THE DOCUMENT COMPANY
FUJI XEROX

# Fuji Xerox

# DocuCentre 719/659/559 Series

# Data Security Kit

# Security Target

August 6, 2004

Version: 1.12

Fuji Xerox Co., Ltd.

Revision History

| No. | Date | Version | Description |
|---|---|---|---|
| 1 | November 25, 2003 | 1.00 | First draft. |
| 2 | December 2, 2003 | 1.01 | Modified the descriptions of the following:<br>- 1. ST Introduction<br>- 5.3. Security Functional Requirement for IT Environment<br>- 8.2. Rationale for Security Requirements<br>Moved the explanation about protected assets to Chapter 2. |
| 3 | December 10, 2003 | 1.02 | Modified the description corresponding to the remarks and reports ASE007-01, ASE008-01, ASE009-01, and ASE010-01. |
| 4 | January 16, 2004 | 1.03 | Modified the description corresponding to the remarks and reports ASE011-01, ASE012-01, ASE013-01, ASE014-01, and ADV004－01. |
| 5 | February 3, 2004 | 1.04 | Modified the description corresponding to the remarks and reports ASE015-01. |
| 6 | February 17, 2004 | 1.05 | Reviewed the entire description. |
| 7 | February 26, 2004 | 1.06 | Reviewed the entire description. |
| 8 | March 25, 2004 | 1.07 | Reviewed the entire description. |
| 9 | April 2, 2004 | 1.08 | Modified the description corresponding to the remarks and reports ASE019-01. |
| 10 | April 15, 2004 | 1.09 | Modified the description corresponding to the remarks and reports ASE020-01. |
| 11 | April 26, 2004 | 1.10 | Modified the description corresponding to the remarks and reports ADV009-01. Modified 8.2. Rationale for Security Requirements. |
| 12 | June 7, 2004 | 1.11 | Modified the description corresponding to the remarks and reports ASE021-01. |
| 13 | August 6, 2004 | 1.12 | Modified the description after receiving the advice. |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |

- Contents -


1. ST Introduction ..... 1
1.1. ST Identification ..... 1
1.2. ST Overview ..... 1
1.3. Evaluation Assurance Level ..... 1
1.4. Applicable PP ..... 2
1.5. Related ST ..... 2
1.6. CC Conformance ..... 2
1.7. Abbreviated Terms ..... 2
1.8. Terms ..... 2
1.9. Reference ..... 6
2. TOE Description ..... 7
2.1. Type of TOE ..... 7
2.2. Usage Environment of TOE ..... 7
2.3. Purpose of Using TOE ..... 7
2.4. Configuration of TOE ..... 7
2.4.1. Physical Configuration ..... 7
2.4.2. Logical Configuration ..... 10
2.5. Persons Related to TOE ..... 13
2.6. Assets protected by TOE ..... 13
2.7. Functions of TOE ..... 15
2.7.1. Security Functions of TOE ..... 15
2.7.2. Non-Security Function of TOE ..... 15
2.8. How to Use TOE ..... 15
3. TOE Security evironment ..... 18
3.1. Assumptions ..... 18
3.2. Threats ..... 18
3.3. Organizational security policies ..... 18
4. Security objectives ..... 19
4.1. Security Objectives for the TOE ..... 19
4.2. Security objectives for the environment ..... 19
4.2.1. Security Objective for IT Environment ..... 19
4.2.2. Security Objectives for Operation and Management ..... 19
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 ..... 21
5.1.3. Class FPT: Protection of the TSF ..... 21
5.2. TOE security assurance requirements ..... 21

5.3. Security requirements for the IT environment ... 22
5.3.1. Class FIA: Identification and Authentication ... 22
5.3.2. Class FMT: Security Management ... 23
5.4. Claim of TOE Security Function Strength ... 25
6. TOE summary specification ... 26
6.1. TOE security functions ... 26
6.1.1. HDD Overwrite Function for Copy Residual Data (SF.OVERWRITE.D) ... 26
6.1.2. HDD Overwrite Function for Print and Scan Residual Data (SF.OVERWRITE.P) ... 27
6.1.3. Data Encryption Function for Print and Scan (SF.ENCRYPTION.P) ... 27
6.1.4. Function that is Realized using Probabilistic or Permutational Mechanisms ... 27
6.2. Assurance measures ... 28
6.2.1. Configuration Management Description (AS.CONFIGURATION) ... 28
6.2.2. TOE Configuration List (AS.CONFIGURATIONLIST) ... 28
6.2.3. Delivery, Introduction, and Operation Procedure Description (AS.DELIVERY) ... 28
6.2.4. Functional Specification (AS.FUNCSPEC) ... 28
6.2.5. High-Level Design Specification (AS.HIGHLDESIGN) ... 29
6.2.6. Correspondence Analysis Description (AS.REPRESENT) ... 29
6.2.7. User Guide for DocuCentre 719/659/559 Series (Data Security Kit) (AS. GUIDANCE) ... 29
6.2.8. Test Plan (AS.TESTPLAN) ... 30
6.2.9. Test-result Report (AS.TESTSPEC) ... 31
6.2.10. Vulnerability Analysis (AS.VULNERABILITY) ... 31
7. PP claims ... 32
7.1. PP reference ... 32
7.2. PP tailoring ... 32
7.3. PP additions ... 32
8. Rationale ... 33
8.1. Security Objectives rationale ... 33
8.2. Security requirements rationale ... 35
8.2.1. Security functional requirements rationale ... 35
8.2.2. Security assurance requirements rationale ... 39
8.3. TOE summary specification rationale ... 39
8.3.1. Function summary specification rationale ... 39
8.3.2. Assurance measures rationale ... 40
8.4. PP claims rationale ... 43

# 1. ST Introduction

## 1.1. ST Identification

(1) ST identification

| | |
|---|---|
| **ST identification** | DocuCentre 719/659/559 Series Data Security Kit Security Target |
| **Version** | 1.12 |
| **Creator** | Fuji Xerox Co., Ltd. |
| **Date** | August 6, 2004 |
| **CC identification** | Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 |
| **PP identification** | None |
| **Keyword** | Digital copy machine, digital multifunction machine, copy, printer, scanner, hard disk drive, to overwrite and erase, and encryption |

(2) TOE identification

| | |
|---|---|
| **TOE identification** | Fuji Xerox DocuCentre 719/659/559 Series Data Security Kit |
| **Version** | DC system ROM Version 512<br>PESS system ROM Version 3.0.4 |
| **Manufacturer** | Fuji Xerox Co., Ltd. |

This Security Target conforms to JIS X5070 and ISO/IEC 15408 (1999).

JIS X5070 is the Japanese translated version of ISO/IEC15408 (1999).

## 1.2. ST Overview

This Security Target describes security-related specifications of Data Security Kit, which is an optional product of digital multifunction machines with digital copy, printer, and scanner functions (“DocuCentre 719CP,” “DocuCentre 659CP,” and “DocuCentre 559CP”), and digital copy machines (”DocuCentre 719,” ”DocuCentre 659,” and “DocuCentre 559”).

Data Security Kit is a product to protect document data that is stored on the hard disk drive after being processed by “DocuCentre 719CP,” “DocuCentre 659CP,” “DocuCentre 559CP,” “DocuCentre 719,” “DocuCentre 659,” or “DocuCentre 559” (hereafter “used document data”) from being disclosed illicitly.

This product provides the following security functions:

- HDD overwrite function for copy residual data
- HDD overwrite function for print and scan residual data
- Data encryption function for print and scan

## 1.3. Evaluation Assurance Level

Evaluation Assurance Level of TOE: **EAL2**

Reason: TOE is to be used in facilities of organizations such as SOHO, general offices, government and municipal offices, and universities. The users are limited to those who are related to the organization.

## 1.4. Applicable PP

There is no applicable Protection Profile.

## 1.5. Related ST

There is no related Security Target.

## 1.6. CC Conformance

This TOE conforms to the following evaluation standards for information security:

- JIS X5070 Part 2 (CC Version 2.1 Part 2) conformant
- JIS X5070 Part 3 (CC Version 2.1 Part 3) conformant
- JIS X5070 EAL2 conformant

## 1.7. Abbreviated Terms

The following abbreviated terms are used in this ST.

| Abbreviation | Definition |
|---|---|
| CC | Common Criteria. |
| DC | Digital Copier. |
| DC-SYS/IPS | DC Control System / Image Processing System. |
| EAL | Evaluation Assurance Level. |
| HDD | Hard Disk Drive. |
| IIT | Image Input Terminal. |
| IOT | Image Output Terminal. |
| IT | Information Technology. |
| MF-SYS | Multifunction Control System. |
| NVRAM | Non-volatile Random Access Memory. |
| PDL | Page Description Language. |
| PP | Protection Profile. |
| PESS | Printer Electrical Subsystem. |
| SEEPROM | Serial Electronically Erasable and Programmable Read Only Memory. |
| SF | Security Function. |
| SFP | Security Function Policy. |
| 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. |
| UI | User Interface. |

## 1.8. Terms

The following terms are used in this ST:

**DocuCentre**

In this ST, “DocuCentre 719CP,” “DocuCentre 659CP,” “DocuCentre 559CP,” “DocuCentre 719,” ”DocuCentre 659,” and “DocuCentre 559” are generically described as DocuCentre.

**General User**

One who uses digital copy, printer, and scanner functions of DocuCentre.

**System Administrator**

One who manages DocuCentre.

**Customer engineer**

Fuji Xerox's engineer who maintains and repairs DocuCentre.

**Attacker**

One who uses TOE with malicious intention.

**Control Panel**

Panel on which the buttons, lamps, and touch panel display that are necessary for operating DocuCentre are arranged.

**User's Client**

Client that is used by general user. General user uses printer and scanner functions of DocuCentre by using printer driver and network scanner utility that are installed on user's client.

**Client for Maintenance**

Client that is used by customer engineer. Customer engineer maintains DocuCentre using the Fuji Xerox's unique software by connecting the client for maintenance to the DocuCentre's local interface for maintenance. This software is only for maintenance and installed on client for maintenance.

**Local Interface for Maintenance**

Only-for-maintenance interface for connecting DocuCentre and client for maintenance. There are two types of interfaces; one is serial port for regular maintenance and the other is parallel port for program download. Maintenance cannot be performed by connecting general computer because the protocol is unique and closed.

**Printer Driver**

Software that converts data on user's client to print data described in page description language (PDL) that can be interpreted by DocuCentre. Used on user's client.

**Print Data**

Data described in page description language (PDL) that can be interpreted by DocuCentre. Print data is converted to bitmap data by decomposing function of TOE.

**Bitmap Data**

Data that is converted by decomposing function from the data scanned in digital copy or scanner functions or the print data sent from user's client in printer function. Bitmap data is compressed using the Fuji Xerox's unique method and stored on the hard disk drive.

**Decomposing Function**

Function to parse print data described in page description language (PDL) and convert it to bitmap data.

**Decompose**

To parse data described in page description language (PDL) and convert it to bitmap data by decomposing function.

**Network Scanner Utility**

Software to access document data stored on the internal hard disk drive of DocuCentre. Used on user's client.

**Printer Function**

Function to decompose and print out print data sent from user's client.

**Storage Print**

Print method in printer function. In this method, bitmap data created by decomposing print data is once stored on the internal hard disk drive of DocuCentre, and printed according to the general-user's instruction from the control panel. There are following three methods:

- Security print
- Sample print
- Print that uses expanded mailbox

**Security Print**

Storage print method, in which the print is enabled by setting a password from the printer driver on user's client and entering the password at the control panel.

**Sample Print**

Storage print method, in which the first copy is normally printed out for checking the print result and then the remaining copies are printed according to the instruction from the control panel.

**Print that uses Expanded Mailbox**

Storage print method, in which decomposed bitmap data is stored in an expanded mailbox and printed according to the instruction from the control panel. Compared to security print and sample print, functions to make settings on stapling, punching, and paper size when printing are added.

**Spool**

Method used in printer function, in which decomposing is started after all the print data sent from user's client is received in the internal memory.

Print data from multiple user's-clients can be received simultaneously using this method.

**Hard-disk-drive Spool**

Uses a hard disk drive as an internal memory for spool.

**Memory Spool**

Uses a volatile memory as an internal memory for spool.

**Non-spool**

Method used in printer function, in which decomposing is performed while print data sent from user's client is being received. In this method, print data from multiple user's-clients cannot be received simultaneously.

**Original**

Texts, pictures, photographs, and others that are scanned in IIT in digital copy or scanner function.

**Digital Copy Function**

Function to scan an original in IIT and print out from IOT, according to the general-user's instruction from the control panel. When multiple copies of the same original are instructed to be printed, the document data is

1) scanned in IIT,

2) stored on the internal hard disk drive of DocuCentre,
3) read from the internal hard disk drive for the same number of times as the number of designated copies, and printed out.

**Scanner Function**

According to the general-user's instruction from the control panel, scans an original in IIT and stores it in an expanded mailbox created in the internal hard disk drive of DocuCentre. The stored document data is retrieved by network scanner utility on user's client.

**Expanded Mailbox**

Logical box created in the hard disk drive of DocuCentre. The following can be stored in this box: the document data scanned by scanner function and the document data for the print that uses an expanded mailbox.

**Document Data**

In this ST, "document data" is used as a generic term for the data including all the image information that pass the inside of DocuCentre when general user uses digital copy, printer, and scanner functions of DocuCentre.

The following are included:

- Bitmap data that is printed in IOT when using digital copy function.
- Print data sent from user's client and bitmap data created by decomposing the data, when using printer function.
- Bitmap data that is stored on the internal hard disk drive when using scanner function.

**Used Document Data**

Document data that becomes "used" after being stored on the internal hard disk drive of DocuCentre.

**Control Data**

Data that are communicated as a command and its response in the communication performed between hardware units that compose DocuCentre.

**Deletion from Hard Disk Drive**

In this ST, "deletion from hard disk drive" means deletion of administrative information. When document data is deleted from the hard disk drive, the deleted document data cannot be accessed in theory because the corresponding administrative information is deleted. However, the document data itself is not cleared. The document data itself remains on the hard disk drive as used document data until new data is written on the same area.

**To Overwrite and Erase**

To overwrite the data area with the specific data when document data stored on the hard disk drive is to be deleted.

## 1.9. Reference

The following are references for this ST:


| | |
|---|---|
| [JIS X5070-1] | JIS X5070 Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model |
| [JIS X5070-2] | JIS X5070 Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional requirements |
| [JIS X5070-3] | JIS X5070 Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance requirements |
| [CC Part 1] | Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version2.1, August 1999 CCIMB-99-031 |
| [CC Part 2] | Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version2.1, August 1999 CCIMB-99-032 |
| [CC Part 3] | Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version2.1, August 1999 CCIMB-99-033 |
| [CEM Part 1] | Common Evaluation Methodology for Information Technology Security Part1: Introduction and General Model Version0.6, November 1997 |
| [CEM Part 2] | Common Evaluation Methodology for Information Technology Security Part2: Evaluation and Methodology Version1.0, August 1999 |
| [PDTR15446] | Information Technology Security techniques Guide for the production of protection profiles and security targets Proposed Draft, April 2000 |
| [Supplement-0210] | CCIMB Interpretations-0210 |

# 2. TOE Description

## 2.1. Type of TOE

TOE is a data security kit that is installed on a digital multifunction machine. This kit is a firmware product to protect used document data, which is stored on the hard disk drive after being processed by digital multifunction machine, from being disclosed illicitly.

TOE is offered as an optional product of Fuji Xerox's digital multifunction machines "DocuCentre 719CP," "DocuCentre 659CP," and "DocuCentre 559CP," and digital copy machines "DocuCentre 719," "DocuCentre 659," and "DocuCentre 559."

## 2.2. Usage Environment of TOE

TOE is assumed to be used in the condition where machine is used as a stand-alone digital multifunction machine (digital copy machine) or machine is used in the network environment where user's client, which requests printing by digital multifunction machine and document-data retrieval from digital multifunction machine, is connected. (Note that there is only stand-alone usage when machine is used as a digital copy machine.)

## 2.3. Purpose of Using TOE

To protect the used document data that is stored on the internal hard disk drive of DocuCentre from being disclosed illicitly.

## 2.4. Configuration of TOE

### 2.4.1. Physical Configuration

Each unit in DocuCentre and physical boundaries within TOE are shown in Figure 1.

DocuCentre consists of four board-units: digital-copy control system (DC-SYS/IPS), printer subsystem (PESS), multifunction control system (MF-SYS), and control panel.

In each of the following sets, the two are connected via the internal interface where document data and control data are communicated:

- DC-SYS/IPS and MF-SYS
- PESS and MF-SYS
- IIT and DC-SYS/IPS
- IOT and DC-SYS/IPS

Control panel and MF-SYS are connected via the internal interface where control data are communicated.

Control panel is for operating / making settings on digital copy, printer, and scanner functions of DocuCentre.

DC-SYS/IPS is a circuit board for controlling digital copy function of DocuCentre. This board has local interfaces for maintenance (RS232C and IEEE1284), and is connected to IIT, IOT, and MF-SYS.

MF-SYS is a circuit board for controlling communication of document data and control data between respective units. This board is connected to DC-SYS/IPS, PESS, and control panel.
PESS is a circuit board for controlling printer and scanner functions. This board has network interface (Ethernet) and local interfaces (IEEE1284 and USB).
TOE is a set of programs for digital-copy control function, which are recorded in the DC system ROM mounted on DC-SYS/IPS, and programs for printer/scanner control function, which are recorded in the PESS system ROM mounted on PESS.
Programs recorded in each ROM, which is a physical configuration item of TOE, are shown in Table 1.

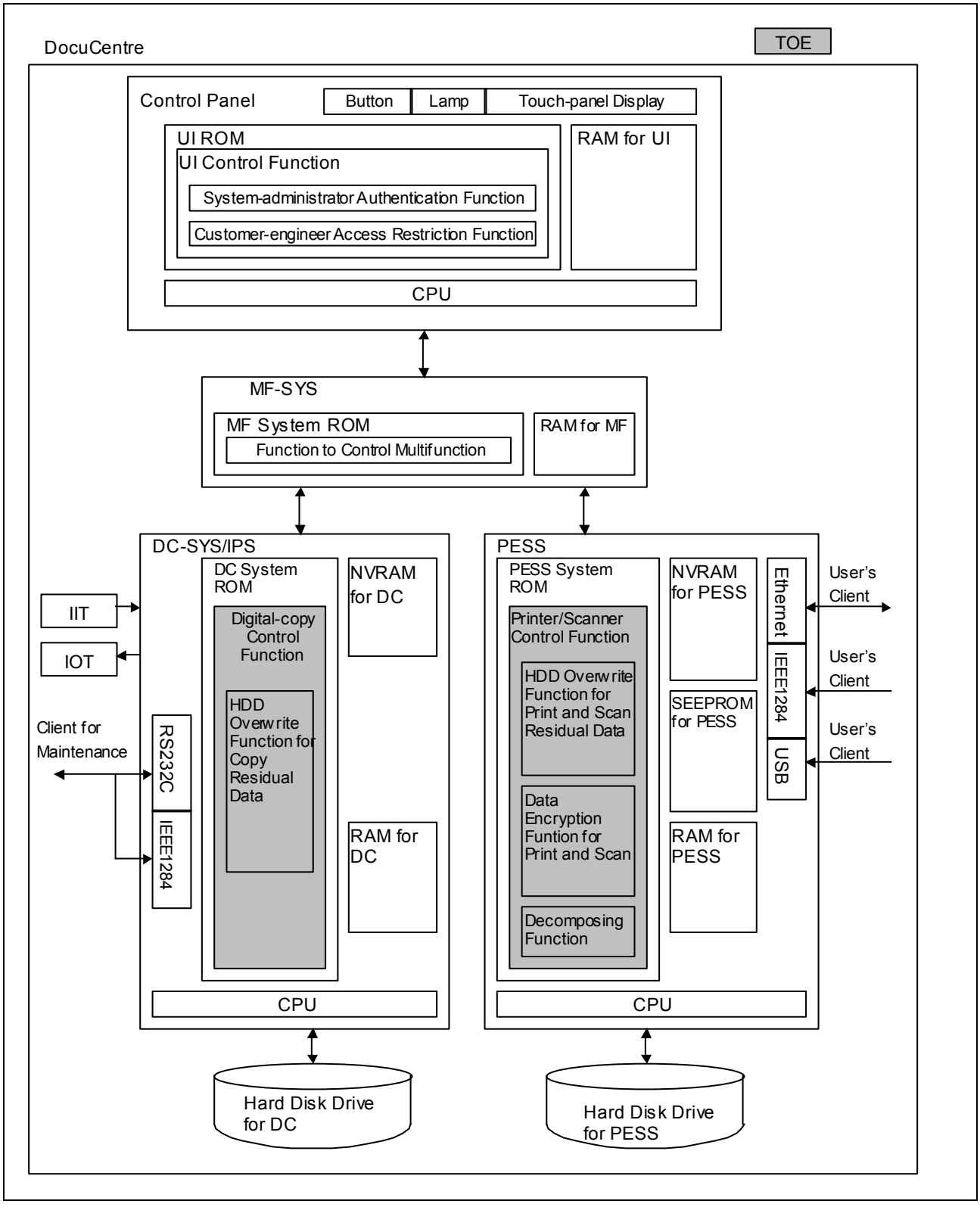


Figure 1: Each Unit in DocuCentre and Physical Boundaries within TOE

Table 1: Physical Configuration Items of TOE

| Configuration item | Stored program |
|---|---|
| DC system ROM | Programs for digital-copy control function are recorded in this ROM, and the following function is provided:<br>- HDD overwrite function for copy residual data |
| PESS system ROM | Programs for printer/scanner control function are recorded in this ROM, and the following functions are provided:<br>- HDD overwrite function for print and scan residual data<br>- Data encryption function for print and scan<br>- Decomposing function |

### 2.4.2. Logical Configuration

Logical configuration of DocuCentre is shown in Figure 2.

DocuCentre provides digital copy, printer, and scanner functions for general users.

Digital copy function is a function to scan an original in IIT and print out from IOT according to the general-user's instruction from the control panel.

Printer function is a function to parse print data sent from user's client, convert it to bitmap data (decompose), and print it out from IOT. There are two types of printer functions. One is normal print, in which data is printed out from IOT without being stored on the hard disk drive. The other is storage print, in which bitmap data is once stored on the internal hard disk drive of DocuCentre, and then printed out from IOT according to the general-user's instruction from the control panel. In printer functions, there are two types of decomposing methods. One is spool method, in which the print data sent from user's client is temporarily received in an memory (internal memory or internal hard disk drive of DocuCentre) and then decomposed. The other is non-spool method, in which decomposing is performed while print data sent from user's client is being received in an internal memory of DocuCentre.

Scanner function is a function to scan an original in IIT and store the data on the internal hard disk drive of DocuCentre according to the general-user's instruction from the control panel. Stored document data can be retrieved using network scanner utility on user's client.

DocuCentre has two internal hard disk drives. One is called "hard disk drive for DC" and used for storing document data that is to be printed out from IOT in copy by digital copy function or print by printer function. The other is called "hard disk drive for PESS" and used for storing document data in spool-method print by printer function, storage print by printer function, or scan by scanner function.

When the document data stored on these hard disk drives are to be deleted after being used, only the administrative information is deleted and the stored data themselves are not cleared. Therefore, such data remain on these hard disk drives as used document data.

TOE provides the security functions described in Table 2 for the used document data stored on these hard disk drives:

Table 2: Security Functions Provided by TOE

| Security function | Hard disk drive for DC | Hard disk drive for PESS |
|---|---|---|
| HDD overwrite function for copy residual data | O | X |
| HDD overwrite function for print and scan residual data | X | O |
| Data encryption function for print and scan | X | O |

O: Function is performed for the data on this hard disk drive.
X: Function is not performed for the data on this hard disk drive.

Logical configuration items of TOE are digital-copy control function provided by the DC system ROM on DC-SYS/IPS, printer/scanner control function provided by the PESS system ROM on PESS, each TOE setting data, and used document data file.

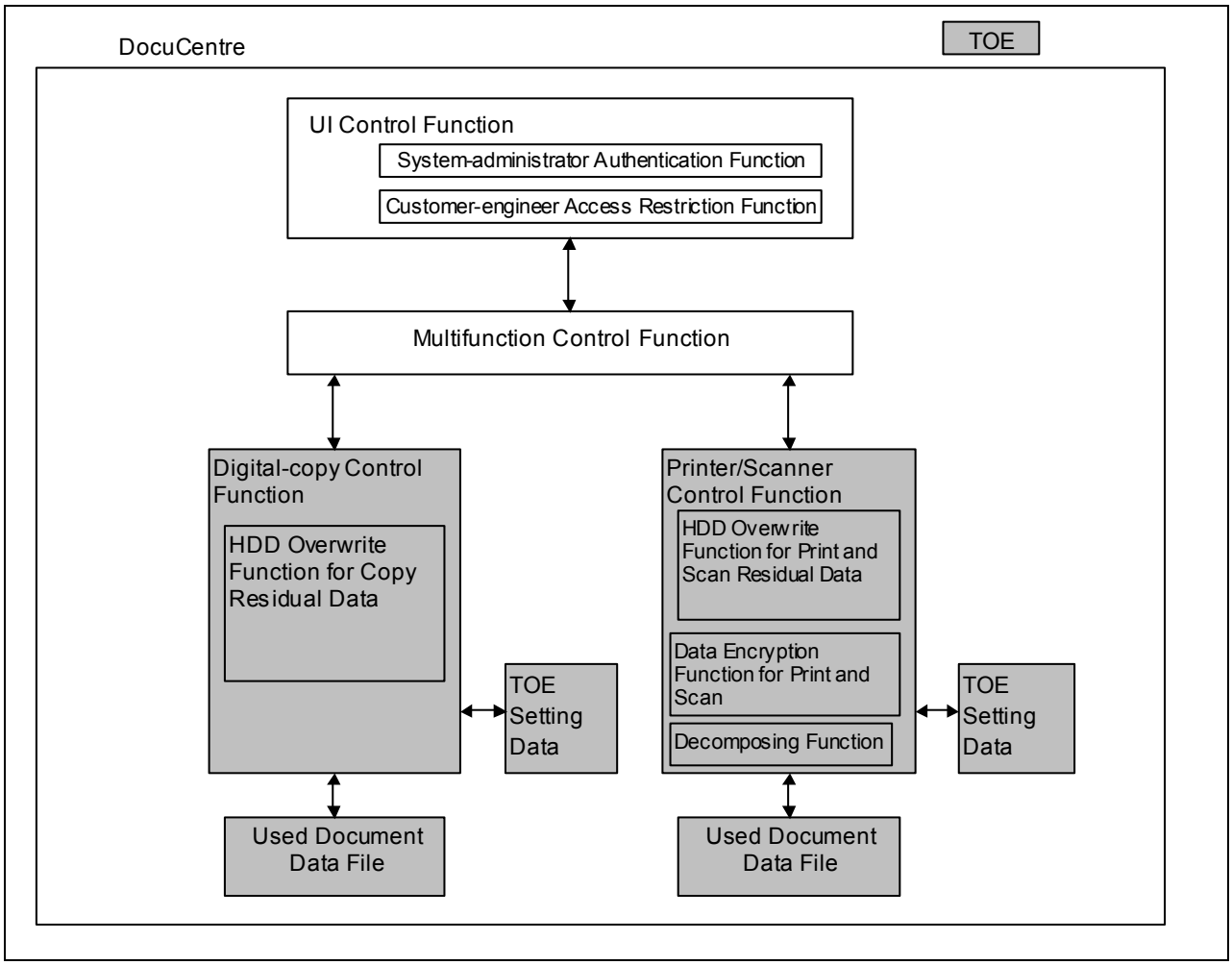


Figure 2: Logical Configuration of TOE

TOE setting data that are recorded in the DocuCentre's NVRAM for DC and SEEPROM for PESS are descried in Table 3.

Table 3: TOE Setting Data in DocuCentre, and Memory Location

| Function | Setting data | Memory location |
|---|---|---|
| Digital-copy control function | Setting for HDD overwrite function | NVRAM for DC |
| Printer/scanner control function | Setting for data encryption function | SEEPROM for PESS |
| | Password for encrypting data stored on the hard disk drive | |

In “setting for HDD overwrite function,” the number of overwriting and erasing used document data recorded on the hard disk drive for DC or that for PESS can be set to one of those described below:

- Not perform: Does not overwrite nor erase.
  Set when security functions of TOE are not used. Lowering of process speed of digital copy, printer, and scanner functions, and restricted items such as forbidding of interrupt copy, all of which are caused by overwriting and erasing, can be avoided.

- Perform (one time): Overwrites and erases with data “0” once.
  Overwriting and erasing makes the recovery of used document data difficult. Has less effect of lowering process speed of copying and printing than three-time overwritings and erasings. Protects used document data by being set in combination with the setting for data encryption function.

- Perform (three times): Overwrites and erases with data “random numbers” twice, and with data “0” once. Recommended setting value. Although the recovery of used document data is difficult after one-time overwriting and erasing, three-time overwritings and erasings make the recovery more difficult. Protects used document data by being set in combination with the setting for data encryption function.

In “setting for data encryption function,” cryptographic operation on document data recorded in the hard disk drive for PESS can be set to either of those described below:

- Not perform: Does not encrypt.
  Set when security functions of TOE are not used. Lowering of process speed due to encryption can be avoided.

- Perform: Encryption makes the parsing of document data difficult. Protects used document data by being set in combination with the setting for HDD overwrite function.

Password for encrypting data stored on the hard disk drive becomes valid when the “setting for data encryption function” is “Perform.” In this condition, user can enter 12-digit number that is used

for generating cryptographic key to encrypt document data recorded on the hard disk drive for PESS.

TOE uses the following functions of IT environment:

- System-administrator authentication function

  When system administrator accesses DocuCentre for using management functions, this function confirms that he or she is a true system-administrator with 7- to 12-digit system-administrator's password entered by him or her.

- Customer-engineer access restriction function

  This function limits the person to change TOE setting data to system administrator.

  When TOE security functions are not used, customer engineer also becomes able to change TOE setting data when the "setting for customer-engineer access restriction function" is set to "Not perform."

## 2.5. Persons Related to TOE

In this ST, the following related persons are assumed.

| Related person | Description |
|---|---|
| Organization's person in charge | Person in charge in the organization where DocuCentre is used and operated. |
| General user | User of digital copy, printer, and scanner functions provided by DocuCentre. |
| System administrator | Person who manages DocuCentre machine. Has a special authority such as to make settings for operations of DocuCentre. Able to access management functions from the control panel of DocuCentre. |
| Customer engineer | Fuji Xerox's engineer who repairs and maintains DocuCentre. |

## 2.6. Assets protected by TOE

Assets protected by TOE are the used document data stored on the DocuCentre's hard disk drive for DC and that for PESS and the TOE setting data stored on the NVRAM for DC and the SEEPROM for PESS.

There are two types of document data; one is bitmap data scanned by digital copy or scanner function, and the other is print data that is sent from user's client. Print data is firstly converted to bitmap data by decomposing function of TOE, and then stored, and printed out. There are two types of used document data; one is used bitmap data and the other is used print data.

Contents, storage mediums, and types of assets protected by TOE are described in Table 4.

Table 4: Contents, Storage Mediums, and Types of Protected Assets

| Protected asset | Description |
|---|---|
| **R.DOCDATA.D (used document data stored on the hard disk drive for DC)** | [Asset contents]<br>Used document data that are stored on the hard disk drive for DC when using digital copy or printer function.<br><br>[Storage mediums] |

| | |
|---|---|
| | Stored on the hard disk drive for DC.<br><br>[Asset types]<br>Types of used document data when using digital copy function:<br>- Bitmap data that becomes “used” when the copying instructed by general user from the control panel is completed.<br>- Bitmap data that becomes “used” when cancel is instructed by general user from the control panel during copying.<br>Types of used document data when using printer function:<br>- Bitmap data that becomes “used” when printing of the print data sent from user’s client is completed.<br>- Bitmap data that becomes “used” when cancel is instructed by general user from the control panel during printing. |
| **R.DOCDATA.P (used document data stored on the hard disk drive for PESS)** | [Asset contents]<br>Used document data that are stored on the hard disk drive for PESS when using printer or scanner function.<br><br>[Storage mediums]<br>Stored on the hard disk drive for PESS.<br><br>[Asset types]<br>Types of used document data when using printer function:<br>- Print data in spool that becomes “used” when printing of the print data set from user’s client is completed in normal print of hard-disk-drive spool method.<br>- Print data in spool that becomes “used” when cancel is instructed by general user from the control panel during printing in normal print of hard-disk-drive spool method.<br>- Print data in spool that becomes “used” when cancel is instructed by user’s client during sending of the print data from user’s client in normal print or storage print of hard-disk-drive spool method.<br>- Print data in spool that becomes “used” when bitmap data is stored on the hard disk drive for PESS after being decomposed in storage print of hard-disk-drive spool method.<br>- Bitmap data that becomes “used” when printing of the stored document data is instructed by general user from the control panel and the printing is completed in storage print.<br>- Bitmap data that becomes “used” when cancel is instructed by general user from the control panel during printing of the document data for storage print.<br>- Bitmap data that becomes “used” when deletion of the stored document data is instructed by general user from the control panel in storage print.<br>Types of used document data when using scanner function:<br>- Bitmap data that becomes “used” when retrieving of the stored document data by network scanner utility on user’s client is finished.<br>- Bitmap data that becomes “used” when deletion of the stored document data is instructed by general user from the control panel.<br>- Bitmap data that becomes “used” when cancel is instructed by general user from the control panel during scanning. |
| **R.CONFDATA (TOE setting data)** | [Asset contents]<br>“Setting for HDD overwrite function,” “setting for data encryption function,” and “password for encrypting data stored on the hard disk drive.”<br><br>[Storage mediums]<br>“Setting for HDD overwrite function” is stored on the DC-SYS/IPS’s NVRAM for DC.*<br>“Setting for data encryption function” and “password for encrypting data stored on the hard disk drive” are stored on the SEEPROM for PESS.* |

* Although data other than those described in Table 4, such as setting data for power-saving time, are stored on the DocuCentre’s NVRAM for DC and SEEPROM for PESS, these data are not the assets to be protected because they are not related to the security functions of TOE.

## 2.7. Functions of TOE

### 2.7.1. Security Functions of TOE

TOE provides the following security functions.

| Function classification | Description |
|---|---|
| HDD overwrite function for copy residual data | Function to perform specific-pattern overwriting and erasing of the used document data stored on the DocuCentre's hard disk drive for DC. When the used document data remains in the hard disk drive because overwriting of the data is not finished such as due to power shutdown, the entire data on the hard disk drive is automatically overwritten and erased according to the "setting for HDD overwrite function" at the next power-on. |
| HDD overwrite function for print and scan residual data | Function to perform specific-pattern overwriting and erasing of the used document data stored on the DocuCentre's hard disk drive for PESS. When the overwriting of the used document data is not finished such as due to power shutdown, the used document data is automatically overwritten and erased according to the "setting for HDD overwrite function" at the next power-on. |
| Data encryption function for print and scan | Function to encrypt document data stored on the DocuCentre's hard disk drive for PESS. |

### 2.7.2. Non-Security Function of TOE

TOE provides the following non-security function.

| Function classification | Description |
|---|---|
| Decomposing function | Used in printer function. Function to parse print data that is described in page description language (PDL) and sent from user's client and to convert the data to bitmap data so that it can be printed out. |

## 2.8. How to Use TOE

Settings for using TOE are made by system administrator. After being authenticated by entering the default system-administrator's password, which is set at the shipment, at the control panel, system administrator makes settings on the following setting items:

**- Changing of system administrator's password**

Set 7- to 12-digit number other than the default value.

**- Setting for customer-engineer access restriction function**

Set to "Perform."

**- Setting for HDD overwrite function**

Set to "Perform (one time)" or "Perform (three times)."

**- Setting for data encryption function**

Set to "Perform."

**- Setting for password for encrypting data stored on the hard disk drive**

Set 12-digit number. (When 11 or less digit number is set, "0" is automatically set for the shortage.)

When general user uses digital copy, printer, and scanner functions of DocuCentre, used document data are stored on the hard disk drive for DC and that for PESS as described in Table 5.

Security functions of TOE operate for these stored used document data according to the system-administrator's setting before general user knows.

Flows of control data and document data between respective units in each function of

DocuCentre are described in Table 5.

Table 5: Data Flow in Each Function of DocuCentre

| Function | | Data type | Data flow |
|---|---|---|---|
| Digital copy | Normal copy | Control data | Control panel→MF-SYS→DC-SYS/IPS |
| | | Document data | IIT→DC-SYS/IPS→Hard disk drive for DC→DC-SYS/IPS→ IOT |
| Printer | Normal print (non-spool) | Control data | User's client→PESS→MF-SYS→DC-SYS/IPS→DC-SYS/IPS →IOT |
| | | Document data (Print data) | User's client→PESS<br>↓ (Creates bitmap data by decomposing at PESS.) |
| | | Document data (Bitmap data) | PESS→MF-SYS→DC-SYS/IPS→Hard disk drive for DC→ DC-SYS/IPS→IOT |
| | Normal print (Hard-disk-drive spool) | Control data | User's client→PESS→Hard disk drive for PESS→PESS → MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | Document data (Print data) | User's client→PESS→Hard disk drive for PESS→PESS<br>↓ (Creates bitmap data by decomposing at PESS.) |
| | | Document data (Bitmap data) | PESS→MF-SYS→DC-SYS/IPS→Hard disk drive for DC→ DC-SYS/IPS→IOT |
| | Storage print (non-spool) | Control data | 1) Storage of document data on the hard disk drive<br>User's client→PESS→Hard disk drive for PESS<br>2) Printing out of document data<br>(Started by operation at the control panel.)<br>Hard disk drive for PESS→PESS→<br>MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | Document data (Print data) | 1) Storage of document data on the hard disk drive<br>User's client→PESS<br>↓ (Creates bitmap data by decomposing at PESS.) |
| | | Document data (Bitmap data) | PESS→Hard disk drive for PESS<br><br>2) Printing out of document data<br>(Started by operation at the control panel.)<br>Hard disk drive for PESS→PESS→MF-SYS→DC-SYS/IPS →Hard disk drive for DC→DC-SYS/IPS→IOT |
| | Storage print (hard-disk-drive spool) | Control data | 1) Storage of document data on the hard disk drive<br>User's client→PESS→Hard disk drive for PESS→<br>PESS→Hard disk drive for PESS<br>2) Printing out of document data<br>(Started by operation at the control panel.)<br>Hard disk drive for PESS→PESS<br>→MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | Document data (Print data) | 1) Storage of document data on the hard disk drive<br>User's client→PESS→Hard disk drive for PESS→PESS<br>↓ (Creates bitmap data by decomposing at PESS.) |
| | | Document data (Bitmap data) | PESS→Hard disk drive for PESS<br><br>2) Printing out of document data<br>(Started by operation at the control panel.)<br>Hard disk drive for PESS→PESS→MF-SYS→DC-SYS/IPS →Hard disk drive for DC→DC-SYS/IPS→IOT |

| | | | |
|---|---|---|---|
| Scanner | Scan storage | Control data | Control panel→MF-SYS→DC-SYS/IPS<br>Control panel→MF-SYS→PESS |
| | | Document data | IIT→DC-SYS/IPS→MF-SYS→PESS→Hard disk drive for PESS |
| | Scan retrieval | Control data | User's client→PESS |
| | | Document data | Hard disk drive for PESS→PESS→User's client |
| Operation at the control panel | | Control data (operation) | Control panel→MF-SYS→DC-SYS/IPS<br>Control panel→MF-SYS→PESS |

# 3. TOE Security evironment

## 3.1. Assumptions

Assumptions related to the operation and use of this TOE are described in Table 6.

Table 6: Assumptions

| Assumption | Contents |
|---|---|
| **A.SECMODE** | <Protection mode><br>System administrator operates TOE in the condition where the “system-administrator’s password” is set to 7- to 12-digit value and the “customer-engineer access restriction function” is set to operate. |
| **A.ADMIN** | <Trust in system administrator><br>System administrator has knowledge necessary to fulfill the assigned role and does not conduct improperly with malicious intention. |

## 3.2. Threats

System administrator, who is given special access authority to TOE, does not fall under “attacker” because he or she is reliable. Security threats and attackers to this TOE are described in Table 7. Attackers are thought to have low-level attack capability.

Table 7: Security Threats

| Threat | Contents | Attacker | Protected asset |
|---|---|---|---|
| **T.RECOVER** | **<Illicit recovery of used document data>**<br>General user and the person who is not related to TOE might recover used document data such as by removing the hard disk drive and connecting it directly to a tool. | - General user<br>- Non-related person | R.DOCDATA.D<br>R.DOCDATA.P |
| **T.CONFDATA** | **<Illicit access to TOE setting data>**<br>General user and the person who is not related to TOE might change settings by accessing TOE setting data from the control panel. This setting data is allowed to be accessed only by system administrator. | - General user<br>- Non-related person | R.CONFDATA |

## 3.3. Organizational security policies

There are no organizational security policies.

# 4. Security objectives

## 4.1. Security Objectives for the TOE

Security objectives for TOE are described in Table 8.

Table 8: Security Objectives for TOE

| Objective | Description |
|---|---|
| **O.RESIDUAL.D** | TOE must make the recovery of used document data stored on the hard disk drive for DC impossible. |
| **O.RESIDUAL.P** | TOE must make the recovery of used document data stored on the hard disk drive for PESS impossible. |
| **O.DECIPHER.P** | TOE must make the parsing of used document data stored on the hard disk drive for PESS difficult. |

## 4.2. Security objectives for the environment

### 4.2.1. Security Objective for IT Environment

Security objective for IT environment is described in Table 9.

Table 9: Security Objective for IT Environment

| Objective | Description |
|---|---|
| **OE.MANAGE** | UI control function must make only the authenticated system-administrator able to change TOE setting data. |

### 4.2.2. Security Objectives for Operation and Management

Security objectives for operation and management are described in Table 10.

Table 10: Security Objectives for Operation and Management

| Objective | Description |
|---|---|
| **OE.AUTH** | System administrator must manage “system-administrator’s password” so that it is prevented from being guessed or disclosed.<br>He or she must set “system-administrator’s password” to 7- to 12-digit value. |
| **OE.FUNCON** | System administrator must operate TOE in the condition where “HDD overwrite function,” “data encryption function,” and “customer-engineer access restriction function” are set to operate. |
| **OE.ADMIN** | To assure that system administrator has knowledge necessary to fulfill the assigned role and does not conduct with malicious intention, organization person in charge must select suitable member and provide management and education. |
| **OE.POWEROFF** | Organization person in charge must educate general user:<br>- to confirm that no processing is being executed, before turning off the power of DocuCentre.<br>- to turn off the power after the processing is finished, when there is a processing being executed. |

# 5. IT security requirements

## 5.1. TOE security functional requirements

Specifies security functional requirements to be realized by TOE.

### 5.1.1. Class FCS: Cryptographic Support

**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: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

**[assignment: list of standards]**

None

**[assignment: cryptographic key generation algorithm]**

Fuji Xerox's unique FXOSENC algorithm

**[assignment: cryptographic key sizes]**

128 bits

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

**FCS_COP.1 Cryptographic Operation**

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

**[assignment: list of standards]**

AES (Advanced Encryption Standard)

**[assignment: cryptographic algorithm]**

Rijndael Algorithm

**[assignment: cryptographic key sizes]**

128 bits

**[assignment: list of cryptographic operations]**

Encryption of document data stored on the hard disk drive for PESS

Decryption of document data stored on the hard disk drive for PESS

Dependencies: ［FDP_ITC.1 Import of user data without 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

**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: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects].

**［selection: allocation of the resource to, deallocation of the resource from］**

Deallocation of the resource from

**[assignment: list of objects]**

Used document data file stored on the hard disk drive for DC

Used document data file stored on the hard disk drive for PESS

Dependencies: No Dependencies

### 5.1.3. Class FPT: Protection of the TSF

**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

## 5.2. TOE security assurance requirements

Evaluation assurance level of TOE is EAL2. Components of EAL2 assurance package provided in [CC Part3] are described below.

Table 11: EAL2 Assurance Requirements

| Assurance class | Assurance component ID | Assurance component | Dependencies |
|---|---|---|---|
| Configuration management | ACM_CAP.2 | Configuration items | None |
| Delivery and operation | ADO_DEL.1 | Delivery procedures | None |

| | | | |
|---|---|---|---|
| | ADO_IGS.1 | Installation, generation, and start-up procedures | AGD_ADM.1 |
| Development | ADV_FSP.1 | Informal functional specification | ADV_RCR.1 |
| | ADV_HLD.1 | Descriptive high-level design | ADV_FSP.1<br>ADV_RCR.1 |
| | ADV_RCR.1 | Informal correspondence demonstration | None |
| Guidance document | AGD_ADM.1 | Administrator guidance | ADV_FSP.1 |
| | AGD_USR.1 | User guidance | ADV_FSP.1 |
| Test | ATE_COV.1 | Evidence of coverage | ADV_FSP.1<br>ATE_FUN.1 |
| | ATE_FUN.1 | Functional tests | None |
| | ATE_IND.2 | Independent testing - sample | ADV_FSP.1<br>ADV_ADM.1<br>AGD_USR.1<br>ATE_FUN.1 |
| Vulnerability assessment | AVA_SOF.1 | Strength of TOE security function evaluation | ADV_FSP. 1<br>ADV_HLD.1 |
| | AVA_VLA.1 | Developer vulnerability analysis | ADV_FSP.1<br>ADV_HLD.1<br>AGD_ADM.1<br>AGD_USR.1 |

## 5.3. Security requirements for the IT environment

Specifies security functional requirement to be realized by IT environment of TOE.

### 5.3.1. Class FIA: Identification and Authentication

**FIA_UID.2 User Identification before Any Action**

Hierarchical to: FIA_UID.1

FIA_UAU.2.1 [Refinement: UI control function] shall require [refinement: system administrator] to identify itself before allowing any other TSF-mediated actions on behalf of the [refinement: system administrator].

Dependencies: No Dependencies

**FIA_UAU.2 User Authentication before Any Action**

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 [Refinement: UI control function] shall require [refinement: system administrator] to succeed in the authentication [refinement: by system-administrator's password] before allowing any other TSF-mediated actions on behalf of the [refinement: system administrator].

Dependencies: FIA_UID.1 Timing of identification

**FIA_UAU.7 Protected Authentication feedback**

Hierarchical to: No other components.

FIA_UAU.7.1 [Refinement: UI control function] shall provide only [assignment: list of feedback] to the user while the authentication of [refinement: system-administrator's password for system-administrator authentication at

the control panel] is in progress.

**[assignment: list of feedback]**

Asterisks (‘*’) of the same number as the digit number of the entered password

Dependencies: FIA_UAU.1 Timing of authentication

### **5.3.2.** Class FMT: Security Management

**FMT_MOF.1(1) Management of security functions behaviour (1)**

Hierarchical to: No other components.

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

**[assignment: list of functions]**

HDD overwrite function for copy residual data

HDD overwrite function for print and scan residual data

**[selection: determine the behavior of, disable, enable, modify the behavior of]**

Determine the behavior of

Disable

Enable

**[assignment: the authorized identified roles]**

System administrator

Dependencies: FMT_SMF.1 Specification of management function

FMT_SMR.1 Security roles

**FMT_MOF.1 (2) Management of security functions behaviour (2)**

Hierarchical to: No other components.

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

**[assignment: list of functions]**

Data encryption function for print and scan

**[selection: determine the behavior of, disable, enable, modify the behavior of]**

Disable

Enable

**[assignment: the authorized identified roles]**

System administrator

Dependencies: FMT_SMF.1 Specification of management function

FMT_SMR.1 Security roles

**FMT_MTD.1 Management of TSF data**

Hierarchical to: No other components.

FMT_MTD.1.1 [Refinement: UI control function] shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

**[assignment: list of TSF data]**

Setting for HDD overwrite function

Setting for data encryption function

Password for encrypting data stored on the hard disk drive

**[selection: change_default, query, modify, delete, clear, [assignment: other operations]]**

Query

Modify

**[assignment: the authorized identified roles]**

System administrator

Dependencies: FMT_SMF.1 Specification of management function

FMT_SMR.1 Security roles

**FMT_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.

FMT_SMF.1.1 [Refinement: UI control function] shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

**[assignment：list of security management functions to be provided by the TSF]**

Functions to manage the management items described in Table 12

Table 12: Functions to Manage Management Items

| Functional requirement | Management requirement | Management item |
|---|---|---|
| FIA_UID.2 | Management of user identification information | None |
| FIA_UAU.2 | Management of authentication data by system administrator and by the user who is related to this data | System-administrator's password |
| FMT_MOF.1 (1) | Management of the group with a role that has a possibility of having interinfluence with TSF function | Fixed to system administrator. |
| FMT_MOF.1 (2) | Management of the group with a role that has a possibility of having interinfluence | Fixed to system administrator. |

| | | |
|---|---|---|
| | with TSF function | |
| FMT_MTD.1 | Management of the group with a role that has a possibility of having interinfluence with TSF data | Fixed to system administrator. |
| FMT_SMR.1 | Management of user group that is a part of the roles | Fixed to system administrator.<br>(Only the person who knows system-administrator's password can be a system administrator.) |

As for FIA_UID.2, management of identification information is not necessary because the user to be identified is fixed to system administrator. Therefore, there is no management item.

As for FMT_MOF.1, FMT_MTD.1, and FMT_SMR.1, only the system administrator who is authenticated with system-administrator's password is managed, and management of group is not performed.

Dependencies: No Dependencies

**FMT_SMR.1 Security roles**

Hierarchical to: No other components.

FMT_SMR.1.1 [Refinement: UI control function] shall maintain the roles [assignment: the authorized identified roles].

**[assignment: the authorized identified roles]**

System administrator

FMT_SMR.1.2 [Refinement: UI control function] shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

## 5.4. Claim of TOE Security Function Strength

Minimum function strength level of TOE security functions is SOF-basic.

There is no security functional requirement of which security function strength is to be claimed.

# 6. TOE summary specification

## 6.1. TOE security functions

This TOE has the following security functions to satisfy TOE security functional requirements:

- HDD overwrite function for copy residual data (SF.OVERWRITE.D)
- HDD overwrite function for print and scan residual data (SF.OVERWRITE.P)
- Data encryption function for print and scan (SF.ENCRYPTION.P)

Relations between TOE security functions and security functional requirements are described in Table 13.

Table 13: Relations between TOE Security Functions and Security Functional Requirements

| TOE security function / Security functional requirement | SF.OVERWRITE.D | SF.OVERWRITE.P | SF.ENCRYPTION.P |
|---|---|---|---|
| FCS_CKM.1 | | | O |
| FCS_COP.1 | | | O |
| FDP_RIP.1 | O | O | |
| FPT_RVM.1 | O | O | O |

O: Shows that it is the security function that satisfies the security functional requirement.

### 6.1.1. HDD Overwrite Function for Copy Residual Data (SF.OVERWRITE.D)

According to the ”setting for HDD overwrite function” that is set by system administrator, this function overwrites and erases the used document data on the hard disk drive for DC using the way described in Table 14.

Flag that shows whether document data currently exists or not is on the hard disk drive for DC. When this flag shows the existence of document data at the time of booting the system, TOE overwrites and erases the entire data on the hard disk drive for DC.

This function is configured to certainly operate because it is realized by unique software that does not have bypass measures.

Table 14: Control of Overwriting

| Number of overwritings | Data to overwrite with |
|---|---|
| One time | 0 |
| Three times | First time: random number<br>Second time: random number<br>Third time: 0 |

### 6.1.2. HDD Overwrite Function for Print and Scan Residual Data (SF.OVERWRITE.P)

According to the ”setting for HDD overwrite function” that is set by system administrator, this function overwrites and erases the used document data on the hard disk drive for PESS using the way described in Table 15.

List of the used document data that are to be overwritten and erased is on the hard disk drive for PESS. When the existence of the used document data is shown in this list at the time of booting the system, this function overwrites and erases the used document data.

This function is configured to certainly operate because it is realized by unique software that does not have bypass measures.

Table 15: Control of Overwriting

| Number of overwritings | Data to overwrite with |
|---|---|
| One time | 0 |
| Three times | First time: random number<br>Second time: random number<br>Third time: 0 |

### 6.1.3. Data Encryption Function for Print and Scan (SF.ENCRYPTION.P)

According to the “setting for data encryption function” that is set by system administrator, this function encrypts and decrypts document data stored on the hard disk drive for PESS. At the time of booting, TOE generates 128-bit cryptographic key using the Fuji Xerox’s unique FXOSENC algorithm and “password for encrypting data stored on the hard disk drive” that is set by system administrator. (When “password for encrypting data stored on the hard disk drive” is the same, the same cryptographic key is generated.)

When storing document data on the hard disk drive for PESS, TOE stores the document data after performing encryption using the cryptographic key generated at the time of booting. When reading the stored document data, TOE also performs decryption using the cryptographic key generated at the time of booting.

The cryptographic key generated at the time of booting is stored on RAM for PESS (volatile RAM) in DocuCentre. Cryptographic key is lost when the power of the mainframe of DocuCentre is shut down.

This function is configured to certainly operate because it is realized by unique software that does not have bypass measures.

This function also uses the encryption mechanism (encryption with Rijndael Algorithm) as a security mechanism.

### 6.1.4. Function that is Realized using Probabilistic or Permutational Mechanisms

Among TOE security functions, there is no function that is realized using probabilistic or permutational mechanisms.

## 6.2. Assurance measures

### 6.2.1. Configuration Management Description (AS.CONFIGURATION)

The following are described in the “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

### 6.2.2. TOE Configuration List (AS.CONFIGURATIONLIST)

The following are described in the “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

### 6.2.3. Delivery, Introduction, and Operation Procedure Description (AS.DELIVERY)

The following are described in the “Delivery, Introduction, and Operation Procedure Description”:

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

Corresponding security assurance requirement:

ADO_DEL.1

ADO_IGS.1

### 6.2.4. Functional Specification (AS.FUNCSPEC)

The following are described in the “Functional Specification”:

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

Corresponding security assurance requirement:
ADV_FSP.1

### 6.2.5. High-Level Design Specification (AS.HIGHLDESIGN)

The following are described in the “High-level Design Specification”:

- TOE security functions’ configuration as seen from the subsystems
- Purpose and usage (including exceptional items and error messages) 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

### 6.2.6. Correspondence Analysis Description (AS.REPRESENT)

The following is described in the “Correspondence Analysis Description”:

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

Corresponding security assurance requirement:
ADV_RCR.1

### 6.2.7. User Guide for DocuCentre 719/659/559 Series (Data Security Kit) (AS. GUIDANCE)

In the development of TOE, Fuji Xerox creates manual (“User Guide for DocuCentre 719/659/559 Series [Data Security Kit]”) and reviews the following in the development department, product evaluation department, and technical support department.

<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 misoperation
  - 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

“User Guide for DocuCentre 719/659/559 Series (Data Security Kit)” is common to system administrator and general user.
The following are described in this user guide.

<Description for system administrator>
- Management functions that are used by system administrator, and its interfaces
- How to manage TOE by ensuring the security
- Notes on the functions that should be managed in the environment where the security is ensured, and notes on authority
- Notes on all the security-related parameters under the management of 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 system administrator, and clear indication of specific measures to be taken

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

Corresponding security assurance requirement:
ADO_DEL.1
ADO_IGS.1
AGD_ADM.1
AGD_USR.1

### **6.2.8.** Test Plan (AS.TESTPLAN)

The following are described in the “Test Plan”:
- Overall plan in which the schedule, skills necessary for testers, and configuration of the system

used for the test are described

- Test items
- Test coverage analysis that verifies that all the functions described in the “Functional Specification” are tested with the test items

Corresponding security assurance requirement:

ATE_COV.1

ATE_FUN.1

ATE_IND.2

### **6.2.9.** Test-result Report (AS.TESTSPEC)

The following are described in the “Test-result Report”:

- Purpose of test
- How to conduct test
- Expected result of test
- Date of conducting test, and the name of the test conductor
- Result of test

Corresponding security assurance requirement:

ATE_FUN.1

### **6.2.10.** Vulnerability Analysis (AS.VULNERABILITY)

The following are described in the “Vulnerability Analysis.” This document verifies that the TOE’s identified vulnerability is not problematic in an assumed environment.

- 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 operation 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_VLA.1

# 7. PP claims

## 7.1. PP reference

There is no referred PP.

## 7.2. PP tailoring

There is no tailoring to PP.

## 7.3. PP additions

There is no addition to PP.

# 8. Rationale

## 8.1. Security Objectives rationale

Correspondences between security objectives and threats/assumptions are described in Table 16.

**(1) Necessity**

Rationale for the necessity of security objectives is described below.

As described in Table 16, all the security objectives correspond to one or more threats/assumptions.

Table 16: Correspondences between Security Objectives and Threats/Assumptions

| Threat/assumption / Security objective | T.RECOVER | T.CONFDATA | A.SECMODE | A.ADMIN |
|---|---|---|---|---|
| O.RESIDUAL.D | O | | | |
| O.RESIDUAL.P | O | | | |
| O.DECIPHER.P | O | | | |
| OE.MANAGE | | O | | |
| OE.AUTH | | | O | |
| OE.FUNCON | O | | O | |
| OE.ADMIN | | | | O |
| OE.POWEROFF | O | | | |

O: Shows that it is the threat or assumption that the security objective corresponds to.

**(2) Sufficiency**

The following describes the rationales that show that the sufficient measures against all the threats to TOE and those for all the assumptions are taken.

As described in Table 16, one or more security objectives correspond to a threat. Threats can be countered when the corresponding security objectives are satisfied.

As described in Table 16, one or more security objectives correspond to an assumption. Assumptions are assured when the corresponding security objectives are satisfied.

Table 17 describes the rationales that show that the measures against threats to TOE and those for assumptions are taken by satisfying the security objectives.

Table 17: Sufficiency of Security Objectives

| Threat/ assumption | Security objective |
|---|---|
| **T.RECOVER** | To counter this threat, all of the following need to be satisfied:<br>- TOE security functions are enabled.<br>- TOE security functions are operated so that they are completely performed.<br>- Recovery of used document data stored on the hard disk drive for DC and that for PESS is made impossible.<br><br>By satisfying the following objectives, **T.RECOVER** can be countered:<br>- **O.RESIDUAL.D**<br>By satisfying **O.RESIDUAL.D**, TOE makes the recovery of used document data stored |

| | |
|---|---|
| | on the hard disk drive for DC impossible.<br>Used document data stored on the hard disk drive for DC is difficult to be parsed because it is bitmap data and recorded after being compressed using the Fuji Xerox's unique method. Additionally, the recovery of data can be made impossible by overwriting and erasing the data by satisfying **O.RESIDUAL.D**.<br>- **O.RESIDUAL.P** and **O.DECIPHER.P**<br>By satisfying **O.RESIDUAL.P** and **O.DECIPHER.P**, TOE makes the recovery of used document data stored on the hard disk drive for PESS impossible.<br>Used document data stored on the hard disk drive for PESS includes print data used in printer function. This print data is sometimes described in text format and is relatively easy to be parsed. Therefore, TOE makes the recovery of used document data stored on the hard disk drive for PESS impossible by encrypting the document data stored on the hard disk drive for PESS by satisfying **O.DECIPHER.P** and then overwriting and erasing the data by satisfying **O.RESIDUAL.P**.<br>- **OE.FUNCON** and **OE.POWEROFF**<br>By satisfying **OE.FUNCON** and **OE.POWEROFF**, TOE security functions are enabled, and can be operated so that they are completely performed.<br>By satisfying **OE.FUNCON**, system administrator operates TOE security functions ("HDD overwrite function for copy residual data," "HDD overwrite function for print and scan residual data" and "data encryption function for print and scan") in the condition where these functions are enabled.<br>By satisfying **OE.POWEROFF**, organization person in charge educates general user to turn off the power after the processing is finished so that the performance of the security functions ("HDD overwrite function for copy residual data" and "HDD overwrite function for print and scan residual data") is not interrupted by power shutdown. |
| **T.CONFDATA** | To counter this threat, the person who changes TOE setting data needs to be limited to the authenticated system-administrator.<br>By satisfying the following objective, **T.CONFDATA** can be countered:<br>- **OE.MANAGE**<br>By satisfying **OE.MANAGE**, only the authenticated system-administrator becomes able to change TOE setting data. |
| **A.SECMODE** | By satisfying the following objectives, **A.SECMODE** can be realized:<br>- **OE.AUTH**<br>By satisfying **OE.AUTH**, system administrator sets the "system-administrator's password" to 7- to 12-digit value.<br>- **OE.FUNCON**<br>By satisfying **OE.FUNCON**, system administrator operates TOE in the condition where the "customer-engineer access restriction function" is set to operate. |
| **A.ADMIN** | By satisfying the following objective, **A.ADMIN** can be realized:<br>- **OE.ADMIN**<br>By satisfying **OE.ADMIN**, organization person in charge selects suitable member for system administrator and provides management and education. |

## 8.2. Security requirements rationale

### 8.2.1. Security functional requirements rationale

**(1) Necessity**

Relations between security functional requirements and security objectives are described in Table 18.

Each TOE security functional requirement corresponds to at least one security objective.

Table 18: Correspondences between Security Functional Requirements and Security Objectives

| Security objective / Security functional requirement | O.RESIDUAL.D | O.RESIDUAL.P | O.DECIPHER.P | OE.MANAGE |
|---|---|---|---|---|
| FCS_CKM.1 | | | O | |
| FCS_COP.1 | | | O | |
| FDP_RIP.1 | O | O | | |
| FPT_RVM.1 | O | O | O | |
| FIA_UID.2 | | | | • |
| FIA_UAU.2 | | | | • |
| FIA_UAU.7 | | | | • |
| FMT_MOF.1 (1) | | | | • |
| FMT_MOF.1 (2) | | | | • |
| FMT_MTD.1 | | | | • |
| FMT_SMF.1 | | | | • |
| FMT_SMR.1 | | | | • |

O: Functional requirement for TOE

•: Functional requirement for IT environment

**(2) Sufficiency**

Table 19 describes that the functional requirements assure all the security objectives for TOE.

Table 19: Sufficiency of Objectives

| Security objective | Functional requirement | Sufficiency |
|---|---|---|
| **O.RESIDUAL.D** | **FDP_RIP.1**<br>**FPT_RVM.1** | By the following security functional requirements, the security objective **O.RESIDUAL.D** in which TOE makes the recovery of used document data stored on the hard disk drive for DC impossible can be realized:<br>- **FDP_RIP.1**<br>By **FDP_RIP.1**, the previous information of the used document data file stored on the hard disk drive for DC is made unavailable.<br>- **FPT_RVM.1**<br>By **FPT_RVM.1**, TOE security functions are certainly invoked and not bypassed. |
| **O.RESIDUAL.P** | **FDP_RIP.1**<br>**FPT_RVM.1** | By the following security functional requirements, the security objective **O.RESIDUAL.P** in which TOE makes the recovery of used document data stored on the hard disk drive for PESS impossible can be realized:<br>- **FDP_RIP.1**<br>By **FDP_RIP.1**, the previous information of the used document data file stored on the hard disk drive for PESS is made unavailable.<br>- **FPT_RVM.1**<br>By **FPT_RVM.1**, TOE security functions are certainly invoked and |

| | | |
|---|---|---|
| | | not bypassed. |
| **O.DECIPHER.P** | **FCS_CKM.1**<br>**FCS_COP.1**<br>**FPT_RVM.1** | By the following security functional requirements, the security objective **O.DECIPHER.P** in which TOE makes the parsing of used document data stored on the hard disk drive for PESS difficult can be realized:<br>- **FCS_CKM.1**<br>By **FCS_CKM.1**, the cryptographic key of the specified cryptographic key size is generated.<br>- **FCS_COP.1**<br>By **FCS_COP.1**, in accordance with the determined cryptographic algorithm and cryptographic key size, the document data stored on the hard disk drive for PESS is encrypted and then decrypted when the data is read.<br>- **FPT_RVM.1**<br>By **FPT_RVM.1**, TOE security functions are certainly invoked and not bypassed. |
| **OE.MANAGE** | **FIA_UID.2**<br>**FIA_UAU.2**<br>**FIA_UAU.7**<br>**FMT_MOF.1 (1)**<br>**FMT_MOF.1 (2)**<br>**FMT_MTD.1**<br>**FMT_SMF.1**<br>**FMT_SMR.1** | By the following security functional requirements, **OE.MANAGE** can be realized:<br>- **FIA_UID.2** and **FIA_UAU.2**<br>By **FIA_UID.2** and **FIA_UAU.2**, identification and authentication are performed before the operation from the control panel when system-administrator's identification and authentication using DocuCentre's UI control function is needed for the operation.<br>- **FIA_UAU.7**<br>By **FIA_UAU.7**, illicit leakage of the authentication information is prevented because the authentication feedback is protected.<br>- **FMT_MTD.1** and **FMT_MOF.1 (1)**<br>"HDD overwrite function for copy residual data" and "HDD overwrite function for print and scan residual data" are assured to be certainly performed because:<br>- by **FMT_MTD.1**, the person who queries and modifies the setting value of the TOE setting data for "setting for HDD overwrite function," "setting for data encryption function," and "password for encrypting data stored on the hard disk drive" is limited only to the system administrator using DocuCentre's UI control function.<br>- by **FMT_MOF.1 (1)**, the person who performs the following for the TOE security functions "HDD overwrite function for copy residual data" and "HDD overwrite function for print and scan residual data" is limited to system administrator:<br>- making of settings on the number of overwritings and erasings in these functions<br>- disabling of these functions<br>- enabling of these functions<br>- **FMT_MOF.1 (2)**<br>By **FMT_MOF.1 (2)**, "data encryption function for print and scan" is assured to be certainly performed because the person who disables and enables the TOE security function "data encryption function for print and scan" is limited to system administrator.<br>- **FMT_SMR.1**<br>By **FMT_SMR.1**, DocuCentre's UI control function limits the security-related role to system administrator by fixing the user with special authority to system administrator.<br>- **FMT_SMF.1**<br>By **FMT_SMF.1**, DocuCentre's UI control function provides security management functions to manage system-administrator's password. |

**(3) Validity of Security Function Strength Level**

Attack capability of the attackers assumed for this TOE is low level. Therefore, “SOF-basic” being the minimum function strength level is appropriate. However, this TOE has no mechanism that is related to the function strength.

**(4) Dependencies of Security Functional Requirements**

Functional requirements that are depended on by security functional requirements and those that are not are described in Table 20.

Table 20: Dependencies of Functional Requirements

| Component | Component that is depended on | Component that is not depended on |
|---|---|---|
| FCS_CKM.1 | FCS_COP.1 | FCS_CKM.4<br>Cryptographic key is generated when booting DocuCentre, and stored on RAM for PESS (volatile RAM). Cryptographic key does not need to be destructed because this key is lost when the power of the mainframe of DocuCentre is shut down.<br>Therefore, the dependency on FCS_CKM.4 does not need to be satisfied.<br>FMT_MSA.2<br>TOE automatically generates the cryptographic key of the fixed 128-bit size from the TOE setting data for “password for encrypting data stored on the hard disk drive” that is set by system administrator.<br>It is not necessary to assure that only the secure value is accepted because the size of this cryptographic key that is automatically generated by TOE is fixed to 128-bit.<br>TOE always uses the automatically-generated cryptographic key, and the security attribute other than the key size does not exist.<br>Therefore, the dependency on FMT_MSA.2 does not need to be satisfied. |
| FCS_COP.1 | FCS_CKM.1 | FCS_CKM.4<br>Cryptographic key is generated when booting DocuCentre, and stored on RAM for PESS (volatile RAM). Cryptographic key does not need to be destructed because this key is lost when the power of the mainframe of DocuCentre is shut down.<br>Therefore, the dependency on FCS_CKM.4 does not need to be satisfied.<br>FMT_MSA.2<br>TOE automatically generates the cryptographic key of the fixed 128-bit size from the TOE setting data for “password for encrypting data stored on the hard disk drive” that is set by system administrator.<br>It is not necessary to assure that only the secure value is accepted because the size of this cryptographic key that is automatically generated by TOE is fixed to 128-bit.<br>TOE always uses the automatically-generated cryptographic key, and the security attribute other than the key size does not exist.<br>Therefore, the dependency on FMT_MSA.2 does not need to be satisfied. |
| FDP_RIP.1 | None | None |
| FIA_UID2 | None | None |
| FIA_UAU.2 | FIA_UID.2 | FIA_UID.1<br>The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1. |
| FIA_UAU.7 | FIA_UID.2 | FIA_UID.1 |

| | | |
|---|---|---|
| | | The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1. |
| FMT_MOF.1 (1) | FMT_SMF.1<br>FMT_SMR.1 | None |
| FMT_MOF.1 (2) | FMT_SMF.1<br>FMT_SMR.1 | None |
| FMT_MTD.1 | FMT_SMF.1<br>FMT_SMR.1 | None |
| FMT_SMF.1 | None | None |
| FMT_SMR.1 | FIA_UID.2 | FIA_UID.1<br>The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the security functional requirement that is an upper hierarchy of FIA_UID.1. |
| FPT_RVM.1 | None | None |

**(5) Interactions among Security Functional Requirements**

Interactions among security functional requirements are verified in Table 21.

Table 21: Interactions among Security Functional Requirements

| Security functional requirement | Security functional requirement that provides protection | |
|---|---|---|
| | Circumvention | Deactivation |
| FCS_CKM.1 | FPT_RVM.1 | FMT_MOF.1 (2) |
| FCS_COP.1 | FPT_RVM.1 | FMT_MOF.1 (2) |
| FDP_RIP.1 | FPT_RVM.1 | FMT_MOF.1 (1) |
| FIA_UID.2 | N/A | N/A |
| FIA_UAU.2 | N/A | N/A |
| FIA_UAU.7 | N/A | N/A |
| FMT_MOF.1 (1) | N/A | N/A |
| FMT_MOF.1 (2) | N/A | N/A |
| FMT_MTD.1 | N/A | N/A |
| FMT_SMF.1 | N/A | N/A |
| FMT_SMR.1 | N/A | N/A |
| FPT_RVM.1 | N/A | N/A |

N/A: There is no security functional requirement that performs mutual support.

Circumvention

FPT_RVM.1

The TOE security functions (FCS_CKM.1 and FCS_COP.1) are configured by unique software that does not have bypass measures, and cannot be replaced with other modules. The functions are also configured to be always performed. Therefore, cryptographic-key generation and cryptographic operation cannot be circumvented, and non-bypassability is ensured.

The TOE security function (FDP_RIP.1) is configured by unique software and cannot be replaced with another module. It is configured so that, when overwriting and erasing are interrupted such as by power shutdown, re-overwriting and re-erasing are performed at the next power-on. Therefore, non-bypassability is ensured.

Deactivation

FMT_MOF.1 (1)

FMT_MOF.1 (1) assures the protection of the “HDD overwrite function for copy residual data” and the “HDD overwrite function for print and scan residual data” (FDP_RIP.1) from being deactivated by a user other than system administrator.

FMT_MOF.1 (2)

FMT_MOF.1 (2) assures the protection of the “data encryption function for print and scan” (FCS_CKM.1 and FCS_COP.1) from being deactivated by a user other than system administrator.

### 8.2.2. Security assurance requirements rationale

Attacker has low-level attack capability and attacks using TOE’s external interface, the control panel. Therefore, evaluation assurance level EAL2 is appropriate because TOE needs to counter low-level attack by an attacker.

## 8.3. TOE summary specification rationale

### 8.3.1. Function summary specification rationale

**(1) Necessity**

Correspondences between security functional requirements and TOE security functions are described in Table 22.

TOE security functions correspond to security functional requirements.

All TOE security functions are necessary to realize the security functional requirements.

Table 22: Correspondences between Security Functional Requirements and TOE Security Functions

| TOE security function / Security functional requirement | SF.OVERWRITE.D | SF.OVERWRITE.P | SF.ENCRYPTION.P |
|---|---|---|---|
| FCS_CKM.1 | | | O |
| FCS_COP.1 | | | O |
| FDP_RIP.1 | O | O | |
| FPT_RVM.1 | O | O | O |

O: Shows that it is the security function that satisfies the security functional requirement.

**(2) Sufficiency**

Table 23 describes that TOE security functions sufficiently realize TOE security functional requirements.

Table 23: Sufficiency of Security Functional Requirements

| Functional requirement | Security function |
|---|---|
| **FCS_CKM.1** | By the following security function, **FCS_CKM.1**, the cryptographic-key generation, can be assured:<br>- **SF.ENCRYPTION.P**<br>By **SF.ENCRYPTION.P**, TOE generates 128-bit cryptographic key, at the time of booting, using the Fuji Xerox's unique FXOSENC algorithm and "password for encrypting data stored on the hard disk drive" set by system administrator. Fuji Xerox's unique FXOSENC algorithm is a secure algorithm that has sufficient complexity. |
| **FCS_COP.1** | By the following security function, **FCS_COP.1**, the cryptographic operation, can be assured:<br>- **SF.ENCRYPTION.P**<br>By **SF.ENCRYPTION.P**, TOE encrypts document data stored on the hard disk drive for PESS using the automatically-generated cryptographic key. |
| **FDP_RIP.1** | By the following security functions, **FDP_RIP.1**, the subset residual information protection, can be assured:<br>- **SF.OVERWRITE.D** and **SF.OVERWRITE.P**<br>By **SF.OVERWRITE.D**, TOE overwrites and erases used document data file stored on the hard disk drive for DC.<br>By **SF.OVERWRITE.P**, TOE overwrites and erases used document data file stored on the hard disk drive for PESS.<br>Both in **SF.OVERWRITE.D** and **SF.OVERWRITE.P**, one-time overwriting (overwriting with "0") or three-time overwritings (overwriting with random number, again with random number, and then with "0") can be selected as a control of overwriting and erasing so that process efficiency or security strength can be prioritized depending on the usage environment of the multifunction machine.<br>When process efficiency is prioritized, the number of overwritings and erasings is "one." One-time overwriting and erasing is appropriate because it has less effect of lowering process speed and can counter low-level attack to recover data.<br>When security strength is prioritized, the number of overwiritngs and erasings is "three." Three-time overwritings and erasings are appropriate because they are more robust (recommended number of overwritings and erasings) and can sufficiently counter low-level attack to recover data, although process speed is lower than one-time overwriting and erasing. |
| **FPT_RVM.1** | By the following security functions, **FPT_RVM.1**, the non-bypassability of TSP, can be assured:<br>- **SF.ENCRYPTION.P**, **SF.OVERWRITE.D**, and **SF.OVERWRITE.P**<br>**SF.ENCRYPTION.P**, **SF.OVERWRITE.D**, and **SF.OVERWRITE.P** are configured to certainly operate because they are configured by unique software that does not have bypass measures. |

### 8.3.2. Assurance measures rationale

Rationales for the necessity and sufficiency of assurance measures are described below.

**(1) Necessity**

Table 24 describes that all the assurance measures described in 6.2. are necessary to realize the security assurance requirements.

All assurance measures are necessary to realize EAL2 security assurance requirements.

Table 24: Correspondences between Assurance Measures and Security Assurance Requirements

| | AS.CONFIGURATION | AS.CONFIGURATIONLIST | AS.DELIVERY | AS.FUNCSPEC | AS.HIGHLDESIGN | AS.REPRESENT | AS.GUIDANCE | AS.TESTPLAN | AS.TESTSPEC | AS.VULNERABILITY |
|---|---|---|---|---|---|---|---|---|---|---|
| ACM_CAP.2 | O | O | | | | | | | | |
| ADO_DEL.1 | | | O | | | | O | | | |
| ADO_IGS.1 | | | O | | | | O | | | |
| ADV_FSP.1 | | | | O | | | | | | |
| ADV_HLD.1 | | | | | O | | | | | |
| ADV_RCR.1 | | | | | | O | | | | |
| AGD_ADM.1 | | | | | | | O | | | |
| AGD_USR.1 | | | | | | | O | | | |
| ATE_COV.1 | | | | | | | | O | | |
| ATE_FUN.1 | | | | | | | | O | O | |
| ATE_IND.2 | | | | | | | | O | | |
| AVA_SOF.1 | - | - | - | - | - | - | - | - | - | - |
| AVA_VLA.1 | | | | | | | | | | O |

O: Shows that it is the assurance measure that satisfies the security assurance requirement.
-: Shows that assurance measure to satisfy the security assurance requirement is not necessary.

**(2) Sufficiency**

Assurance measures that correspond to each security assurance requirement and the sufficiency of the measures to satisfy the requirement are described below.

**1. ACM_CAP.2 Authorization Controls**

[Corresponding assurance measure]

The following documents are provided. By these documents, the requirements such as naming rule for identifying TOE version, list of configuration items, and unique identifier of each configuration item can be satisfied:

- “Configuration Management Description” (AS. CONFIGURATION)
- “TOE Configuration List” (AS. CONFIGURATIONLIST)

**2. ADO_DEL.1 Delivery Procedures**

[Corresponding assurance measure]

The following documents are provided. By these documents, the requirements such as TOE identification and maintenance of the integrity of TOE in transit, details of delivery procedures, and system-administrator’s TOE checking method can be satisfied:

- “Delivery, Introduction, and Operation Procedure Description” (AS. DELIVERY)
- “User Guide for DocuCentre 719/659/559 Series (Data Security Kit)” (AS. GUIDANCE)

**3. ADO_IGS.1 Installation, Generation, and Start-up Procedures**

[Corresponding assurance measure]

The following documents are provided. By these documents, the requirements such as procedure / checking method for TOE installation/activation and how to deal with exceptional events can be satisfied:

- “Delivery, Introduction, and Operation Procedure Description” (AS. DELIVERY)
- “User Guide for DocuCentre 719/659/559 Series (Data Security Kit)” (AS. GUIDANCE)

**4. ADV_FSP.1 Informal Functional Specification**

[Corresponding assurance measure]

The following document is provided. By this document, the requirements such as consistent/complete description of TOE security functions and its external interfaces, and detail description of external interfaces can be satisfied:

- “Functional Specification” (AS.FUNCSPEC)

**5. ADV_HLD.1 Security Enforcing High-level Design**

[Corresponding assurance measure]

The following document is provided. By this document, the requirements such as consistent description of TOE security functions’ configuration, identification/description of interfaces among subsystems, and identification of subsystems that provide security functions can be satisfied:

- “High-level Design Specification” (AS.HIGHLDESIGN)

**6. ADV_RCR.1 Informal Correspondence Demonstration**

[Corresponding assurance measure]

The following document is provided. By this document, the requirements such as TOE security functions’ complete correspondence in each level (TOE summary specification, functional specification, and configuration design specification that are described in this ST) can be satisfied:

- “Correspondence Analysis Description” (AS.REPRESENT)

**7. AGD_ADM.1 Administrator Guidance**

[Corresponding assurance measure]

The following document is provided. By this document, the requirements such as description of management functions / interfaces that can be used by system administrator, assumption about system-administrator’s responsibility and behavior, and measures to deal with warning messages can be satisfied:

- “User Guide for DocuCentre 719/659/559 Series (Data Security Kit)” (AS. GUIDANCE)

**8. AGD_USR.1 User Guidance**

[Corresponding assurance measure]

The following document is provided. By this document, the requirements such as description of security functions / interfaces that can be used by general user, assumption about general-user's responsibility and behavior, and measures to deal with warning messages can be satisfied:

- "User Guide for DocuCentre 719/659/559 Series (Data Security Kit)" (AS. GUIDANCE)

**9. ATE_COV.1 Analysis of Coverage**

[Corresponding assurance measure]

The following document is provided. By this document, the requirement of sufficiency/integrity of TOE security function test can be satisfied:

- "Test Plan" (AS.TESTPLAN)

**10. ATE_FUN.1 Functional Tests**

[Corresponding assurance measure]

The following documents are provided. By these documents, the requirement that TOE security functions are certainly tested can be satisfied:

- "Test Plan" (AS.TESTPLAN)
- "Test-result Report" (AS.TESTSPEC)

**11. ATE_IND.2 Independent Testing - Sample**

[Corresponding assurance measure]

The following document is provided. By this document, the requirements of recreation of the environment for testing TOE security functions and provision of test materials can be satisfied:

- "Test Plan" (AS.TESTPLAN)

**12. AVA_SOF.1 Security Function Strength Evaluation**

This TOE has no mechanism that is related to the function strength.

Therefore, there is no assurance measure to be taken.

**13. AVA_VLA.1 Developer Vulnerability Analysis**

[Corresponding assurance measure]

The following document is provided. By this document, the requirement for checking that the TOE's identified vulnerability is not illicitly used in an assumed environment can be satisfied:

- "Vulnerability Analysis" (AS.VULNERABILITY)

## 8.4. PP claims rationale

There is no applicable PP.