2: Security functional requirements, dated August 2005, CCMB-2005-08-002 (Translation version 1.0, dated December 2005, translated by Information-Technology Promotion Agency, Japan)
［CC Part 3］	Common Criteria for Information Technology Security Evaluation - Version 2.3 Part 3: Security assurance requirements, dated August 2005, CCMB-2005-08-003 (Translation version 1.0, dated December 2005, translated by Information-Technology Promotion Agency, Japan)
［CEM］	Common Methodology for Information Technology Security Evaluation - Version 2.3 Evaluation Methodology, dated August 2005, CCMB-2005-08-004 (Translation version 1.0, dated December 2005, translated by Information-Technology Promotion Agency, Japan)
［ISO/IEC TR15446］	WD N3374, Guide for the Production of PPs and STs - Version 0.93 (Provisional translation, dated January 2004, translated by Information-Technology Promotion Agency, Japan)
［I-0512］	Interpretations-0512 (December 2005, by Information-Technology Promotion Agency, Japan)

1.5. Acronyms and Terminology

1.5.1. 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
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
IIT	Image Input Terminal
IOT	Image Output Terminal
IT	Information Technology
IP	Internet Protocol
IPSec	Security Architecture for Internet Protocol
Kerberos	A network authentication protocol which uses secret-key cryptography
LDAP	Lightweight Directory Access Protocol
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
SNMPv3	Simple Network Management Protocol, Version 3
SOF	Strength of Function
SSLv3/TLSv1 (SSL/TLS）	Secure Socket Layer, Version 3 / Transport Layer Security, Version 1
ST	Security Target
S/MIME	Secure/Multipurpose Internet Mail Extensions
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy

1.5.2. 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, key operator, and system administrator privilege (SA).
General User	Any person who uses copy, scan, fax, and print functions of MFP.
Key Operator	An authorized user who manages MFP maintenance and configures TOE security functions.
System Administrator Privilege (SA)	A user authorized by key operator to manage MFP maintenance and configure TOE security functions.
System Administrator	An authorized user who manages MFP maintenance and configures TOE security functions. This term covers both key operator and SA.
Customer Engineer (CE)	This term is equivalent to customer service engineer, a Xerox 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 and SA to operate the MFP.
System Administrator Client	A client for system administrator. An administrator can refer to and rewrite TOE configuration data of MFP via Web browser.
User Client	This term covers both general user client and system administrator client.
CentreWare Internet Service (CWIS)	A service to retrieve the document data scanned by MFP from Mailbox. It also enables a system administrator to refer to and rewrite TOE configuration data via Web browser.
Tool Mode	An operation mode that enables a system administrator to refer to and rewrite TOE configuration 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.
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.
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 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.

Term	Definition
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.
Print Function	A function to decompose and print out the print data transmitted by a user client.
Print-Control Function	A function to control the device to enable print operation.
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 for the Store Print: • Private Print Jobs are stored only when MFP authenticates a user with his/her ID and password which were preset in the print driver on a general user client. When the user is authenticated with his/her ID and password entered from the control panel, he/she can start print operation. • 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 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.
Copy Function	A function in which original is read from IIT and then printed 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 required number of copies can be made.
Copy Control Function	A function to control the device to enable copy operation.
Scan Function	According to the general user's instruction from the control panel, the original data is read from IIT and then stored into Mailbox within the MFP internal HDD. The stored document data can be retrieved via standard Web browser by CWIS or Network Scan Utility function.
Scan Control Function	A function to control the device to enable scan operation.

Term	Definition
Network Scan Function	A function in which original data is read from IIT and then transmitted 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.
Network Scan Control Function	A function to control the device to enable network scan operation.
Fax Function	A function 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 and then printed out from the recipient's IOT.
Fax Control Function	A function to control the device to enable fax operation.
Direct Fax (D-Fax） Function	A fax function in which data is sent via public telephone line directly from a user client. The data is first sent to MFP as a print job and then to the destination without being printed out.
Internet Fax (iFax) Function	A fax function in which the data is sent or received via the Internet, not public telephone line.
D-Fax / i-Fax Control Function	A function to control the device to enable D-Fax / iFax operation.
Mailbox	A logical box created in the MFP internal HDD. Mailbox stores the scanned document data or the data to be printed later. 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.
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.

Term	Definition
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 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 Configuration 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, 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 a 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.
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.
Network	A general term to indicate both external and internal networks.
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 MFP.

2. TOE DESCRIPTION

This chapter describes a TOE overview, assumption of TOE users, logical and physical scopes of TOE, and the assets protected by this TOE.

2.1. TOE Overview

2.1.1. Product Type

This TOE, categorized as an IT product, is the MFP which has the following functions: copy, print, scan, fax-control which enables fax communication through linkage with the external fax board, and Fax-Flow Security to prevent unauthorized access from the outside. The TOE is the product which controls the whole MFP and protects the data that is transmitted over the encryption communication protocols. These protocols protect the security of the TOE configuration data and the document data on the internal network between TOE and the remote.
The TOE also protects, from unauthorized disclosure, the data in the internal HDD: the stored document data after being processed and the used document data.

2.1.2. Function Types

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

Table 1: Function Types and Capabilities

MFP functions	Function types (standard/optional)	Function capabilities
- Basic Function	Standard Function	- CWIS - Hard Disk Data Overwrite - Hard Disk Data Encryption - System Administrator’s Security Management - Internal Network Data Protection - User Authentication - Customer Engineer Operation Restriction - Security Audit Log
- Copy - Print		- Copy function - Print function
- Scan - Network Scan	Optional Function (Scan Kit)	- Scan function - Network Scan function
- Fax - i-Fax, D-Fax	Optional Function (Fax Board not to be evaluated)	- Fax function - i-Fax, D-Fax functions - Fax Flow Security

2.1.3. Service Overview

2.1.3.1. 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.

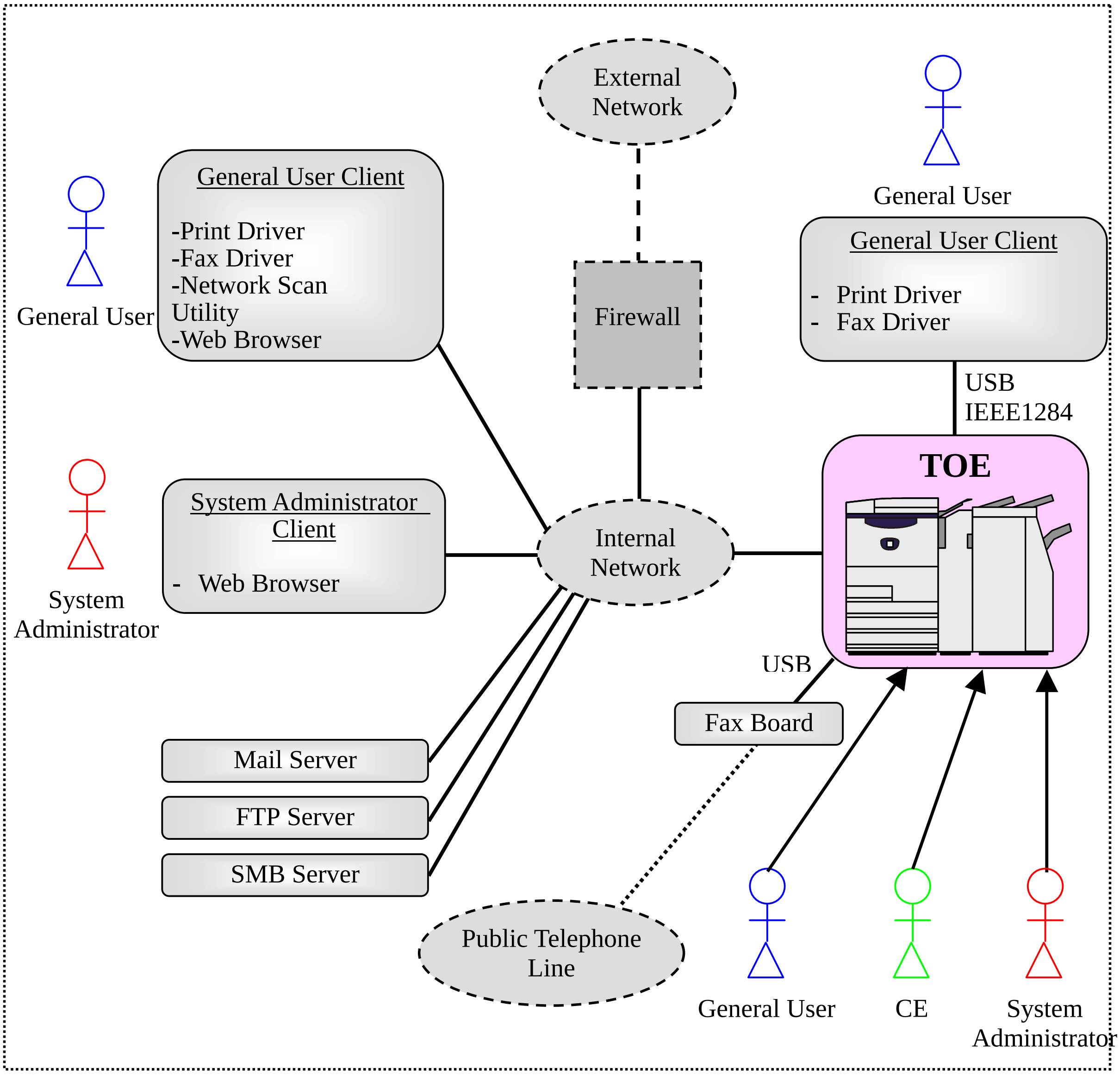

Figure 1: Intended Operational Environment

The following conditions are intended for the internal network environment linked to MFP:

(1) General user client:

When a client is linked to the MFP via the internal network and 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 configurations which user 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 or IEEE1284 and print driver and fax driver are installed to the client, the user can request the MFP to print and fax the document data.

(2) System administrator client:

A system administrator can refer to and change TOE configuration data and download security audit log data via Web browser.

(3) Mail server:

The MFP sends/receives document data to/from Mail server via mail protocol.

(4) FTP server:

The MFP sends document data to FTP server via FTP.

(5) SMB server:

The MFP sends document data to SMB server via SMB.

(6) 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 OSs of general user client (1) and system administrator client (2) are assumed to be Windows 2000, Windows XP, and Windows Vista.

2.1.3.2. Security Function Overview

The following are the overview of the security functions provided by this TOE:

- Hard Disk Data Overwrite prevents unauthorized disclosure of used document data. The document data created during each job processing is temporarily stored in the internal HDD. After each job is completed, the used data is overwritten with new data by this function.

  The function of Hard Disk Data Encryption is also provided to prevent unauthorized disclosure of the document data which was created during each job processing. The document data is encrypted before stored into the internal HDD.
- Internal Network Data Protection protects the security of communication data (document data, security audit log data, and TOE configuration data). The TOE supports general encryption communication protocols such as SSL/TLS, IPSec, SNMPv3, and S/MIME, which enable the secure data transmission between TOE and the remote.
- Security Audit Log monitors unauthorized use of TOE or attempts to it. 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.
- System Administrator’s Security Management restricts the right to configure TOE security functions to the authenticated system administrator. To refer to or renew TOE operational configurations, a system administrator needs to enter his/her ID and password from the control panel and Web browser.
- User Authentication restricts the right to use TOE functions to the authenticated general user. To use TOE, a user needs to enter his/her ID and password from the control panel, Web browser, or Network Scan Utility.

- Customer Engineer Operation Restriction enables a system administrator to inhibit CE from configuring TOE security functions. This function prevents configuration change by an attacker who is impersonating CE.
- FAX Flow Security prevents unauthorized access to the internal network via telephone line or a modem used for fax function. The data other than fax data cannot flow into the internal network so that unauthorized access is blocked.

2.2. 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 (Key operator and SA)	A user who is authorized to manage the device using the tool mode. The system administrator can refer to and rewrite, via Web browser or the control panel, the TOE configuration for device operation and that for security functions.

2.3. Logical Scope and Boundary

The TOE logical scope consists of each function of the programs recorded in Controller ROM. Figure 2 shows the logical architecture of the TOE.

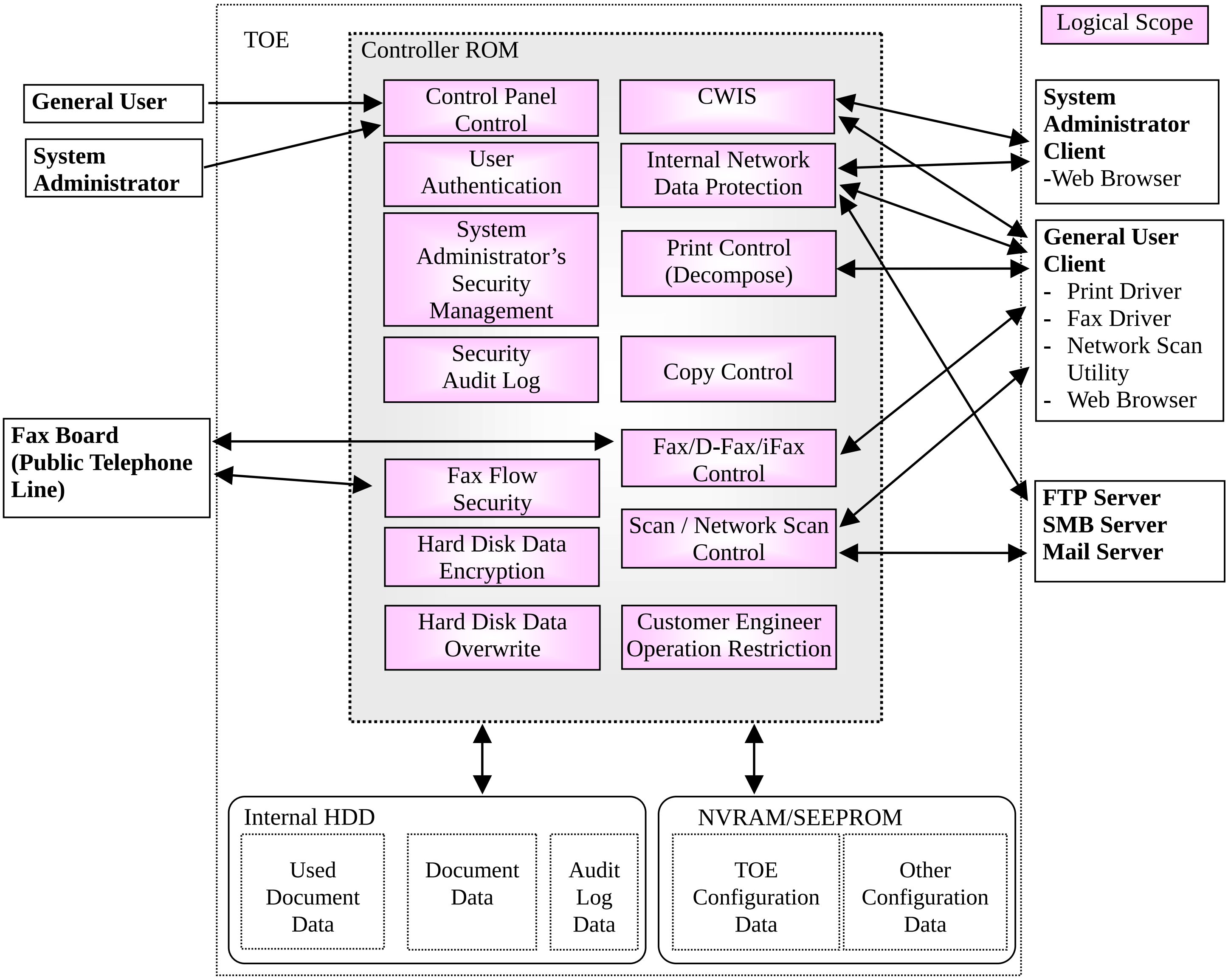

Figure 2: MFP Units and TOE Logical Scope

2.3.1. Basic Functions

The TOE provides the functions of control panel, copy, print, scan, fax, iFax / D-Fax, and CWIS to general user.

2.3.1.1. Control Panel Function

Control panel function is for general user and system administrator to operate MFP functions. Buttons, lamps, and a touch screen panel are mounted on the control panel.

2.3.1.2. 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.

2.3.1.3. Print Function

Print function is to print out the data according to the instruction from 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.

2.3.1.4. 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 then 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.

2.3.1.5. 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 then sent to the destination via public telephone line. The document data is received from the sender's machine and then printed out from the recipient's IOT.

2.3.1.6. iFax / D-Fax Functions

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 then sent to the destination via the Internet. The document data is received from the sender's machine via the Internet and then printed out from the recipient's IOT.

D-Fax function is to directly fax document data to the destination. According to the general user's instruction from his/her 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.

2.3.1.7. CWIS Function

CWIS is to retrieve the scanned document data and the received fax data from the internal HDD according to the instruction from Web browser of the general user client.

A system administrator can also access and rewrite TOE configuration data in the function of System Administrator's Security Management. For this, the system administrator must be authenticated by his/her ID and password entered from Web browser of the system administrator client.

2.3.2. Security Functions

The TOE is a MFP and not a general-purpose computer nor software. Therefore, its security functions are not architecturally jeopardized by such factors as bypass, destruction, interception, and alteration. The security functions provided by the TOE are the following:

2.3.2.1. 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 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.

2.3.2.2. Hard Disk Data Encryption (TSF_CIPHER)

The document data and security audit log data are encrypted before stored into the internal HDD.

2.3.2.3. User Authentication (TSF_USER_AUTH)

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

Only the authenticated general user can use the following functions:
(1) Functions controlled by the MFP control panel:
Copy, fax (send), iFax (send), 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.)
(2) Functions controlled by Network Scan Utility of general user client:
Function to retrieve document data from Mailbox
(3) 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 print function by file designation from CWIS (Private Print function).

Figure 3 shows the authentication flow of the above functions.

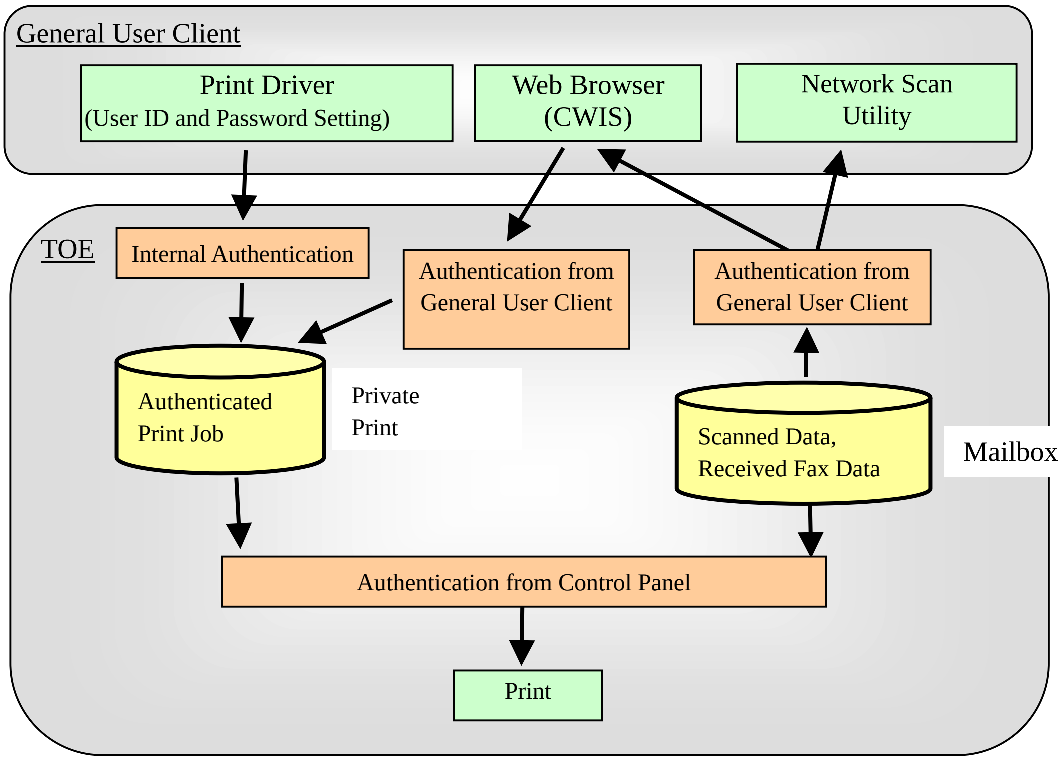

Figure 3: Authentication Flow for Private Print and Mailbox

- Private Print Function

To enable this function, the user needs to configure the MFP to "store an authenticated job to Private Print area*" and also needs to preset his/her ID and password from print driver of the general user client. When a general user sends a print request from print driver, the MFP compares the user ID and password against those preset in the MFP. 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 the general user client.
To refer to the stored print data, a general 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 scanned data and received fax data can be stored into Mailbox from IIT and fax board which are not shown in Figure 3.
To store the scanned data into Mailbox, a general 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 store the received fax data into Mailbox, user authentication is not required. Among the received fax

data transmitted over public telephone line, the following data are automatically classified and stored into each corresponding Mailbox: the received fax data whose corresponding Mailbox is specified by the sender, the received fax data from a particular sender (the data is classified according to the sender's telephone number), and the received fax data from an unknown sender.

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 MFP compares the user ID and password preset in the device against those entered by the general user from the control panel, CWIS, or Network Scan Utility.

Besides Personal Mailbox, Shared Mailbox is provided so that authorized general users can share the same Mailbox. Only a key operator can create the Shared Mailbox.

2.3.2.4. 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 tool 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;
- Configure the cryptographic seed key for Hard Disk Data Encryption;
- Enable or disable use of password entered from MFP control panel in user authentication;
- Change the ID and password of key operator (only a key operator is privileged);
- Change the ID and password of SA and general user;
- Set the allowable number of system administrator's authentication failures before access denial;
- Configure the minimum password length (for general user and SA);
- Enable or disable Customer Engineer Operation Restriction;
- Enable/disable SSL/TLS communication and configure the detail;
- Enable/disable IPSec communication and configure the detail;
- Enable/disable S/MIME communication and configure the detail;
- Enable/disable Scheduled Image Overwrite and set the time;
- Configure User Authentication;
- Set date and time.

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

- Change the ID and password of key operator (only a key operator is privileged);
- Change the ID and password of SA and general user;
- Set the allowable number of system administrator's authentication failures before access denial;
- Enable or disable Audit Log;
- Enable/disable SSL/TLS communication and configure the detail;

- Enable/disable IPSec communication and configure the detail;
- Enable/disable SNMPv3 communication and configure the detail;
- Configure the authentication password for SNMPv3 communication;
- Enable/disable S/MIME communication and configure the detail;
- Download/upload and create an X.509 certificate;
- Enable/disable Scheduled Image Overwrite and set the time;
- Configure User Authentication.

2.3.2.5. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

A system administrator can restrict CE's operation in the tool mode to inhibit CE from referring to or changing TOE security configurations. This function can prevent configuration change by an attacker who is impersonating CE.

2.3.2.6. Security Audit Log (TSF_FAU)

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 the system administrator can supervise or analyze the log data by downloading it in the form of tab-delimited text file via Web browser. To download the log data, SSL/TLS communication needs to be enabled.

2.3.2.7. Internal Network Data Protection (TSF_NET_PROT)

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

- SSL/TLS
- IPSec
- SNMPv3
- S/MIME

2.3.2.8. 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 inside or its internal network via the fax board.

2.4. Physical Scope and Boundary

Figure 4 shows configuration of each unit and TOE physical scope.

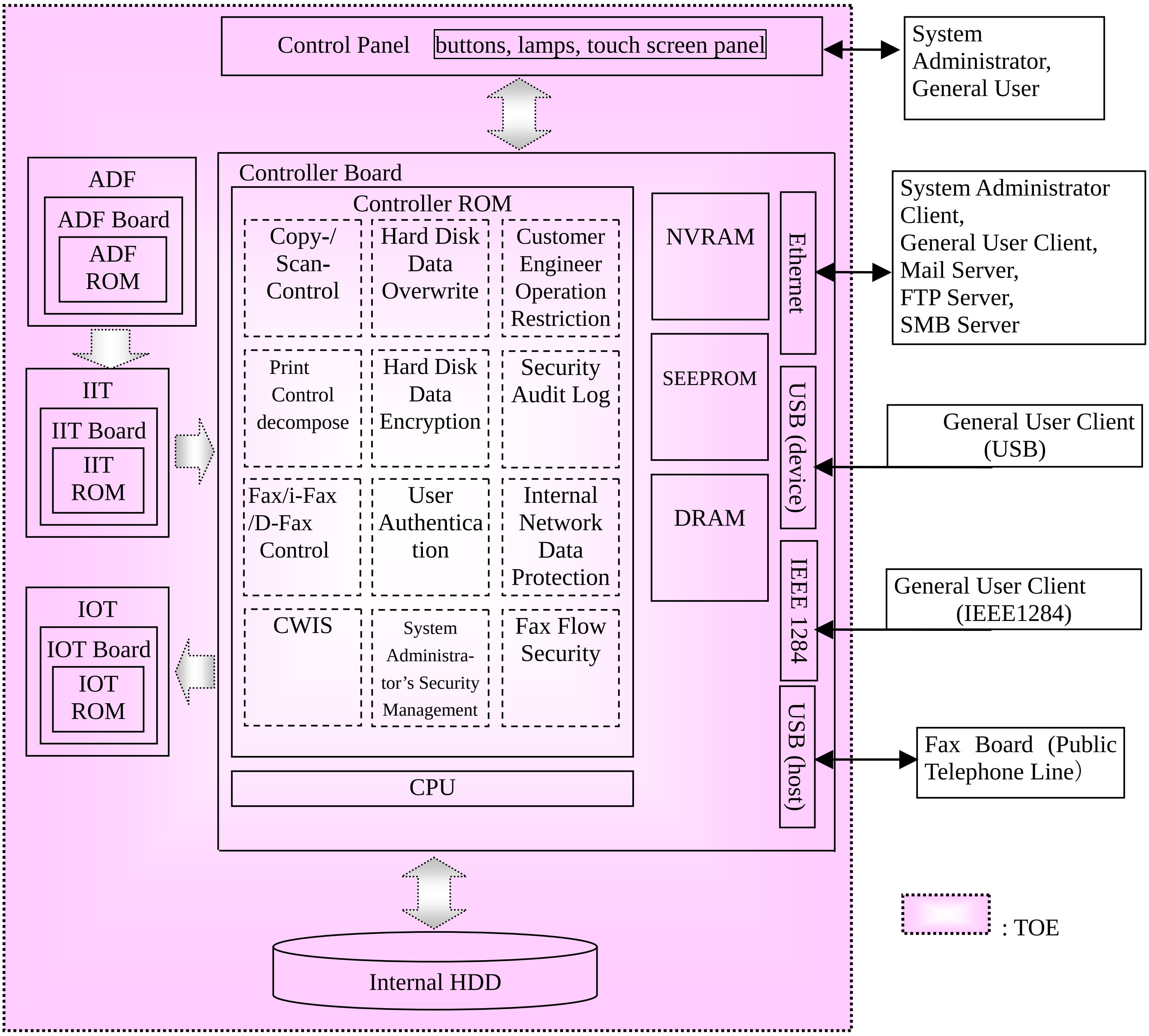
Control Panel
buttons, lamps, touch screen panel
System Administrator, General User
ADF
ADF Board
ADF ROM
IIT
IIT Board
IIT ROM
IOT
IOT Board
IOT ROM
Controller Board
Controller ROM
Copy-/ Scan-Control
Hard Disk Data Overwrite
Customer Engineer Operation Restriction
Print Control decompose
Hard Disk Data Encryption
Security Audit Log
Fax/i-Fax /D-Fax Control
User Authentication
Internal Network Data Protection
CWIS
System Administrator's Security Management
Fax Flow Security
NVRAM
SEEPROM
DRAM
Ethernet
USB (device)
IEEE 1284
USB (host)
CPU
System Administrator Client, General User Client, Mail Server, FTP Server, SMB Server
General User Client (USB)
General User Client (IEEE1284)
Fax Board (Public Telephone Line）
: TOE
Internal HDD

Figure 4: MFP Units and TOE Physical Scope

The physical scope of this TOE is the whole MFP except fax board. The TOE physical scope consists of the PWB units of controller board, control panel, ADF board, IIT board, and IOT board.

The controller board is connected to the control panel and the ADF board 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 print interfaces (IEEE1284 and USB device） 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, print, scan, and fax.

The ADF (Automatic Document Feeder) is a device to automatically feed more than one original.

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

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

2.5. Assets Protected by TOE

This TOE protects the following assets:

- Right to use MFP functions
  The general user’s right to use each function of TOE is assumed as an asset to be protected.
- Document data stored for job processing
  When a general user uses MFP functions of copy, print, fax, 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 MFP from the 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.
- Used document data
  When a general user uses MFP functions of copy, print, fax, 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.
- 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 MFP by CWIS function. The log data is assumed as an asset to be protected.
- TOE configuration data
  A system administrator can configure TOE security functions from the MFP control panel or system administrator client by the function of System Administrator’s Security Management. The configuration data stored in the TOE (see Table 3) can be a threat to other assets if used without authorization and is assumed as an asset to be protected.

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. This is because TOE functions prevent the access to the internal network from public telephone line and it cannot be a threat.

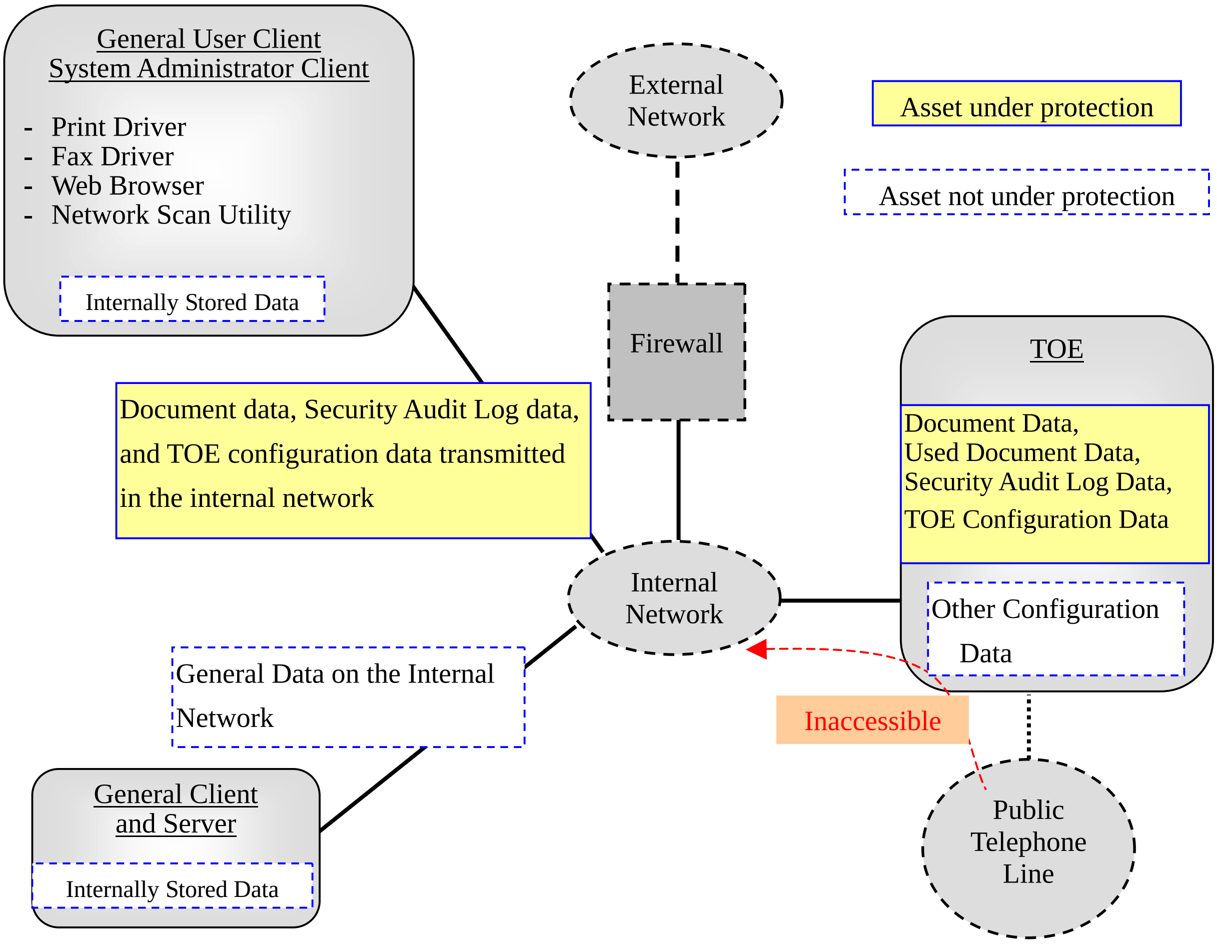

Figure 5: Assets under and not under Protection

Table 3 categorizes the TOE configuration data recorded in NVRAM and SEEPROM of the controller board.

Table 3: Categories of TOE Configuration Data

Categories of TOE Configuration Data (Note)
Data on Hard Disk Data Overwrite
Data on Hard Disk Data Encryption
Data on System Administrator’s Security Management
Data on Customer Engineer Operation Restriction
Data on Internal Network Data Protection
Data on Security Audit Log
Data on Mailbox
Data on User Authentication
Data on date and time

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

3. TOE SECURITY ENVIRONMENT

This chapter describes the security aspects of the intended environment for the TOE. This includes assumptions regarding the TOE, threats to the TOE, and organizational security policy.

3.1. Assumptions

Table 4 shows the assumptions for the operation and use of this TOE.

Table 4: 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: 9 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 • Type of authentication: User Authentication enabled • Length of user password (for general user and SA): 9 characters or more • Private Print configuration: store an authenticated job to Private Print area • Audit Log: enabled • SNMPv3 communication: enabled • Length of authentication password for SNMPv3 communication: 8 characters or more • SSL/TLS communication: enabled • IPSec communication: enabled • S/MIME communication: enabled • SMB communication: disabled • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters • Scheduled Image Overwrite: enabled

3.2. Threats

Table 5 identifies the threats addressed by the TOE. These threats are considered to be users with public knowledge of how the TOE operates. The attackers are considered to have low-level attack capability.

Table 5: Threats Addressed by the TOE

Threat (Identifier)	Description
Unauthorized retrieval of document data and security audit log 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 stored document data, used document data, and security audit log data.
Unauthorized access to document data and TOE configuration data	
T.CONFDATA	An attacker may access, read, or alter, from control panel or Web browser, the TOE configuration 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.
Interception of document data and TOE configuration data	
T.COMM_TAP	An attacker may intercept or alter document data, security audit log data, and TOE configuration data on the internal network.
T.CONSUME	An attacker may access TOE and use TOE functions without authorization.

3.3. Organizational Security Policy

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

Table 6: Organizational Security Policy

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

4. SECURITY OBJECTIVES

This section describes the security objectives for the TOE and for the environment.

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

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 encrypts the document data and security audit log data to be stored in the internal HDD so that they cannot be analyzed even if retrieved.
O.COMM_SEC	The TOE protects the document data, security audit log data, and TOE configuration data on the internal network between TOE and the remote from interception and alteration.
O.FAX_SEC	The TOE must prevent the unauthorized access to internal network via fax modem from public telephone line.
O.MANAGE	The TOE must inhibit a general user from accessing TOE configuration data and security audit log data. The TOE allows only the authenticated system administrator to access the tool mode which enables security function configuration.
O.RESIDUAL	The TOE must prevent the used document data in the internal HDD from being reproduced or recovered.
O.USER	The TOE must provide the function for a general user to identify TOE user and allow only the proper user to read the document data.
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	An administrator of organization assigns an appropriate and reliable person for TOE management as a system administrator and trains him/her.
OE.AUTH	A system administrator needs to configure the TOE security functions as follows. • Use of password entered from MFP control panel in user authentication: enabled • Length of system administrator password: 9 characters or more • Access denial due to authentication failure of system administrator ID:

Security Objectives (Identifier)	Description
	enabled • Allowable number of system administrator's authentication failures before access denial: 5 • Customer Engineer Operation Restriction: enabled • Type of authentication: User Authentication enabled (select Local Authentication) • Length of user password (for general user and SA): 9 characters or more • Private Print configuration: store an authenticated job 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 configuration data are protected from interception. • SNMPv3 communication: enabled • Length of authentication password for SNMPv3 communication: 8 characters or more • SSL/TLS communication: enabled • IPSec communication: enabled • S/MIME communication: enabled • SMB communication: disabled
OE.FUNCTION	A system administrator needs to configure the TOE functions of Hard Disk Data Overwrite, Hard Disk Data Encryption, and Security Audit Log as follows. • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters • Scheduled Image Overwrite: enabled • Security Audit Log: enabled

5. IT SECURITY REQUIREMENTS

This chapter describes TOE security requirements and the security functional requirements to the IT environment.

5.1. TOE Security Functional Requirements

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

5.1.1. Class FAU: Security Audit

(1) FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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: *not specified*] level of audit; and

c) [assignment: *Individually defined auditable events*].

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, and the outcome (success or failure) of the event; and for each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *none*].

Dependencies: FPT_STM.1 Reliable time stamps

Table 9 shows the actions to be audited (defined by CC) and the corresponding auditable events (events to be recorded as execution log) of TOE.

Table 9: 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	Basic: Reading of information from the audit records.	*Basic: Successful download of audit log data.*
FAU_SAR.2	Basic: Unsuccessful attempts to read information from the audit records.	*Basic: Unsuccessful download of audit log data.*
FAU_STG.1	None	-
FAU_STG.4	Basic: Actions taken due to the audit storage failure.	*None*
FCS_CKM.1	Minimal: Success and failure of the activity.	*None*

	Basic: The object attribute(s), and object value(s) excluding any sensitive information (*e.g.* secret or private keys).	
FCS_COP.1	Minimal: Success and failure, and the type of cryptographic operation. Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	*None*
FDP_ACC.1	None	-
FDP_ACF.1	Minimal: Successful requests to perform an operation on an object covered by the SFP. Basic: All requests to perform an operation on an object covered by the SFP. 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	Minimal: Decisions to permit requested information flows. Basic: All decisions on requests for information flow. Detailed: The specific security attributes used in making an information flow enforcement decision. 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	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_UAU.2	Minimal: Unsuccessful use of the authentication mechanism; Basic: All use of the authentication mechanism.	*<Minimal>* *Continuous authentication failures.*

FIA_UAU.7	None	-
FIA_UID.2	Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; Basic: All use of the user identification mechanism, including the user identity provided.	*<Minimal>* *Continuous authentication failures.*
FMT_MOF.1	Basic: All modifications in the behavior of the functions in the TSF.	*<Basic>* *Changes in security function configuration.*
FMT_MSA.1	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	Basic: Modifications of the default setting of permissive or restrictive rules. Basic: All modifications of the initial values of security attributes.	*<Individually defined auditable events>* *Successful/unsuccessful authentication of system administrator.*
FMT_MTD.1 .	Basic: All modifications to the values of TSF data.	*<Individually defined auditable events>* *Changes in security function configuration.*
FMT_SMF.1	Minimal: Use of the management functions.	*<Individually defined auditable events>* *Successful/unsuccessful authentication of system administrator.*
FMT_SMR.1	Minimal: modifications to the group of users that are part of a role; Detailed: every use of the rights of a role.	*<Individually defined auditable events>* *Successful/unsuccessful authentication of system administrator.*
FPT_RVM.1	None	-
FPT_STM.1	Minimal: changes to the time; Detailed: providing a timestamp.	*<Minimal>* *Changes in time setting.*
FTP_TRP.1	Minimal: Failures of the trusted path functions. Minimal: Identification of the user	*<Individually defined auditable events>* *Creation/deletion of certificates.*

	associated with all trusted path failures, if available. Basic: All attempted uses of the trusted path functions. Basic: Identification of the user associated with all trusted path invocations, if available.	

(2) FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [assignment: *system administrator*] with the capability to read [assignment: *all log 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.

Dependencies: FAU_GEN.1 Audit data generation

(3) FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

(4) FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized delete.

FAU_STG.1.2 The TSF shall be able to [selection: *prevent*] unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

(5) FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall [selection: *overwrite the oldest stored audit records*] and [assignment: *no other actions to be taken*] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2. Class FCS: Cryptographic support

(1) FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *the Fuji Xerox's standard method, FXOSENC*] and specified cryptographic key sizes [assignment: *128 bits*] that meet the following: [assignment: *none*].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

(2) FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1 The TSF shall perform [assignment: *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*] in accordance with a specified cryptographic algorithm [assignment: *AES*] and cryptographic key sizes [assignment: *128 bits*] that meet the following: [assignment: *FIPS PUB 197*].

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3. Class FDP: User data protection

(1) FDP_ACC.1 Subset access control

Hierarchical to: No other components

FDP_ACC.1.1 The TSF shall enforce the [assignment: *MFP access control SFP*] on [assignment: *subjects, objects, and operations between subjects and objects listed in Table 10*].

Table 10: Operations between Subjects and Objects Covered by MFP Access Control SFP

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

General user process	*Mailbox*	*Creation of Personal Mailbox* *Deletion of Personal Mailbox* *Storage of document data* *Retrieval of document data* *Deletion of document data*
	Store Print	*Storage of document data* *Deletion of document data* *Retrieval of document data*

Dependencies: FDP_ACF.1 Security attribute based access control

(2) FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

FDP_ACF.1.1 The TSF shall enforce the [assignment: *MFP access control SFP*] to objects based on the following: [assignment: *general user identification information corresponding to the general user process, owner identification information corresponding to each Mailbox, and owner identification information 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: *the rules, shown in Table 11, for controlling the access of the controlled subjects to the controlled objects for the controlled operations*].

Table 11: Rules for Access Control

General User Process
Rules for Mailbox Operation
- *Creation of Personal Mailbox* *In the general user process to create Personal Mailbox, the Personal Mailbox in which general user identification information is set as its owner is created.* - *Deletion of Personal Mailbox* *When the general user identification information of the general user process matches the owner identification information 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 identification information of the general user process matches the owner identification information 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
- *Storage of document data* *In the general user process to store document data, the Store Print area in which*

general user identification information is set as its owner is created. The document data is then stored inside. - *Deletion and retrieval of document data* *When the general user identification information of the general user process matches the owner identification information 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.*
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: *the rules, shown in Table 12, for explicitly authorizing access of the subject to an object based on security attributes*].

Table 12: Rules for Explicit Access Authorization

Key Operator Process
Rule for Mailbox Operation
- *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, 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*: no rules to explicitly deny the access*].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

(3) FDP_IFC.1 Subset information flow control

Hierarchical to: No other components

FDP_IFC.1.1 The TSF shall enforce the [assignment: *fax information flow control SFP*] on [assignment: *subjects, information, and operations to cause the information flow, listed in Table 13.*]

Table 13: 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*

Dependencies: FDP_IFF.1 Simple security attribute

(4) FDP_IFF.1 Simple security attribute

Hierarchical to: No other components

FDP_IFF.1.1 The TSF shall enforce the [assignment: *fax information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *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*: 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: *none*].

FDP_IFF.1.4 The TSF shall provide the following [assignment: *none*].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *none*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

(5) FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: No other components

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *deallocation of the resource from*] the following objects: [assignment: *used document data stored in the internal HDD*].

Dependencies: No dependencies.

5.1.4. Class FIA: Identification and authentication

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

Hierarchical to: No other components

FIA_AFL.1.1 (1) The TSF shall detect when [selection: [assignment: *five*]] unsuccessful authentication attempts occur related to [assignment: *system* *administrator authentication*].

FIA_AFL.1.2 (1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *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*].

Dependencies: FIA_UAU.1 Timing of Authentication

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

Hierarchical to: No other components

FIA_AFL.1.1 (2) The TSF shall detect when [selection: [assignment: *one*]] unsuccessful authentication attempts occur related to [assignment: *general user authentication*].

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

Dependencies: FIA_UAU.1 Timing of Authentication

(2) FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

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.

Dependencies: FIA_UID.1 Timing of identification

(3) FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only [assignment: *display of asterisks (“*”) to hide the entered password characters*] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

(4) FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

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

Dependencies: No dependencies.

5.1.5. Class FMT: Security management

(1) FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *enable, disable, or modify the behavior of*] the functions [assignment: *for security listed in Table 14*] to [assignment: *the roles listed in Table 14*].

Table 14: List of Security Functions

TSF Data	Behavior	Role
Customer Engineer Operation Restriction	*Enable, disable*	*Key operator, SA*
Hard Disk Data Encryption	*Enable, disable*	*Key operator, SA*
System Administrator's Security Management	*Enable, disable, modify*	*Key operator, SA*
Security Audit Log	*Enable, disable*	*Key operator, SA*
User Authentication	*Enable, disable, modify*	*Key operator, SA*
Internal Network Data Protection	*Enable, disable, modify*	*Key operator, SA*
Hard Disk Data Overwrite	*Enable, disable, modify*	*Key operator, SA*

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

(2) FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce the [assignment: *MFP access control SFP*] to restrict the ability to [selection: *query, delete*, [assignment: *create*]] the security attributes [assignment: *general user identifier, Mailbox owner identifier, and Store Print owner identifier*] to [assignment: *the operations and roles listed in Table 15*].

Table 15: Security Attributes and Authorized Roles

Security Attribute	Operation	Role
General user identifier	*Query, delete, create*	*Key operator, SA*
Mailbox owner identifier (Personal Mailbox)	*Query, delete, create*	*General user*
	Query, delete,	*Key operator*
Mailbox owner identifier (Shared Mailbox)	*Query, delete, create*	*Key operator*
Store Print owner identifier	*Query, delete*	*Key operator, SA, general user*

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

(3) FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

FMT_MSA.3.1 The TSF shall enforce the [assignment: *MFP access control SFP*] to provide [selection, choose one of: *permissive*, [assignment*: none]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *none*] to specify alternative initial values to override the default values when an object or information is created.

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

(4) FMT_MTD.1 Management of TSF data
Hierarchical to: No other components
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *query, modify, delete*, [assignment: *none*] the [assignment: *TSF data listed in Table 16*] to [assignment: *the operations and roles listed in Table 16*].

Table 16: Operation of TSF Data

TSF Data	Operation	Role
Information on key operator	*Query, modify*	*Key operator*
Information on SA	*Query, modify*	*Key operator, SA*
Information on Customer Engineer Operation Restriction	*Query, modify*	*Key operator, SA*
Information on Hard Disk Data Encryption	*Query, modify*	*Key operator, SA*
Information on System Administrator's Security Management	*Query, modify*	*Key operator, SA*
Information on Security Audit Log	*Query, modify*	*Key operator, SA*
Information on User Authentication (authentication information of key operator, SA, and general user)	*Query, modify, delete*	*Key operator, SA*
Information on User Authentication (general user's own authentication information)	*Query, modify*	*General user*
Information on Internal Network Data Protection	*Query, modify, delete*	*Key operator, SA*
Information on Hard Disk Data Overwrite	*Query, modify*	*Key operator, SA*
Information on date and time	*Query, modify*	*Key operator, SA*

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

(5) FMT_SMF. Specification of Management Functions
Hierarchical to: No other components
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: S*ecurity Management Functions listed in Table17*].

Table 17: Security Management Functions Provided by TSF

Functional requirements	Management items defined by CC	Management functions of TOE
FAU_GEN.1	None	-
FAU_SAR.1	Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	*System Administrator's Security Management*
FAU_SAR.2	None	-
FAU_STG.1	None	-
FAU_STG.4	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	The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (*e.g.* public, private, secret), validity period, and use (*e.g.* digital signature, key encryption, key agreement, data encryption).	*None* *Reason: Management of changes in cryptographic-key attribute is not necessary because the size of cryptographic key is fixed and there are no other attributes.*
FCS_COP.1	None	-
FDP_ACC.1	None	-
FDP_ACF.1	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	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	The choice of when to perform residual information protection (*i.e.* upon allocation or deallocation) could be made configurable within the TOE.	*None* *Reason: The timing is fixed to the time of document-data deletion.*
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.	*System Administrator's Security Management:* *a) Management of allowable number of system administrator's authentication failures* *b) 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.	*System Administrator's Security Management:* *Management of information on system administrator (ID and password)*
FIA_UAU.7	None	-
FIA_UID.2	The management of the user identities.	*None* *Reason: Access is managed using user authentication information (ID and password).*

FMT_MOF.1	Managing the group of roles that can interact with the functions in the TSF;	*None* *Reason: The role group is only a system administrator and is not managed.*
FMT_MSA.1	Managing the group of roles that can interact with the security attributes.	*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.	*None* *Reason: The role group is only a system administrator and is not managed.*
FMT_MTD.1.	Managing the group of roles that can interact with the TSF data.	*None* *Reason: The role group is only a system administrator and is not managed.*
FMT_SMF.1	None	-
FMT_SMR.1	Managing the group of users that are part of a role.	*None* *Reason: The role group is fixed and is not managed.*
FPT_RVM.1	None	-
FPT_STM.1	Management of the time.	*None* *Reason: Managed by system administrator*
FTP_TRP.1	Configuring the actions that require trusted path, if supported.	*Internal Network Data Protection:* *(Configuration of encryption and management of certificate information)*

Dependencies: No dependencies.

(6) FMT_SMR.1 (1) Security role

Hierarchical to: No other components.

FMT_SMR.1.1 (1) The TSF shall maintain the roles [assignment: *system administrator*].

FMT_SMR.1.2 (1) The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of Identification

(7) FMT_SMR.1 (2) Security role

Hierarchical to: No other components.

FMT_SMR.1.1 (2) The TSF shall maintain the roles [assignment: *general user*].

FMT_SMR.1.2 (2) The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.6. Class FPT: Protection of TSF

(1) FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

(2) FPT_STM.1 Quantity reliance time stamp

Hierarchical to: No other components

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

5.1.7. Class FTP: Trusted path/channels

(1) FTP_TRP.1 Trusted path

Hierarchical to: No other components

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: [assignment: *TOE communication service via Web, communication service for print driver, communication service for fax driver, communication service for network utility, and other services which require trusted path*]].

Dependencies: No dependencies.

5.1.8. TOE Security Function Strength

Minimum function strength level of TOE security functions is SOF-basic. TOE security functional requirements that use probabilistic or permutational mechanisms are FIA_AFL.1 (1), FIA_AFL.1 (2), FIA_UAU.2, and FIA_UAU.7.

5.2. TOE Security Assurance Requirements

The requirements for the TOE security assurance are described to Table 18.

The evaluation assurance level of TOE is EAL2. All the requirement components for assurance have quoted directly the component of EAL2 specified by [the CC part 3].

Table 18: EAL2 Assurance Requirements

Assurance Requirements	Assurance Component Name	Dependencies
Class ACM: Configuration management		
ACM_CAP.2	Configuration items	None
Class ADO: Delivery and operation		
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
Class ADV: Development		
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1

Assurance Requirements	Assurance Component Name	Dependencies
ADV_RCR.1	Informal correspondence demonstration	None
Class AGD: Guidance document		
AGD_ADM.1	Administrator guidance	ADV_FSP.1,
AGD_USR.1	User guidance	ADV_FSP.1
Class ATE: Tests		
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-Sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
Class AVA: Vulnerability assessment		
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.3. Security Requirements for the IT Environment

There is no security functional requirement provided by IT environment of TOE.

6. TOE SUMMARY SPECIFICATION

This chapter describes TOE summary specification.

6.1. TOE Security Functions

This TOE provides the following security functions to satisfy the TOE security functional requirements described in section 5.1 of this ST.
Table 19 shows the relations between the security functional requirements and TOE security functions.

(1) Hard Disk Data Overwrite (TSF_IOW)

(2) Hard Disk Data Encryption (TSF_CIPHER)

(3) User Authentication (TSF_USER_AUTH)

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

(5) Customer Engineer Operation Restriction (TSF_CE_LIMIT)

(6) Security Audit Log (TSF_FAU)

(7) Internal Network Data Protection (TSF_NET_PROT)

(8) Fax Flow Security (TSF_FAX_FLOW)

The TOE is a MFP and not a general-purpose computer nor software. Therefore, its security functions are not architecturally jeopardized by such factors as bypass, destruction, interception, and alteration. The logical framework of TOE processing is that every "session" of the MFP is unique so that each TOE security function cannot have bypass measures. Moreover, the TOE security functional requirements control the object transfer between the TOE and its environment so that the interactions between a user and the TOE satisfy the following:

- A user cannot transfer data between domains.
- A user cannot upload the feasible codes, objects, or configuration files to the TOE.
- A user cannot refer to or rewrite the domain data.

The security functions provided by this TOE are configured to certainly operate because it is realized by unique software within the controller ROM, which does not have bypass measures.

Table 19: Relations between Security Functional Requirements and TOE Security Functions

Security functions TOE security functional requirements	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT	TSF_FAX_FLOW
FAU_GEN.1						O		
FAU_SAR.1						O		
FAU_SAR.2						O		
FAU_STG.1						O		
FAU_STG.4						O		
FCS_CKM.1		O						
FCS_COP.1		O						
FDP_ACC.1			O	O				
FDP_ACF.1			O	O				
FDP_IFC.1								O
FDP_IFF.1								O
FDP_RIP.1	O							
FIA_AFL.1 (1)			O					
FIA_AFL.1 (2)			O					
FIA_UAU.2			O					
FIA_UAU.7			O					
FIA_UID.2			O					
FMT_MOF.1				O	O			
FMT_MSA.1			O	O				
FMT_MSA.3				O				
FMT_MTD.1				O	O			
FMT_SMF.1				O				
FMT_SMR.1 (1)				O				
FMT_SMR.1 (2)			O					
FPT_RVM.1	O	O	O	O	O	O	O	O
FPT_STM.1						O		
FTP_TRP.1							O	

6.1.1. Hard Disk Data Overwrite (TSF_IOW)

According to Hard Disk Data Overwrite which is configured by a system administrator using the tool mode, the document data area in the internal HDD is deleted by either one- or three-pass 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 shown in this list at the time of booting the system, this function overwrites and deletes the used document data.

Additionally, Scheduled Image Overwrite function is provided to delete the stored data at the specific time scheduled by a system administrator.

Hard Disk Data Overwrite is configured to certainly operate because it is realized by unique software that does not have bypass measures.

6.1.2. Hard Disk Data Encryption (TSF_CIPHER)

According to Hard Disk Data Encryption which is configured by a system administrator using the tool mode, the document data to be stored into the internal HDD is encrypted.

Using the cryptographic seed key for Hard Disk Data Encryption that was set by a system administrator using the tool mode, TOE generates 128-bit cryptographic key by the Fuji Xerox’s unique FXOSENC method algorithm at the time of booting. (When the cryptographic seed key for Hard Disk Data Encryption is the same, the same cryptographic key is generated.)

Before the data is stored into the internal HDD, it is encrypted with the cryptographic key generated at the time of booting. The stored document data is read after being decrypted with the cryptographic key generated at the time of booting.

As a security mechanism, the cryptographic key is generated using the cryptographic mechanism (encryption with Rijndael Algorithm) at the time of booting and stored on DRAM on the controller board. The cryptographic key is lost when the main unit is powered off.

Hard Disk Data Encryption is configured to certainly operate because it is realized by unique software that does not have bypass measures.

6.1.3. User Authentication (TSF_USER_AUTH)

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

Only the authenticated general user can use the following functions:

(1) Functions controlled by the MFP control panel:

Copy, fax (send),iFax (send), scan, network scan, Mailbox, 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.)

(2) Functions controlled by Network Scan Utility of general user client:

Function to retrieve document data from Mailbox.

(3) 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 print function by file designation from CWIS (Private Print function).

- Private Print Function

To enable this function, the user needs to configure the MFP to "store an authenticated job to Private Print area*" and also needs to preset his/her ID and password from print driver of the general user client. When a general user sends a print request from print driver, the MFP compares the user ID and password against those preset in the MFP. 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.

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 files designated within the general user client.

To refer to the stored print data, a general 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 scanned data and received fax data can be stored into Mailbox from IIT and fax board which are not shown in Figure 3.

To store the scanned data into Mailbox, a general 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 store the received fax data into Mailbox, user authentication is not required. Among the received fax data transmitted over public telephone line, the following data are automatically classified and stored into each corresponding Mailbox: the received fax data whose corresponding Mailbox is specified by the sender, the received fax data from a particular sender (the data is classified according to the sender's telephone number), and the received fax data from an unknown sender.

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 MFP compares the user ID and password preset in the MFP against those entered by the general user from the control panel, CWIS, or Network Scan Utility.

Besides Personal Mailbox, Shared Mailbox is provided so that authorized general users can share the same Mailbox. Only a key operator can create the Shared Mailbox.

* Mailbox can be categorized into Shared Mailbox and Personal Mailbox and operates as follows:

	Personal Mailbox	Shared Mailbox
Creation of Mailbox	Available for general user	Available for key operator
Deletion of	Available for registered general	Available for key operator

Mailbox	user and key operator	
Storage of document data	Available for registered general user and key operator	Available for general user and key operator
Retrieval of document data	Available for registered general user and key operator	Available for general user and key operator
Deletion of document data	Available for registered general user and key operator	Available for general user and key operator

- To identify and authenticate a system administrator (key operator and SA）, the MFP compares the system administrator ID and password preset in the MFP against those entered from the control panel or CWIS of the system administrator client. Only when the authentication is succeeded, he/she can access System Administrator’s Security Management.
- When the authentication of a general user fails for wrong ID and password, the control panel displays "authentication was failed" and requires reentry of the user information.
  Web browser and Network Scan Utility also require reentry of the user information.
- When the authentication of a system administrator fails for wrong ID and password, reentry of the user information is required just as the general user’s authentication failure. However, when unsuccessful authentication attempts occurred five times, the control panel does not accept any operation except power cycle; Web browser does not accept authentication operation until the main unit is cycled.
- Only a system administrator can create, change, and delete the general user ID. A general user can change his/her own password from the control panel.

The entered password characters are all displayed as asterisks (“*”) to hide the password.
User Authentication is configured to certainly operate because it is realized by unique software that does not have bypass measures.

6.1.4. System Administrator’s Security Management (TSF_FMT)

To accord a privilege to a specific user, this function allows only the authenticated system administrator to access the tool mode which enables him/her to refer to and configure the following security functions from the control panel:

- Refer to the setting of TSF_IOW and enable/disable it;
- Refer to the setting of TSF_CIPHER and enable/disable it;
- Configure the cryptographic seed key for Hard Disk Data Encryption;
- Refer to the setting of use of password entered from MFP control panel in user authentication and enable/disable it;
- Refer to the setting of key operator ID and change the 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 TSF_CE_LIMIT and enable/disable it;
- Refer to the setting of SSL/TLS communication of TSF_NET_PROT, enable/disable it, and configure the details;
- Refer to the setting of IPSec communication of TSF_NET_PROT, enable/disable it, and configure the details;
- Refer to the setting of S/MIME communication of TSF_NET_PROT, enable/disable it, and configure the details;
- Refer to the setting of Scheduled Image Overwrite, enable/disable it, and set the time;
- Refer to the setting of TSF_USER_AUTH and enable/disable Local Authentication;
- Refer to and set date and time.

Additionally, the function of TSF_FMT allows only an authenticated system administrator to configure the following TOE security functions via CWIS. The system administrator needs to be authenticated via the Web browser which is securely connectable with HTTPS.

- Refer to the setting of key operator ID and change the 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 the setting of TSF_FAU and enable/disable it,
  （When TSF_FAU 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 TSF_NET_PROT, enable/disable it, and configure the details;
- Refer to the setting of IPSec communication of TSF_NET_PROT, enable/disable it, and configure the details;
- Refer to the setting of SNMPv3 communication of TSF_NET_PROT, enable/disable it, and configure the details;
- Configure authentication password for SNMPv3 communication;
- Refer to the setting of S/MIME communication of TSF_NET_PROT, enable/disable it, and configure the details;
- Download/upload and create an X.509 certificate;
- Refer to the setting of Scheduled Image Overwrite, enable/disable it, and set the time;
- Refer to the setting of TSF_USER_AUTH and enable/disable Local Authentication.

System Administrator’s Security Management is configured to certainly operate because it is realized by unique software that does not have bypass measures.

6.1.5. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

According to Customer Engineer Operation Restriction which is configured by a system administrator using the tool mode, a system administrator can restrict CE’s operation in the tool mode. This prevents

TOE security configurations from being referred to or changed by CE.

Customer Engineer Operation Restriction is configured to certainly operate because it is realized by unique software that does not have bypass measures.

6.1.6. Security Audit Log (TSF_FAU)

According to Security Audit Log which is configured by a system administrator using the tool 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.

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.

A system administrator can access the audit log only via Web browser and the access from the control panel is inhibited. Therefore, the system administrator needs to log in from Web browser to access the audit log. 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.

Table 20 shows the details of the audit log data.

Table 20: 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 User ID), Failed (Invalid Password), Failed
	Logout	
	Locked System Administrator Authentication	- (Number of authentication failures recorded)
	Detected continuous Authentication Fail	
Change in Audit Policy		
Audit Policy	Audit Log	Enable/Disable
Job Status		
Job Status	Print	Completed, Completed with Warnings, Canceled by User, Canceled by Shutdown, Aborted, Unknown
	Copy	
	Scan	
	Fax	
	Mailbox	
	Print Reports	
	Job Flow Service	

Change in Device Settings		
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	
	Import Address Book	
	Export Address Book	
	Export Audit Log	

Security Audit Log is configured to certainly operate because it is realized by unique software that does not have bypass measures.

6.1.7. Internal Network Data Protection (TSF_NET_PROT)

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

(1) SSL/TLS

According to the SSL/TLS communication which is configured by a system administrator using the tool mode, SSL/TLS ensuring secure data transmission is supported. This protects the security of document data, security audit log data, and TOE configuration 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 MFP 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.

(2) IPSec

According to the IPSec communication which is configured by a system administrator using the tool mode, IPSec ensuring secure data transmission is supported. This protects the security of document data, security audit log data, and TOE configuration 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 MFP 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

(3) SNMPv3

According to the SNMPv3 communication which is configured by a system administrator using the tool mode, SNMPv3 is supported. This is one of the security solutions for the network management protocol, SNMP. As defined in IETF RFC3414, SNMPv3 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 SNMPv3 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 MFP main unit.

Cryptographic key generated as SNMPv3 at every session:

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

(4) S/MIME

According to the S/MIME communication which is configured by a system administrator using the tool 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 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 MFP 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

6.1.8. Fax Flow Security (TSF_FAX_FLOW)

The data received from public telephone line must not be sent to the internal network at any case.

6.2. Security Function Strength Level

Among the TOE security functions, is realized by the probabilistic or permutational mechanism. Its function strength level is SOF-basic.

6.3. Assurance Measures

This TOE satisfies the evaluation assurance level of EAL 2. Table 21 shows the TOE's security assurance measures which meet the TOE Security Assurance Requirements described in section 5.2 of this ST.

Table 21: Assurance Components and Assurance Measures

Assurance Requirements	Security Assurance Requirements	Assurance Measures (Identifier)
Class ACM:	Configuration Management	
ACM_CAP.2	Configuration Item	Configuration Management Description TOE Configuration List
Class ADO:	Operation and Delivery	
ADO_DEL.1	Delivery Procedure	Delivery, Introduction, and Operation Procedure Description
ADO_IGS.1	Installation, Generation, and Start-Up Procedures	User Guide
Class ADV:	Development	
ADV_FSP.1	Informal Functional Specification	Functional Specification Disclosure Paper

Assurance Requirements	Security Assurance Requirements	Assurance Measures (Identifier)
ADV_HLD.1	Descriptive High-Level Design	High-Level Design Specification
ADV_RCR.1	Informal Correspondence Demonstration	Correspondence Analysis Description
Class AGD:	Guidance Document	
AGD_ADM.1	Administrator Guidance	User Guide
AGD_USR.1	User Guidance	
Class ATE:	Test	
ATE_COV.1	Evidence of Coverage	Test Plan and Report
ATE_FUN.1	Functional Test	
ATE_IND.2	Independent Testing - Sample	
Class AVA:	Vulnerability Assessment	
AVA1_SOF.1	Evaluation of Security Function Strength	Vulnerability Analysis
AVA1_VLA.1	Developer Vulnerability Analysis	

6.3.1. Configuration Management Description （TAS_CONFIG）

The following are described in the "WorkCentre 7346 Configuration Management Description":

- Function and usage of configuration management system
- Naming rule for the unique identification of TOE
- Configuration items that are included in TOE
- Unique identifier of each configuration item
- How to track the changing history of TOE configuration items

Corresponding security assurance requirement:

- ACM_CAP.2

6.3.2. TOE Configuration List （TAS_CONFIG_LIST）

The following are described in the "WorkCentre 7346 TOE Configuration List":

- TOE configuration items that correspond to the evidential materials
- Version for uniquely identifying TOE configuration items

Corresponding security assurance requirement:

- ACM_CAP.2

6.3.3. Delivery, Introduction, and Operation Procedure Description （TAS_DELIVERY）

The following are described in the "WorkCentre 7346 Delivery, Introduction, and Operation Procedure Description”:

- Procedure to identify TOE and maintain the integrity of TOE in transit
- All procedures that are applied from the creation environment to the delivery to user, for maintaining the security of TOE
- Method to check that TOE is correct when user receives it
- Notes on the security of introduction, installation, and booting, and method to check the correct introduction, installation, and booting
- Exceptional events and measures to deal with such events
- Minimum system requirement that is necessary for the safe introduction and installation

Corresponding security assurance requirement:

- ADO_DEL.1
- ADO_IGS.1

6.3.4. Functional Specification （TAS_FUNC_SPEC）

The following are described in the "WorkCentre 7346 Functional Specification":

- All security functions of TOE, and its external interfaces (only when such interfaces exist)
- Purpose, function, and usage (including parameter, exceptional item, and error message) of the above-described external interfaces
- Complete description of TOE security functions

Corresponding security assurance requirement:

- ADV_FSP.1

6.3.5. High-Level Design Specification （TAS_HIGHLDESIGN）

The following are described in the "WorkCentre 7346 High-Level Design Specifications":

- TOE security functions’ configuration as seen from the subsystems
- Purpose and usage (including exceptional item and error message) of the interfaces among all the subsystems
- Identification of the subsystems that provide security functions and those that do not

Corresponding security assurance requirement:

- ADV_HLD.1

6.3.6. Correspondence Analysis Description （TAS_REPRESENT）

The following are described in the " WorkCentre 7346 Correspondence Analysis Description":

- Analysis of the accurate and complete reflection of security functions in all the design phases

Corresponding security assurance requirement:

- ADV_RCR.1

6.3.7. User Guide （TAS_GUIDANCE）

In the development of TOE, Fuji Xerox creates manuals (Xerox WorkCentre 7300 Series System Administrator's Guide and Xerox WorkCentre 7346 Security Function Supplementary Guide) and reviews the following in the development department, product evaluation department, and technical support department.

(1) Review contents

- Checks the manual’s description of the influence on the security, the policy for maintaining the security, the operation mode, and the contents of the following:

  What to do after the occurrence of the trouble of the hardware or software related to TOE,
  What to do after the occurrence of operational error,
  What to do at the time of initial setting,
  What to do at the recovery from the trouble.

- Checks the unified terminology in all the manuals
- Checks the clarity, rationality, and consistency of the description in the manual
- Checks the consistency among the descriptions in TOE functional specification, test specification, and manual

“Xerox WorkCentre 7300 Series System Administrator's Guide” and “Xerox WorkCentre 7346 Security Function Supplementary Guide” are common to system administrator and general user. The following are described in these user guides.

(2) Description for system administrator

- Management functions that are used by a system administrator, and its interfaces
- How to manage TOE by ensuring the security
- Notes on the functions and authority that should be managed in the environment where the security is ensured
- Notes on all the security-related parameters under the management of a system administrator, and notes on the parameter values
- Types of all the security events that are related to management functions
- Assumptions about system-administrator’s responsibility and behavior
- Contents of warning messages to a system administrator, and clear indication of specific measures to be taken

(3) Description for general user

- How to use the security functions that can be used by a general user
- Functions that are used by a general user, and their interfaces
- Notes on the functions and authority that should be used in the environment where the security is ensured
- Assumptions about general user’s responsibility and behavior
- Contents of warning messages to general user, and clear indication of the specific measures to be taken

Corresponding security assurance requirement:

- ADO_DEL.1
- ADO_IGS.1
- AGD_ADM.1
- AGD_USR.1

6.3.8. Test Plan and Report （TAS_TEST）

The following are described in the "WorkCentre 7346 Test Plan and Report":

- Overall plan which describes the schedule, skills necessary for testers, and configuration of the system used for the test
- Test items
- Test coverage analysis that verifies that all the functions described in the “WorkCentre 7346 Functional Specification” are tested with the test items
- Purpose of each test item
- How to conduct each test item
- Expected result of each test item
- Date of conducting each test item, and name of the test conductor
- Result of each test item.

Corresponding security assurance requirement:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.3.9. Vulnerability Analysis （TAS_VULNERABILITY）

Fuji Xerox creates “WorkCentre 7346 Vulnerability Analysis” to check and evaluate the security strength and vulnerability of TOE. This document verifies that the TOE’s security strength and identified vulnerability are not problematic in an assumed environment. The following are described in the document:

(1) Security strength

- Result of analyzing that the security strength of TOE security function is the same or more of the minimum strength specified in this ST and the same or more of the strength specified in each specification
- Result of checking that strength analysis is conducted to all the functions that use the techniques of probability theory, permutation, combination, and others
- Result of verifying the validity of the assumption of security strength analysis

(2) Vulnerability

- Confirmation of vulnerability analysis being conducted using the information on general security issues and all the materials provided for the evaluation
- Result of testing that all the identified vulnerability is not problematic in an assumed operational environment
- Result of checking that notes on vulnerability related to TOE configuration and settings for functions’

operation-conditions are described in the manual

Corresponding security assurance requirement:

- AVA1_SOF.1
- AVA1_VLA.1

7. PP CLAIMS

This chapter describes Protection Profile (PP) claims.

7.1. PP Reference

There is no reference to PP.

7.2. PP Tailoring

There is no refinement to PP.

7.3. PP Addition

There is no addition to PP.

8. RATIONALE

This chapter describes security objectives rationale, security requirements rationale, and rationale for TOE summary specification.

8.1. Security Objectives Rationale

Table 22 shows the correspondences between TOE/environment security objectives and TOE security environments such as assumptions, threats, and security policy of organization. Table 23 describes that each TOE security environment is assured by TOE/environment security objectives.

Table 22: Correspondences between TOE/Environment Security Objectives and TOE Security Environment

TOE security environment TOE/environment security objectives	A.ADMIN	A.SECMODE	T.RECOVER	T.CONFDATA	T.COMM_TAP	T.DATA_SEC	T.CONSUME	P.FAX_OPT
O.AUDITS				O		O		
O.CIPHER			O					
O.COMM_SEC					O			
O.FAX_SEC								O
O.MANAGE				O		O		
O.RESIDUAL			O					
O.USER						O	O	
O.RESTRICT							O	
OE.ADMIN	O							
OE.AUTH		O		O		O		
OE.COMMS_SEC		O			O			
OE.FUNCTION		O	O			O		

Table 23: Security Objectives Rationale for Each TOE Security Environment

TOE Security Environment	TOE 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

TOE Security Environment	TOE Security Objectives Rationale
	By OE.AUTH, a system administrator sets an appropriate ID and password and enables user authentication. - OE.COMMS_SEC By OE.COMMS_SEC, the internal network data (incl. document data, security audit log data, and TOE configuration data) are protected from interception. - OE.FUNCTION By OE.FUNCTION, Hard Disk Data Overwrite, Hard Disk Data Encryption, and Security Audit Log are enabled.
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 reading-out of the document data and security 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. - O.CIPHER 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 and security audit log data. - O.RESIDUAL 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: - 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, Customer Engineer Operation Restriction) and permits only the authenticated system administrator to change the TOE configuration 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 TOE security functions and to refer to / update the TOE configuration data. - O.AUDITS By O.AUDITS, the audit log function necessary to monitor unauthorized access and the security audit log data are provided.

TOE Security Environment	TOE Security Objectives Rationale
T.CONSUME	By satisfying the following objectives, T.CONSUME can be countered. - O.USER By O.USER, only the authenticated user is allowed to use the MFP. - O.RESTRICT 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. - O.COMM_SEC By O.COMM_SEC, only the legitimate user is allowed to use the MFP through Network Authentication of encryption communication protocol. 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 configuration data). - OE.COMMS_SEC By OE.COMMS_SEC, the document data, security audit log data, and TOE configuration data on the internal network can be protected from interception.
T.DATA_SEC	By satisfying the following objectives, T.DATA_SEC can be countered. - OE.AUTH and OE.FUNCTION By OE.AUTH and OE.FUNCTION, it is necessary to enable the following password and user authentication function and the 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. - O.USER By O.USER, only the authenticated user is allowed to read out the document data and security log data stored in the internal HDD. - O.MANAGE By O.MANAGE, only the authenticated system administrator is allowed to configure the security functions. - O.AUDITS By O.AUDITS, the audit log function necessary to monitor unauthorized access and the security audit log data are provided.
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.

8.2. Security Requirements Rationale

8.2.1. Security Functional Requirements Rationale

Table 24 shows the correspondences between security functional requirements and security objectives. Table 25 describes the rationale demonstrating that each security objective is assured by TOE security functional requirements.

Table 24: Correspondences between Security Functional Requirements and Security Objectives

Security Objectives TOE Security Functional Requirements	O.AUDITS	O.CIPHER	O.COMM_SEC	O.FAX_SEC	O.MANAGE	O.RESIDUAL	O.RESTRICT	O.USER
FAU_GEN.1	O							
FAU_SAR.1	O							
FAU_SAR.2	O				O			
FAU_STG.1	O							
FAU_STG.4	O							
FCS_CKM.1		O				O		
FCS_COP.1		O				O		
FDP_ACC.1								O
FDP_ACF.1								O
FDP_IFC.1				O				
FDP_IFF.1				O				
FDP_RIP.1						O		
FIA_AFL.1 (1)					O			
FIA_AFL.1 (2)							O	O
FIA_UAU.2					O		O	O
FIA_UAU.7					O		O	O
FIA_UID.2					O		O	O
FMT_MOF.1					O			
FMT_MSA.1								O
FMT_MSA.3								O
FMT_MTD.1					O			
FMT_SMF.1					O			
FMT_SMR.1 (1)					O			
FMT_SMR.1 (2)								O
FPT_RVM.1	O	O	O	O	O	O	O	O

Security Objectives TOE Security Functional Requirements	O.AUDITS	O.CIPHER	O.COMM_SEC	O.FAX_SEC	O.MANAGE	O.RESIDUAL	O.RESTRICT	O.USER
FPT_STM.1	O							
FTP_TRP.1			O					

Table 25: Security Objectives to SFR Rationale

Security Objectives	Security Functional Requirement 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. - FDP_IFF.1: The flow is fixed. No event is to be monitored. - FAU_SAR.1 By FAU_SAR.1, the authorized system administrator can read the security audit log data from an audit log file. - FAU_SAR.2 By FAU_SAR.2, only the authorized system administrator can access the audit log. - FAU_STG.1 By FAU_STG.1, the security audit log data stored in an audit log file is protected from unauthorized deletion and modification. - FAU_STG.4 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. - FPT_STM.1 By FPT_STM.1, the auditable events are recorded with time stamp in the audit log, using highly reliable clock of TOE. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not

Security Objectives	Security Functional Requirement Rationale
	bypassed. Thus, the functional requirements related to this objective are surely conducted.
O.CIPHER	O. CIPHER is an objective that encrypts the document data and security audit log 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 in the internal HDD is encrypted and then decrypted when the data is read, in accordance with the determined cryptographic algorithm and cryptographic key size. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.
O.COMM_SEC	O.COMM_SEC is an objective that protects the document data, security log data, and TOE configuration data on the internal network from interception and alteration. By satisfying the following security objectives, O.COMM_SEC can be realized: - FTP_TRP.1 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 configuration data on the internal network can be protected from threats. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.
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. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely

Security Objectives	Security Functional Requirement Rationale
	conducted.
O.MANAGE	O. MANAGE is an objective that allows only an authenticated system administrator to access the tool mode for security function setting and inhibits a general user from accessing the TOE configuration data and security audit log data. By satisfying the following security objectives, O.MANAGE can be realized: - FAU_SAR.2 By FAU_SAR.2, only the authorized system administrator can access the audit log. - FIA_AFL.1 (1) 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. - FIA_UAU.2 By FIA_UAU.2, user authentication is performed to identify a proper system administrator or individual. - FIA_UAU.7 By FIA_UAU.7, illicit leakage of the authentication information is prevented because the authentication feedback is protected. - FIA_UID.2 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, modify, or delete TSF data. - FMT_SMF.1 By FMT_SMF.1, TOE security management functions are provided for system administrator. - FMT_SMR.1 (1) 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. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.

Security Objectives	Security Functional Requirement Rationale
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 objectives, O.RESIDUAL can be realized: - FCS_CKM.1 and FCS_COP.1 By FCS_CKM.1 and FCS_COP.1, the used document data stored in the internal HDD is encrypted and is made unavailable. - FDP_RIP.1 By FDP_RIP.1, the previous information of the used document data file stored in the internal HDD is made unavailable. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.
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 realized: - FIA_AFL.1 (2) By FIA_AFL.1 (2), when user authentication fails, “incorrect password” message is displayed, requesting password re-entry. - FIA_UAU.2 and FIA_UID.2 By FIA_UIA.2 and FIA_UID.2, user authentication is performed to identify a proper general user. - FIA_UAU.7 By FIA_UAU.7, illicit leakage of the authentication information is prevented because the authentication feedback is protected. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. 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 read the document data. By satisfying the following security objectives, O.USER can be realized: - FDP_ACC.1 and FDP_ACF.1 By FDP_ACC.1 and FDP_ACF.1, user authentication is performed. Only authorized general user is allowed to operate the objects. - FIA_AFL.1 (2) By FIA_AFL.1 (2), when user authentication fails, “incorrect password” message is displayed, requesting password re-entry. - FIA_UAU.2 and FIA_UID.2 By FIA_UAU.2 and FIA_UID.2, user authentication is performed to identify a

Security Objectives	Security Functional Requirement Rationale
	proper general user. - FIA_UAU.7 By FIA_UAU.7, illicit leakage of the authentication information is prevented because the authentication feedback is protected. - FMT_MSA.1 By FMT_MSA.1, the query, deletion, and creation of security attributes are managed. - FMT_SMR.1 (2) By FMT_SMR.1 (2), the role of general user is maintained and associated with the general user. - FPT_RVM.1 By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.

8.2.2. Rationale for Security Functional Requirement of IT Environment

There is no security functional requirement provided by TOE IT environment.

8.2.3. Rationale for Minimum Functional Strength Level

This ST is intended for MFP, which is used within the facilities of the organization such as general office on internal network and public telephone line network. Therefore, the TOE has low risk level towards assumed threats.
Therefore, the minimum functional strength level is SOF-basic. The dishonest act by low-level attacker using public information can be fully countered.

The functional strength level of FIA_AFL.1 (1), FIA_AFL.1 (2), FIA_UAU.2, and FIA_UAU.7 is SOF-basic, satisfying the functional security strength that TOE requires.

8.2.4. Dependencies of Security Functional Requirements

Table 26 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 26: 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	FAU_SAR.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
Restricted audit review		
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	FMT_MSA.2: TOE automatically generates the cryptographic key of the fixed 128-bit size from the TOE setting data that was set by system administrator. For this, it is not necessary to assure that only the secure value is accepted. Therefore, the dependency on FMT_MSA.2 does not need to be satisfied.
		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	FMT_MSA.2: TOE automatically generates the cryptographic key of the fixed 128-bit size from the TOE setting data that was set by system administrator. For this, it is not necessary to assure that only the secure value is accepted. Therefore, the dependency on FMT_MSA.2 does not need to be satisfied.
		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.

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_IFC.1 Subset information flow control	FDP_IFF.1	-
FDP_IFF.1 Simple security attributes	FDP_IFC.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_UAU.2 User authentication before any action	-	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_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 (1)	-
FMT_MSA.1 Management of security attributes	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.3 Static attribute initialization	FMT_MSA.1 FMT_SMR.1	-
FMT_MTD.1 Management of TSF data	FMT_SMF.1 FMT_SMR.1 (1)	-
FMT_SMF.1 Specification of management functions	None	
FMT_SMR.1 (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.
FMT_SMR.1 (2) 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_RVM.1 Non-bypassability of the TSP	None	
FPT_STM.1 Reliable time stamp	None	
FTP_TRP.1 Trusted Path	None	

8.2.5. Interactions among Security Functional Requirements

Table 27 describes the interactions among TOE security functional requirements.

Table 27: Interactions among Security Functional Requirements

Functional Requirement		Bypass Prevention	De-activation Prevention
Functional Requirement ID	Requirement Name		
FAU_GEN.1	Audit data generation	FPT_RVM.1	FMT_MOF.1
FAU_SAR.1	Audit review	FPT_RVM.1	FMT_MOF.1
FAU_SAR.2	Restricted audit review	FPT_RVM.1	FMT_MOF.1
FAU_STG.1	Protected audit trail storage	FPT_RVM.1	FMT_MOF.1
FAU_STG.4	Prevention of audit data loss	FPT_RVM.1	FMT_MOF.1
FCS_CKM.1	Cryptographic key generation	FPT_RVM.1	FMT_MOF.1
FCS_COP.1	Cryptographic operation	FPT_RVM.1	FMT_MOF.1
FDP_ACC.1	Subset access control	FPT_RVM.1	FMT_MOF.1
FDP_ACF.1	Access control functions	FPT_RVM.1	FMT_MOF.1

Functional Requirement		Bypass Prevention	De-activation Prevention
Functional Requirement ID	Requirement Name		
FDP_IFC.1	Subset information flow control	FPT_RVM.1	FMT_MOF.1
FDP_IFF.1	Simple security attribute	FPT_RVM.1	FMT_MOF.1
FDP_RIP.1	Subset residual information protection	FPT_RVM.1	FMT_MOF.1
FIA_AFL.1 (1)	Authentication failure handling	FPT_RVM.1	-
FIA_AFL.1 (2)	Authentication failure handling	FPT_RVM.1	-
FIA_UAU.2	User authentication before any action	FPT_RVM.1	-
FIA_UAU.7	Protected authentication feedback	FPT_RVM.1	-
FIA_UID.2	User identification before any action	FPT_RVM.1	-
FMT_MOF.1	Management of security functions behavior	-	-
FMT_MSA.1	Management of security attributes	FPT_RVM.1	-
FMT_MSA.3	Static attribute initialization	FPT_RVM.1	-
FMT_MTD.1	Management of TSF data	FPT_RVM.1	-
FMT_SMF.1	Specification of management functions	-	-
FMT_SMR.1 (1)	Security roles	-	-
FMT_SMR.1 (2)	Security roles	-	-
FPT_RVM.1	Non-bypassability of the TSP	-	-
FPT_STM.1	Reliable time stamp	FPT_RVM.1	FMT_MOF.1
FTP_TRP.1	Trusted Path	FPT_RVM.1	FMT_MOF.1

8.2.5.1. Bypass Prevention

Table 28 describes the rationale for bypass prevention of each security functional requirement that is defined in the Table 27: “Interactions among Security Functional Requirements.”

Table 28: Bypass Prevention Rationale for Security Functional Requirements

Functional Requirement	Bypass Prevention Rationale for Functional Requirements
FPT_RVM.1	
FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FAU_STG.1 FAU_STG.4 FPT_STM.1	These security functional requirements are configured by unique software that does not have bypass measures and cannot be replaced with another software or module. Based on system administrator setting, every time an auditable event occurs, the fact is always recorded in the audit log file with time stamp. Therefore, audit log function cannot be circumvented, and non-bypassability is ensured.

Functional Requirement	Bypass Prevention Rationale for Functional Requirements
FCS_CKM.1 FCS_COP.1	These security functional requirements are configured by unique software that does not have bypass measures and cannot be replaced with another software or module. Based on system administrator setting, the functions are configured to certainly operate. Therefore, cryptographic-key generation and cryptographic operation cannot be circumvented, and non-bypassability is ensured.
FDP_ACC.1 FDP_ACF.1 FIA_AFL.1 (1) FIA_AFL.1 (2) FIA_UAU.2 FIA_UAU.7 FIA_UID.2	These security functional requirements are configured by unique software that does not have bypass measures and cannot be replaced with another software or module. Also, the function of identification and authentication of system administrator is always performed when functions that require user authentication are accessed. Therefore, "user identification before any action," "user authentication before any action," and "protected authentication-feedback" cannot be circumvented, and non-bypassability is ensured. For authentication of system administrator, there is no function to cancel the authentication-denial status that occurs when the number of access denials due to authentication failure reaches its maximum. The operations other than power cycle are disabled. For authentication of general user, an error message is displayed and user authentication cannot be circumvented. Moreover, there is no function to cancel user authentication failure status. Therefore, user authentication cannot be circumvented, and non-bypassability is ensured.
FDP_IFC.1 FDP_IFF.1	These security functional requirements are configured by unique software that does not have bypass measures and cannot be replaced with another software or module. The data received from public telephone line can never be sent to the internal network at any case. Therefore, this function cannot be circumvented, and non-bypassability is ensured.
FTP_TRP.1	This security functional requirement is configured by unique software that does not have bypass measures and cannot be replaced with another software or module. Based on system administrator setting, the function is also configured to certainly operate. In the communication between TOE and the remote, the document data, security audit log data, and TQE configuration data on the internal network are protected from interception. Thus, this function cannot be circumvented, and non-bypassability is ensured.
FDP_RIP.1	This security functional requirement is configured by unique software that does not have bypass measures and cannot be replaced with another software or module. Based on system administrator setting, the functions are also configured to certainly operate. In addition, the TOE is configured that, when overwrite processing is stopped due

Functional Requirement	Bypass Prevention Rationale for Functional Requirements
	to power off, the overwrite deletion processing is re-started by power-on. Thus, this function cannot be circumvented, and non-bypassability is ensured.
FMT_MTD.1	This security functional requirement is configured by unique software that does not have bypass measures and cannot be replaced with another software or module. When TSF data is accessed, the authentication of system administrator always needs to be performed. Thus, this function cannot be circumvented, and non-bypassability is ensured.

8.2.5.2. De-activation Prevention

Table 29 describes the rationale for de-activation prevention of each security functional requirement that is defined in the Table 27: "Interactions among Security Functional Requirements."

Table 29: De-activation Prevention Rationale for Security Functional Requirements

Functional Requirement	De-activation Prevention Rationale for Functional Requirements
FMT_MOF.1	
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, FPT_STM.1	The person who manages the behavior of the following TOE security functions is limited to the system administrator permitted by FMT_MOF.1. Thus, the behavior is protected from being de-activated by general users other than system administrator. - Hard Disk Data Overwrite (TSF_IOW) - Hard Disk Data Encryption (TSF_CIPHER) - System Administrator's Security Management (TSF_FMT) - Customer Engineer Operation Restriction (TSF_CE_LIMIT) - Security Audit Log (TSF_FAU) - Internal network data protection function (TSF_NET_PROTECT) - User authentication function (TSF_USER_AUTH)

8.2.5.3. Interference

Although this TOE is connected to the public telephone line, no unauthorized objects can exist since fax flow security function denies external access at any event. For other interfaces than fax as well, since only a system administrator is allowed to manage the behaviors of security functions, no unauthorized programs and objects can exist. Therefore, access control is not necessary and TOE security functions are not destroyed.

8.2.5.4. Detection of Defeat

For each security function, the audit log is generated on the auditable events listed in Table 9. This enables posterior analysis of security function operations and detects/notifies the possibility of security infringement according to its significance level.

8.2.6. Consistency Rationale between Security Functional Requirements

Some of TOE security functional requirements require security management functions. In [CC Part 2], the management activity that can be foreseen for each functional requirement is assigned as a management requirement of each component. Table 30 shows the management functions that each functional requirement component requires.

The security management functions that are defined in FMT_SMF.1 of "Specification of Management Functions" are in line with the management functions defined in Table 30. Thus, TOE security functional requirements are internally consistent in terms of security management functions.

Table 30: Management Requirements of TOE Security Functions

Functional Requirement		Management functions Required for Each Component
Component	Name	
FAU_GEN.1	Audit data generation	Management of audit log data
FAU_SAR.1	Audit review	-
FAU_SAR.2	Restricted audit review	-
FAU_STG.1	Protected audit trail storage	-
FAU_STG.4	Prevention of audit data loss	-
FCS_CKM.1	Cryptographic key generation	Management of cryptographic seed key data
FCS_COP.1	Cryptographic operation	-
FDP_ACC.1	Subset access control	Management of authorized system administrator ID
FDP_ACF.1	Access control functions	Management of authorized system administrator ID
FDP_IFC.1	Subset information flow control	-
FDP_IFF.1	Simple security attribute	-
FDP_RIP.1	Subset residual information protection	Management of the used document data stored in the internal HDD
FIA_AFL.1 (1)	Authentication failure handling	Management of the number of times for authentication failures
FIA_AFL.1 (2)	Authentication failure handling	-
FIA_UAU.2	User authentication before any action	• Management of system administrator ID • Management of system administrator password data
FIA_UAU.7	Protected authentication feedback	-
FIA_UID.2	User identification before any action	-

Functional Requirement		Management functions Required for Each Component
Component	Name	
FMT_MOF.1	Management of security function behavior	Management of the following function settings: • Hard Disk Data Overwrite (TSF_IOW) • Hard Disk Data Encryption (TSF_CIPHER) • System Administrator's Security Management (TSF_FMT) • Customer Engineer Operation Restriction (TSF_CE_LIMIT) • Security Audit Log (TSF_FAU) • FAX Flow Security (TSF_FAX_FLOW) • Internal network data protection function (TSF_NET_PROTECT) • User authentication function (TSF_USER_AUTH)
FMT_MSA.1	Management of security attributes	• Management of an identifier
FMT_MSA.3	Static attribute initialization	• Management of a suitable default value
FMT_MTD.1	Management of TSF data	• Management of TSF data configuration
FMT_SMF.1	Specification of management functions	-
FMT_SMR.1 (1)	Security roles	-
FMT_SMR.1 (2)	Security roles	-
FPT_RVM.1	Non-bypassability of the TSP	-
FPT_STM.1	Reliable time stamp	Management of date and time
FTP_TRP.1	Trusted Path	-

8.2.7. Requirement Rationale for Security Assurance

This TOE is a MFP, a commercial product. The threats include: attack by a low-level attacker from control panel and Web browser and from network scanner utility via a TOE external interface; interception and alteration of data on the internal network; and reading-out of internal HDD information with commercial tool connected.

Therefore, the TOE is assigned EAL2 assurance level that is supposed to be enough for business use.

8.3. TOE Summary Specification Rationale

8.3.1. Rationale for TOE Security Function Requirements

Table 31 describes the rationale upon which each TOE security functional requirement is satisfied by the corresponding security function as defined in Table 19: “Relations between Security Functional Requirements and TOE Security Functions” in the section “6.1 TOE Security Functions.”

Table 31: Rationale for Relations between Security Functional Requirements and TOE Security Functions

Functional Requirement	Rationale for Relations between Security Function Requirements and TOE Security Functions
FAU_GEN.1	By TSF_FAU, the defined auditable event is recorded in the audit log and the audit data is generated.
FAU_SAR.1	By TSF_FAU, all the information recorded in the audit log can be read.
FAU_SAR.2	By TSF_FAU, the person who reads the audit log is limited to the authenticated system administrator.
FAU_STG.1	By TSF_FAU, the audit log data is protected from untrusted alteration and modification.
FAU_STG.4	By TSF_FAU, 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.
FCS_CKM.1	By TSF_CIPHER, 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.
FCS_COP.1	By TSF_CIPHER, TOE uses the automatically-generated encryption key and can encrypt/decrypt the document data and security audit log data in the internal HDD.
FDP_ACC.1 FDP_ACF.1	By TSF_USER_AUTH, a system administrator needs to perform user authentication before accessing the tool mode. By TSF_USER_AUTH, a general user needs to perform user authentication before accessing the Mailbox or the Store Print. By TSF_FMT, the person who accesses the tool mode is limited to the authenticated system administrator.
FDP_IFC.1 FDP_IFF.1	By TSF_FAX_FLOW, the data received from public telephone line is not sent to the internal network. Thus, the internal network is not accessed.
FDP_RIP.1	By TSF_IOW, TOE overwrites and deletes the used document data file stored in the internal HDD. To control overwrite/delete function, two options are available: one pass (zero) overwrite procedure and three pass (random number / random number / zero) overwrite procedure. 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 and thus can fully confront the low-level attacks trying to reproduce the data. Therefore, three pass is an appropriate number of times to overwrite.
FIA_AFL.1 (1)	By TSF_USER_AUTH, a system administrator needs to perform user authentication before accessing the tool mode. The function for authentication failure handling is provided. When the defined number of access denials due to unsuccessful authentication attempts with system administrator ID has been met or surpassed, any operation except power cycle is disabled.

Functional Requirement	Rationale for Relations between Security Function Requirements and TOE Security Functions
FIA_AFL.1 (2)	By TSF_USER_AUTH, a general user needs to perform user authentication before using MFP functions. However, when the entered password does not match the one set by a proper user, the message saying "incorrect password" is displayed, requesting re-entry of the password.
FIA_UAU.2	By TSF_USER_AUTH, TOE requests a user to enter the password before permitting a system administrator to operate at the control panel or a system administrator or general user to operate at Web browser. The entered password is compared 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.
FIA_UAU.7	By TSF_USER_AUTH, 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.
FIA_UID.2	By TSF_USER_AUTH, TOE requests a user to enter the user ID before permitting a system administrator to operate at the control panel or a system administrator or a general user to operate at Web browser. 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.
FMT_MOF.1	By TSF_FMT and TSF_CE_LIMIT, TOE permits the authenticated system administrator to set the TOE configuration data. The person who changes the TOE configuration data is limited to system administrator.
FMT_MSA.1	By TSF_FMT, TOE limits the person who queries/deletes/creates the identifier of general user and that for Shared Mailbox to system administrator. By TSF_USER_AUTH, TOE permits the authenticated user to query/delete/create the identifier for Personal Mailbox and Store Print.
FMT_MSA.3	By TSF_FMT, TOE offers an appropriate default value.
FMT_MTD.1	By TSF_FMT and TSF_CE_LIMIT, TOE limits the person who changes the TOE configuration data to the authenticated system administrator.
FMT_SMF.1	By TSF_FMT, TOE limits the person who changes the TOE configuration data to the authenticated system administrator.
FMT_SMR.1 (1)	By TSF_FMT, a system administrator's role is maintained and the role is associated with the system administrator.
FMT_SMR.1 (2)	By TSF_USER_AUTH, a general user's role is maintained and the role is associated with the proper general user.
FPT_RVM.1	All TOE security functions are configured to certainly operate because they are realized by unique software that does not have bypass measures.
FPT_STM.1	By TSF_FAU, the time stamp of TOE’s clock function is issued when the defined

Functional Requirement	Rationale for Relations between Security Function Requirements and TOE Security Functions
	auditable event is recorded in the audit log file.
FTP_TRP.1	By TSF_NET_PROT, the document data, security audit log data, and TOE configuration data are protected by the encryption communication protocol that ensures secure data communication between TOE and the remote. 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.

8.3.2. Security Function Strength Rationale

Among TOE security functions, the function which is realized by probabilistic or permutational mechanism is the ID password method of User Authentication (TSF_USER_AUTH). Its function strength is SOF-basic that is claimed in “6.2 Security Function Strength Level.” This satisfies the minimum function strength level SOF-basic that is claimed in “5.1.8 TOE Security Function Strength.” Therefore, both levels are consistent.

8.3.3. Security Assurance Measures Rationale

Table 32 describes the correspondences between assurance measures and security assurance requirements. Table 33 shows that each assurance measure is assured by security assurance requirements. All assurance measures are necessary to realize EAL2 security assurance requirements.

Table 32: Correspondences between Assurance Measures and Security Assurance Requirements

Assurance Measures (identifier) Security Assurance Requirements	TAS_CONFIG	TAS_CONFIG_LIST	TAS_DELIVERY	TAS_FUNC_SPEC	TAS_DISC_PAPER	TAS_HIGHLDESIGN	TAS_REPRESENT	TAS_GUIDANCE	TAS_TEST	TAS_VULNERABILITY
ACM_CAP.2	O	O								
ADO_DEL.1			O					O		
ADO_IGS.1			O					O		
ADV_FSP.1				O	O					
ADV_HLD.1						O				
ADV_RCR.1							O			
AGD_ADM.1								O		
AGD_USR.1								O		
ATE_COV.1									O	

Assurance Measures (identifier) / Security Assurance Requirements	TAS_CONFIG	TAS_CONFIG_LIST	TAS_DELIVERY	TAS_FUNC_SPEC	TAS_DISC_PAPER	TAS_HIGHLDESIGN	TAS_REPRESENT	TAS_GUIDANCE	TAS_TEST	TAS_VULNERABILITY
ATE_FUN.1									O	
ATE_IND.2									O	
AVA_SOF.1										O
AVA_VLA.1										O

Table 33: Sufficiency of Security Assurance Requirements by Assurance Measures

Assurance Measures (identifier)	Assurance Requirement	Sufficiency of Security Assurance Requirements
TAS_CONFIG TAS_CONFIG_LIST	WorkCentre 7346 Configuration Management Description WorkCentre 7346 TOE Configuration List	
	ACM_CAP.2	These documents satisfy the requirements such as naming rule for the unique identification of TOE version, list of configuration items, and unique identifier of each configuration item.
TAS_DELIVERY	WorkCentre 7346 Delivery, Introduction, and Operation Procedure Description	
	ADO_DEL.1	This document satisfies the requirements such as procedure to identify TOE and maintain the integrity of TOE in transit, all procedures that are applied from the creation environment to the delivery to user, and method for a system administrator to check that TOE is correct.
	ADO_IGS.1	This document satisfies the requirements such as notes on security of installation, start-up procedures, method to check that TOE is correct, and measures to deal with exceptional events.
TAS_FUNC_SPEC	WorkCentre 7346 Functional Specification	
	ADV_FSP.1	These documents satisfy the requirements such as the consistent/complete description on TOE security functions and its external interfaces and the detail description of external interfaces.
TAS_HIGHLDESIGN	WorkCentre 7346 Series High-Level Design Specification	

Assurance Measures (identifier)	Assurance Requirement	Sufficiency of Security Assurance Requirements
	ADV_HLD.1	This document satisfies the requirements such as consistent description on TOE security functions configuration, identification/description of interfaces between subsystems, and identification of the subsystems that provide security functions and those that do not.
TAS_REPRESENT	WorkCentre 7346 Correspondence Analysis Description	
	ADV_RCR.1	This document satisfies the requirements for TOE security functions' complete correspondence at each level (TOE summary specification, functional specification, and configuration design specification that are described in this ST).
TAS_GUIDANCE	Xerox WorkCentre 7300 Series System Administrator's Guide, Xerox WorkCentre 7346 Security Function Supplementary Guide	
	ADO_DEL.1	This document satisfies the requirements such as procedure to identify TOE and maintain the integrity of TOE in transit, all procedures that are applied from the creation environment to the delivery to user, and method for a system administrator to check that TOE is correct.
	ADO_IGS.1	This document satisfies the requirements such as notes on security of installation, start-up procedures, method to check that TOE is correct, and measures to deal with exceptional events.
	AGD_ADM.1	This document satisfies the requirements for descriptions on management functions and interfaces available for system administrator, assumptions on system administrator's responsibility and behavior, and measures against warning messages.
	AGD_USR.1	This document satisfies the requirements for descriptions on management functions and interfaces available for general user, assumptions on general user's responsibility and behavior, and measures against warning messages.
TAS_TEST	WorkCentre 7346 Test Plan and Report	
	ATE_COV.1	This document satisfies the requirement for checking the sufficiency/integrity of TOE security functions.
	ATE_FUN.1	This document satisfies the requirement for checking that all the TOE security functions are executed as specified.

Assurance Measures (identifier)	Assurance Requirement	Sufficiency of Security Assurance Requirements
	ATE_IND.2	This document satisfies the requirement for recreating the test environment for TOE security functions and providing the test materials.
TAS_VULNERABILITY	WorkCentre 7346 Vulnerability Analysis	
	AVA_SOF.1	This document satisfies the sufficiency of TOE security strength.
	AVA_VLA.1	This document satisfies the requirement for checking that the identified vulnerability of TOE is not illicitly used in an assumed environment.

As in Table 18 of “5.2 TOE Security Assurance Requirements,” one or more assurance measures correspond to all the TOE security assurance requirements necessary for EAL2. The assurance measures cover the evidences that TOE security assurance requirements defined in this ST request. Therefore, the evidences that TOE security assurance requirements for EAL2 request are all satisfied.

8.4. PP Claims Rationale

There is no applicable PP.