



Fuji Xerox
ApeosPort-II C7500/C6500/C5400,
DocuCentre-II C7500/C6500/C5400
Series Controller Software
for Asia Pacific

Security Target

Version 1.0.7

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

- Table of Contents -

| | | |
|----------|--|----|
| 1. | ST OVERVIEW | 1 |
| 1.1. | ST Identification | 1 |
| 1.2. | ST Overview | 1 |
| 1.3. | Common Criteria Conformance Claim | 2 |
| 1.4. | References | 2 |
| 1.5. | Acronyms and Terminology | 3 |
| 1.5.1. | Acronyms..... | 3 |
| 1.5.2. | Terminology..... | 3 |
| 2. | TOE DESCRIPTION | 7 |
| 2.1. | TOE Overview..... | 7 |
| 2.1.1. | Product Type | 7 |
| 2.1.2. | Service Overview..... | 7 |
| 2.1.2.1. | Environment Assumptions..... | 7 |
| 2.1.2.2. | Security Function Overview | 9 |
| 2.2. | User Assumptions | 9 |
| 2.3. | Logical Scope and Boundary..... | 10 |
| 2.3.1. | Basic Functions..... | 10 |
| 2.3.1.1. | Control Panel Function | 10 |
| 2.3.1.2. | Copy Function | 11 |
| 2.3.1.3. | Print Function | 11 |
| 2.3.1.4. | Scan Function, Network Scan Function..... | 11 |
| 2.3.1.5. | CWIS Function | 11 |
| 2.3.2. | Security Functions | 11 |
| 2.3.2.1. | Hard Disk Data Overwrite (TSF_IOW) | 11 |
| 2.3.2.2. | Hard Disk Data Encryption (TSF_CIPHER)..... | 11 |
| 2.3.2.3. | System Administrator’s Security Management (TSF_FMT)..... | 11 |
| 2.3.2.4. | Customer Engineer Operation Restriction (TSF_CE_LIMIT) | 12 |
| 2.4. | Physical Scope and Boundary | 12 |
| 2.5. | Assets Protected by TOE | 14 |
| 3. | TOE SECURITY ENVIRONMENT | 16 |
| 3.1. | Assumptions | 16 |
| 3.2. | Threats | 16 |
| 3.3. | Organizational Security Policy | 17 |
| 4. | SECURITY OBJECTIVES | 18 |
| 4.1. | Security Objectives for the TOE..... | 18 |
| 4.2. | Security Objectives for the Environment | 18 |

| | | |
|--------|---|----|
| 5. | IT SECURITY REQUIREMENTS..... | 20 |
| 5.1. | TOE Security Functional Requirements..... | 20 |
| 5.1.1. | Class FCS: Cryptographic support..... | 20 |
| 5.1.2. | Class FDP: User data protection..... | 20 |
| 5.1.3. | Class FIA: Identification and authentication | 21 |
| 5.1.4. | Class FMT: Security management..... | 21 |
| 5.1.5. | Class FPT: Protection of TSF..... | 23 |
| 5.1.6. | TOE Security Function Strength..... | 24 |
| 5.2. | TOE Security Assurance Requirements | 24 |
| 5.3. | Security Requirements for the IT Environment | 24 |
| 6. | TOE SUMMARY SPECIFICATION..... | 25 |
| 6.1. | TOE Security Functions | 25 |
| 6.1.1. | Hard Disk Data Overwrite (TSF_IOW) | 26 |
| 6.1.2. | Hard Disk Data Encryption (TSF_CIPHER)..... | 26 |
| 6.1.3. | S..... | 26 |
| 6.1.4. | C..... | 27 |
| 6.2. | Security Function Strength Level..... | 28 |
| 6.3. | Assurance Measures | 28 |
| 6.3.1. | Configuration Management Description (TAS_CONFIG)..... | 29 |
| 6.3.2. | TOE Configuration List (TAS_CONFIG_LIST)..... | 29 |
| 6.3.3. | Delivery, Introduction, and Operation Procedure Description (TAS_DELIVERY)..... | 29 |
| 6.3.4. | Functional Specification (TAS_FUNC_SPEC)..... | 29 |
| 6.3.5. | High-Level Design Specification (TAS_HIGHLDESIGN) | 30 |
| 6.3.6. | Correspondence Analysis Description (TAS_REPRESENT)..... | 30 |
| 6.3.7. | User Guide (TAS_GUIDANCE)..... | 30 |
| 6.3.8. | Test Plan and Report (TAS_TEST) | 31 |
| 6.3.9. | Vulnerability Analysis (TAS_VULNERABILITY) | 32 |
| 7. | PP CLAIMS..... | 33 |
| 7.1. | PP Reference..... | 33 |
| 7.2. | PP Tailoring | 33 |
| 7.3. | PP Addition..... | 33 |
| 8. | RATIONALE..... | 34 |
| 8.1. | Security Objectives Rationale | 34 |
| 8.2. | Security Requirements Rationale | 36 |
| 8.2.1. | Security Functional Requirements Rationale..... | 36 |
| 8.2.2. | Rationale for Security Functional Requirement of IT Environment..... | 38 |
| 8.2.3. | Rationale for Minimum Functional Strength Level..... | 38 |
| 8.2.4. | Dependencies of Security Functional Requirements | 38 |
| 8.2.5. | Interactions among Security Functional Requirements | 40 |

| | | |
|----------|--|----|
| 8.2.5.1. | Bypass Prevention | 41 |
| 8.2.5.2. | De-activation Prevention | 42 |
| 8.2.5.3. | Interference | 42 |
| 8.2.5.4. | Detection of Defeat..... | 42 |
| 8.2.6. | Consistency Rationale between Security Functional Requirements | 43 |
| 8.2.7. | Requirement Rationale for Security Assurance | 43 |
| 8.3. | TOE Summary Specification Rationale | 44 |
| 8.3.1. | Rationale for TOE Security Function Requirements | 44 |
| 8.3.2. | Security Function Strength Rationale | 45 |
| 8.3.3. | Security Assurance Measures Rationale | 45 |
| 8.4. | PP Claims Rationale | 49 |

-

List of Figures and Tables -

| | |
|--|----|
| Figure 1: Intended Operational Environment | 8 |
| Figure 2: MFP Units and TOE Logical Scope | 10 |
| Figure 3: MFP Units and TOE Physical Scope..... | 13 |
| Figure 4: Assets under and not under Protection | 14 |
| | |
| Table 1: User Role Assumptions..... | 9 |
| Table 2: Categories of TOE Configuration Data | 15 |
| Table 3: Assumptions..... | 16 |
| Table 4: Threats Addressed by the TOE | 17 |
| Table 5: Security Objectives for the TOE..... | 18 |
| Table 6: Security Objectives for the Environment..... | 18 |
| Table 7: List of Security Functions..... | 22 |
| Table 8: Operation of TSF Data..... | 22 |
| Table 9: Security Management Functions Provided by TSF | 22 |
| Table 10: EAL2 Assurance Requirements | 24 |
| Table 11: Relations between Security Functional Requirements and TOE Security Functions | 25 |
| Table 12: Assurance Components and Assurance Measures | 28 |
| Table 13: Correspondences between TOE/Environment Security Objectives and TOE Security Environment | 34 |
| Table 14: Security Objectives Rationale for Each TOE Security Environment | 34 |
| Table 15: Correspondences between Security Functional Requirements and Security Objectives | 36 |
| Table 16: Security Objectives to SFR Rationale..... | 36 |
| Table 17: Dependencies of Functional Security Requirements | 38 |
| Table 18: Interactions among Security Functional Requirements | 40 |
| Table 19: Bypass Prevention Rationale for Security Functional Requirements | 41 |
| Table 20: De-activation Prevention Rationale for Security Functional Requirements | 42 |
| Table 21: Management Requirements of TOE Security Functions | 43 |
| Table 22: Rationale for Relations between Security Functional Requirements and TOE Security Functions | 44 |
| Table 23: Correspondences between Assurance Measures and Security Assurance Requirements | 46 |
| Table 24: Sufficiency of Security Assurance Requirements by Assurance Measures | 46 |

1. ST OVERVIEW

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: Fuji Xerox ApeosPort-II C7500/C6500/C5400, DocuCentre-II C7500/C6500/C5400 Series Controller Software for Asia Pacific Security Target

ST Version: 1.0.7

Author: Fuji Xerox Co., Ltd.

Publication Date: December 20, 2007

CC Common Criteria for Information Technology Security Evaluation, Version 2.3

Identification: ISO/IEC 15408 (2005) Interpretations-0512

Keywords: Multifunction System, Multi Function Peripheral, Copy, Print, Scan, Internal Hard Disk Drive, Document Overwrite, Document Encryption

(2) TOE Identification

Fuji Xerox ApeosPort-II C7500, Fuji Xerox ApeosPort-II C6500, Fuji Xerox ApeosPort-II C5400, Fuji Xerox DocuCentre-II C7500, Fuji Xerox DocuCentre-II C6500, and Fuji Xerox DocuCentre-II C5400 are identified by the same TOE identification and use the same ROM version:

TOE Identification: Fuji Xerox ApeosPort-II C7500/C6500/C5400, DocuCentre-II C7500/C6500/C5400 Series Controller Software for Asia Pacific

Version: Controller ROM Ver. 2.100.0

Manufacturer: Fuji Xerox Co., Ltd.

1.2. ST Overview

This ST provides the security specifications of the controller software of ApeosPort-II DocuCentre-II C7500/C6500/C5400 series (hereinafter referred to as “MFP”). This controller software is also used to realize functions of a data security kit, an option of the MFP.

MFP is the short name of Multi Function Peripheral which has copy, print, and scan functions. The data security kit is an option which protects, from unauthorized disclosure, the document data which is stored in the internal HDD after being processed by the MFP (hereinafter referred to as “used document data”).

This TOE provides the following security functions:

- 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).

1.3. Common Criteria Conformance Claim

This ST conforms to the following evaluation standards for information security (CC). The ST 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 Security Certification Office, IT Security Center, 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 Security Certification Office, IT Security Center, 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 Security Certification Office, IT Security Center, 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 Security Certification Office, IT Security Center, 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 IT Security Center, Information-Technology Promotion Agency, Japan) |
| [I-0512] | Interpretations-0512 (Translation version 1.0, dated December 2005, translated by Information Security Certification Office, IT Security Center, |

| Short Name | Document Title |
|------------|---|
| | 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 |
| MFP | Multi Function Peripheral |
| NVRAM | Non Volatile Random Access Memory |
| PDL | Page Description Language |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| SEEPROM | Serial Electronically Erasable and Programmable Read Only Memory |
| SF | Security Function |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SMTP | Simple Mail Transfer Protocol |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSFI | TSF Interface |
| 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>i.e.</i> general user, customer |

| Term | Definition |
|------------------------------------|---|
| | service engineer, and system administrator. |
| General User | Any person who uses copy, scan, and print functions of MFP. |
| System Administrator | An authorized user who manages MFP maintenance and configures TOE security functions. |
| 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. |
| System Administrator Client | A client for system administrator. An administrator can refer to and rewrite TOE configuration data of MFP via Web browser. |
| 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. |
| System Administrator 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. |
| Network Scan Utility | Software for a general user client to retrieve the document data stored in Mailbox of MFP. |
| Print Driver | Software for a general user to convert the data on a general user client into the print data written in page description language (PDL), a readable format for MFP. |
| Print Data | The data written in PDL, a readable format for MFP, which is to be converted into bitmap data by TOE decompose function. |
| Control Data | The data that is transmitted by command and response interactions. This is one type of data transmitted between MFP hardware units. |
| Bitmap Data | The decomposed data of the data read by copy function and the print data transmitted from a user client to MFP. Bitmap data is stored into the internal HDD after being compressed in the unique process. |
| Decompose Function | A function to analyze and convert the print data written in PDL into bitmap data. |
| Decompose | To analyze and convert the data written in PDL into bitmap data by decompose function. |
| 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 |

| Term | Definition |
|-------------------------------|--|
| | <p>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:</p> <ul style="list-style-type: none"> • Security Print A user can start print operation by entering his/her password from the control panel. The user password needs to be preset from the print driver of the general user client. • Sample Print When printing several copies, only one copy is printed out first as a sample document. A user can check its quality and print out the remaining copies by sending an instruction from the control panel. • 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 by copy function. |
| Copy Function | A function in which an 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 for one original is ordered, 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 | <p>A function in which the original data is read from IIT and then stored into Mailbox within the MFP internal HDD according to the general user's instruction from the control panel.</p> <p>The stored document data can be retrieved via standard Web browser by CWIS or Network Scan Utility function.</p> |
| Scan Control Function | A function to control the device to enable scan operation. |
| 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. |
| Mailbox | A logical box created in the MFP internal HDD. The scanned document data or the data to be printed later can be stored inside. |
| Document Data | Document data means all the image data transmitted across the MFP when copy, print, or scan function is operated by a general user. The document data includes: |

| Term | Definition |
|--|---|
| | <ul style="list-style-type: none"> • Bitmap data read from IIT and printed out from IOT (copy function); • Print data sent by general user client and its decomposed bitmap data (print function); • Bitmap data read from IIT and then stored into the internal HDD (scan function). |
| Used Document Data | The remaining data in the MFP internal HDD even after deletion. The document data is first stored into the internal HDD, used, and then only its file is deleted. |
| Internally Stored Data | The data which is stored in the general user client or in the general client and server, but does not include data regarding TOE functions. |
| TOE Configuration Data | The data which is created by/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, and Mailbox. |
| General Client and Server | Client and server which do not 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, a 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 over the same storage area. |
| Overwrite | To write over the area of the document data stored in the internal HDD when deleting the data. |
| Cryptographic Seed Key | The 12 alphanumeric characters to be entered by a user. When data in the internal HDD can be encrypted, a cryptographic key is generated based on the cryptographic seed key. |
| Cryptographic Key | The 128-bit data which is automatically generated based on the cryptographic seed key. Before the data is stored into the internal HDD, it is encrypted with the cryptographic key. |
| Network | A general term to indicate both external and internal networks. |
| External Network | The network which cannot be managed by the organization that manages TOE. This does not include the internal network. |
| Internal Network | Channels between MFP and highly reliable remote server / client PC. The channels are located in the network of the organization, the owner of TOE, and are protected from the security risks coming from the external network. |

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 controller software for MFP and has the copy, print, and scan functions. The TOE is provided as the firmware product which controls the whole MFP and protects the TOE configuration data against threats. The TOE is stored on the controller ROM which is on the controller board.

The TOE is also used for the data security kit which is a MFP option to protect, from unauthorized disclosure, the used document data which is stored in the internal HDD after being processed by the MFP.

2.1.2. Service Overview

2.1.2.1. Environment Assumptions

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

Figure 1: Intended Operational Environment shows the intended environment for TOE operation.

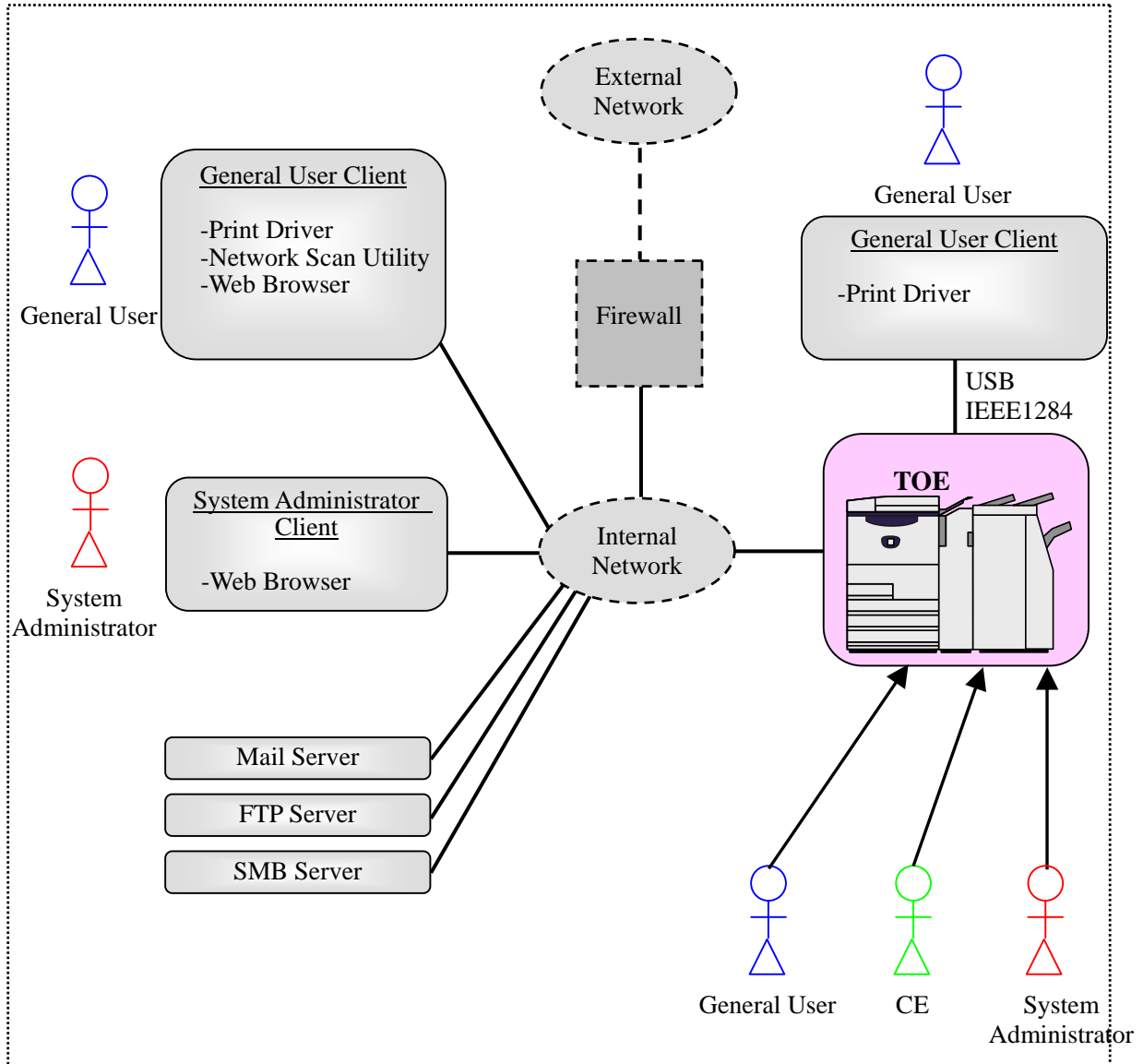


Figure 1: Intended Operational Environment

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 the print driver / Network Scan Utility are installed to a client, the general user can request the MFP to print/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 he/she registered to the MFP: Mailbox name, password, access control and automatic deletion of document.

When the client is linked to the MFP locally via USB or IEEE1284 and print driver is installed to the client, the user can request the MFP to print the document data.

(2) System administrator client:

A system administrator can refer to and change TOE configuration 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.

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

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

2.1.2.2. Security Function Overview

The overview of the functions provided by this TOE is the following:

- 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.
- 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 or Web browser.
- 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.

2.2. User Assumptions

Table 1 specifies the roles of TOE users assumed in this ST.

Table 1: User Role Assumptions

| User | Role Description |
|-------------------------------|---|
| An organization administrator | An administrator or responsible official of the organization which owns and uses TOE. |
| General user | A user of TOE functions such as copy and print. |
| System administrator | A user who is authorized to manage the device using the system administrator 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. |

| User | Role Description |
|--------------------------------|--|
| Customer service engineer (CE) | A user who configures the TOE operational configurations using the interface for CE. |

2.3. Logical Scope and Boundary

The logical scope of this TOE consists of each function of the controller software recorded on the controller ROM, used document data, and TOE configuration data.

Figure 2 shows the logical architecture of the MFP.

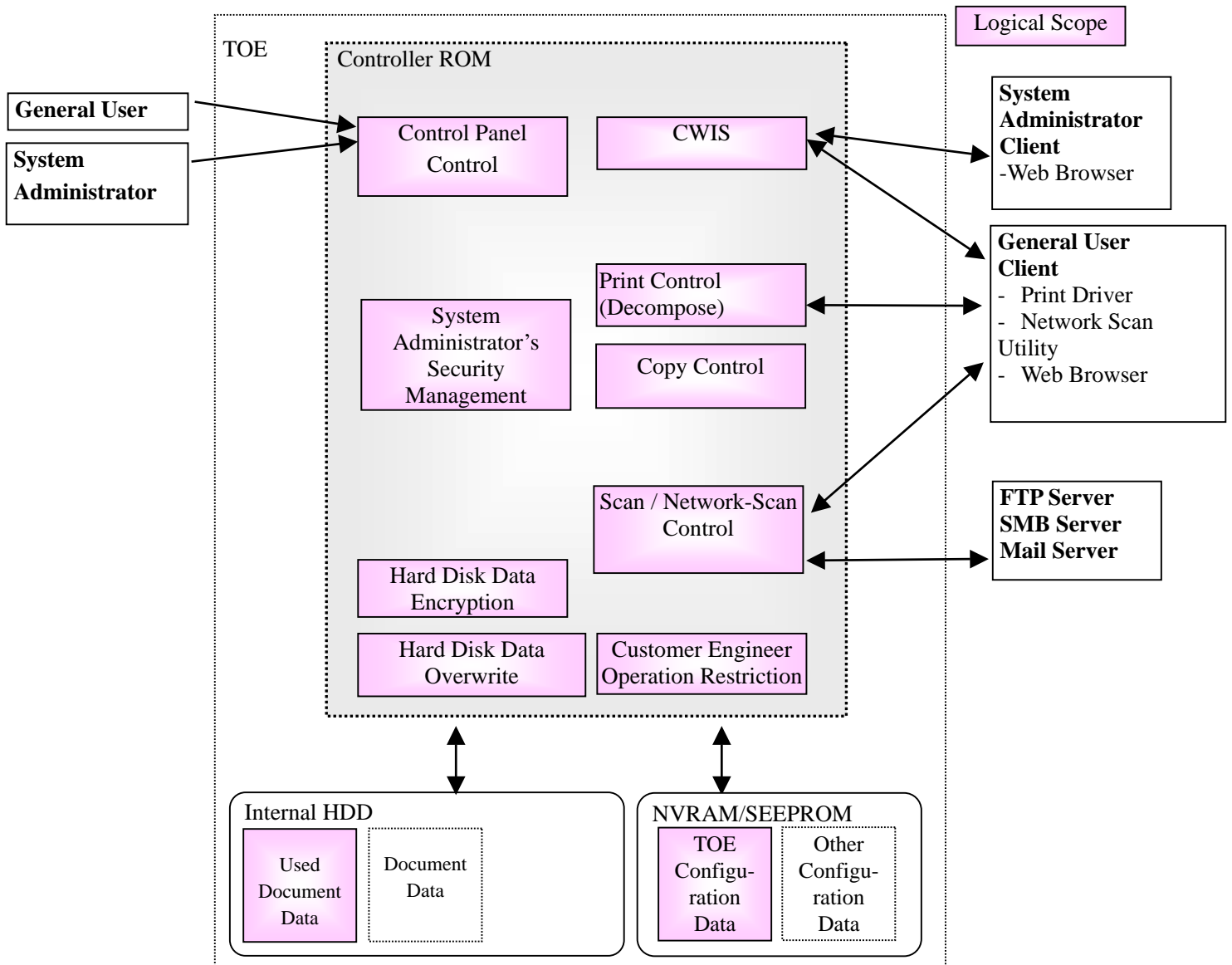


Figure 2: MFP Units and TOE Logical Scope

2.3.1. Basic Functions

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

2.3.1.1. Control Panel Function

Control panel function is a user interface function for general user and system administrator to operate

MFP functions.

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 the general user client. The print data created via print driver is sent to the MFP to be analyzed, decomposed, and printed out from IOT. The print function is of two types: the normal print in which the data is printed out from IOT directly after decomposed and the Store Print in which the bitmap data is temporarily stored in the internal HDD and then printed out from IOT according to the general user's instruction from the control panel.

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. CWIS Function

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

CWIS also enables System Administrator's Security Management by which a system administrator can access and rewrite TOE configuration data. For this, a 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 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.

2.3.2.2. Hard Disk Data Encryption (TSF_CIPHER)

The document data is encrypted before stored into the internal HDD.

2.3.2.3. System Administrator's Security Management (TSF_FMT)

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

- Enable or disable Hard Disk Data Overwrite;

- Enable or disable Hard Disk Data Encryption;
- 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 system administrator;
- Set the allowable number of system administrator's authentication failures before access denial;
- Enable or disable Customer Engineer Operation Restriction.

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 system administrator;
- Set the allowable number of system administrator's authentication failures before access denial.

2.3.2.4. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

A system administrator can restrict CE's operation in the system administrator mode to inhibit CE from referring to or changing the configurations of the following TOE security functions. Customer Engineer Operation Restriction can prevent configuration change by an attacker who is impersonating CE.

- Hard Disk Data Overwrite;
- Hard Disk Data Encryption;
- Enable or disable use of password entered from MFP control panel in user authentication;
- Setting of system administrator ID/password;
- Setting of access denial due to authentication failure of system administrator identification;
- Customer Engineer Operation Restriction.

2.4. Physical Scope and Boundary

The physical scope of this TOE is the controller software recorded on the controller ROM which is mounted on the controller board. shows configuration of each unit and TOE physical scope.

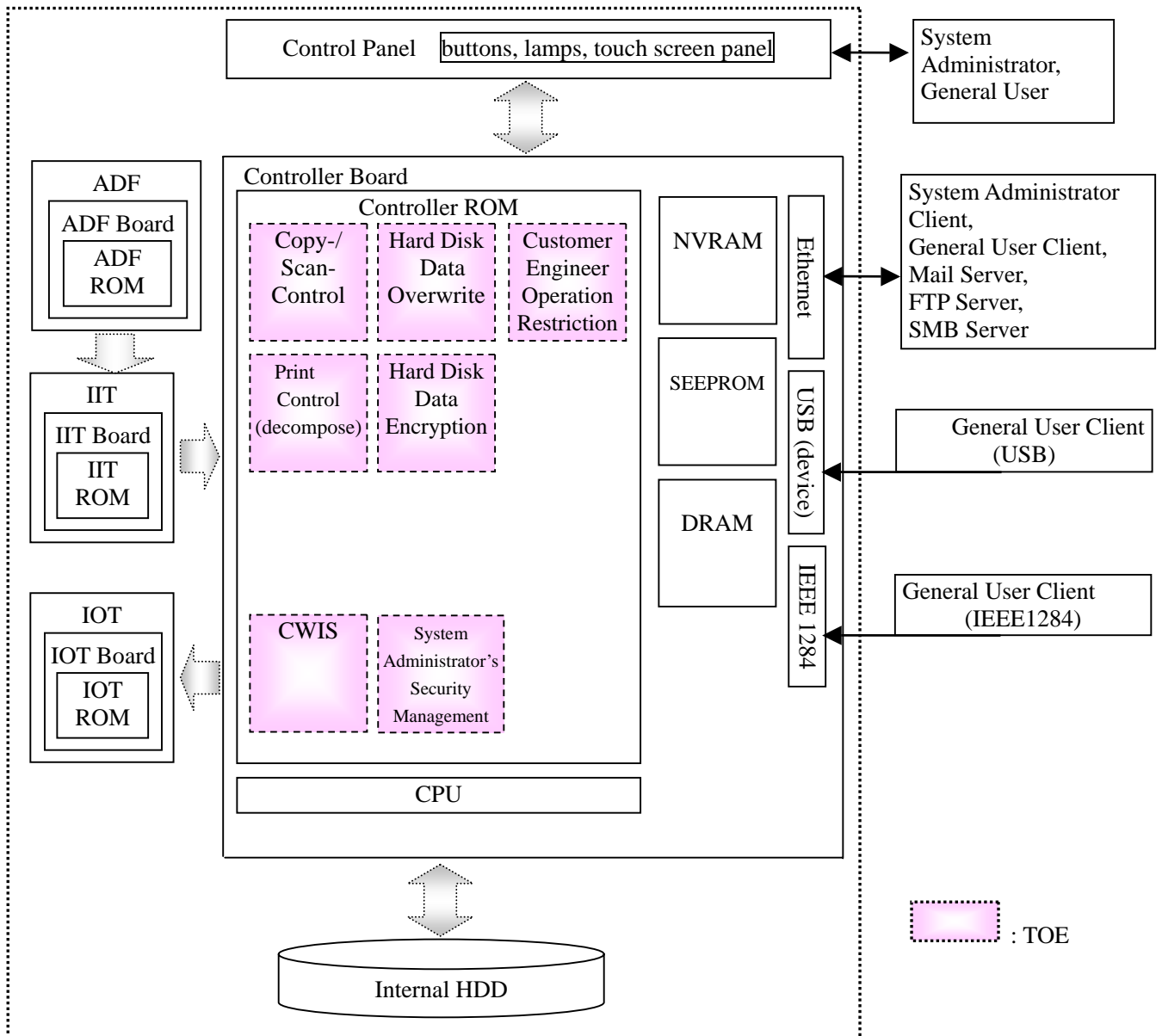


Figure 3: MFP Units and TOE Physical Scope

The MFP consists of the PWB units of controller board and control panel, IIT, and IOT.

The controller board is connected to the control panel via the internal interfaces which transmit control data; the controller board is also connected to the IIT board and IOT board via the internal interfaces which transmit document data and control data.

The controller board is a PWB which controls MFP functions of copy, print, and scan. The board has a network interface (Ethernet) and local interfaces (IEEE1284 and USB) and is connected to the IIT board and IOT board.

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

The IIT (Image Input Terminal) is a device to scan an original and send its data to the controller board for copy, print, and scan 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 (Figure 4):

- Used document data

When a general user uses MFP functions such as copy 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. Therefore, it 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 System Administrator's Security Management. The configuration data stored in the TOE (see Table 2) can be a threat to other assets if used without authorization. Therefore, it is assumed as an asset to be protected.

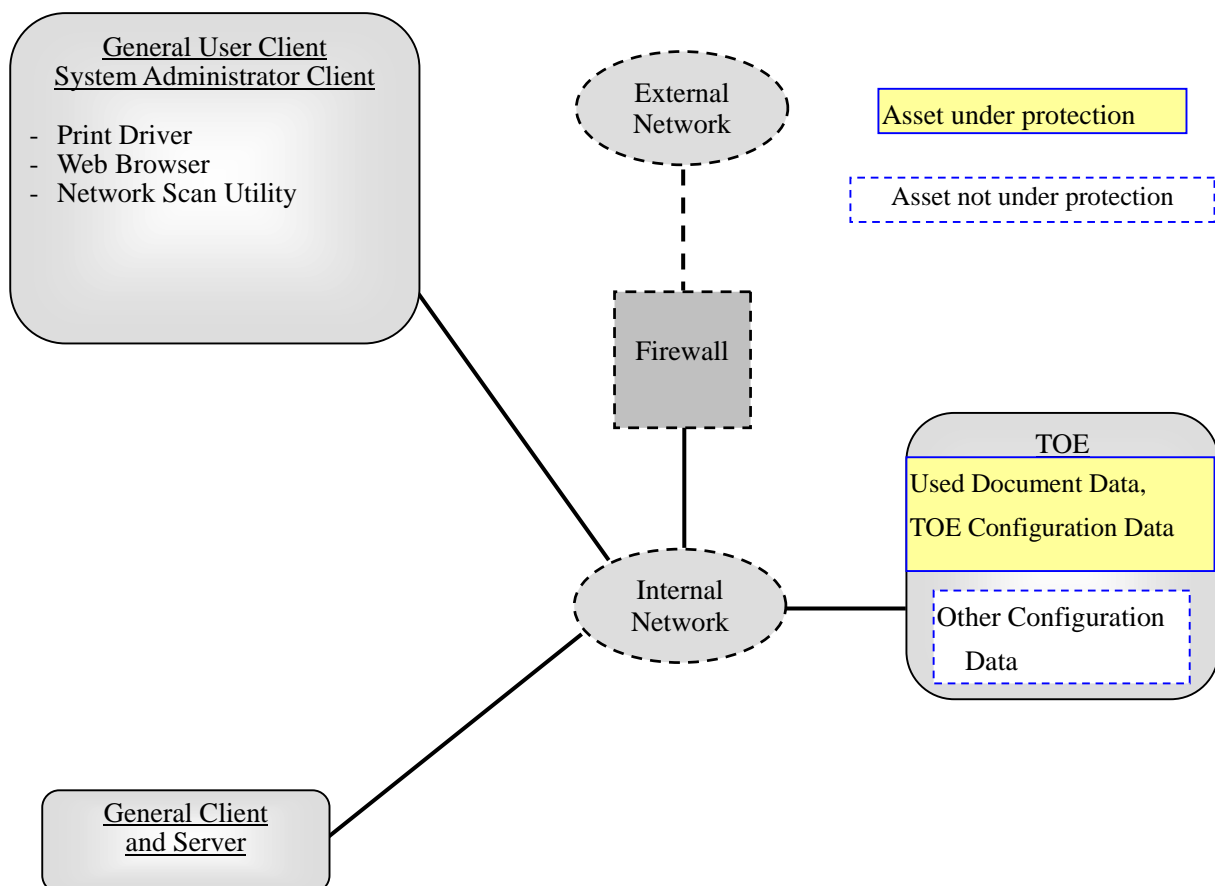


Figure 4: Assets under and not under Protection

Table 2 categorizes the TOE configuration data recorded on NVRAM and SEEPROM of the controller board.

Table 2: 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 Mailbox |

Note) Configuration data other than TOE configuration data are also stored on 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 3 shows the assumptions for the operation and use of this TOE.

Table 3: 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 | <p>A system administrator shall configure the TOE as follows.</p> <ul style="list-style-type: none"> • Use of password entered from MFP control panel in user authentication: enabled • Length of system administrator password: 7 characters or more • Access denial due to authentication failure of system administrator ID: enabled • Allowable number of system administrator's authentication failures before access denial: 5 • Customer Engineer Operation Restriction: enabled • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters |
| Network Connection Assumption | |
| A.NET | <ul style="list-style-type: none"> • Interception on the internal network of the MFP with the TOE installed shall be disabled. • When the internal network of the MFP with the TOE installed is linked to the external network, access to the MFP from the external network shall be disabled. |

3.2. Threats

Table 4 identifies the threats addressed by the TOE. These threats are considered to be users with public knowledge of how the TOE operates. An attacker is considered to have low-level attack capability.

Table 4: Threats Addressed by the TOE

| Threat (Identifier) | Description |
|---|---|
| Unauthorized reproduction of document data stored in the internal HDD | |
| T.RECOVER | An attacker may remove the internal HDD and connect it to commercial tools so that he/she can read out and leak the used document data inside. |
| Unauthorized access to TOE 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. |

3.3. Organizational Security Policy

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

4. SECURITY OBJECTIVES

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

4.1. Security Objectives for the TOE

Table 5 defines the security objectives to be accomplished by the TOE.

Table 5: Security Objectives for the TOE

| Objectives (Identifier) | Description |
|-------------------------|--|
| O.CIPHER | The TOE encrypts the used document data to be stored into the HDD so that it cannot be analyzed even if retrieved. |
| O.MANAGE | The TOE must inhibit a general user from accessing TOE configuration data. The TOE allows only the authenticated system administrator to access the system administrator mode which enables him/her to configure the security functions. |
| O.RESIDUAL | The TOE must prevent the used document data in the internal HDD from being reproduced or recovered. |

4.2. Security Objectives for the Environment

Table 6 defines the security objectives for the TOE environment.

Table 6: Security Objectives for the Environment

| Security Objectives (Identifier) | Description |
|----------------------------------|---|
| OE.ADMIN | An organization administrator shall assign an appropriate and reliable person for TOE management as a system administrator and train him/her. |
| OE.AUTH | A system administrator shall configure the TOE security functions as follows. <ul style="list-style-type: none"> • Use of password entered from MFP control panel in user authentication: enabled • Length of system administrator password: 7 characters or more • Allowable number of system administrator's authentication failures before access denial: 5 • Customer Engineer Operation Restriction: enabled |
| OE.FUNCTION | A system administrator shall configure the TOE security functions as follows. <ul style="list-style-type: none"> • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 |

| Security Objectives (Identifier) | Description |
|-------------------------------------|---|
| | characters |
| OE.NET | <p>An organization person in charge shall have a user install a device (client) and configure it properly to prevent interception on the internal network of the MFP with the TOE installed.</p> <p>An organization person in charge shall have a system administrator install a device (Firewall) and configure it properly to block the access from the external network to the MFP with the TOE installed.</p> |

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 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: <i>the Fuji Xerox's standard method, FXOSEC</i>] and specified cryptographic key sizes [assignment: <i>128 bits</i>] that meet the following: [assignment: <i>none</i>]. |
| | 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: <i>encryption of the document data to be stored into the internal HDD and decryption of the document data retrieved from the internal HDD</i>] in accordance with a specified cryptographic algorithm [assignment: <i>AES</i>] and cryptographic key sizes [assignment: <i>128 bits</i>] that meet the following: [assignment: <i>FIPS PUB 197</i>]. |
| | Dependencies: : | [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes |

5.1.2. Class FDP: User data protection

- (1) 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.

5.1.3. Class FIA: Identification and authentication

- (1) FIA_AFL.1 Authentication failure handling
- Hierarchical to: No other components
- FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *five*]] unsuccessful authentication attempts occur related to [assignment: *system administrator authentication*].
- FIA_AFL.1.2 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
- (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.

5.1.4. 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 7*]

to [assignment: *system administrator*].

Table 7: List of Security Functions

| TSF Data | Behavior |
|---|--------------------------------|
| <i>Customer Engineer Operation Restriction</i> | <i>Enable, disable</i> |
| <i>Hard Disk Data Encryption</i> | <i>Enable, disable</i> |
| <i>System Administrator's Security Management</i> | <i>Enable, disable, modify</i> |
| <i>Hard Disk Data Overwrite</i> | <i>Enable, disable, modify</i> |

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

- (2) 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 and modify*
 [assignment: *none*] the [assignment: *TSF data listed in Table 8*] to
 [assignment: *system administrator*].

Table 8: Operation of TSF Data

| TSF Data |
|---|
| <i>Information on system administrator</i> |
| <i>Information on Customer Engineer Operation Restriction</i> |
| <i>Information on Hard Disk Data Encryption</i> |
| <i>Information on Hard Disk Data Overwrite</i> |

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

- (3) FMT_SMF.1 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: *Security Management Functions listed in Table 9*].

Table 9: Security Management Functions Provided by TSF

| Functional requirements | Management items defined by CC | Management functions of TOE |
|-------------------------|---|---|
| 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). | <i>None</i> <i>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.</i> |

| | | |
|------------|---|---|
| FCS_COP.1 | None | - |
| 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. | <i>None Reason: The timing is fixed to the time of document-data deletion.</i> |
| 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. | <i>System Administrator's Security Management: a) Management of allowable number of system administrator's authentication failures b) Denial of machine operation</i> |
| 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. | <i>System Administrator's Security Management: Management of information on system administrator (ID and password)</i> |
| FIA_UAU.7 | None | - |
| FIA_UID.2 | The management of the user identities. | <i>System Administrator's Security Management: Management of information on system administrator (ID and password)</i> |
| FMT_MOF.1 | Managing the group of roles that can interact with the functions in the TSF; | <i>None Reason: The role group is only a system administrator and is not managed.</i> |
| FMT_MTD.1. | Managing the group of roles that can interact with the TSF data. | <i>None Reason: The role group is only a system administrator and is not managed.</i> |
| FMT_SMF.1 | None | - |
| FMT_SMR.1 | Managing the group of users that are part of a role. | <i>None Reason: The role group is fixed and is not managed.</i> |
| FPT_RVM.1 | None | - |

- Dependencies: FIA_UID.1 Timing of Identification
- (4) FMT_SMR.1 Security role
- Hierarchical to: No other components.
- FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *system administrator*].
- FMT_SMR.1.2 The TSF shall be able to associate users with roles.
- Dependencies: FIA_UID.1 Timing of identification

5.1.5. 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.

5.1.6. 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, FIA_UAU.2, and FIA_UAU.7.

5.2. TOE Security Assurance Requirements

The requirements for the TOE security assurance are described by Table 10.

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 10: 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 |
| 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 11 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) System Administrator’s Security Management (TSF_FMT)
- (4) Customer Engineer Operation Restriction (TSF_CE_LIMIT)

The TOE is 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 11: Relations between Security Functional Requirements and TOE Security Functions

| Security functions | | | | |
|--------------------------------------|---------|------------|---------|--------------|
| TOE security functional requirements | TSF_IOW | TSF_CIPHER | TSF_FMT | TSF_CE_LIMIT |
| FCS_CKM.1 | | | | |
| FCS_COP.1 | | | | |
| FDP_RIP.1 | | | | |
| FIA_AFL.1 | | | | |
| FIA_UAU.2 | | | | |
| FIA_UAU.7 | | | | |

| Security functions | | | | |
|--------------------------------------|---------|------------|---------|--------------|
| TOE security functional requirements | TSE_IOW | TSE_CIPHER | TSE_FMT | TSE_CE_LIMIT |
| FIA_UID.2 | | | | |
| FMT_MOF.1 | | | | |
| FMT_MTD.1 | | | | |
| FMT_SMF.1 | | | | |
| FMT_SMR.1 | | | | |
| FPT_RVM.1 | | | | |

6.1.1. Hard Disk Data Overwrite (TSE_IOW)

According to Hard Disk Data Overwrite which is configured by a system administrator using the system administrator 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 found in this list at the time of booting the TOE, this function overwrites and deletes the used document data.

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 (TSE_CIPHER)

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

Using the "hard disk data encryption seed key" that was set by a system administrator using the system administrator mode, TOE generates 128-bit cryptographic key by the Fuji Xerox's unique FXOSENK method algorithm at the time of booting. (When the "hard disk data encryption seed key" 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 then 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. System Administrator's Security Management (TSE_FMT)

To accord a privilege to a specific user, this function allows only the authorized system administrator to access the system administrator mode which enables him/her to refer to and configure the following

security functions from the control panel.

- 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 system administrator ID 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_CE_LIMIT and enable/disable it.

Additionally, the TSF_FMT allows only an authorized system administrator to configure the following TOE security functions via CWIS. For this, a system administrator needs to be authenticated via the Web browser.

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

System Administrator's Security Management limits access to the above security functions to only the authenticated system administrator. To authenticate a system administrator, the MFP compares the system administrator ID and password preset in the MFP against those entered from the control panel or CWIS. When the authentication of a system administrator fails for wrong ID and password, reentry of the user information is required. 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.

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. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

According to Customer Engineer Operation Restriction which is configured by a system administrator using the system administrator mode, a system administrator can restrict CE's operation in the system administrator mode. This prevents TOE security configurations from being referred to or changed by CE. For this, CE cannot refer to or change the configurations of the following TOE security functions.

- Hard Disk Data Overwrite;
- Hard Disk Data Encryption;
- Setting of system administrator ID and password;
- Setting of access denial due to authentication failure of system administrator;
- Customer Engineer Operation Restriction.

Customer Engineer Operation Restriction is configured to certainly operate because it is realized by unique

software that does not have bypass measures.

6.2. Security Function Strength Level

Among the TOE security functions, System Administrator's Security Management (TSF_FMT) 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 12 shows the TOE's security assurance measures which meet the TOE Security Assurance Requirements described in section 5.2 of this ST.

Table 12: Assurance Components and Assurance Measures

| Assurance Requirements | Security Assurance Requirements | Assurance Measures (Identifier) |
|-------------------------------------|---|---|
| Class ACM: Configuration Management | | |
| ACM_CAP.2 | Configuration Item | TOE Configuration List Configuration Management Description |
| 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 |
| 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 | | |
| AVA_SOF.1 | Evaluation of Security Function Strength | Vulnerability Analysis |
| AVA_VLA.1 | Developer Vulnerability Analysis | |

6.3.1. Configuration Management Description (TAS_CONFIG)

The following are described in the "ApeosPort-II DocuCentre-II C7500 (AP) Series 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 "ApeosPort-II DocuCentre-II C7500 (AP) Series 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 "ApeosPort-II DocuCentre-II C7500 (AP) Series 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 requirements:

- ADO_DEL.1
- ADO_IGS.1

6.3.4. Functional Specification (TAS_FUNC_SPEC)

The following are described in the "WorkCentre 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series Correspondence Analysis Description":

- Analysis of whether the security functions are reflected accurately and completely 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 (ApeosPort-II C7500/C6500/C5400 DocuCentre-II C7500/C6500/C5400 User Guide and ApeosPort-II C7500/C6500/C5400 DocuCentre-II C7500/C6500/C5400 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.

“ApeosPort-II C7500/C6500/C5400 DocuCentre-II C7500/C6500/C5400 User Guide” and “ApeosPort-II C7500/C6500/C5400 DocuCentre-II C7500/C6500/C5400 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 requirements:

- 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 "ApeosPort-II DocuCentre-II C7500 (AP) Series 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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 requirements:

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

6.3.9. Vulnerability Analysis (TAS_VULNERABILITY)

Fuji Xerox creates “WorkCentre 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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:

- AVA_SOF.1
- AVA_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 13 shows the correspondences between TOE/environment security objectives and TOE security environments such as assumptions, threats, and security policy of organization. Table 14 describes that each TOE security environment is assured by TOE/environment security objectives.

Table 13: Correspondences between TOE/Environment Security Objectives and TOE Security Environment

| TOE security environment \ TOE/environment security objectives | A.ADMIN | A.SECMODE | A.NET | T.RECOVER | T.CONFDATA |
|--|---------|-----------|-------|-----------|------------|
| O.CIPHER | | | | | |
| O.MANAGE | | | | | |
| O.RESIDUAL | | | | | |
| OE.ADMIN | | | | | |
| OE.AUTH | | | | | |
| OE.FUNCTION | | | | | |
| OE.NET | | | | | |

Table 14: 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 By OE.AUTH, a system administrator sets an appropriate ID and password and enables Customer Engineer Operation Restriction. - OE.FUNCTION By OE.FUNCTION, Hard Disk Data Overwrite and Hard Disk Data |

| TOE Security Environment | TOE Security Objectives Rationale |
|--------------------------|--|
| | Encryption are enabled, which disables the recovery of the used document data in the internal HDD. |
| A.NET | <p>A.NET is an intended environment in which interception on the internal network of MFP and attack by general public from the external network are inhibited. By satisfying the following objective, A.NET can be realized:</p> <ul style="list-style-type: none"> - OE.NET <p>By OE.NET, interception on the internal network and the access to the MFP from the external network are disabled. To prevent interception, a device (client) is installed and properly configured. For example, it is configured to encrypt the data transmitted between MFP and the client. To block the access to the MFP from the external network, a device (Firewall) is installed and properly configured.</p> |
| T.RECOVER | <p>By satisfying the following objective, T.RECOVER can be countered:</p> <ul style="list-style-type: none"> - OE.FUNCTION <p>By OE.FUNCTION, it is necessary to enable the TOE security functions (i.e. Hard Disk Data Overwrite and Hard Disk Data Encryption) and disable the recovery of the used document data in the internal HDD. To be specific, this threat can be countered by the following security objectives: O.RESIDUAL and O.CIPHER.</p> <ul style="list-style-type: none"> - O.CIPHER <p>By O.CIPHER, the document data to be stored into the internal HDD is encrypted.</p> <ul style="list-style-type: none"> - O.RESIDUAL <p>By O.RESIDUAL, the used document data is overwritten and deleted to disable the reproduction of the used document data stored in the internal HDD.</p> |
| T.CONFDATA | <p>By satisfying the following objective, T.CONFDATA can be countered:</p> <ul style="list-style-type: none"> - OE.AUTH <p>By OE.AUTH, it is necessary to enable the security functions (i.e. User Authentication with Password, System Administrator Password, Allowable Number of System Administrator's Authentication Failures before Access Denial, and Customer Engineer Operation Restriction) and permits only the authenticated system administrator to change the TOE configuration data. To be specific, this threat can be countered by the following security objective:</p> <ul style="list-style-type: none"> - O.MANAGE <p>By O.MANAGE, only the authenticated system administrator is allowed to enable/disable the TOE security functions and to refer to / update the TOE configuration data.</p> |

8.2. Security Requirements Rationale

8.2.1. Security Functional Requirements Rationale

Table 15 shows the correspondences between security functional requirements and security objectives. Table 16 describes the rationale demonstrating that each security objective is assured by TOE security functional requirements.

Table 15: Correspondences between Security Functional Requirements and Security Objectives

| TOE Security Functional Requirements | Security Objectives | | |
|---|---------------------|----------|------------|
| | O.CIPHER | O.MANAGE | O.RESIDUAL |
| FCS_CKM.1 | | | |
| FCS_COP.1 | | | |
| FDP_RIP.1 | | | |
| FIA_AFL.1 | | | |
| FIA_UAU.2 | | | |
| FIA_UAU.7 | | | |
| FIA_UID.2 | | | |
| FMT_MOF.1 | | | |
| FMT_MTD.1 | | | |
| FMT_SMF.1 | | | |
| FMT_SMR.1 | | | |
| FPT_RVM.1 | | | |

Table 16: Security Objectives to SFR Rationale

| Security Objectives | Security Functional Requirement Rationale |
|---------------------|--|
| O.CIPHER | <p>O. CIPHER is an objective that encrypts the used document data in the internal HDD so that they cannot be analyzed even if retrieved.</p> <p>By satisfying the following security objectives, O.CIPHER can be realized.</p> <ul style="list-style-type: none"> - FCS_CKM.1 <p>By FCS_CKM.1, the cryptographic key is generated in accordance with the specified cryptographic key size (128 bits).</p> <ul style="list-style-type: none"> - FCS_COP.1 <p>By FCS_COP.1, the document data to be stored into the internal HDD is encrypted and then decrypted when the data is read, in accordance with the</p> |

| Security Objectives | Security Functional Requirement Rationale |
|---------------------|--|
| | <p>determined cryptographic algorithm and cryptographic key size.</p> <p>- FPT_RVM.1</p> <p>By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.</p> |
| O.MANAGE | <p>O. MANAGE is an objective that allows only an authenticated system administrator to access the system administrator mode for security function setting and inhibits a general user from accessing the TOE configuration data.</p> <p>By satisfying the following security objectives, O.MANAGE can be realized:</p> <p>- FIA_AFL.1</p> <p>By FIA_AFL.1, successive attacks are prevented because the power needs to be cycled when the number of system administrator authentication failures reaches the defined number of times.</p> <p>- FIA_UAU.2</p> <p>By FIA_UAU.2, user authentication is performed to identify a proper system administrator or individual.</p> <p>- FIA_UAU.7</p> <p>By FIA_UAU.7, illicit leakage of the authentication information is prevented because the authentication feedback is protected.</p> <p>- FIA_UID.2</p> <p>By FIA_UID2, user authentication is performed to identify a proper system administrator or individual.</p> <p>- FMT_MOF.1</p> <p>By FMT_MOF.1, the person who enables/disables TOE security functions and makes functional settings is limited to system administrator.</p> <p>- FMT_MTD.1</p> <p>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.</p> <p>- FMT_SMF.1</p> <p>By FMT_SMF.1, TOE security management functions are provided for system administrator.</p> <p>- FMT_SMR.1</p> <p>By FMT_SMR.1, the role related to the security is limited to system administrator by maintaining the role of system administrator as a user who has special authority.</p> <p>- FPT_RVM.1</p> <p>By FPT_RVM.1, TOE security functions are certainly invoked and not</p> |

| Security Objectives | Security Functional Requirement Rationale |
|---------------------|---|
| | bypassed. Thus, the functional requirements related to this objective are surely conducted. |
| O.RESIDUAL | <p>O.RESIDUAL is an objective that disables the reproduction and recovery of the used document data in the internal HDD.</p> <p>By satisfying the following security objectives, O.RESIDUAL can be realized:</p> <ul style="list-style-type: none"> - FDP_RIP.1 <p>By FDP_RIP.1, the previous information of the used document data file stored in the internal HDD is made unavailable.</p> <ul style="list-style-type: none"> - FPT_RVM.1 <p>By FPT_RVM.1, TOE security functions are certainly invoked and not bypassed. Thus, the functional requirements related to this objective are surely conducted.</p> |

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 supports data overwrite and network scan. The MFP is used within the facilities of the organization such as general office on internal network. Thus, 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, 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 17 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 17: 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 |

| Functional Requirement | Dependencies of Functional Requirements | |
|---|---|---|
| Requirement and its name | Requirement that is dependent on | Requirement that is not dependent on and its rationale |
| <p>FCS_CKM.1 Cryptographic key generation</p> | <p>FCS_COP.1</p> | <p>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.</p> <p>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.</p> |
| <p>FCS_COP.1 Cryptographic operation</p> | <p>FCS_CKM.1</p> | <p>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.</p> <p>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.</p> |
| <p>FDP_RIP.1 Subset residual information protection</p> | <p>None</p> | |
| <p>FIA_AFL.1 Authentication failure handling</p> | <p>FIA_UAU.2</p> | <p>FIA_UAU.1: The dependency on FIA_UAU.1 is satisfied because FIA_UAU.2 is the functional security requirement</p> |

| Functional Requirement | Dependencies of Functional Requirements | |
|--|---|--|
| Requirement and its name | Requirement that is dependent on | Requirement that is not dependent on and its rationale |
| | | 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 | |
| FMT_MTD.1 Management of TSF data | FMT_SMF.1, FMT_SMR.1 | |
| FMT_SMF.1 Specification of management functions | | None |
| FMT_SMR.1 Security roles | FIA_UID.2 | FIA_UID.1: The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1. |
| FPT_RVM.1 Non-bypassability of the TSP | | None |

8.2.5. Interactions among Security Functional Requirements

Table 18 describes the interactions among TOE security functional requirements.

Table 18: Interactions among Security Functional Requirements

| Functional Requirement | | Bypass Prevention | De-activation Prevention |
|---------------------------|------------------------------|-------------------|--------------------------|
| Functional Requirement ID | Requirement Name | | |
| FCS_CKM.1 | Cryptographic key generation | FPT_RVM.1 | FMT_MOF.1 |
| FCS_COP.1 | Cryptographic operation | FPT_RVM.1 | FMT_MOF.1 |

| Functional Requirement | | Bypass Prevention | De-activation Prevention |
|---------------------------|---|-------------------|--------------------------|
| Functional Requirement ID | Requirement Name | | |
| FDP_RIP.1 | Subset residual information protection | FPT_RVM.1 | FMT_MOF.1 |
| FIA_AFL.1 | 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_MTD.1 | Management of TSF data | FPT_RVM.1 | |
| FMT_SMF.1 | Specification of management functions | | |
| FMT_SMR.1 | Security roles | | |
| FPT_RVM.1 | Non-bypassability of the TSP | | |

8.2.5.1. Bypass Prevention

Table 19 describes the rationale for bypass prevention of each security functional requirement that is defined in the Table 18: “Interactions among Security Functional Requirements.”

Table 19: Bypass Prevention Rationale for Security Functional Requirements

| Functional Requirement | Bypass Prevention Rationale for Functional Requirements |
|--|--|
| FPT_RVM.1 | |
| 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. |
| FIA_AFL.1 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. Any operation other than power cycle is disabled. |
| FDP_RIP.1 | This security functional requirement is configured by unique software that does not |

| Functional Requirement | Bypass Prevention Rationale for Functional Requirements |
|------------------------|---|
| | <p>have bypass measures and cannot be replaced with another software or module.</p> <p>Based on system administrator setting, the functions are also configured to certainly operate.</p> <p>In addition, the TOE is configured that, when overwrite processing is stopped due to power off, the overwrite deletion processing is re-started by power-on. Thus, this function cannot be circumvented, and non-bypassability is ensured.</p> |
| FMT_MTD.1 | <p>This security functional requirement is configured by unique software that does not have bypass measures and cannot be replaced with another software or module.</p> <p>When TOE configuration data is accessed, the authentication of system administrator always needs to be performed. Thus, this function cannot be circumvented, and non-bypassability is ensured.</p> |

8.2.5.2. De-activation Prevention

Table 20 describes the rationale for de-activation prevention of each security functional requirement that is defined in the Table 18: “Interactions among Security Functional Requirements.”

Table 20: De-activation Prevention Rationale for Security Functional Requirements

| Functional Requirement | De-activation Prevention Rationale for Functional Requirements |
|---------------------------------------|--|
| FMT_MOF.1 | |
| FCS_CKM.1, FCS_COP.1, FDP_RIP.1 | <p>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.</p> <ul style="list-style-type: none"> • 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) |

8.2.5.3. Interference

Since this TOE allows only a system administrator to manage the behaviors of security functions, neither unauthorized programs nor objects can exist. Therefore, access control is not necessary and TOE security functions are not destroyed.

8.2.5.4. Detection of Defeat

Identification authentication allows only an identified administrator to operate the administrator interface, System Administrator’s Security Management (TSF_FMT). Thus, a general user, untrusted subject, cannot disable (defeat) TOE security functions using the administrator interface.

Attack on password is realistically impossible for the following reasons:

- 1) The power needs to be cycled when the number of successive authentication failures reaches five (FIA_AFL.1).
- 2) The minimum password length is specified as seven characters (Assumptions).

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 21 shows the management functions that each functional requirement component requires.

The security management functions that are defined in FMT_SMT.1 of "Specification of Management Functions" are in line with the management functions defined in Table 21. Thus, TOE security functional requirements are internally consistent in terms of security management functions.

Table 21: Management Requirements of TOE Security Functions

| Functional Requirement | | Management Functions Required for Each Component |
|------------------------|--|---|
| Component | Name | |
| FCS_CKM.1 | Cryptographic key generation | Management of cryptographic key data |
| FCS_COP.1 | Cryptographic operation | - |
| FDP_RIP.1 | Subset residual information protection | Management of the used document data stored in the internal HDD |
| FIA_AFL.1 | Authentication failure handling | Management of the number of times for authentication failures |
| FIA_UAU.2 | User authentication before any action | <ul style="list-style-type: none"> • 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 | |
| FMT_MOF.1 | Management of security function behavior | Management of the following function settings: <ul style="list-style-type: none"> • 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) |
| FMT_MTD.1 | Management of TSF data | Management of TSF data configuration |
| FMT_SMF.1 | Specification of management functions | |
| FMT_SMR.1 | Security roles | |
| FPT_RVM.1 | Non-bypassability of the TSP | |

8.2.7. Requirement Rationale for Security Assurance

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

administrator's client and reading-out of information by removing the internal HDD and connecting it to a commercial tool.

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 22 describes the rationale upon which each TOE security functional requirement is satisfied by the corresponding security function as defined in Table 11: "Relations between Security Functional Requirements and TOE Security Functions" in the section "6.1 TOE Security Functions."

Table 22: Rationale for Relations between Security Functional Requirements and TOE Security Functions

| Functional Requirement | Rationale for Relations between Security Function Requirements and TOE Security Functions |
|------------------------|---|
| 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 FXOSEC 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 in the internal HDD. |
| 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 | By TSF_FMT, a system administrator needs to perform user authentication before accessing the system administrator mode. The function for authentication failure handling is provided. When the defined number of access denials due to unsuccessful authentication attempts of system administrator ID has been met or surpassed, any operation except power cycle is disabled. |
| FIA_UAU.2 | By TSF_FMT, TOE requests a user to enter the password before permitting a system administrator to operate at the control panel or Web browser. The entered password is compared against the password registered on the TOE. |

| Functional Requirement | Rationale for Relations between Security Function Requirements and TOE Security Functions |
|------------------------|---|
| | 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_FMT, 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 system administrator authentication. |
| FIA_UID.2 | By TSF_FMT, TOE requests a user to enter the user ID before permitting a system administrator to operate at the control panel or 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_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 | By TSF_FMT, a system administrator's role is maintained and the role is associated with the system administrator. |
| 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. |

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 System Administrator’s Security Management (TSF_FMT). 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 “5.1.6 TOE Security Function Strength.” Therefore, both levels are consistent.

8.3.3. Security Assurance Measures Rationale

Table 23 describes the correspondences between assurance measures and security assurance requirements. Table 24 shows that each assurance measure is assured by security assurance requirements. All assurance measures are necessary to realize EAL2 security assurance requirements.

Table 23: Correspondences between Assurance Measures and Security Assurance Requirements

| Assurance Measures (identifier) | TAS_CONFIG | TAS_CONFIG_LIST | TAS_DELIVERY | TAS_FUNC_SPEC | TAS_HIGHLDESIGN | TAS_REPRESENT | TAS_GUIDANCE | TAS_TEST | TAS_VULNERABILITY |
|------------------------------------|------------|-----------------|--------------|---------------|-----------------|---------------|--------------|----------|-------------------|
| ACM_CAP.2 | | | | | | | | | |
| ADO_DEL.1 | | | | | | | | | |
| ADO_IGS.1 | | | | | | | | | |
| ADV_FSP.1 | | | | | | | | | |
| ADV_HLD.1 | | | | | | | | | |
| ADV_RCR.1 | | | | | | | | | |
| AGD_ADM.1 | | | | | | | | | |
| AGD_USR.1 | | | | | | | | | |
| ATE_COV.1 | | | | | | | | | |
| ATE_FUN.1 | | | | | | | | | |
| ATE_IND.2 | | | | | | | | | |
| AVA_SOF.1 | | | | | | | | | |
| AVA_VLA.1 | | | | | | | | | |

Table 24: Sufficiency of Security Assurance Requirements by Assurance Measures

| Assurance Measures (identifier) | Assurance Requirement | Sufficiency of Security Assurance Requirements |
|------------------------------------|--|---|
| TAS_CONFIG | ApeosPort-II DocuCentre-II C7500 (AP) Series Configuration Management Description | |
| TAS_CONFIG_LIST | ApeosPort-II DocuCentre-II C7500 (AP) Series 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 | ApeosPort-II DocuCentre-II C7500 (AP) Series Delivery, Introduction, and Operation Procedure Description | |

| Assurance Measures (identifier) | Assurance Requirement | Sufficiency of Security Assurance Requirements |
|---------------------------------|--|---|
| | 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series High-Level Design Specification | |
| | 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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 | ApeosPort-II C7500/C6500/C5400 DocuCentre-II C7500/C6500/C5400 User Guide and ApeosPort-II C7500/C6500/C5400 DocuCentre-II C7500/C6500/C5400 Security Function Supplementary Guide | |

| Assurance Measures (identifier) | Assurance Requirement | Sufficiency of Security Assurance Requirements |
|---------------------------------|--|---|
| | 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 | ApeosPort-II DocuCentre-II C7500 (AP) Series 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. |
| | 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 7232 Series, ApeosPort-II 5010 (AP) Series, and ApeosPort-II DocuCentre-II C7500 (AP) Series 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 10 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.