Multi-Functional Printer (Digital Copier)

7222/7322/7228/7235 Series

Security Target

Version 10

This document is a translation of the security target written in Japanese which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

March 24, 2004

Konica-Minolta Business Technologies, Inc.

Revision History

Rev. No.	Revision	Approved by	Checked by	Created by
1	● Initial Version	11/28/2003 Koichi Kitamoto	11/28/2003 Takashi Ito	11/28/2003 Akihiko Oda
2	● Ch 2: Addition of Scan to PC(SMB) function and Error revision ● Ch 2: Revised Fig 2.2 (user box is included in TOE) ● Ch 2: Revised description of WRITE function ● Ch 3: Revised description of T.ACCESS ● Ch 4: Revised description of O.RESIDUAL ● Ch 4: Revised description of O.DATAACCESS ● Ch 4: Revised description of OE.USR ● Ch 5: Revised description of FDP_ACC.1, FAU_GEN.1, GMT_MOF.1[2], FMT_MOF1[3] ● Ch 5: Deletion of FMT_MTD.1[1], Changed FMT_MTD.1[2] and FMT_MTD1[3] to FMT_MTD.1[1] and FMT_MTD1[2] each ● Ch 5: Deletion of FMT_SMR.1 ● Ch 6: Revised description according to above mentioned revision ● Ch 8: Revised description according to above mentioned revision	1/5/2004 Koichi Kitamoto	1/5/2004 Takashi Ito	1/5/2004 Akihiko Oda

Rev. No.	Revision	Approved by	Checked by	Created by
3	● Ch 2: Revised Fig 2.2 and Fig.2.3(removal of hatching part of user box, addition of plural figure of user boxes and document data files) ● Ch 2: Added “plural user boxes and document data files” description ● Ch 2: Revised description TOE function ● Ch 2: Added description of ISW function to CE function ● Ch 3: Added description of ASM_NET, ASM_SECMODE, OSP_MANAGE ● Ch 3: Revised description T.ACCESS ● Ch 4: Added description of OE.NET and OE.SECMODE ● Ch 4: Revised description O.DATAACCESS, O.CE and O.AUDIT ● Ch 5: Detailed description of FIA_UID.2 secret ● Ch 5: Detailed description of FIA_UID.2 and FIA_UAU.2 user ● Ch 5: Detailed description of FMT_MSA.3 security attribute ● Ch 5: Added description of FMT_SMR.1, FMT_MTD.1[3][4] and FPT_SEP.1 ● Ch 5: Deletion of FMT_MSA.1[2] ● Ch 5: Revised description FDP_ACF.1.2 and FAU_GEN.1.1 ● Ch 5: Deletion of FMT_MOF.1[1][2], Changed FMT_MOF.1[3] to FMT_MOF.1 and revised description of FMT_MOF.1 ● Ch 5: Revised description FMT_SMF.1 management items (continued)	2/6/2004 Koichi Kitamoto	2/6/2004 Takashi Ito	2/6/2004 Akihiko Oda

Rev. No.	Revision	Approved by	Checked by	Created by
(cont.)	● Ch 6: Revised description IA.ADM_ADD, IA_ADM_AUTH. IA.CE_AUTH, IA.PASS, ACL.USR, RD.TEMP, AUD.LOG, MNG_MODE and MNG.ADM ● Ch 8: Revised description according to above mentioned revision (Above revisions are amended according to O.R. from ASE-001-01 to ASE-005-01.) ● Ch 8: Revised description of related document names in table 6.1 ● According to ASE-006-01, Deleted of SMB explanation in table 2.1 and instead added to table 2.2 ● According to ASE-007-01, added PC(SMB) function description to 6.1.2	2/6/2004 Koichi Kitamoto	2/6/2004 Takashi Ito	2/6/2004 Akihiko Oda
4	● Confirmed the formal name of TOE and revised related description ● Addition of TOE overseas name	2/6/2004 Koichi Kitamoto	2/6/2004 Takashi Ito	2/6/2004 Akihiko Oda
5	● Ch 2: Revised description of TOE scope ● Ch 2: Deleted description of general users' register/delete in management function ● Ch 3: Added description of OSR.RIP ● Ch 4: Added description of O.RIP ● Ch 5: Added description of FDP_ACC.1[2] and FDP_ACF.1[2] ● Ch 5: Deleted description of document data file identifier ● Deleted description of FMT_MSA.1[3] and FMT_MSA.1[4] items in 8.3.1	10/9/2003 Koichi Kitamoto	10/9/2003 Takashi Ito	10/9/2003 Akihiko Oda

Rev. No.	**Revision**	**Approved by**	**Checked by**	**Created by**
6	● According to ASE-010-01, added explanation of TOE name and installed machines series in 1.2 ● Revised Fig 2.2 (hatching area)	2/24/2004 Koichi Kitamoto	2/24/2004 Takashi Ito	2/24/2004 Akihiko Oda
7	● Addition of document (Guidance in English) in 6.3 ● 6.1.5: Revised MNG.MODE ● Error revision	3/11/2004 Koichi Kitamoto	3/11/2004 Takashi Ito	3/11/2004 Akihiko Oda
8	● According to ASE-011-01, added explanation of TOE security environment ● According to ASE-012-01, added explanation of TOE security environment	3/16/2004 Koichi Kitamoto	3/16/2004 Takashi Ito	3/16/2004 Akihiko Oda
9	● Detailed description of FMT_MSA.3.1 and Revised description of 8.3.3 explanation	3/23/2004 Koichi Kitamoto	3/23/2004 Takashi Ito	3/23/2004 Akihiko Oda
10	● Error revision	3/24/2004 Koichi Kitamoto	3/24/2004 Takashi Ito	3/24/2004 Akihiko Oda

Table of Contents

Table of Contents: Figures

Table of Contents: Tables

1. ST Introduction

1.1. ST Identification

1.1.1. ST Identification

Name:	Multi-Functional Printer (Digital Copier) 7222/7322/7228/7235 Series Security Target
Version:	Version 10
Creation Date:	March 24, 2004
Producer:	Konica-Minolta Business Technologies, Inc.

1.1.2. TOE Identification

Name:	7222/7322/7228/7235 System Control Software (Japan) 7222/7228/7235 Control Software (Overseas)
Version:	10.0000
Developer:	Konica-Minolta Business Technologies, Inc.

7222/7322/7228/7235 System Control Software(Japan) and *7222/7228/7235 Control Software(Overseas)* are identical but differ only in their name. (Because of the lack of 7322 series product overseas, its name is omitted in the latter software title.) The name "*7222/7322/7228/7235 System Control Software"* is used hereafter as for TOE.

1.1.3. Used CC version

JIS X 5070:2000

Note: The Japanese versions are used as for the following materials.

- Common Criteria for Information Technology Security Evaluation Part 1: Overview and General Model, version 2.1, August 1999, CCIMB-99-031 (Japanese)
- Common Criteria for Information Technology Security Evaluation Part 2: Security Structure Requirements, version 2.1, August 1999, CCIMB-99-032 (Japanese)
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, version 2.1, August 1999, CCIMB-99-033 (Japanese)

1.2. ST Overview

This ST describes *7222/7322/7228/7235 System Control Software* loaded into *Sitios 7222 series, 7322 series, 7228 series, 7235 series* digital copiers (hereafter, all series together called as *7222/7322/7228/7235 Series*). *7222/7322/7228/7235 System Control Software* is a product of Konica-Minolta Business Technologies, Inc.

7222/7322/7228/7235 System Control Software includes the following functions such as used for copying, printing and faxing: copy, print, fax, scan to FTP, scan to email, scan to PC(SMB), PC-Fax save, i-Fax. The TOE is *7222/7322/7228/7235 System Control Software*. The assets handled by TOE functions are document data.

1.3. CC Conformance Claim

For security function requirements

Part 2 conformant

For security assurance requirements

Part 3 conformant

Evaluation assurance level

EAL 3 conformant

1.4. Reference Materials

- Common Criteria for Information Technology Security Evaluation

  Part 1: Introduction and general model

  August 1999 Version 2.1 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation

  Part 2: Security functional requirements

  August 1999 Version 2.1 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation

  Part 3: Security assurance requirements

  August 1999 Version 2.1 CCIMB-99-033
- Common Criteria CCIMB Interpretations-0210
- Common Criteria Supplement 0210
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part 1, 99/12
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part 2, 99/12
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part 3, 99/12

2. TOE Description

2.1. TOE Type

Digital copier software products containing network functions.

2.2. Terminology

No.	Term	Explanation
1	User BOX	Directory storing document data (see No. 2).
2	Document Data	Data for digitized information such as letters and figures.
3	Paper Documents	Paper-based documents bearing information such as letters and figures.
4	Operation Panel	Touch panel display and operation buttons integrated into 7222/7322/7228/7235 Series cabinet.
5	Internal Network	Network as LAN in organization introducing 7222/7322/7228/7235 Series. Connected to the client PC and each server (Mail server, FTP server, etc.).
6	External Network	Network other than the internal network (See No. 5). Internet, etc.
7	SMB	Application Protocol to be used for communication between PCs on the Network in Microsoft OS.

2.3. TOE Overview

The TOE is *7222/7322/7228/7235 Control Software*. The *7222/7322/7228/7235 Series* loaded with the TOE is a series of digital copiers with network functions, and it offers functions such as copy/print/fax, operation control of the 7222/7322/7228/7235 Series, and maintenance control of the 7222/7322/7228/7235 Series.

Figure 2-1. 7222/7322/7228/7235 Series Operating Environment illustrates a typical office environment using the *7222/7322/7228/7235 Series*.

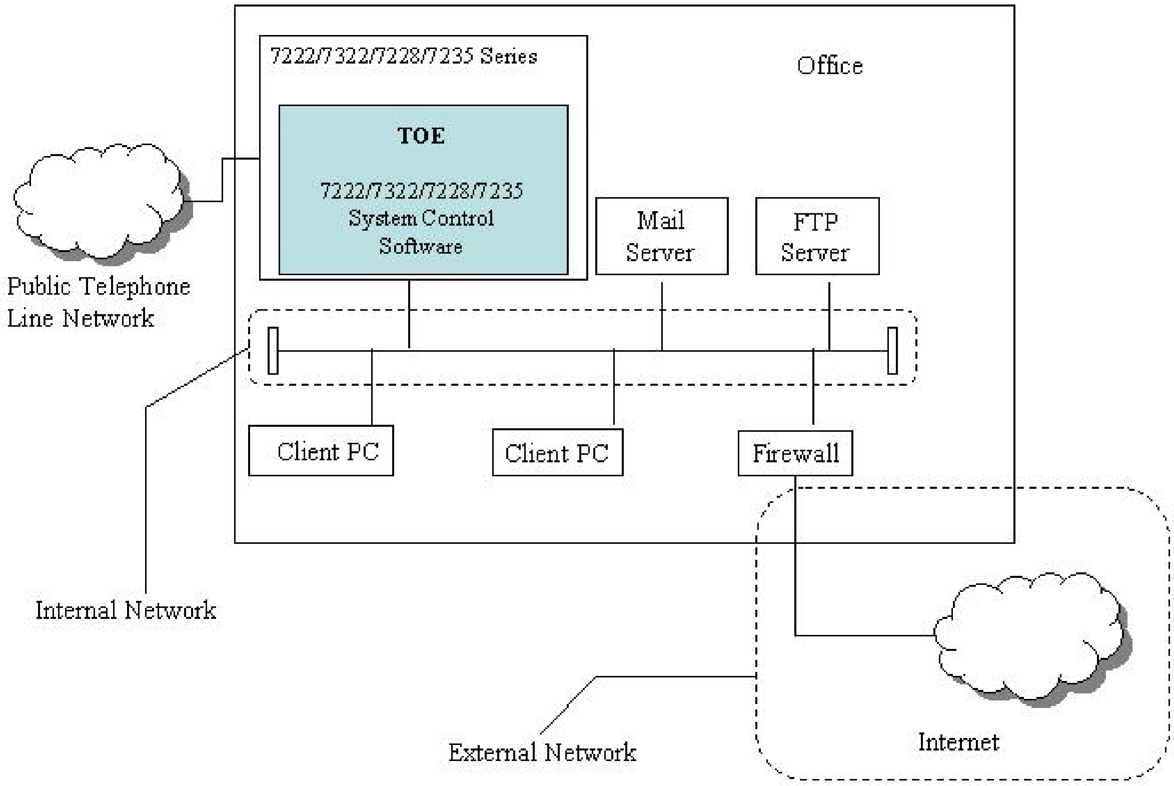

Figure 2-1. 7222/7322/7228/7235 Series Operating Environment

The TOE has functions for sending and receiving document data through internal networks and public telephone line networks. Accordingly, the 7222/7322/7228/7235 Series loaded with the TOE is connected to an internal network and a public telephone line network as shown in **Figure 2-1. 7222/7322/7228/7235 Series Operating Environment**. The internal network connects a mail server and FTP server to allow to send data from general user client PCs or the 7222/7322/7228/7235 Series. The TOE does not have an external network interface. When an external network is connected, it shall be connected through a firewall in order to protect each device in the internal network.

2.4. 7222/7322/7228/7235 Series Participants and Roles

7222/7322/7228/7235 Series participants and roles are described as follows.

- General Users

General users belong to the organization introducing the 7222/7322/7228/7235 Series and utilize the user functions such as copying, printing, and faxing in 7222/7322/7228/7235 Series. By registering with the TOE, general users can own a User Box on the optional HDD of 7222/7322/7228/7235 Series.

- Administrators

Administrators belong to the organization introducing the 7222/7322/7228/7235 Series and perform operational administration management of the 7222/7322/7228/7235 Series. Administrators use operational administration functions provided by the 7222/7322/7228/7235 Series.

- Managers

Managers belong to the organization introducing the 7222/7322/7228/7235 Series and designate administrators.

- CE (Customer Engineers)

CE belong to the company entrusted to maintain the 7222/7322/7228/7235 Series. CE use operational administration functions provided by the 7222/7322/7228/7235 Series. CE makes 7222/7322/7228/7235 Series maintenance contracts with managers and administrators.

- Fax Users

Fax users utilize the fax function connected through the public telephone line network and send document data to the 7222/7322/7228/7235 Series.

General users, administrators and CE are called as product related personnel.

2.5. TOE Structure

Figure 2-2. TOE Structure illustrates the structure of this TOE.

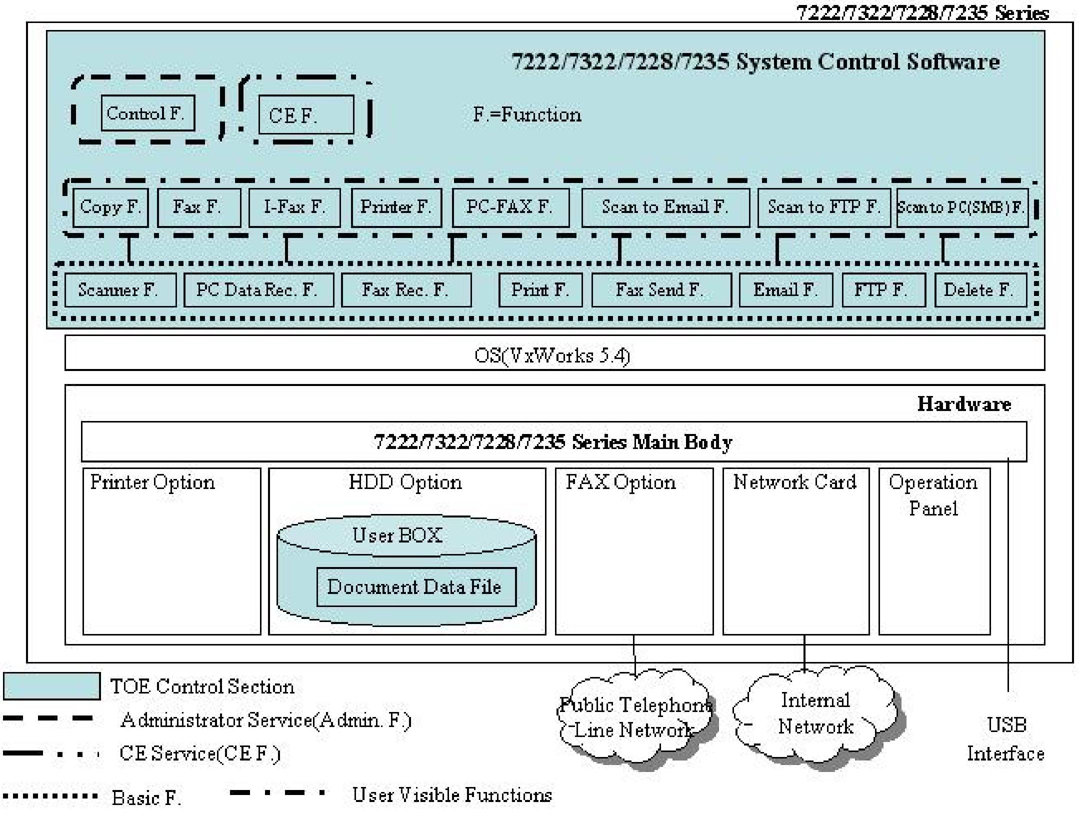

Figure 2-2. TOE Structure

The 7222/7322/7228/7235 Series is built up with hardware, OS, and *7222/7322/7228/7235 System Control Software*. The hardware includes 7222/7322/7228/7235 Series main unit components, a printer option, a HDD option, a fax option, an operations panel, and a network card. The 7222/7322/7228/7235 Series main unit components include a scanner for digitizing paper documents. The USB interface is used for connection to a computer when installing the TOE. The printer option print letters and graphics on printer paper. The HDD option provides a memory storage device. The fax option provides a public telephone line port for connection to a public telephone line network and a modem for converting analog signals to digital signals. VxWorks 5.4 is used as the OS. The 7222/7322/7228/7235 System Control Software operates on the OS (VxWorks 5.4). The OS controls input/output of document data for the hardware and for the 7222/7322/7228/7235 System Control Software.

User Boxes are created on the memory storage of the optional HDD by operation of 7222/7322/7228/7235 System Control Software. Document data files storing document data are in the User Box. Multiple User Boxes can be created on the 7222/7322/7228/7235 Series. The range of TOE control is shown by the shaded area of **Figure 2-2. TOE Structure**.

The 7222/7322/7228/7235 Series receives requests for processing from fax users or CE through a public telephone line network, or from users through the operation panel, or from users through a network. The TOE executes those processing requests.

2.6. 7222/7322/7228/7235 System Control Software Structure

The 7222/7322/7228/7235 System Control Software has the following functions.

2.6.1. Basic Functions

Basic functions are functions that utilize the document data stored in the User Box by a general user or fax user. The User Box is identified by a User Box identifier, and a User Box password is set for each User Box in order to confirm the authenticity of the owner of each User Box. An overview of basic functions is shown in **Figure 2-3. Basic Functions Processing Concepts**.

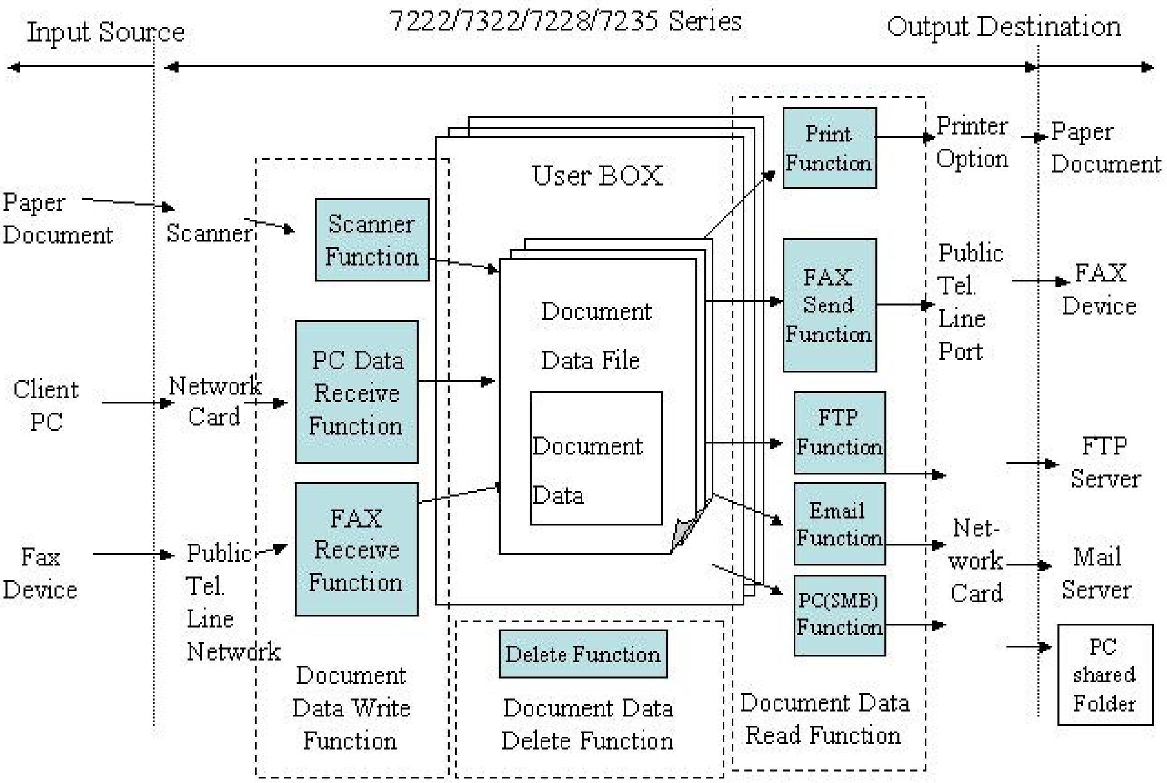

Figure 2-3. Basic Functions Processing Concepts

Basic functions are writing, reading and deleting of document data.

As shown in **Table 2-1. User Viewable Functions and Basic Functions Support**, executions of functions visible to the user are enabled by execution of basic functions. Basic functions will be described as follows.

Table 2-1. User Viewable Functions and Basic Functions Support

No.	Functions Visible to the User	Basic Functions
1	Copy function	Scanner function and printing function
2	Fax function	Scanner function and fax sending function; fax receiving function and printing function
3	i-Fax function	PC data receiving function and email function
4	Printer function	PC data receiving function and printing function
5	PC-Fax function	PC data receiving function and fax sending function
6	Scan to Email function	Scanner function and email function
7	Scan to FTP function	Scanner function and FTP function

8	Scan to PC(SMB) function	Scanner function and PC(SMB) function
9	Document data deleting function	Deleting function

Functions utilizing the User Box illustrated in **Figure 2-3. Basic Functions Processing Concepts** are described below.

2.6.1.1. Document Data Write Function

This function provides a process to write document data additionally in the User Box by following three methods. (It cannot overwrite.)

(1) Scanner Function

A general user enters instructions from the operation panel, then the information of the paper document is read by the scanner and converted to document data, and the document data is saved in the User Box.

(2) PC Data Receive Function

A general user enters instructions from a client PC, and document data is routed through the internal network and saved in the User Box.

(3) Fax Receive Function

A fax user sends a fax, then the document data is received from the fax device connected to the public telephone line network, and the document data is saved in the User Box.

2.6.1.2. Document Data Read Function

This function provides a process to read document data from the User Box by following four methods, while ensuring that the data is protected from output processing by another user. This function can only be used from the operation panel.

(1) Print Function

A general user enters the User Box identifier and User Box password using the operation panel and prints only document data contained in the User Box belonging to the user.

(2) Fax Send Function

A general user enters the User Box identifier and User Box password using the operation panel and sends to a fax device connected to a public telephone line network only document data contained in the User Box belonging to the user.

(3) Email Function

A general user enters the User Box identifier and User Box password using the operation panel, attaches to an email only document data contained in the User Box belonging to the user, and sends the mail to the mail server.

(4) FTP Function

A general user enters the User Box identifier and User Box password using the operation panel and sends to the FTP server only document data contained in the User Box belonging to the user.

(5) PC(SMB) Function

A general user enters the User Box identifier and User Box password using the operation panel and sends to the shared folder in PC only document data contained in the User Box belonging to the user.

2.6.1.3. Document Data Delete Function

A general user enters the User Box identifier and User Box password and is able to delete only the document data contained in the user's own User Box. This function can only be used from the operation panel.

2.6.2. Management Functions

Management functions can be used by administrators, only after identification and authentication have been completed. These functions are available only through the operation panel. Administrators use control functions to set TOE network information and establish operational settings for functions belonging to the TOE. In addition, control functions manage information related to operation of the digital copier, such as creating/modifying/deleting the attributes of User Boxes, printing log(audit) information, initializing the HDD, controlling the number of printed copies, troubleshooting, and checking the shortage of toner.

2.6.3. CE Functions

CE functions can be used by CE for the following functions only after identification and authentication have been completed.

- Service Setting Mode

CE uses the operation panel to utilize service setting mode functions and execute password registration and changes for administrators.

- KRDS

CE uses a computer connected through a public line network to collect information for the purpose of maintaining the hardware, such as number of prints, number of jams, and toner shortage. KRDS also communicates along with the procedures that conform to International Standards Agreement G3 for fax transmission set by CCITTT.30.

- ISW

CE uses a computer connected through USB interface to the 7222/7322/7228/7235 Series to perform operations and establish initial settings for updating the TOE.

2.7. Assets to be protected

Assets to be protected by the TOE are listed below.

- Document data stored in the User Box.

3. TOE Security Environment

3.1. Assumptions

ASM.PLACE TOE Installation Conditions

The TOE is connected to the internal network, and it is installed in a physically protected area and is allowed to be used only by product related personnel.

ASM.PHYSICAL Chassis Protection

The HDD storing the document data cannot be removed by anyone other than CE.

ASM.NET Internal Network Installation Conditions

The TOE is connected to an internal network that does not cause any disclosure of document data.

ASM.ADMIN Trustworthy Administrators

Administrators are personnel with sufficient skill and trustworthiness for controlling the TOE, and they do not engage in inappropriate actions.

ASM.CE CE Conditions

CE does not engage in inappropriate actions.

ASM.USR Management of General Users

Administrators control and encourage general users to keep in proper operation from the security viewpoint.

ASM.SECMODE Security Functions Execution

Administrators always keep the security functions in operation.

3.2. Threats

T.ACCESS Inappropriate Access

There is a threat for a general user to delete or disclose the document data in a User Box belonging to another general user through operations from the operational panel.

3.3. Organization Security Policies

OSP.MANAGE Availability of TOE

Developer of TOE offers the TOE to users through CE of the retailer.

OSP.RIP Handling of Used Document Data

The TOE makes it impossible to reuse the document data when they are once deleted and unnecessary any more.

4. Security Objectives

4.1. Security Objectives of the TOE

O.IA Identification and Authentication at Use

The TOE identifies and authenticates administrators, CE and general users possessing their own User Box, who try to access to the TOE.

O.MANAGE Availability of Administrative Functions

The TOE offers functions that allow administrators to control User Boxes.

O.CE Availability of CE Functions

The TOE offers functions that allow CE to make administrative functions available to administrators.

O.DATAACCESS Document Data Access Restrictions

The TOE permits reading and deleting of document data within a User Box only by the general user who own the User Box.

O.AUDIT Recording of Log(Audit)

The TOE records the events related to access for assets to be protected as log(audit) data. In addition, referring to the log(audit) is limited to administrators.

O.RIP Handling of Deleted Data

The TOE offers automatic functions to make the document data unable to reuse when it is once deleted.

4.2. Security Objectives for the Environment

OE.TIME Availability of Time

The OS offers “correct time information” to the TOE.

OE.PLACE Installation Location Management

Administrators connect the TOE to the internal network and locate it in an area that is physically protected and allowed to be used only by product related personnel.

OE.NET Network Control

Administrators use equipment that performs internal network communications securely and construct a network environment that does not disclose document data.

OE.SECMODE Security Functions Control

Administrators activate all TOE security functions.

OE.USR Training of General User

Administrators provide education and awareness for general users in order to maintain the TOE in a secure condition.

- General users keep User Box identifiers and User Box passwords in secret.

OE.ADMIN Administrator Conditions

Managers should select and manage administrators who have sufficient skills and trustworthiness.

OE.PHYSICAL Physical Control

The HDD storing document data is physically protected by a structure that makes no one but CE it possible to remove HDD.

OE.CE CE Authentication

Managers and administrators make a maintenance contract with CE. The maintenance contract clearly describes principles prohibiting inappropriate actions.

5. IT Security Requirements

5.1. TOE Security Requirements

5.1.1. TOE Security Function Requirements

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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.

Details: “Users” → Administrators, CE, and general users possessing a User Box

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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.

Details: “Users” → Administrators, CE, and general users possessing a User Box

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1

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

[assignment: list of feedback]

- Password letters entered by operator are shown as multiple dummy characters (*)

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [assignment: number] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

[assignment: list of authentication events]

- Number of unsuccessful attempts for administrators, CE, and general users possessing a User Box

[assignment: number]

- 1 time

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions].

[assignment: list of actions]

- Next authentication attempt cannot be made until 5 seconds elapses for administrators, CE, and general users possessing a User Box that have had an unsuccessful authentication attempt.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

[assignment: a defined quality metric]

- Define the password quality standard as follows.

  Password length: 8 characters exactly

  Character types: English upper case letters, English lower case letters, numerals

  Permission conditions: Password cannot be identical to password used before first password is set; password cannot be composed of identical characters

Details: “Secrets” → “Administrator Passwords,” “CE Passwords,” and “User Box Passwords”

Dependencies: No dependencies

FIA_ACC.1[1] Subset access control

Hierarchical to: No other components.

FIA_ACC.1.1

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

[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

- Subjects: User receiving function 1: Process for receiving requests to access the User Box of a general user who possesses a User Box.
- Objects: User Box
- Operations:

  1. Reads document data in User Box
  2. Deletes document data in User Box

[assignment: access control SFP]

- Access Control Policy 1

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1[2]Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

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

- Subjects: User receiving function 2: Process for receiving requests to access the User Box of an administrator.
- Objects: User Box
- Operations:

  1. Reads document data in User Box
  2. Deletes document data in User Box

[assignment: access control SFP]

- Access Control Policy 2

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1[1] Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [assignment: access control SFP] to objects based on [assignment: security attributes, named groups of security attributes].

[assignment: security attributes, named groups of security attributes]

- Security properties: User Box identifier
- Named security properties group: None

[assignment: access control SFP]

- Access Control Policy 1

FDP_ACF.1.2

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

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

Permits reading or deleting of all document data within a User Box specified by the following procedure.

- The User Box identifier associated with user receiving function 1 matches the User Box identifier associated with the User Box.

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

- None

FDP_ACF.1.4

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

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

- None

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1[2] Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [assignment: access control SFP] to objects based on [assignment: security attributes, named groups of security attributes].

[assignment: security attributes, named groups of security attributes]

- Security properties: User Box identifier
- Named security properties group: None

[assignment: access control SFP]

- Access Control Policy 2

FDP_ACF.1.2

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

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

Executes one of the following:

- Permits creating of a User Box associated with the User Box identifier when the User Box identifier associated with user receiving function 2 is not registered.
- Permits deleting of a User Box associated with the User Box identifier when the User Box identifier associated with user receiving function 2 is registered.

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

- None

FDP_ACF.1.4

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

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

- None

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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]

- Delete allotted resources from

[assignment: list of objects]

- User Box

Dependencies: No dependencies

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

(a) Start-up and shutdown of the audit functions;

(b) All auditable events for the [selection: minimum, basic, detailed, not specified] level of audit; and

(c) [assignment: other specifically defined auditable events].

[selection: minimum, basic, detailed, not specified]

- Not defined

[assignment: other specifically defined auditable events]

- Audit events are recorded in **Table 5-1.**

Table 5-1. Events That Become Audit Targets

Function Component	Audit(Log) Data
FIA_UID.2	Successful or unsuccessful identification at time of identifying administrators, CE, and general users possessing User Boxes.
FIA_UAU.2	Successful or unsuccessful authentication at time of authenticating administrators, CE, and general users possessing User Boxes.
FIA_AFL.1	Unsuccessful authentications reaching threshold for administrators, CE, and general users possessing User Boxes.
FIA_SOS.1	Denial or acceptance of authentication data at time of registration or modification for acceptable values of authentication data.
FDP_ACF.1	Successful or unsuccessful request at execution of operations for object.
FMT_SMF.1	Use of control functions (FIA_UID.2, FIA_UAU.2, FMT_MTD.1, MFT_MSA.1, FMT_MSA.3, FMT_SMR.1)

FAU_GEN.1.2

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

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

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

[assignment: other audit relevant information]

- None

Dependencies: FPT_STM.1 Reliable time stamps

FAU_STG.1 Protected audit trial storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to [selection: prevent, detect] modifications to the audit records.

[selection: prevent, detect]

- Prevent

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1

The TSF shall [selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records'] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

[selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records']

- Write to stored audit records at maximum speed

[assignment: other actions to be taken in case of audit storage failure]

- None

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.

[assignment: authorized users]

- Administrators

[assignment: list of audit information]

- Audit data shown in Table 5.1 Events That Become Audit Targets regulated by FAU_GEN.1.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

FMT_MTD.1[1] Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[assignment: list of TSF data]

- Administrator password

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

- Change, Other operation

[assignment: other operations]

- Register

[assignment: the authorized identified roles]

- CE

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MTD.1[2] Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[assignment: list of TSF data]

- CE password

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

- Change

[assignment: other operations]

- None

[assignment: the authorized identified roles]

- CE

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MTD.1[3] Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[assignment: list of TSF data]

- User Box password

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

- Change

[assignment: other operations]

- None

[assignment: the authorized identified roles]

- Administrator

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MTD.1[4] Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[assignment: list of TSF data]

- User Box password

[selection: change default, query, modify, delete, clear, [assignment: other operations]] Other operation

[assignment: other operations]

- Change only the User Box password of the general user who possesses the User Box.

[assignment: the authorized identified roles]

- General user who possesses the User Box

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

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

[assignment: list of security attributes]

- User Box identifier

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

- Delete
- Other operation

[assignment: other operations]

- Register

[assignment: the authorized identified roles]

- Administrator

[assignment: access control SFP, information flow control SFP]

- Access Control Policy 2

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection: restrictive, permissive, other property] default values for security attributes that are used to enforce the SFP.

[selection: restrictive, permissive, other property]

- Restrictive

[assignment: access control SFP, information flow control SFP]

- Access Control Policy 2

Details: “Security Attributes” → “User Box Identifier”

FMT_MSA.3.2

The TSF shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

[assignment: the authorized identified roles]

- Administrators

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [assignment: the authorized identified roles].

[assignment: the authorized identified roles]

- Administrators
- CE
- General users possessing a User Box

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

[assignment: list of functions]

- Security Intensification function: Function enabling all security functions

[selection: determine the behaviour of, disable, enable, modify the behaviour of]

- Allow operation

[assignment: the authorized identified roles]

- Administrators

Dependence: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_SMF.1 Specification of management functions

The TSF 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]

- Shown in **Table 5-2. List of Security Management Functions.**

Table 5-2. List of Security Management Functions

Function Requirement Components	**Management Items**	**Management Item**
FIA_UID.2	Management of user identification data	User Box identifier
FIA_UAU.2	Management of authentication data by related user	Administrator password CE password User Box password
	Management of authentication data by user related to this data	Administrator password CE password User Box password
FIA_UAU.7	None	
FIA_SOS.1	Management of measure used for verification of password	No management item because measure used for password verification cannot be modified
FIA_AFL.1	Management of threshold for unsuccessful authentication attempts	No management item because threshold is fixed and cannot be modified
	Management of actions available at authentication failure event	No management item because actions are fixed and cannot be modified
FDP_ACC.1[1]	None	
FDP_ACC.1[2]	None	

Function Requirement Components	**Management Items**	**Management Item**
FDP_ACF.1[1]	Management of properties used in decision based on explicit access or denial	User Box identifier
FDP_ACF.1[2]	Management of properties used in decision based on explicit access or denial	User Box identifier
FDP_RIP.1	Selection of time when to protect the remaining data (specifically, for allotment or cancellation of allotment) is available by setting in TOE	No management item because protection of remaining data is always executed
FAU_GEN.1	None	
FAU_STG.1	None	
FAU_STG.4	Preservation of actions executed at log data storage failure	No management item because actions executed at log storage failure cannot be modified
FAU_SAR.1	Preservation of user groups having reading privileges for log records(deleting, modifying, adding)	No management item because only administrators possess reading privileges for log records and this cannot be modified
FAU_SAR.2	None	
FMT_MTD.1[1]	Management of groups which give reciprocally influence with TSF data	CE password
FMT_MTD.1[2]	Management of groups which give reciprocally influence with TSF data	CE password
FMT_MTD.1[3]	Management of groups which give reciprocally influence with TSF data	Administrator password
FMT_MTD.1[4]	Management of groups which give reciprocally influence with TSF data	User Box password

Function Requirement Components	**Management Items**	**Management Item**
FMT_MSA.1	Management of groups which give reciprocally influence with security properties	Administrator password
FMT_MSA.3	Management of groups which specify the initial set data	Administrator password
	Management of permission and restriction for default value settings of prescribed access control SFP	No management item because default values are fixed
FMT_SMR.1	Management of user groups which is a part of roles	CE password Administrator password User Box password
FPT_SEP.1	None	
FMT_MOF.1	Management of groups which give reciprocally influence with TSF function	Administrator password
FMT_SMF.1	None	
FMT_RVM.1	None	

Dependencies: No Dependencies

FPT_RVM.1 Non-bypass ability 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

FPT_SEP.1 TSP domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.2. TOE Security Assurance Requirements

This TOE emphasizes quality assurance level EAL3, a sufficient level for commercial products.

TOE security assurance requirements corresponding to EAL3 are shown in **Table 5-3. TOE Security Assurance Requirements List**.

Table 5-3. TOE Security Assurance Requirements List

Security Class	Security Requirement
Structure Management	ACM_CAP.3 CM capabilities
	ACM_SCP.1 CM scope
Delivery and Implementation	ADO_DEL.1 Delivery
	ADO_IGS.1 Installation, Generation and Startup
Development	ADV_FSP.1 Functions Specification
	ADV_HLD.2 High Level Design
	ADV_RCR.1 Representation Correspondence
Guidance Documents	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Life Cycle Support	ALC_DVS.1 Development Security
Test	ATE_COV.2 Coverage
	ATE_DPT.1 Depth
	ATE_FUN.1 Functional Tests
	ATE_IND.2 Independent Testing
Fragility Assessment	AVA_MSU.1 Misuse
	AVA_SOF.1 Strength of TOE Security Functions
	AVA_VLA.1 Vulnerability Analysis

5.2. Security Requirements for the IT Environment

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

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

Details: “TSF” → “OS”

Dependencies: No dependencies

5.3. Security Strength of Function

The object of TOE strength function is the password mechanism, and there are the following two TOE function components in this ST.

FAI_SOS.1 (password verification), FIA_AFL.1 (handling at authentication failure)

Both above mentioned function requirements satisfies SOF-standards. In addition, for TOE minimum function strength, SOF-Basic are satisfied.

6. TOE Summary Specifications

6.1. TOE Security Functions

6.1.1. Identification Authentication

The Identification Authentication function provides the following security functions group.

Function Name	Security Function Specification	TOE Security Function Requirement
IA.ADM_ADD Administrator Registration	IA.ADM_ADD registers administrators for the TOE. Only CE operate IA.ADM_ADD. CE register the passwords of administrators. IA.ADM_ADD provides an interface for administrator registration. The administrator registration interface requests password input for registering administrator. For passwords input by administrators, following rules are used to verify the permitted values. • The password must be 8 characters • The password must be composed of English upper case letters, English lower case letters, and numerals • The password prohibits the values which are identical to the last password to be used • The password prohibits a series of the same characters to be used In verification of permitted values, administrators are registered when the above rules are observed. When the above rules are not observed, registration is denied.	FIA_SOS.1 FMT_MTD.1[1] FMT_SMF.1 FMT_SMR.1 FPT_SEP.1 FPT_RVM.1

Function Name	Security Function Specification	TOE Security Function Requirement
IA.ADM_AUTH Administrator Identification and Authentication	IA.ADM_AUTH identifies that an administrator is registered in the TOE and authenticates that the operator is the administrator before the operator can use the TOE. IA.ADM_AUTH does not permit any operation of administrator functions before identification and authentication of the administrator. The interface for administrator identification and authentication requests input of the password registered by IA.ADM_ADD or modified by IA_PASS. IA.ADM_AUTH identifies administrators through the interface display for administrator identification and authentication, and it authenticates the administrator by the input password. When the administrator inputs the password, dummy characters (*) are shown in place of the input password. When authentication is unsuccessful, the interface for administrator identification and authentication is displayed after 5 seconds.	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_SEP.1 FPT_RVM.1
IA.CE_AUTH CE Identification and Authentication	IA.CE_AUTH identifies that a CE is registered in the TOE and authenticates that the operator is the CE before the operator can use the TOE. IA.CE_AUTH does not permit any operation of CE functions before identification and authentication of the CE. It requests input of the password modified by IA_PASS. IA.CE_AUTH identifies CE through the interface display for CE identification and authentication, and it authenticates the CE by the input password. When the CE inputs the password, dummy characters (*) are shown in place of the input password. When authentication is unsuccessful, the interface for CE identification and authentication is displayed after 5 seconds.	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_SEP.1 FPT_RVM.1

Function Name	Security Function Specification	TOE Security Function Requirement
IA.PASS Password Modification	IA.PASS modifies an administrator password, CE password or User Box password that is the authentication data for the administrator, CE or general user possessing a User Box. IA.PASS presents an interface for password modification and requests input of a new password. Password modification is available depending on the user as follows. CE: CE passwords, administrator passwords Administrator: User Box passwords General user possessing a User Box: The User Box password for user's own User Box. For the password input by product related personnel, acceptable values are verified according to the following rules. • The password must be 8 characters • The password must be formed with English upper case letters, English lower case letters, or numerals • The password prohibits values which are identical to the last password to be used • The password prohibits a series of the same characters to be used In verification of permitted values, password is modified when the above rules are observed.	FIA_SOS.1 FMT_MTD.1[1] FMT_MTD.1[2] FMT_MTD.1[3] FMT_MTD.1[4] FMT_SMF.1 FMT_SMR.1 FPT_SEP.1 FPT_RVM.1

6.1.2. Access Control

The Access Control function provide the following security functions group.

Function Name	Security Function Specification	TOE Security Function Requirement
ACL.USR General User Access Rules and Control	ACL.USR identifies and authenticates a general user possessing a User Box, and controls the available range of operations for a general user by the following access rules after the general user is authenticated. ACL.USR identifies and authenticates the general user possessing a User Box based on the User Box password and User Box identifier. Dummy characters (*) are displayed for the entered User Box password when the User Box password is input. After authentication, the following operations are permitted to the document data in the User Box identified by the authenticated User Box identifier. • Reading and printing of document data • Reading and sending of document data to fax device • Reading and sending of document data to FTP server • Reading and sending of document data to mail server • Reading and sending of document data to shared PC folder • Deleting of document data Regarding deletion of document data in a User Box, RD.TEMP is read and the document data is deleted. When identification and authentication are unsuccessful, the identification and authentication interface is made effective after 5 seconds.	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FIA_ACC.1[1] FIA_ACF.1[1] FPT_SEP.1 FPT_RVM.1

6.1.3. Remaining Data Protection

The Remaining Data Protection function provides the following security functions group.

Function Name	Security Function Specification	TOE Security Function Requirement
RD.TEMP Remaining Data Protection	RD.TEMP always executes after deletion of TOE document data, and it overwrites the document data stored area on HDD with meaningless characters.	FDP_RIP.1 FPT_SEP.1 FPT_RVM.1

6.1.4. Log(Audit)

The Log function provides the following security functions group.

Function Name	Security Function Specification	TOE Security Function Requirement
AUD.LOG Log Data Recording	Records log data for the operations of security functions. Events that become log data are shown below. • Start and end of log functions • Successful and unsuccessful identification authentications for administrators, CE, and general users possessing User Boxes • Successful and unsuccessful password registration occurrences for administrators and general users possessing User Boxes • Successful and unsuccessful password modification occurrences for administrators, CE, and general users possessing User Boxes • Successful document data readings • Successful document data deletions	FAU_GEN.1 FPT_SEP.1 FPT_RVM.1
AUD.MNG Log Area Management	AUD.MNG manages the log storage area for creation and saving of log data. The area storing log data is memory area with a ring buffer format. AUD.MNG overwrites log data starting from the head of the log storage area again when the storage area of log data is exhausted.	FAU_STG.4 FPT_SEP.1 FPT_RVM.1

6.1.5. Control Support

The Control Support function provides the following security functions group.

Function Name	**Security Function Specification**	**TOE Security Function Requirement**
MNG.MODE Security Intensification Mode Setting	MNG.MODE permits and executes only for administrators the function (Security Intensification function) that makes all TOE security functions in effect.	FMT_MOF.1 FPT_SEP.1 FPT_RVM.1
MNG.ADM Control Support Function (Administrator)	MNG.ADM permits and executes only for administrators the following processing. • Creation of User Box, registration of User Box identifier, and setting of User Box password • Deletion of User Box identifier, complete elimination of document data in User Box and deletion of User Boxes by RD.TEMP (Deletion of all User Box identifiers, elimination of all document data for all User Boxes and deletion of all User Boxes by RD.TEMP are the initialization of HDD.) • Log data query (not an log data deletion function) For the Use Box password input by administrator, acceptable values are verified according to the following rules. • The password must be 8 characters • The password must be formed with English upper case letters, English lower case letters, or numerals • The password prohibits values which are identical to the last password to be used • The password prohibits a series of the same characters to be used Regarding verification of permitted values, administrators are registered when the above rules are observed. When the above rules are not observed,	FDP_ACC.1[2] FDP_ACF.1[2] FIA_SOS.1 FMT.MAS.1, FMT_MAS.3, FAU_STG.1 FAU_SAR.2 FAU_SAR.1 FMT_SMF.1 FMT_SMR.1 FPT_SEP.1 FPT_RVM.1

Function Name	Security Function Specification	TOE Security Function Requirement
	registration is denied. Log data queries are shown in a format that administrators can refer to, and they include event generation data and time (year, month, day, hour, minute, second), operation subject identification data, and event result data.	

6.2. Security Strength of Function

This TOE satisfies SOF-standards security functions strength for the password mechanism. The password mechanism is comprised of Identification Authentication functions (IA.ADM_ADD and IA.PASS) and the Administrative Support function (MNG.ADM).

6.3. Assurance Measures

The developer develops according to the security assurance requirements and the development contract regulated by the developer organization. Related documents for security requirements and components of security assurance requirements that meet EAL3 are shown in **Table 6-1. EAL3 Assurance Requirements and Related Documents**.

Table 6-1. EAL3 Assurance Requirements and Related Documents

Security Requirement Item	Component	Related Document
Configuration Management	ACM_CAP.3	7222/7322/7228/7235 Configuration Management Plan 7222/7322/7228/7235 Design Documents List 7222/7322/7228/7235 Source Code List
	ACM_SCP.1	7222/7322/7228/7235 Configuration Management Plan 7222/7322/7228/7235 Design Documents List 7222/7322/7228/7235 Source Code List

Security Requirement Item	Component	Related Document
Delivery and operation	ADO_DEL.1	7222/7322/7228/7235 Delivery Regulations Manual 7222/7322/7228/7235 User’s Guide: Copy (Japanese) 7222/7322/7228/7235 User’s Guide: Network/Scanner (Japanese) 7222/7322/7228/7235 User’s Guide: Security (Japanese) 7222/7322/7228/7235 User’s Guide: Document Folder (Japanese) 7145/7222/7322/7228/7235 Service Manual: Field Service (Japanese) 7222/7228/7235 User’s Guide Copier 7222/7228/7235 User’s Guide Network Setup and Scanner Operations 7222/7228/7235 User’s Guide Security 7222/7228/7235 User’s Guide Document Folder Operations 7145/7222/7228/7235 Service Manual Field Service

Security Requirement Item	Component	Related Document
	ADO_IGS.1	7222/7322/7228/7235 Installation/Operation Regulations Manual 7222/7322/7228/7235 User’s Guide: Copy (Japanese) 7222/7322/7228/7235 User’s Guide: Network/Scanner (Japanese) 7222/7322/7228/7235 User’s Guide: Security (Japanese) 7222/7322/7228/7235 User’s Guide: Document Folder (Japanese) 7145/7222/7322/7228/7235 Service Manual: Field Service (Japanese) 7222/7322/7228/7235 Installation Manual (Japanese) 7222/7228/7235 User’s Guide Copier 7222/7228/7235 User’s Guide Network Setup and Scanner Operations 7222/7228/7235 User’s Guide Security 7222/7228/7235 User’s Guide Document Folder Operations 7145/7222/7228/7235 Service Manual Field Service 7222/7322/7228/7235 Installation Manual
Development	ASV_FSP.1	7222/7322/7228/7235 Security Function Specifications
	ADV_HLD.2	7222/7322/7228/7235 Security Function Specifications
	ADV_RCR.1	7222/7322/7228/7235 Function correspondence analysis

Security Requirement Item	**Component**	**Related Document**
Guidance Documents	AGD_ADM.1	7222/7322/7228/7235 User’s Guide: Copy (Japanese) 7222/7322/7228/7235 User’s Guide: Network/Scanner (Japanese) 7222/7322/7228/7235 User’s Guide: Security (Japanese) 7222/7322/7228/7235 User’s Guide: Document Folder (Japanese) 7145/7222/7322/7228/7235 Service Manual: Field Service (Japanese) 7222/7228/7235 User’s Guide Copier 7222/7228/7235 User’s Guide Network Setup and Scanner Operations 7222/7228/7235 User’s Guide Security 7222/7228/7235 User’s Guide Document Folder Operations 7145/7222/7228/7235 Service Manual Field Service
	AGD_USR.1	7222/7322/7228/7235 User’s Guide: Copy (Japanese) 7222/7322/7228/7235 User’s Guide: Network/Scanner (Japanese) 7222/7322/7228/7235 User’s Guide: Security (Japanese) 7222/7322/7228/7235 User’s Guide: Document Folder (Japanese) 7222/7228/7235 User’s Guide Copier 7222/7228/7235 User’s Guide Network Setup and Scanner Operations 7222/7228/7235 User’s Guide Security 7222/7228/7235 User’s Guide Document Folder Operations
Life Cycle Support	ALC_DVS.1	7222/7322/7228/7235 Development security instructions
Test	ATE_COV.2	7222/7322/7228/7235 Test specification and results report

Security Requirement Item	Component	Related Document
	ATE_DPT.1	7222/7322/7228/7235 Depth analysis report
	ATE_FUN.1	7222/7322/7228/7235 Test specification and results report
	ATE_IND.2	None (7222/7322/7228/7235 Test Set)
Fragility Assessment	AVA_MSU.1	7222/7322/7228/7235 User’s Guide: Copy (Japanese) 7222/7322/7228/7235 User’s Guide: Network/Scanner (Japanese) 7222/7322/7228/7235 User’s Guide: Security (Japanese) 7222/7322/7228/7235 User’s Guide: Document Folder (Japanese) 7145/7222/7322/7228/7235 Service Manual: Field Service (Japanese) 7222/7228/7235 User’s Guide Copier 7222/7228/7235 User’s Guide Network Setup and Scanner Operations 7222/7228/7235 User’s Guide Security 7222/7228/7235 User’s Guide Document Folder Operations 7145/7222/7228/7235 Service Manual Field Service
	AVA_SOF.1	7222/7322/7228/7235 Vulnerability analysis report
	AVA_VLA.1	7222/7322/7228/7235 Vulnerability analysis report

7. PP Claims

There is no conformance to a PP in this ST.

8. Rationale

8.1. Security Measure Policies Rationale

Relationships between Security Measure Policies in relation to threats are shown in **Table 8-1. Threats and Required Conditions, and Security Measure Policies Support**.

Table 8-1. Threats and Required Conditions, and Security Measure Policies Support

Threats/Prerequisite Conditions Security Measure Policies	T.ACCESS	ASM.PLACE	ASM.PHYSICAL	ASM.SECMODE	ASM.NET	ASM.ADMIN	ASM.CE	ASM.USR	OSP.MANAGE	OSP.RIP
O.IA (Identification and authentication at use)	X								X	
O.MANAGE (offering of control functions)	X									
O.CE (offering of CE functions)										X
O.DATAACCESS (document data access restrictions)	X									
O.AUDIT (log data recording)	X									
O.RIP (deleted data processing)										X

Threats/Prerequisite Conditions Security Measure Policies	T.ACCESS	ASM.PLACE	ASM.PHYSICAL	ASM.SECMODE	ASM.NET	ASM.ADMIN	ASM.CE	ASM.USR	OSP.MANAGE	OSP.RIP
OE.TIME (time usage)	X									
OE.PLACE (installation location management)		X								
OE.NET (network management)					X					
OE.USR (general user training)								X		
OE.ADMIN (administrator conditions)						X				
OE.CE (CE security)								X		
OE.PHYSICAL (physical management)			X							
OE.SECMODE (security functions management)				X						

The basis for **Table 8-1. Threats and Required Conditions, and Security Measure Policies Support** is given below.

T.ACCESS: Unauthorized Access

The TSF identification authenticates administrators by O.IA. The TSF offers to identified and authenticated administrators a function for controlling User Boxes by O.MANAGE. Administrators decide the owners of User Boxes using this management function. The TSF uses O.DATAACCESS to permit reading and deleting of document data in a User Box only to the authorized general user possessing a User Box who has been authenticated by O.IA.

In addition, because operations related to access functions to document data for *Assets Becoming Security Targets* are recorded as log(audit) data by O.AUDIT and OE.TIME along with exact time, it is effective for detection of unauthorized operation to the User Box document data possessed by another general user.

As explained above, threats to T.ACCESS can be resisted by countermeasure policies of O.IA, O.MANAGE, O.DATAACCESS, and OE.TIME.

ASM.PLACE: TOE Installation Conditions

According to OE.PLACE, the TOE is installed in a space allowing operation only for product related personnel connected to the internal network. TOE access can be restricted to only product related personnel.

As explained above, prerequisite condition ASM.PLACE can be implemented by countermeasure policy OE.PLACE.

ASM.PHYSICAL: Cabinet Protection

With OE.PHYSICAL the HDD is physically protected by a mechanical structure that cannot be removed by anyone other than CE.

As explained above, prerequisite condition ASM.PHYSICAL can be implemented by countermeasure policy OE.PHYSICAL.

ASM.SECMODE: Security Function Execution

With OE.SECMODE, administrator make all TOE security functions effective. Security functions are always operated in this way.

As explained above, prerequisite condition ASM.SECMODE can be implemented by countermeasure policy OE.SECMODE.

ASM.NET: Internal Network Installation Conditions

With OE.NET, administrators setup the TOE in the internal network from where no disclosure of document data happen. This implementation is possible by installing a device that encrypts communications of TOE between the internal network and the TOE.

As explained above, prerequisite condition ASM.NET can be implemented by countermeasure policy

OE.NET.

ASM_ADMIN: Trustworthy Administrators

With OE.ADMIN, administrator conditions are regulated. Managers select individuals of sufficient skill and trustworthiness to be administrators.

As explained above, prerequisite condition ASM.ADMIN can be implemented by countermeasure policy OE.ADMIN.

ASM.CE: Maintenance Contract

With OE.CE, organizations installing the TOE are regulated to make a maintenance contract with mentioning that CE and the organization responsible for TOE maintenance will not perform inappropriate actions.

As explained above, prerequisite condition ASM.CE can be implemented by countermeasure policy OE.CE.

ASM.USR: General User Control

With OE.USR, administrators control and encourage general users to keep in proper operation from the security viewpoint This promotes general users to have the necessary knowledge (dangers of data disclosure on the HDD, and its countermeasure, maintaining of secrecy of User Box identifiers and User Box passwords) and to take actions for protecting security.

As explained above, prerequisite condition ASM.USR can be implemented by countermeasure policy OE.USR.

OSP.MANAGE: CE and Administrator Role Responsibilities

With O.IA, the TSF identifies and authenticates CE. The TSF offers to authenticated identified CE the functions enabling administrator to use control functions by O.CE. This enables usage for administrators.

As explained above, organization security policy OSP.MANAGE can be implemented by countermeasure policy O.IA and O.CE.

OSP.RIP: Used Document Data Handling

With O.RIP, the TSF offers a function that automatically creates a condition wherein document data cannot be reused when it is once deleted. So O.RIP makes it impossible to reuse the document data when they are once deleted and unnecessary any more.

As explained above, organization security policy OSP.RIP can be implemented by countermeasure policy O.RIP.

8.2. Security Requirements Rationale

8.2.1. Rationale for Security Function Requirements

Support for TOE security function requirements related to Security Measure Policies are shown in **Table 8-2. Security Measure Policies and TOE Security Function Requirements Support**.

Table 8-2. Security Measure Policies and TOE Security Function Requirements Support

Security Measure Policies TOE Security Function Requirements		O.IA	O.MANAGE	O.CE	O.DATAACCESS	O.AUDIT	O.RIP	OE.TIME
TOE Security Function Requirements	FIA_UID.2	X						
	FIA_UAU.2	X						
	FIA_UAU.7	X						
	FIA_AFL.1	X						
	FIA_SOS.1	X	X	X				
	FDP_ACC.1[1]				X			
	FDP_ACC.1[2]		X					
	FDP_ACF.1[1]				X			
	FDP_ACF.1[2]		X					
	FDP_RIP.1						X	
	FAU_GEN.1					X		
	FAU_STG.1					X		
	FAU_STG.4					X		
	FAU_SAR.1					X		
	FAU_SAR.2					X		
	FMT_MTD.1[1]			X				
	FMT_MTD.1[2]			X				

Security Measure Policies TOE Security Function Requirements		O.IA	O.MANAGE	O.CE	O.DATAACCESS	O.AUDIT	O.RIP	OE.TIME
	FMT_MTD.1[3]		X					
	FMT_MTD.1[4]	X						
	FMT_MSA.1		X					
	FMT_MSA.3		X					
	FMT_SMR.1	X	X	X	X			
	FPT_SEP.1	X	X	X	X	X	X	
	FMT_MOF.1	X	X	X	X	X	X	
	FPT_RVM.1	X	X	X	X	X	X	
	FMT_SMF.1	X	X	X	X			
Security functions for the IT environment	FPT_STM.1							X

The rationale for **Table 8-2. Security Measure Policies and TOE Security Function Requirements Support** is given below.

O.IA: Identification and Authentication at Use

By identifying CE status using FIA_UID.2, and by authenticating the identity of CE using FIA_UAU.2, it can be confirmed as the operation of an authorized CE.

By identifying administrator status using FIA_UID.2, and by authenticating the identity of administrator using FIA_UAU.2, it can be confirmed as the operation of and authorized administrator.

By identifying status as a general user possessing a User Box using FIA_UID.2, and by authenticating the identity of general user possessing a User Box using FIA_UAU.2, it can be confirmed as the operation of an authorized general user possessing a User Box.

When authentication is unsuccessful for administrator, CE, or general user possessing a User Box, the next authentication attempt is delayed by 5 seconds using FIA_AFL.1 for administrator, CE, or general user possessing a User Box, and time interval is increased for successful authentication of the authorized user for the CE, administrator, or the general user possessing a User Box. To conceal the password, dummy characters (*) are entered and shown in the password field by FIA_UAU.7.

Modification of a password for a User Box possessed by a general user is permitted by FMT_MTD.1[4] for authenticated general user possessing a User Box. By modifying a password, the possibility for coinciding with a User Box password entered by an unauthenticated user is decreased.

When a User Box password is modified, the User Box password is verified according to password rules set by FIA_SOS.1, so the modifications of the User Box password to be easily disclosed is suppressed.

Management of passwords is specified with FMT_SMF.1. Administrators, CE, and general users possessing a User Box are preserved with FMT_SMR.1. These functions are neither bypassed with FPT_RVM.1 nor falsified by using FMT_SEP.1, and become effective operations by FMT_MOF.1.

By combining these functional requirements, this security objective O.IA is realized.

O.MANAGE: Offering of Administrator Functions

Administrators are authenticated by using O.IA. User Boxes are created by administrators with registering User Box identifiers by using FDP_ACC.1[2], FDP_ACF.1[2], FMT_MSA.3 and FMT_MSA.1. Initially, the use of User Box is not permitted to anyone, because of the condition in which a User Box password is not available to anyone, but by modifying the User Box password using FMT_MTD.1[3], it can be available. Subsequently, the general user becomes the owner of that User Box by knowing the User Box identifier of the User Box. In addition, when registering a User Box password, conforming to the password rules set by FIA_SOS.1 is verified, and registration of User Box passwords to be easily disclosed is suppressed. Furthermore, User Box together with stored document data can be deleted by administrator’s deletion of the User Box identifier using FDP_ACC.1[2], FDP_ACF.1[2], and FDP_MSA.1.

Management of User Box identifiers and User Box passwords is specified with FMT_SMF.1. Administrators, CE, and general user possessing target User Boxes are preserved with FMT_SMR.1. These functions are neither bypassed with FPT_RVM.1 nor falsified by using FMT_MOF.1, and become effective operations by FMT_MOF.1.

By combining these functional requirements, this security objective O.MANAGE is realized.

O.CE: Offering of CE Functions

CE can register administrator passwords by using FMT_MTD.1[1]. Administrators are registered in the TOE by registering the administrator passwords, and are allowed to begin the operations as administrators. In addition, because CE can modify a CE’s own password by using FMT_MTD.1[2], CE can modify CE and administrator passwords at appropriate intervals. By modifying a password, the possibility for coinciding with CE or administrator password entered by a general user is decreased..

Management of User Box identifiers and User Box passwords is specified with FMT_SMF.1. Administrators and CE are preserved with FMT_SMR.1. These functions are neither bypassed with

FPT_RVM.1 nor falsified by using FMT_MOF.1, and become effective operations by FMT_MOF.1.

By combining these functional requirements, this security objective O.CE is realized.

O.DATAACCESS: Document Data Access Restrictions

General users possessing a target User Box can be authenticated by O.IA. Moreover, FDP_ACC.1[1] and FDP_ACF.1[1] can be used to control access to a User Box. O.DATAACCESS permits reception function (subject) of user to perform functions of reading and deleting operations of document data in a User Box possessed by an authorized general user. As described above, only the general user possessing the User Box can operate the document data within the User Box.

The general user possessing a target User Box is preserved using FMT_SMR.1. These functions are neither bypassed with FPT_RVM.1 nor falsified by using FMT_MOF.1, and become effective operations by FMT_MOF.1.

By combining these functional requirements, this security objective O.DATAACCESS is realized.

O.AUDIT: Log(Audit) Data Recording

Necessary log data is recorded by FAU_GEN.1. The log storage area is protected by FAU_STG.1, and when the log storage area is exhausted, overwriting of log recordings for the old log area is executed by FAU_STG.4. Log data collection is neither bypassed with FPT_RVM.1 nor falsified by using FMT_SEP.1, and become effective operations by FMT_MOF.1 . As described above, required log data is collected and safely protected.

Log data reading by those other than administrators is prohibited by FAU_SAR.2. Offering of log data as a referable format is executed by FAU_SAR.1. As described above, auditing of log data is possible.

By combining these functional requirements, this security objective O.AUDIT is realized.

O.RIP: Deleted Data Processing

When document data is deleted, it is possible to make a condition in which automatically erased data cannot be reused by using FDP.RIP.1 to delete the area of the HDD storing the document data. These functions are neither bypassed with FPT_RVM.1 nor falsified by using FMT_MOF.1, and become effective operations by FMT_MOF.1.

By combining these functional requirements, this security objective OE.RIP is realized.

OE.TIME: Time Usage

This countermeasure policy establishes that time data used by the TOE is controlled by the OS, and so rationale is based on the following.

The OS is implemented the time stamp function and it is offered to the TOE by FPT_STM.1.

By combining these functional requirements, this security objective OE.TIME is realized.

8.2.2. Dependent Relationships Between TOE Security Function Requirements

Dependent relationships between TOE security function requirements are shown in **Table 8-3.**

Dependent Relationships Between TOE Security Function Requirements, and they fulfill all the required dependent relationships.

Table 8-3. Dependent Relationships Between TOE Security Function Requirements

No.	TOE Security Function Requirements	Low Level	Dependent Relationship	Ref. No.	Note
1	FIA_UID.2	FIA_UID.1	None		
2	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	None	Mediation action of FIA_UID.1 is not needed, so FIA_UID.2 is used.
3	FIA_UAU.7	None	FIA_UAU.1	None	Mediation action of FIA_UAU.1 is not needed, so FIA_UAU.2 is used.
4	FIA_AFL.1	None	FIA_UAU.1	None	Mediation action of FIA_UAU.1 is not needed, so FIA_UAU.2 is used.
5	FIA_SOS.1	None	None		
6	FDP_ACC.1[1]	None	FDP_ACF.1	8	
7	FDP_ACC.1[2]	None	FDP_ACF.1	9	
8	FDP_ACF.1	None	FDP_ACC.1 FMT_MSA.3	6 None	Regarding to FMT_MSA.3, is fulfilled by dependent relationship of FDP_ACF.1[2] which is access control for identical objects.
9	FDP_ACF.1[2]	None	FDP_ACC.1 FMT_MSA.3	7 21	
10	FDP_RIP.1	None	None		
11	FAU_GEN.1	None	FPT_STM.1	27	
12	FAU_STG.1	None	FAU_GEN.1	11	

No.	TOE Security Function Requirements	Low Level	Dependent Relationship	Ref. No.	Note
13	FAU_STG.4	FAU_STG.3	FAU_STG.1	12	
14	FAU_SAR.1	None	FAU_GEN.1	11	
15	FAU_SAR.2	None	FAU_SAR.1	14	
16	FMT_MTD.1[1]	None	FMT_SMR.1 FMT_SMF.1	24 23	
17	FMT_MTD.1[2]	None	FMT_SMR.1 FMT_SMF.1	24 23	
18	FMT_MTD.1[3]	None	FMT_SMR.1 FMT_SMF.1	24 23	
19	FMT_MTD.1[4]	None	FMT_SMR.1 FMT_SMF.1	24 23	
20	FMT_MSA.1	None	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	6 24 23	
21	FMT_MSA.3	None	FMT_MSA.1 FMT_SMR.1	20 24	
22	FMT_MOF.1	None	FMT_SMR.1 FMT_SMF.1	24 23	
23	FMT_SMF.1	None	None		
24	FMT_SMR.1	None	FIA_UID.1	None	Mediation action of FIA_UAU.1 is not needed, so FIA_UAU.2 is used.
25	FPT_SEP.1	None	None		

No.	TOE Security Function Requirements	Low Level	Dependent Relationship	Ref. No.	Note
26	FPT_RVM.1	None	None		
27	FPT_STM.1	None	None		

8.2.3. Reciprocal Utilization of TOE Security Function Requirements

No.	TOE Security Function Requirement	Function offering safeguard		
		Falsification	Detour	Deactivation
1	FIA_UID.2	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
2	FIA_UAU.2	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
3	FIA_UAU.7	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
4	FIA_AFL.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
5	FIA_SOS.1	FPT_SEP.1	None	FMT_MOF.1
6	FDP_ACC.1[1]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
7	FDP_ACC.1[2]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
8	FDP_ACF.1[1]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
9	FDP_ACF.1[2]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
10	FDP_RIP.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
11	FAU_GEN.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
12	FAU_STG.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
13	FAU_STG.4	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
14	FAU_SAR.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
15	FAU_SAR.2	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
16	FMT_MTD.1[1]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
17	FMT_MTD.1[2]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
18	FMT_MTD.1[3]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
19	FMT_MTD.1[4]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
20	FMT_MSA.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
21	FMT_MSA.3	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
22	FMT_MOF.1	FPT_SEP.1	FPT_RVM.1	
23	FMT_SMF.1	FPT_SEP.1	None	FMT_MOF.1
24	FMT_SMR.1	FPT_SEP.1	None	FMT_MOF.1
25	FPT_SEP.1		None	FMT_MOF.1
26	FPT_RVM.1	FPT_SEP.1		FMT_MOF.1
27	FTP_STM.1	None	None	None

[Detour] FPT_RVM.1

Upon using TOE management functions and CE functions, administrator and CE execute identification authentication (FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1).

User Box document data is accessed by access control (FDP_ACC.1[1][2] and FDP_ACF.1[1][2]).

Document data becomes always unreadable after its use (FDP_RIP.1).

Log data is always collected (FAU_GEN.1, FAU_STG.4).

Reference to log data is possible only for administrators (FAU_SAR.1, FAU_SAR.2, FAU_STG.1).

Operation of each TSF data and security properties are possible only for correspondent users (FAU_SAR.2, FMT_MTD.1[1]~[4], FMT_MSA.1, FMT_MSA.3, FMT_MOF.1).

In order to execute the above items prevents with certainty, detours are prevented by FPT_RVM.1.

[Deactivation] FMT_MOF.1

The prevention of TSF deactivation is realized by activating the Security Intensification Mode by FMT_MOF.1.

[Falsification]

The TOE is made by FPT_SEP.1 so as to suppress the TSF falsification from other unauthorized subjects. Accordingly, The prevention of TSF falsification is realized.

8.2.4. Consistency of Security Functions Strength for Security Measure Policies

This TOE assumes to be operated under the secured conditions from the physical aspect and the human interaction aspect. For this reason, in 5.3 Security Functions Strength, security strength satisfies SOF-Basic which is able to resist sufficiently the attacks from threat agents with low level attack capabilities.

Implementation measures assuring safe operation of the TOE are shown below.

- The TOE uses time data managed by the OS.
- The TOE is installed in a place where only product related personnel can operate it.
- Administrators establish the environment so data cannot be disclosed from the internal network.
- Administrators arrange training and encourage general users to maintain secure TOE condition.
- Administrators manage the TOE not to be attacked physically.
- Managers select individuals of sufficient skill and trustworthiness to be administrators.
- Managers or administrators make a maintenance contract with CE. The maintenance contract clearly defines that CE will not perform inappropriate actions.

The above implementation countermeasures specify the threat agent with the following profile.

Attack Capability: Low Level

To avoid unauthorized operation to the TOE by a threat agent possessing the attack capability listed above, the TOE is implemented the identification authentication function and access control function. In addition, the TOE implements the log(audit) function to monitor operation of the TOE.

The above items provide sufficient resistance to a threat agent possessing the attack capability listed above, thus, the selection of the SOF-Basic as the minimum strength of function is reasonable.

8.2.5. Rationale for Assurance Requirements

This TOE is a product for commercial use and requires developer analysis for function strength and analysis for evident fragility in order to resist threat agents possessing low level attack capability, as the results of considering the specifications of TOE functions and external interfaces, developer test and etc., . And therefore, the selection of EAL3, which provides an adequate assurance level is reasonable.

8.3. Rationale for TOE Summary Specifications

8.3.1. Compatibility of Security Function Requirements for TOE Summary Specifications

Relationships between security function requirements conforming to TOE summary specifications are shown in **Table 8-4. TOE Summary Specifications and Security Function Requirements Support**.

Table 8-4. TOE Summary Specifications and Security Function Requirements Support

TOE Summary Specification TOE Security Function Requirement	IA.ADM/ADD	IA.ADM/AUTH	IA.CE/AUTH	IA.PASS	ACL.USR	RD.TEMP	AUD.LOG	AUD.MNG	MNG.MODE	MNG.ADM
FIA_UID.2		X	X		X					
FIA_UAU.2		X	X		X					
FIA_UAU.7		X	X		X					
FIA_AFL.1		X	X		X					
FIA_SOS.1	X			X						X
FDP_ACC.1[1]					X					
FDP_ACC.1[2]										X
FDP_ACF.1[1]					X					
FDP_ACF.1[2]										X
FDP_RIP.1					X	X				
FAU_GEN.1							X			
FAU_STG.1										X
FAU_STG.4								X		
FAU_SAR.1										X
FAU_SAR.2										X
FMT_MTD.1[1]	X			X						
FMT_MTD.1[2]				X						
FMT_MTD.1[3]				X						
FMT_MTD.1[4]				X						

TOE Summary Specification / TOE Security Function Requirement	IA.ADM/ADD	IA.ADM/AUTH	IA.CE/AUTH	IA.PASS	ACL.USR	RD.TEMP	AUD.LOG	AUD.MNG	MNG.MODE	MNG.ADM
FMT_MSA.1										X
FMT_MSA.3										X
FMT_MOF.1									X	
FMT_SMF.1	X			X						X
FMT_SMR.1	X			X						X
FPT_SEP.1	X	X	X	X	X	X	X	X	X	X
FPT_RVM.1	X	X	X	X	X	X	X	X	X	X

The rationale for **Table 8-4. TOE Summary Specifications and Security Function Requirements Support** is given below.

FIA_UID.2

IA.ADM_AUTH identifies administrators. IA.CE _AUTH identifies CE. ACL.USR identifies general users possessing User Boxes.

As described above, FIA_UID.2 can be realized by implementing IA.ADM_AUTH, IA.CE_AUTH and ACL.USR.

FIA_UAU.2

IA.ADM_AUTH identifies administrators. IA.CE _AUTH identifies CE. ACL.USR identifies general users possessing User Boxes.

As described above, FIA_UAU.2 can be realized by implementing IA.ADM_AUTH, IA.CE_AUTH and ACL.USR.

FIA_UAU.7

Input characters are displayed by dummy characters (*) by using IA.ADM_AUTH at password entry for administrator authentication, by using IA.CE_AUTH at password entry for CE authentication, and by using ACL.USR at password entry for general users possessing User Boxes.

As described above, FIA_UAU.7 can be realized by implementing IA.ADM_AUTH, IA.CE_AUTH and ACL.USR.

FIA_SOS.1

Input passwords are verified in the permitted range, based on password rules, by using IA.ADM_ADD for administrator password registration, by using MNG.ADM for User Box password registration, by using IA.PASS for administrator, CE, and User Box passwords modification.

As described above, FIA_SOS.1 can be realized by implementing IA.ADM_ADD, MNG.ADM and IA.PASS.

FIA_AFL.1

Next authentication attempt is not executed until after 5 seconds for administrators and CE when authentication is unsuccessful for administrators using IA.ADM_AUTH or for CE using IA.CE_AUTH.

As described above, FIA_AFL.1 can be realized by implementing IA.ADM_AUTH and IA.CE_AUTH.

FDP_ACC.1[1]

ACL.USR executes reading and deleting of document data using based on Access Control Policy 1.

As described above, FDP_ACC.1[1] can be realized by implementing ACL.USR.

FDP_ACC.1[2]

MNG.ADM executes creating and deleting of User Boxes based on Access Control Policy 2.

As described above, FDP_ACC.1[2] can be realized by implementing MNG.ADM.

FDP_ACF.1[1]

ACL.USR executes reading and deleting of document data based on Access Control Policy 1.

As described above, FDP_ACF.1[1] can be realized by implementing ACL.USR.

FDP_ACF.1[2]

MNG.ADM executes creating and deleting of User Boxes based on Access Control Policy 2.

As described above, FDP_ACF.1[2] can be realized by implementing MNG.ADM.

FDP_RIP.1

After ACL.USR calls RD.TEMP and erase document data by using RD.TEMP. It becomes impossible to reuse of document data after deleting the document data by USR. ACL..

After MNG.ADM calls RD.TEMP and erase document data by using RD.TEMP. It becomes impossible to reuse of document data after deleting the document data by MNG.ADM.

As described above, FDP_RIP.1 can be realized by implementing RD.TEMP and ACL.USER.

FAU_GEN.1

AUD.LOG records log data related to operation of security functions.

As described above, FAU_GEN.1 can be realized by implementing AUD.LOG.

FAU_STG.1

MNG.ADM implements function permitting only administrators access to log data in storage area.

As described above, FAU_STG.1 can be realized by implementing MNG.ADM.

FAU_STG.4

AUD.MNG overwrites log data over old storage area when log storage area is exhausted.

As described above, FAU_STG.4 can be realized by implementing AUD.MNG.

FAU_SAR.1

AUD.LOG creates log data as in a format allowing administrators to reference during audit recording.

As described above, FAU_SAR.1 can be realized by implementing AUD.LOG.

FAU_SAR.2

MNG.ADM controls to allow only administrators to reference log data.

As described above, FAU_SAR.2 can be realized by implementing MNG.ADM.

FMT_MTD.1[1]

IA.ADM_ADD permits only CE to register administrator passwords and IA.PASS permits only CE to modify administrator passwords.

As described above, FMT_MTD.1[1] can be realized by implementing IA.ADM_ADD and IA.PASS.

FMT_MTD.1[2]

IA.PASS permits only CE to modify CE passwords.

As described above, FMT_MTD.1[2] can be realized by implementing IA.PASS.

FMT_MSA.1

MNG.ADM permits only administrators to register and delete User Box identifiers for creating and deleting User Boxes.

As described above, FMT_MSA.1 can be realized by implementing MNG.ADM.

FMT_MSA.3

MNG.ADM permits only administrators to register User Box identifiers and set User Box passwords which are necessary for User Box initialization. By registering the User Box identifier, User Box is created in a restricted condition that nobody can use, and by setting the User Box password, the User

Box can be used by the general user.

As described above, FMT_MSA.3 can be realized by implementing MNG.ADM.

FMT_MOF.1

MNG.MODE permits administrators to set validity/invalidity of all security functions regulated by this ST.

As described above, FMT_MOF.1 can be realized by implementing MNG.ADM.

FMT_SMF.1

IA.ADM_ADD implements function to manage administrator passwords. IA.PASS implements function to manage administrator, CE, and User Box passwords. MNG.ADM implements function to manage User Boxes.

As described above, FMT_SMF.1 can be realized by implementing IA.ADM_ADD, IA.PASS, and MNG.ADM.

FMT_SMR.1

By registering User Box identifiers and User Box passwords and by modifying CE, administrator, and User Box passwords, preservation of roles are realized. IA.ADM_ADD implements registration of administrators. MNG.ADM implements registration of general users possessing a User Box. IA.PASS implements modifications of administrator, CE and User Box passwords.

As described above, FMT_SMR.1 can be realized by implementing IA.ADM_ADD, IA.PASS, and MNG.ADM.

FPT_SEP.1

Unauthorized subjects do not destroy the TSF by implementing IA.ADM_ADD, IA.ADM_AUTH, IA.CE_AUTH, IA.PASS, ACL.USR, RD.TEMP, AUD.LOG, AUD.MNG, MNG.MODE, and MNG.ADM.

As described above, FMT_SEP.1 can be realized.

FPT.RVM.1

IA.ADM_ADD, IA.ADM_AUTH, IA.CE_AUTH, IA.PASS, ACL.USR, RD.TEMP, AUD.LOG, AUD.MNG, MNG.MODE, and MNG.ADM are always implemented.

As described above, FPT_RVM.1 can be realized.

8.3.2. Rationale for Security Functions Strength

As described in 6.2 Security Functions Strength, SOF-Basic is satisfied for the password mechanism of the identification authentication functions (IA.ADM_ADD and IA.PASS) and the control support function (MNG.ADM). As described in 5.3 Security Functions Strength, minimum function strength for security function requirements satisfies SOF-standards, and is consistent with SOF-Basic as described in 6.2 Security Functions Strength .

8.3.3. Rationale for Assurance measures

The assurance measures support for all TOE security assurance requirements required by EAL3 as described in 6.3 Assurance measures. In addition, it includes the proofs required by TOE security assurance requirements regulated by this ST, by the related agreements shown in the assurance measures.

Accordingly, the security assurance requirements in regards to EAL3 can be realized.

8.4. PP Claims Rationale

There is no conformance to a PP in this ST.