Multi functional printer
(digital copier)
bizhub PRO 950
Security Target
Version : 5

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

March 16, 2009
Konica Minolta Business Technologies, Inc.

Document Revision History

Version	Description	Approved by	Checked by	Created by
1	- Initial version	03/28/2008 Masaru Ushio	03/28/2008 Kazuo Yasuda	03/28/2008 Junji Satou
2	-Changing of desicribed TOE identification and management Version. - Modification for error in writing (Box reading → Box save, TOE scope)	11/07/2008 Masaru Ushio	11/07/2008 Kazuo Yasuda	11/07/2008 Junji Satou
3	-Modification for the security action of environment/assumption/installation condition with installation management. Add to the HDD protection by using password of HDD. -Modification of the content and name of component applied CC2.3.	12/18/2008 Masaru Ushio	12/18/2008 Kazuo Yasuda	12/18/2008 Junji Satou
4	-Changing of the controller control program version.	01/15/2009 Masaru Ushio	01/15/2009 Kazuo Yasuda	01/15/2009 Junji Satou
5	- Modification for the security attribute class of the FDP ACF.1[1] and FDP ACF.1[2]. - Delete the definition of FMT MTD.1[2] and FMT MTD.1[3].	03/16/2009 Masaru Ushio	03/16/2009 Kazuo Yasuda	03/16/2009 Junji Satou

Table of Contents

List of Figures

List of Tables

1. ST Introduction

1.1. ST Identification

1.1.1. ST Identification and Management

Title: Multi functional printer (digital copier) bizhub PRO 950 Security Target

Version: 5

Created on: March 16, 2009

Created by: Konica Minolta Business Technologies, Inc.

1.1.2. TOE Identification and Management

Title: Japan : bizhub PRO 950 zentai seigyo software

・This software consists of two components below.

Gazou seigyo program (Gazou seigyo I1)

Controller seigyo program (IC control P)

Overseas : bizhub PRO 950 control software

・This software consists of two components below.

Image control program (Image control I1)

Controller control program (IC control P)

Note）”Image control program” and “Controller control program” for overseas are the same products as “Gazou seigyo program” and “Controller seigyo program” for Japan respectively, with different calling names.

Version:

Image control program (Image control I1)	: 00I1-G00-10
Controller control program (IC control P)	: 00P1-G00-11

Created by: Konica Minolta Business Technologies, Inc.

“bizhub PRO 950 zentai seigyo software” for Japan is the same product as “bizhub PRO 950 control software” for overseas, with different calling name. It is called bizhub PRO 950 control software, hereafter.

1.1.3. Used CC Version

CC Version 2.3, ISO/IEC 15408:2005

Note）The following references are used for Japanese version.

- Common Criteria for Information Technology Security Evaluation
  Part 1：Introduction and general model
  August 2005 Version 2.3 CCIMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2：Security functional requirements
  August 2005 Version 2.3 CCIMB-2005-002
- Common Criteria for Information Technology Security Evaluation
  Part 3：Security assurance requirements
  August 2005 Version 2.3 CCIMB-2005-003

1.2. ST Overview

This Security Target (ST) describes bizhub PRO 950 control software installed in digital MFP bizhub PRO 950 (it is called bizhub PRO 950 series, hereafter.) manufactured by Konica Minolta Business Technologies, Inc.

Bizhub PRO 950 control software prevents the document data from disclosing during the use of functions such as copier and printer. To protect the document data, it has a “User BOX” function and a variety of management capabilities, additional highly confidential HDD (Hard Disk Drive) to store the document.

1.3. CC Conformance

Part 2 Extension
Part 3 Conformant
EAL3 Conformant

1.4. Reference

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 2005 Version 2.3 CCIMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 2005 Version 2.3 CCIMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements
  August 2005 Version 2.3 CCIMB-2005-08-003

- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part1, 2005/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part2, 2005/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part3, 2005/12

2. TOE Description

2.1. TOE Type

The TOE is software product with the digital MFP that is installed the network function.

2.2. Terminology

No.	Term	Description
1	User BOX	This is the directory to store the document data (Refer to No.2 below).
2	Document data	This is the electronic data converted from the information such as characters and figures.
3	Paper document	This is the paper document with the information such as characters and figures.
4	Operation panel	This is the touch panel display with each operation buttons, attached to the main frame of bizhub PRO 950 series.
5	Internal network	This is the LAN in an office which introduces bizhub PRO 950 series, and is connected with the client PC and several servers such as mail server and FTP server.
6	External network	This is the network (like internet) except the internal Network (Refer to the above No.5).
7	SMB	This is the application protocol to communicate between the computers on the network under Microsoft-OS series.

2.3. TOE Overview

The TOE is all of the bizhub PRO 950 control software. Bizhub PRO 950 series with this TOE are digital MFPs with the network function, and provide each function for the use of copier and printer etc, the operation management and the maintenance management. Figure 2.1 shows the expected operating environment with bizhub PRO 950 series in office.

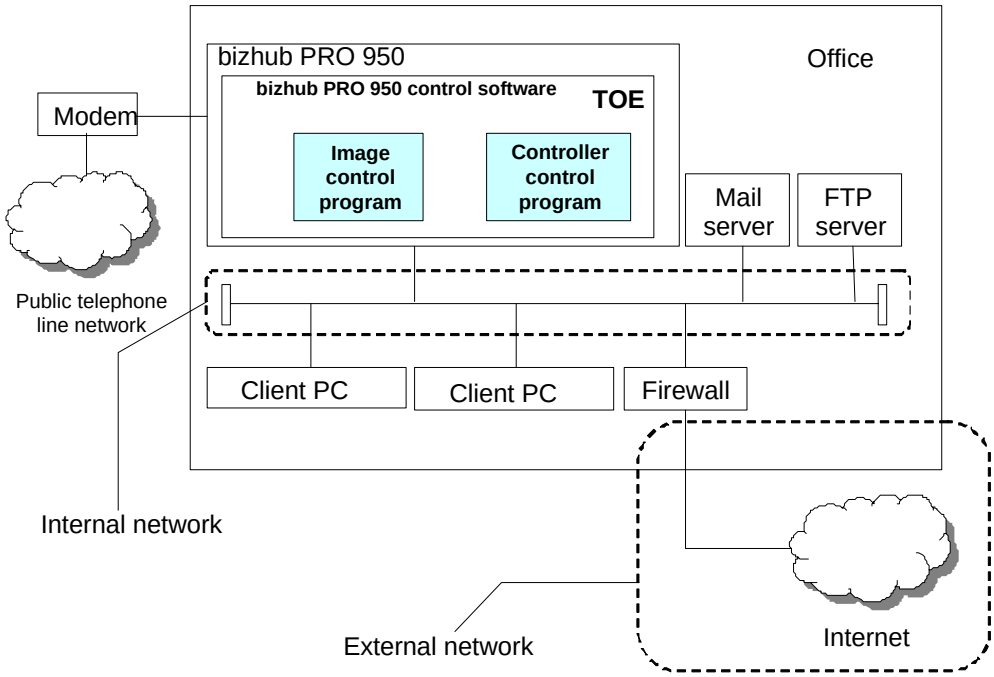

Figure 2.1 Operating Environment of bizhub PRO 950 Series

The TOE has a function to send and receive the document data in the internal network, therefore, bizhub PRO 950 series including the TOE is connected with the internal network and public telephone line network as shown in Figure 2.1. The internal network is connected with the client PC of general user, mail server and FTP server, to which bizhub PRO 950 series sends the data. The TOE does not have the interface with the external network. The TOE is connected with the external network only through Firewall, so as to protect each of equipments on the internal network.

2.4. Related Persons and Their Roles for bizhub PRO 950 Series

The following shows the related persons with bizhub PRO 950 series and their roles.

- General user

  General user enrolled at the organization that bizhub PRO 950 series is installed, uses the user function regarding the capabilities such as copier and printer. By registering in the TOE, he/she can own the User BOX on the HDD (Hard Disc Drive) in bizhub PRO 950 series. He/She has the fundamental knowledge concerning IT, and can attack TOE using the opened information, however, he/she is not assumed to create any new attack by using the unopened information.

- Administrator

  Administrator enrolled at the organization that bizhub PRO 950 series is installed, carries out the operation and management of bizhub PRO 950 series. He/She uses the function of the operation and management that bizhub PRO 950 series provides.

- Responsible person

  Responsible person enrolled at the organization that bizhub PRO 950 series is installed, appoints the administrator.

- CE

  CE enrolled at the company undertaken the maintenance of bizhub PRO 950 series, carries out the maintenance of bizhub PRO 950 series using the function of the maintenance and management that bizhub PRO 950 series provides. He/She closes the maintenance contract for bizhub PRO 950 series with the responsible person or administrator.

The product-related persons are the general user, administrator, and CE.

2.5. TOE Structure

Figure 2.2 shows the structure of this TOE.

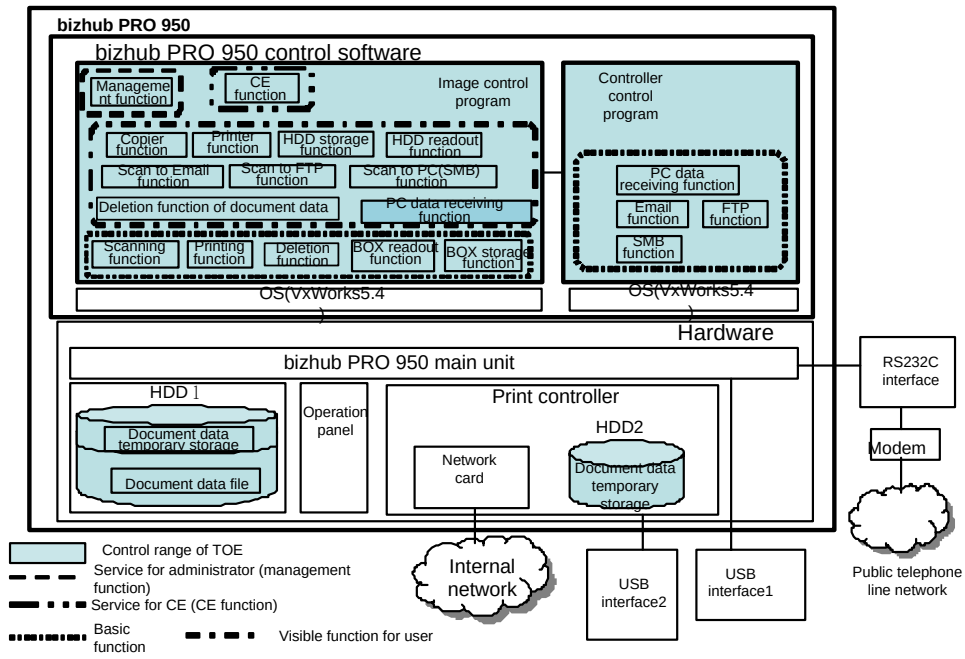

Figure 2.2 TOE Structure

Bizhub PRO 950 series consists of buzhub PRO 950 series main unit hardware, print controller, HDD1, HDD2, operation panel, and network card. And bizhub PRO 950 control software consists of the image control program and the controller control program. The main unit of bizhub PRO 950 series has the scanning function that converts the paper document to electronic data, and the printing function that prints characters and figures on the paper. The print controller performs the data exchange of the received PC data to print characters and figures on the paper. The USB interface1 are used to connect with the computer for the maintenance to set and create theTOE, and cannot be accessed the document data. The USB interface2 is to connect locally with the client PC and execute printing. The HDD1 is the storage device that stores the data (temporary storage is also possible). The HDD2 is the storage device that stores temporarily the data.Bizhub PRO 950 control software operates with OS. The OS controls input and output of the document data for the hardware and bizhub PRO 950 control software. The image control program controls the management function, CE function, user functions (refer to the later Table 2.1 : copier, printer, scan to Email, scan to FTP, scan to PC (SMB), HDD storage, HDD readout, document data deletion functions) and basic function (scanning, printing, deletion, BOX storage, BOX readout functions,and PC data receiving

function). The controller control program controls the basic function such as Email, FTP, SMB(*1), and PC data receiving functions.

(*1)SMB function sends the image data by means of SMB protocol(*2).

(*2)SMB protocol (Server Message Block protocol), used with Microsoft-OS series such as DOS and Windows, is for the file service, and has the capabilities of the file sharing service, print sharing service, compuer name browsing, communication between the processes, and mail slot function etc.

The User BOX is created on the storage device of HDD1 according to the action of bizhub PRO 950 control software. The Sub BOX is created in the User BOX and has the document data file that stores the document data. The plural User BOXes can be created on bizhub PRO 950 series. The plural Sub BOXes can exist in the User BOX, and several document data files can exist in the Sub BOX of User BOX. The hatching parts in Figure 2.2 show the control range of TOE.

Bizhub PRO 950 series takes any processing request by the product-related person from the operation panel or network, then the TOE executes the task.

2.6. Functional Structure of bizhub PRO 950 Control Software

Bizhub PRO 950 control software has the following functions.

2.6.1. Basic Function

The document data entered from the scanner is once stored into the temporary storage areas of DRAM and HDD1. The document data from the client PC is stored into the HDD2 temporary storage, and the data exchange is executed, then it is once stored into the temporary storage areas of DRAM and HDD1. These data are outputted to the User BOX in the HDD1 or the printer, or through the HDD2 temporary storage, the FTP server, mail server, PC sharing folder. The document data in the User BOX of HDD1 is once stored into the temporary storage areas of DRAM and HDD1, then outputted to the printer. The data stored into the DRAM temporary storage vanishes by turning the power off. The HDD1 temporary storage and DRAM temporary storage are the areas to store temporarily the data.

Basic functions are used to operate the document data. The User BOX is identified by the User BOX identifier, and the User BOX password is set for every User BOX so as to confirm the validity of the owner of each User BOX. The valid owner of User BOX can access all the document data in his/her User BOX. Figure 2.3 shows the processing overview of basic functions.

The Sub BOX is created in the User BOX, and the document data is stored together into the Sub BOX.

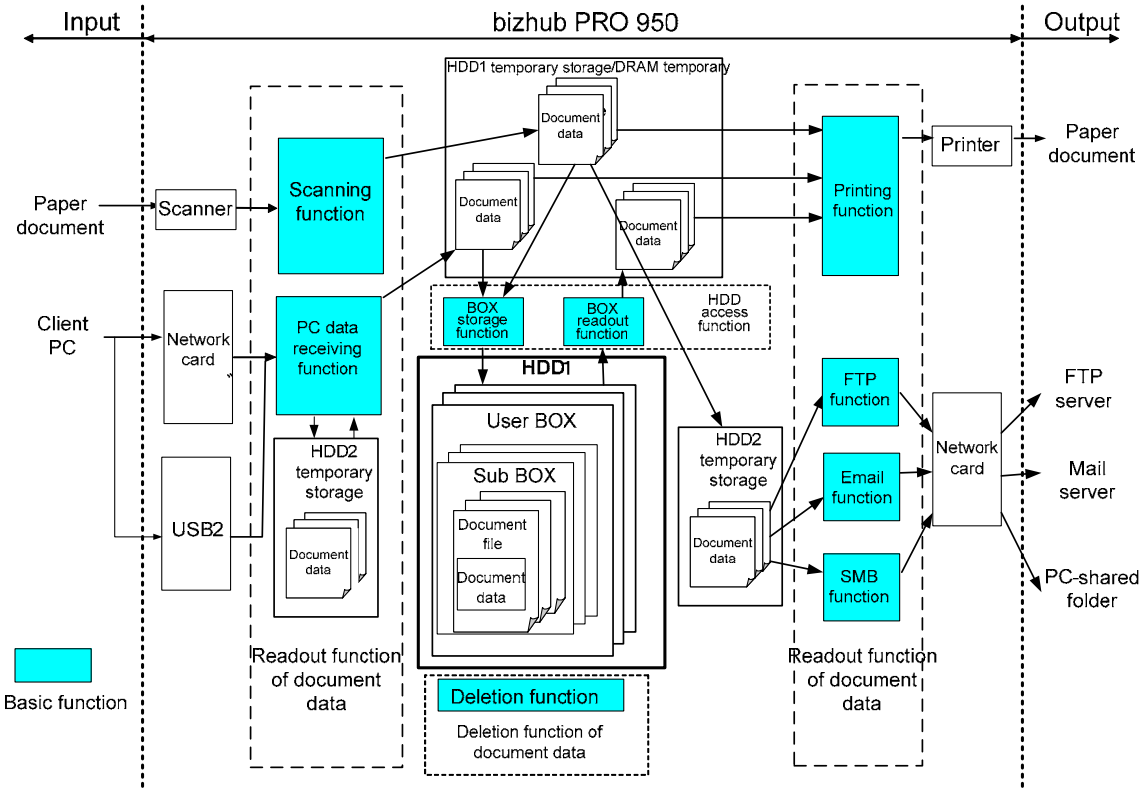

Figure 2.3 Processing Architecture of Basic Function

As indicated in Figure 2.1, executing the basic functions can make the user functions work. The following explains the basic functions.

Table 2.1 Correspondence between User Functions and Basic Functions

No	User function	Basic function
1	Copier function	Scanning function and Printing function
2	Printer function	PC data receiving function and Printing function
3	Scan to Email function	Scanning function and Email function
4	Scan to FTP function	Scanning function and FTP function
5	Scan to PC（SMB） function	Scanning function and SMB function
6	HDD storage function	Scanning function or PC data receiving function, and BOX storage function
7	HDD readout function	BOX readout function and Printing function
8	Document data deletion function	Deletion function

The basic functions shown in Figure 2.3 are described below.

(1) Scanning function

By request from the operation panel by a general user, the information of paper document is read from the scanner, converted to the document data, and stored into the HDD1 temporary storage or DRAM temporary storage.

(2) PC data receiving function

By request through the internal network or USB2 from the client PC by a general user, the document data is stored into the HDD2 temporary storage, executed the data exchange, and stored into the HDD1 temporary storage or DRAM temporary storage.

(3) BOX storage function

The temporary document data in the HDD1 temporary storage or in the DRAM temporary storage is stored into the User BOX additionally.

(4) BOX readout function

The document data in the User BOX is temporarily read out to the HDD1 temporary storage or DRAM temporary storage. This function is permitted only for the valid user authenticated by the User BOX password.

(5) Printing function

The temporary document data in the HDD1 temporary storage or in the DRAM temporary storage is printed out.

(6) Email function

The document data gotten by the scanning function, which is stored temporarily into the HDD1 temporary storage or DRAM temporary storage, is attached to a mail via the HDD2 temporary storage, and sent to the mail server.

(7) FTP function

The document data gotten by the scanning function, which is stored temporarily into the HDD1 temporary storage or DRAM temporary storage, is sent to the FTP server via the HDD2 temporary storage.

(8) SMB function

The document data gotten by the scanning function, which is stored temporarily into the HDD1 temporary storage or DRAM temporary storage, is sent to the shared folder of PC that is connected with the internal network via the HDD2 temporary storage.

(9) Deletion function

The document data in the User BOX, associated with the User BOX identifier, is deleted.

2.6.2. Management Function

The management function can be permitted to use by the administrator, only after the successful identification and authentication. This function can be used from the operation panel only. The administrator conducts the setting for the network information of TOE and the operational setting for the TOE function through this management function. Moreover the management function controls the related information for the operation of digital MFP, such as the creation/attribution change/ deletion of User BOX, the printing of audit information, the initialization process of HDD1 and HDD2 (initialization of data, password setting to prevent the unauthorized readout of data), the management of troubleshooting/toner/number of prints.

2.6.3. CE Function

The CE function can be permitted to use the following functions by the CE, only after the successful identification and authentication

- Service setting mode

  The CE executes the registration and change of the administrator password by using the function of service setting mode from the operation panel.

- CSRC (CS Remote Care)

  The CE gets the information for the hardware maintenance such as the number of prints, jam frequency, and out of toner, by accessing bizhub PRO 920 series from the computer connected through the public line network or the Internet. CSRC is executed with RS232C interface or Email interface. The RS232C interface, that is to say transmission rule with modem, here uses an original communication protocol. Email uses also an original message communication protocol, and this CSRC does not have the interface to the document data.

2.7. Asset to be protected

The asset to be protected by the TOE is the document data stored to HDD1 and HDD2 of bizhub PRO 950.The TOE does not prevent the deletion of document data, because the user

owns its original data in his/her PC or on the paper.

3. TOE Security Environment

3.1. Assumptions

ASM.PLACE Installation condition for the TOE

The TOE shall be installed in the area where only the product-related person can operate.

ASM.NET Setting condition for the internal network

The TOE shall be connected with the internal network that the disclosure of document data will not occur.

ASM.ADMIN Reliable administrator

The administrator shall not carry out an illegal act.

ASM.CE Personal condition for the CE

The CE shall not carry out an illegal act.

ASM.USR Management of the general user

The general user shall not disclose his/her own User BOX password.

3.2. Threats

T.ACCESS Unauthorized access to the BOX

When a general user uses the user function from the operation panel, there is a possible threat of disclosing the document data that the other general user owns in his/her User BOX.

T.HDDACCESS Unauthorized access to the HDD

- When a general user connects the HDD1 with an illegal device, there is a possible threat of disclosing the document data in the HDD1.
- When a general user connects the HDD2 with an illegal device, there is a possible threat of disclosing the document data in the HDD2.

T.IMPADMIN Impersonation of the CE and administrator

- When a general user uses illegally the interfaces for CE function and administrator function, there is a possible threat of disclosing the document data.

4. Security Objectives Policies

4.1. Security Objectives Policies for the TOE

O.IA Identification and authentication when using

The TOE identifies and authorizes the administrator, CE, or general user who owns the User BOX, who try to access the TOE.

O.MANAGE Provision of the management function

The TOE provides the administrator with functions to manage securely the User BOX and the HDD that stores the document data (i.e. functions to manage and set the HDD lock password).

O.CE Provision of the CE function

The TOE provides the CE with the function that allow the administrator to use the management function.

O.DATAACCESS Access limit to the document data

The TOE permits to read out the document data in the User BOX only for the general user who owns that User BOX.

O.AUDIT Record of the audit information

The TOE records the event related with the access function to “asset to be protected” as the audit information. The reference of audit information is limited only for the administrator.

4.2. Security Objectives Policies for the Environment

OE.PLACE Management of the installed place

The administrator shall install the TOE in the area where only the product-related person can operate.

OE.WATCH Monitor by Administrator

The administrator shall monitor the TOE not to use unauthorized access by general user, and shall forbid to enter the area (room) where TOE was installed by bolting the room.

OE.NET Management of the network

The administrator shall connect the TOE with the internal network protected with Firewall so that the document data does not disclose, by using the equipment capable for secure communication.

OE.USR Instruction for the general user

The administrator shall instruct a general user not to disclose the User BOX password.

OE.ADMIN Personal condition for the administrator

The responsible person shall select a person as the administrator who does not carry out an illegal act.

OE.HDD Protection of the HDD

The HDD1 and HDD2 for storing the document data shall prevent the unauthorized access by means of the HDD lock password.

OE.CE Assurance of the CE

The responsible person or administrator shall close the maintenance contract with the CE. The contract shall be specified a statement that CE will not carry out an illegal act.

5. IT Security Requirements

5.1. TOE Security Requirements

5.1.1. TOE Security Functional 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.

Refinement : “User” →
Administrator, CE, and General user who owns the 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.

Refinement : "User" →
Administrator, CE, and General user who owns the 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]

- Dummy characters (*) for the number of password characters entered by the operator

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]
- Unsuccessful authentication to the administrator, CE, and general user who owns the User BOX

[assignment: number]
- 1

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]
- The administrator, CE, or general user who owns the User BOX authenticated unsuccessfully cannot execute for five seconds the next authentication trial.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1[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]

- The quality metric of password is defined as below.

  Length of password: 8 to 64 characters

  Types of structured characters: English one-byte capital letters, small letters, and numerals

  Permitted condition: Prohibition of the same password with that used one generation ago

Refinement: "Secret" →
"User BOX password"

Dependencies: No dependencies

FIA_SOS.1[2] 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]

- The quality metric of password is defined as below.

Length of password: 8 characters

Types of structured characters: English one-byte capital letters, small letters, and numerals

Permitted condition: Prohibition of the same password with that used one generation ago

Refinement: "Secret" →
"Administrator password" and "CE password"

Dependencies: No dependencies

FDP_ACC.1[1] 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]

- Subject:User reception function 1: Process that receives the request to access the User BOX of the general user who owns the User BOX
- Object:User BOX
- Operation:
  1) Read out the document data in the 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]

- Subject:User reception function 2: Process that receives the request to access the User BOX of the administrator
- Object:User BOX
- Operation:
  1) Creation of the 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]
- Subject: Process that receives the request to access the User BOX
- Security attribute: User BOX identifier
- Named group of security attribute: None
- Objects:User BOX
- Security attribute of objects: User BOX identifier; User BOX identifier
- Named group of security attribute: 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]
Reading out the document data in the User BOX specified below is permitted.
- The User BOX identifier associated with the user reception function 1 corresponds to the User BOX identifier associated with the User BOX.

FDP_ACF.1.3

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

access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise 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 initialisation

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]
- Subject: process to the receives the request to access the User BOX
- Security attributes: User BOX identifier
- Named groups of security attributes: None
- Objects: User BOX
- Security attributes of objects: User BOX identifier
- Named groups of security attributes: 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]
The following is executed.
- In case that the User BOX identifier associated with the user reception function 2 is not registered, the creation of User BOX associated with the User BOX identirfier is permitted.

FDP_ACF.1.3

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

[assignment: rules, based on security attributes, that explicitly authorise 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 initialisation

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 specified

[assignment: other specifically defined auditable events]

- Table 5.1 shows the events targeted to audit.

Table 5.1 Auditable Events

Functional component	Audit information
FIA_UID.2	Success and failure of identification in identifying of administrator, CE, general user who owns User BOX
FIA_UAU.2	Success and failure of identification in identifying of administrator, CE, general user who owns User BOX
FIA_AFL.1	Attainment to the threshold value of unsuccessful authentication of administrator, CE, general user who owns User BOX
FIA_SOS.1[1]	Acceptance of the tested authentication information
FIA_SOS.1[2]	Acceptance of the tested authentication information
FDP_SOS.1	Acceptance of the tested authentication information
FDP_ACF.1[1]	Request of success in executing of the operation for the object
FDP_ACF.1[2]	Request of success in executing of the operation for the object
FMT_SMF.1	Use of management function
FDP_MTD.1	Success of the value of administrator data

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 trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised 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 authorised 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 authorised user with special rights', 'overwrite the oldest stored audit records']
- Overwrite the oldest stored audit records

[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: authorised users] with the capability to read [assignment: list of audit information] from the audit records.

[assignment: authorised users]
- Administrator

[assignment: list of audit information]
- Audit information shown in “Table 5.1 Auditable Events” regulated in 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 authorised identified roles].

[assignment: list of TSF data]
- Administrator password

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

[assignment: other operations]
- Registration

[assignment: the authorised 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 authorised identified roles].

[assignment: list of TSF data]
- CE password

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

[assignment: other operations]
None

[assignment: the authorised 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 authorised identified roles].

[assignment: list of TSF data]
- User BOX password

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

[assignment: other operations]
None

[assignment: the authorised 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 authorised identified roles].

[assignment: list of TSF data]
- User BOX password

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

[assignment: other operations]
- Modify for only the password of general user who owns User BOX

[assignment: the authorised identified roles]
- Role of the general user who owns User BOX

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1[5] 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 authorised identified roles].

[assignment: list of TSF data]
- Administrator password

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

[assignment: the authorised identified roles]
- Administrator

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 authorised identified roles].

[assignment: list of security attributes]
- User BOX identifier

[selection: change_default, query, modify, delete, [assignment: other operations]]
- Other operations

[assignment: other operations]
- Registration

[assignment: the authorised 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 initialisation

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: other function]
- None

[assignment: access control SFP, information flow control SFP]
- Access control policy 2

Refinement: “security attributes” → “User BOX identifier”

FMT_MSA.3.2

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

[assignment: the authorised identified roles]
- Administrator

Dependencies: 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 authorised identified roles].

[assignment: the authorised identified roles]

- Administrator
- CE
- Role of the general user who owns 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 authorised identified roles].

[assignment: list of functions]

- Function 1, Function 2, Function 3, and Function 4
  - Function 1: Check function of password length
  - Function 2: HDD identification/authentication function
  - Function 3: Record function of audit information
  - Function 4: Identification/authentication function

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

Disable, Enable

[assignment: the authorised identified roles]

- Administrator

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

[assignment: list of security management functions to be provided by the TSF]
- Table 5.2 shows the list of security management functions.

Table 5.2 List of Management Requirements

N/A : Not Applicable

Required function	Required management	Management item
FIA_UID.2	Management of the user identification information	User BOX identifier
FIA_UAU.2	Management of authenticated data by the CE	Administrator password
	Management of authenticated data by the administrator	User BOX password
	Management of authenticated data by the user related to this data	Administrator password CE password User BOX password
FIA_UAU.7	N/A	
FIA_SOS.1[1]	Management of the scale used for the validation of secret	There is no management item since the scale used for the validation of secret cannot be changed.
FIA_SOS.1[2]	Management of the scale used for the validation of secret	There is no management item since the scale used for the validation of secret cannot be changed.

Required function	Required management	Management item
FDP_SOS.1	Management of the scale used for the validation of secret for IT environment	There is no management item since the scale used for the validation of secret for IT environment cannot be changed.
FIA_AFL.1	Management of the threshold value for unsuccessful authentication trial	There is no management item since the threshold value is fixed and cannot be changed.
	Management of action taken in the event of authentication failure	There is no management item since the action is fixed and cannot be changed.
FDP_ACC.1[1]	N/A	
FDP_ACC.1[2]	N/A	
FDP_ACF.1[1]	Management of attribution used for decision based on explicit access or rejection	User BOX identifier
FDP_ACF.1[2]	Management of attribution used for decision based on explicit access or rejection	User BOX identifier
FAU_GEN.1	N/A	
FAU_STG.1	N/A	
FAU_STG.4	Maintenance of action taken in unsuccess-ful audit storage	There is no management item since the action taken in unsuccessful audit storage cannot be changed.
FAU_SAR.1	Maintenance of the user group having a right to read the audit record (deletion, modification, addition)	There is no management item since a right to read the audit record is for the administrator and cannot be changed.
FAU_SAR.2	N/A	
FMT_MTD.1[1]	Management of the group that has a role that may affect TSF data with each other	There is no management item since the role of CE is fixed for a person.
FMT_MTD.1[2]	Management of the group that has a role that may affect TSF data with each other	There is no management item since the role of CE is fixed for a person.
FMT_MTD.1[3]	Management of the group that has a role that may affect TSF data with each other	There is no management item since the role of administrator is fixed for a person.

Required function	Required management	Management item
FMT_MTD.1[4]	Management of the group that has a role that may affect TSF data with each other	There is no management item since the role of general user who owns User BOX is fixed.
FMT_MTD.1[5]	Management of the group that has a role that may affect TSF data with each other	There is no management item since the role of administrator is fixed for a person.
FMT_MSA.1	Management of the group that have a role that may affect security attribution with each other	There is no management item since the role of administrator is fixed for a person.
FMT_MSA.3	Management of the group that has a role in specifying the default value	There is no management item since the role of administrator is fixed for a person.
	Management of the permitted or limited setting of the default value for the specified access control SFP	There is no management item since the default value is fixed.
FMT_SMR.1	Management of the user group that carries out part of the role	There is no management item since the roles of CE, administrator, and general user that owns User BOX is fixed.
FMT_MOF.1	Management of the group that has a role that may affect TSF function with each other	There is no management item since the role of administrator is fixed for a person.
FMT_SMF.1	N/A	
FMT_RVM.1	N/A	
FDP_MTD.1	Management of the group that has a role that may affect TSF data with each other	There is no management item since the role of administrator is fixed for a person.

Dependencies: No Dependencies

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

This ST newly creates and uses the TOE security functional requirements (FDP_MTD.1 Management of administrator data and FDP_SOS.1 Verification of secrets of IT environment) without referring to CCPart2. The administrator data means the control data of security function for IT environment to which only the administrator can access.

FDP_MTD.1 Management of administrator data

FDP_MTD.1 Management of administrator data allows the authenticated users to manage the administrator data.

Management:**FDP_MTD.1**

The following actions could be considered for the management functions in FMT management.

a) managing the group of roles that can interact with the administrator data.

Audit:**FDP_MTD.1**

FAU_GEN The following actions should be auditable if Security audit data generation is included in the PP/ST.

a) Basic: All modifications in the value of the administrator data.

Hierarchical to: No other components.

FDP_MTD.1.1

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

[assignment:list of administrator data]

HDD lock password

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

Modify

[assignment: the authorised identified roles]

Administrator

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

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.

.

Dependencies: No dependencies

FDP_SOS.1 Verification of secrets of IT environment

FDP_SOS.1 Verification of secrets of IT environment requires the TSF to verify that secrets of IT environment meet defined quality metrics.

Management: FDP_SOS.1

The following actions could be considered for the management functions in FMT.

a) the management of the metric used to verify the secrets IT environment.

Audit: FDP_SOS.1

FAU_GEN The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Rejection by the TSF of any tested secret of IT environment;

b) Basic: Rejection or acceptance by the TSF of any tested secret of IT environment;

c) Detailed: Identification of any changes to the defined quality metrics.

Hierarchical to: No other components.

FDP_SOS.1.1

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

[assignment: a defined quality metric]

- The quality metric of password is defined as below.

Length of password: 8 to 32 characters

Types of structured characters: English one-byte capital letters, small letters, and numerals

Permitted condition: None

Refinement: “Secret of IT environment” → “HDD lock password”

Dependencies: No dependencies

5.1.2. TOE Security Assurance Requirements

This TOE asserts EAL3 that is a sufficient level as quality assurance for commercial office products. Table 5.3 summarizes the applied TOE security assurance requirements to EAL3.

Table 5.3 List of TOE Security Assurance Requirements

Assurance class	Assurance requirement
Configuration management	ACM_CAP.3 Authentication management
	ACM_SCP.1 TOE CM coverage
Distribution and operation	ADO_DEL.1 Distribution procedures
	ADO_IGS.1 Installation, creation, startup procedures
Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance document	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support	ALC_DVS.1 Identification of security measures
Test	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing：High-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

FIA_UID.2[E] User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1[E]

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

Refinement: “TSF” → “HDD”

Dependencies: No dependencies

FIA_UAU.2[E]　User authentication before any action

Hierarchical to：FIA_UAU.1

FIA_UAU.2.1[E]

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: “TSF” → “HDD”

Dependencies: FIA_UID.1 Timing of identification

5.3. Security Function Strength

The following three password mechanisms are targeted for the claim of TOE function strength, and the subsequence seven components of TOE functions are targeted for this ST.

Password mechanisms and corresponding TOE function components

1 User BOX password authentication function
FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1[1]

2 Administrator password/CE password authentication function
FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1[2]

3 HDD lock password authentication function
FDP_SOS.1

TOE component functions

FIA_UID.2（User identification）
FIA_UAU.2（User authentication）
FIA_UAU.7（Protected authentication feedback）
FIA_SOS.1[1](Verification of secrets)
FIA_SOS.1[2]（Verification of secrets）
FDP_SOS.1（Verification of secrets of IT environment）
FIA_AFL.1（Authentication failure handling）

The SOF-Basic is claimed for the above seven TOE function of requirements and the minimum TOE function strength.

6. TOE Summary Specification

6.1. TOE Security Function

6.1.1. Identification and Authentication Function

The identification and authentication function provides the following a group of security functions.

Function title	Specification of security function	TOE security functional requirement
IA.ADM_ADD Registration of administrator	IA.ADM_ADD registers the administrator in the TOE. Only the CE operates IA.ADM_ADD. The CE registers the administrator password. IA.ADM_ADD provides the interface for administrator registration. It requests to enter the applicable password to the administrator who is registered. For the password entered by the administrator, the permitted value is validated according to the following rules. - Password of 8 characters - Password of English characters, one-byte capital letters, small letters, and numerals - Prohibition of the same password with that used one generation ago In the validation of permitted value, the administrator is registered if the rules are obeyed, and it is rejected if not so.	FIA_SOS.1[2] FMT_MTD.1[1] FMT_SMF.1 FMT_SMR.1 FPT_RVM.1
IA.ADM_AUTH Identification and authentica-tion of administ-rator	Before the operator uses the TOE, IA.ADM_AUTH identifies that he/she is the registered administrator in the TOE and authorizes that he/she is the valid administrator. IA.ADM_AUTH does not permit to operate all the management functions before the identification and authentication of administrator. The interface for the identification and authentication of administrator requests to enter the password registered in IA.ADM_ADD and	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1

	changed in IA_PASS. IA.ADM_AUTH identificates that he/she is the administrator by the indication of interface for the identification and authentication of administrator, and authorizes that he/she is the valid administrator using the entered password. When the administrator enters the password, dummy characters (*) are displayed in stead of the entered password. In case of unsuccessful authentication, the interface for the identification and authentication of administrator is provided after five seconds.	
IA.CE_AUTH Identification and authentication of CE	Before the operator uses the TOE, IA.CE_AUTH identifies that he/she is the registered CE in the TOE and authorizes that he/she is the valid CE. IA.CE_AUTH does not permit to operate all the CE functions before the identification and authentication of CE. It requests to enter the password changed in IA_PASS. IA.CE_AUTH identificates that he/she is the CE by the indication of interface for the identification and authentication of CE, and authorizes that he/she is the valid CE using the entered password. When the CE enters the password, dummy characters (*) are displayed in stead of the entered password. In case of unsuccessful authentication, the interface for the identification and authentication of CE is provided after five seconds.	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1
IA.PASS Change of password	IA.PASS changes the password of administrator, CE, and general user who owns User BOX, which are the authori-zation information for the administrator, CE, and general user who owns User BOX. IA.PASS provides the interface for password change and requests to enter the new password. The following shows the changeable passwords by the type of user. CE : CE password, Administrator password	FIA_SOS.1[1] FIA_SOS.1[2] FMT_MTD.1[1] FMT_MTD.1[2] FMT_MTD.1[3] FMT_MTD.1[4] FMT_MTD.1[5] FMT_SMF.1 FMT_SMR.1 FPT_RVM.1

	Administrator : Administrator password, User BOX password General user who owns User BOX : User BOX password of his/her own User BOX For the password entered by the product-related persons, the permitted value is validated according to the following rules. - CE and administrator passwords of 8 characters - User BOX password of 8 to 32 characters - Password of English characters, one-byte capital letters, small letters, and numerals - Prohibition of the same password with that used one generation ago In the validation of permitted value, the administrator is registered if the rules are obeyed, and it is rejected if not so.	

6.1.2. Access Control Function

The access control function provides the following a group of security functions.

Function title	Specification of security function	TOE security functional requirement
ACL.USR Access rule and control to general user	ACL.USR identifies and authorizes the general user who owns User BOX and limits the operatable coverage for the general user according to the access rules after he/she is authenticated to be the valid user. ACL.USR identifies and authorizes the general user who owns User BOX by the User BOX identifier and User BOX password. When the User BOX password is entered, dummy characters (*) are displayed in stead of the entered User BOX password. After the successful identification and authentication, the following operation is permitted for the document data in the User BOX shown by the identified and authenticated User BOX identifier. - Reading out and printing of document data	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FDP_ACC.1[1] FDP_ACF.1[1] FPT_RVM.1

	In case of unsuccessful identification and authentication, the interface for the identification and authentication is allowed to be valid after five seconds.	

6.1.3. Audit Function

The audit function provides the following a group of security functions.

Function title	Specification of security function	TOE security functional requirement
AUD.LOG Record of audit information	AUD.LOG records with an accurate time the audit information regarding the action of security functions. The following shows the auditable events. - Startup and shutdown of audit functions - Success and failure in identifying and authorizing of administrator, CE, general user who owns User BOX - Success in registering password of administrator and general user who owns User BOX - Success in changing password and HDD lock password of administrator, CE, and general user who owns User BOX - Success in reading out of document data	FAU_GEN.1 FPT_RVM.1 FPT_STM.1
AUD.MNG Management of audit area	AUD.MNG manages the audit storage area in order to create and store the audit information. The area to store the audit information is the ring buffer formed memory area. In case that the storage area of audit information is exhausted, AUD.MNG overwrites the audit information from the beginning of the storage area.	FAU_STG.4 FPT_RVM.1

6.1.4. Management Support Function

The management function provides the following a group of security functions.

Function title	Specification of security function	TOE security functional requirement
MNG.MODE Setting of security reinforcement	MNG.MODE permits only the administrator to execute only the administrator the check function of TOE password length, the HDD identification and authentication function,	FMT_MOF.1 FPT_RVM.1

mode	the record function of audit information, the function that validates identification and authentication, and the function that stops their functions.	
MNG.ADM Management support function (Administrator)	MNG.ADM permits only the administrator to execute the following operations. - Creation of User BOX, registration of User BOX identifier, and setting of User BOX password - Inquiry of audit information (No the deletion function of audit information) For the User BOX password entered by the administrator, the permitted value is validated according to the following rules. - Password of 8 to 32 characters - Password of English characters, one-byte capital letters, small letters, and numerals - Prohibition of the same password with that used one generation ago In the validation of permitted value, the administrator is registered if the rules are obeyed, and it is rejected if not so. The inquiry of audit information has the information for the date and time (year/month/day/hour/minute/second) of events occurrence, operational subjective identification, and the result of events. It is displayed in a form that the administrator can refer.	FDP_ACC.1[2] FDP_ACF.1[2] FIA_SOS.1[1] FMT_MSA.1 FMT_MSA.3 FAU_STG.1 FAU_SAR.2 FAU_SAR.1 FMT_SMF.1 FMT_SMR.1 FPT_RVM.1
MNG.HDD HDD lock password	MNG.HDD permits only the administrator to execute the following operations.	FDP_SOS.1 FDP_MTD.1 FPT_RVM.1

function	・Change of HDD lock password For the HDD lock password entered by the administrator, the permitted value is validated according to the following rules. - Password of 8 to 32 characters - Password of English characters, one-byte capital letters, small letters, and numerals In the validation of permitted value, the HDD lock password is set and changed in the HDD device if the rules are obeyed, and the change is rejected if not so.	

6.2. Security Function Strength

This TOE claims the security function strength of SOF-Basic for the password mechanism. The applicable password mechanism is the identification and authentication function (IA.ADM_AUTH, IA.CE_AUTH, ACL.USR, IA.ADM_ADD, and IA.PASS), and the management support function (MNG.ADM and MNG.HDD).

6.3. Assurance Measures

The developer shall develop according to the assurance requirements and the development rules regulated by the development organization. Table 6.1 shows the components and the related requirements of security assurance requirements that fulfill EAL3.

Table 6.1 Assurance Requirements and Related Documents for EAL3

Assurance requirements item	Component	Related document
Configuration management	ACM_CAP.3	bizhub PRO 950 Configuration Management Plan bizhub PRO 950 List of Design Documents bizhub PRO 950 List 1 of Source Codes bizhub PRO 950 List 2 of Source Codes
	ACM_SCP.1	bizhub PRO 950 Configuration Management Plan bizhub PRO 950 List of Design Documents bizhub PRO 950 List 1 of Source Codes bizhub PRO 950 List 2 of Source Codes

Distribution and operation	ADO_DEL.1	bizhub PRO 950 Distribution regulations bizhub PRO 950 Installation Manual(Japanese) bizhub PRO 950 User's Guide Copier(Japanese) bizhub PRO 950 User's Guide POD Administrator's Reference (Japanese) bizhub PRO 950 User's Guide Network Scanner (Japanese) bizhub PRO 950 User's Guide Security (Japanese) bizhub PRO 950 User's Guide Printer(Japanese) bizhub PRO 950 Service Manual Field Service (Japanese) bizhub PRO 950 User's Guide Copier (English) bizhub PRO 950 User's Guide POD Administrator's Reference (English) bizhub PRO 950 User's Guide Network Scanner (English) bizhub PRO 950 User's Guide Security (English) bizhub PRO 950 User's Guide Printer (English) bizhub PRO 950 SERVICE MANUAL Field Service (English) bizhub PRO 950 INSTALLATION MANUAL (English)

	ADO_IGS.1	bizhub PRO 950 Introduction and Operation Regulations bizhub PRO 950 Installation Manual (Japanese) bizhub PRO 950 User's Guide Copier (Japanese) bizhub PRO 950 User's Guide POD Administrator's Reference (Japanese) bizhub PRO 950 User's Guide Network Scanner (Japanese) bizhub PRO 950 User's Guide Security (Japanese) bizhub PRO 950 User's Guide Printer (Japanese) bizhub PRO 950 Service Manual Field Service (Japanese) bizhub PRO 950 SERVICE MANUAL Field Service (English) bizhub PRO 950 INSTALLATION MANUAL (English) bizhub PRO 950 User's Guide Copier (English) bizhub PRO 950 User's Guide POD Administrator's Reference (English) bizhub PRO 950 User's Guide Network Scanner (English) bizhub PRO 950 User's Guide Security (English) bizhub PRO 950 User's Guide Printer (English)
Development	ADV_FSP.1	bizhub PRO 950 Functional Specifications
	ADV_HLD.2	bizhub PRO 950 Functional Specifications
	ADV_RCR.1	bizhub PRO 950 Functional Correspondence Report

Guidance document	AGD_ADM.1	bizhub PRO 950 Installation Manual (Japanese) bizhub PRO 950 User's Guide Copier (Japanese) bizhub PRO 950 User's Guide POD Administrator's Reference (Japanese) bizhub PRO 950 User's Guide Network Scanner (Japanese) bizhub PRO 950 User's Guide Security (Japanese) bizhub PRO 950 User's Guide Printer (Japanese) bizhub PRO 950 Service Manual Field Service (Japanese) bizhub PRO 950 INSTALLATION MANUAL (English) bizhub PRO 950 User's Guide Copier (English) bizhub PRO 950 User's Guide POD Administrator's Reference (English) bizhub PRO 950 User's Guide Network Scanner (English) bizhub PRO 950 User's Guide Security (English) bizhub PRO 950 User's Guide Printer (English) bizhub PRO 950 SERVICE MANUAL Field Service (English)
	AGD_USR.1	bizhub PRO 950 User's Guide Copier (Japanese) bizhub PRO 950 User's Guide POD Administrator's Reference (Japanese) bizhub PRO 950 User's Guide Network Scanner (Japanese) bizhub PRO 950 User's Guide Security (Japanese) bizhub PRO 950 User's Guide Printer (Japanese) bizhub PRO 950 User's Guide Copier (English) bizhub PRO 950 User's Guide POD Administrator's Reference (English) bizhub PRO 950 User's Guide Network Scanner (English) bizhub PRO 950 User's Guide Security (English) bizhub PRO 950 User's Guide Printer (English)
Life cycle support	ALC_DVS.1	bizhub PRO 950 Development Security Regulations

Test	ATE_COV.2	bizhub PRO 950 Functional Test Report
	ATE_DPT.1	bizhub PRO 950 Functional Analysis Report
	ATE_FUN.1	bizhub PRO 950 Functional Test Report
	ATE_IND.2	None（bizhub PRO 950 test set）
Vulnerability assessment	AVA_MSU.1	bizhub PRO 920 Installation and Operation Regulations bizhub PRO 950 Installation Manual (Japanese) bizhub PRO 950 User's Guide Copier (Japanese) bizhub PRO 950 User's Guide POD Administrator's Reference (Japanese) bizhub PRO 950 User's Guide Network Scanner (Japanese) bizhub PRO 950 User's Guide Security (Japanese) bizhub PRO 950 User's Guide Printer (Japanese) bizhub PRO 950 Service Manual Field Service (Japanese) bizhub PRO 950 INSTALLATION MANUAL (English) bizhub PRO 950 User's Guide Copier (English) bizhubPRO 950 User's Guide POD Administrator's Reference (English) bizhub PRO 950 User's Guide Network Scanner (English) bizhub PRO 950 User's Guide Security (English) bizhub PRO 950 User's Guide Printer (English) bizhub PRO 950 SERVICE MANUAL Field Service (English)
	AVA_SOF.1	bizhub PRO 950 Vulnerability Analysis Report
	AVA_VLA.1	bizhub PRO 950 Vulnerability Analysis Report

7. PP Claim

There is no applicable PP in this ST.

8. Rationale

8.1. Security Objectives Policies Rationale

Table 8.1 shows the correspondence relation of the security objectives policy to the threat and assumptions.

Table 8.1 Correspondence between Threats, Assumptions, and Security Objectives Policies

Threat/Assumption/ organizational security policy / Security objectives policy	T.HDDACCESS	T.ACCESS	T.IMPADMIN	ASM.PLACE	ASM.NET	ASM.ADMIN	ASM.CE	ASM.USR
O.IA (Identification and authentication when using)	✔	✔	✔					
O.MANAGE (Provision of the management function)	✔		✔					
O.CE (Provision of the CE function)			✔					
O.DATAACCESS (Access limit to the document data)		✔	✔					
O.AUDIT (Record of the audit information)	✔	✔	✔					
OE.PLACE (Management of the installed place)				✔				
OE.NET (Management of the network)					✔			
OE.USR (Instruction for the general user)								✔
OE.ADMIN (Personal condition for the administrator)						✔		
OE.CE (Assurance of CE)							✔	
OE.WATCH（Monitor by Administrator）	✔							

OE.HDD（Access limit to the HDD itself）	✔							

The following shows the rationale for Table 8.1.

T.HDDACCESS：Unauthorized access to the HDD

TSF changes and manages the HDD lock password of HDD1 and HDD2 in the management function of O.MANAGE by the valid administrator identified in O.IA. Moreover TSF makes it possible to detect the trial of unauthorized use to the applicable management function by anyone except the administrator, because it records the failed identification and authentication of administrator as audit information in O.AUDIT. In OE.HDD, the HDD1 and HDD2 execute the identification and authentication, then the access is limited to only the TOE that is valid user, therefore, the unauthorized access to HDD1 and HDD2 is prevented. As above mentioned, the threat - T.HDDACCESS can be resisted by O.IA, O.MANAGE, O.AUDIT, OE.WATCH, and OE.HDD of the security objectives policies.

T.ACCESS：Unauthorized access to the BOX

TSF permits only the valid general user, who owns the User BOX identified and authenticated in O.IA, to read out the document data in the User BOX in O.DATAACCESS. Moreover TOE makes it possible to detect the unauthorized operation to the document data in the User BOX that the general user owns, because it records the operation regarding the access function to the document data that is “asset to be protected” as audit information in O.AUDIT. As above mentioned, the threat - T.ACCESS can be resisted by O.IA, O.DATAACCESS, and O.AUDIT of the security objectives policies.

T.IMPADMIN：Impersonation of the CE and administrator

TSF identifies and authorizes the CE in O.IA. TSF provides the valid CE identified and Authenticated with the function to decide the administrator in O.CE. TSF identifies and authorizes the decided administrator in O.IA. TSF provides the valid administrator identified and authenticated with the function to manage the User BOX in O.MANAGE. The administrator decides the owner of User BOX using this funtion. TSF permits only the valid general user who owns the User BOX identified and authenticated in O.IA, to read out the document data in the User BOX in O.DATAACCESS. Moreover TSF makes it possible to detect the conduct operated to impersonate the administrator, because it records the failed identification and authentication of CE and administrator as audit information in O.AUDIT.

As above mentioned, the threat - T.IMPADMIN can be resisted by O.IA, O.CE, O.MANAGE, O.DATAACCESS, and O.AUDIT of security objectives policies.

ASM.PLACE：Installation condition for the TOE

In OE.PLACE, TOE is installed in the area where only the product-related person can operate, therefore, the access to TOE is limited to only the product-related person.

As above mentioned, the assumption - ASM.PLACE can be realized by OE.PLACE of security objectives policy.

ASM.NET：Setting condition for internal network

In OE.NET, TOE is installed in the internal network that the disclosure of document data will not occur. It is possible to realize by constructing with the equipment that encrypts the communication of internal network.

As above mentioned, the assumption - ASM.NET can be realized by OE.NET of security objectives policies.

ASM.ADMIN：Reliable administrator

OE.ADMIN regulates the condition of administrator. The responsible person selects a person who does not carry out an illegal act as the administrator.

As above mentioned, the assumption - ASM.ADMIN can be realized by OE.ADMIN of security objectives policies.

ASM.CE：Maintenance contract

OE.CE regulates for the organization that introduces the TOE to close the maintenance contract specified a statement that the organization and CE in charge of the maintenance of TOE will not carry out an illegal.

As above mentioned, the assumption - ASM.CE can be realized by OE.CE of the security objectives policies.

ASM.USR：Management of general user

The administrator instructs the general user not to disclose the User BOX password to others in OE.USR, therefore, the general user does not disclose his/her own User BOX password.

As above mentioned, the assumption - ASM.USR can be realized by OE.USR of the security objectives policies.

8.2. Security Requirements Rationale

8.2.1. Security Functional Requirements Rationale

8.2.1.1. Reason for the adoption of security functional requirements FDP_MTD.1 and FDP_SOS.1

Requirement : The control of security function and the validation of secret for IT environment are executed in TOE security functional requirements

TSF is necessary to protect the HDD lock password used for the identification and authentication from being changed so that OE.HDD can correctly execute the identification and authentication, therefore, TOE security functional requirements are required.

HDD lock password is the secret of IT environment as well as the TSF data of HDD for IT environment. They are the user data in terms of the TOE. However they have practically a characteristic of TSF data that only the administrator handles because the data controls the security function for IT environment. Such data cannot be handled by the FMT/FIA class of TOE and is not the target access control for the general user.

In case that the management of this data is handled in FDP_ACC/FDP_ACF, the permitted condition cannot be written (due to permission at all times) because the corresponding subject is only the administrator. Moreover the HDD lock password cannot be handled by the FIA class because it is “secret of IT environment”. Therefore, newly the functional requirements with management characteristic is required to be defined in the FDP class.

These TOE security functional requirements are created following as FMT_MTD.1, FIA_SOS.1 of the management requirements.

8.2.1.2. Correspondence between security objectives policies and IT security functional requirements

Requirements shows the correspondence relation of the TOE security functional requirements to the security objectives policies.

Table 8.2 Correspondence between Security Objectives Policies and IT Security Functional Requirements

IT security functional requirement \ Security objectives policy		O.IA	O.MANAGE	O.CE	O.DATAACCESS	O.AUDIT	OE.HDD
TOE security functional requirement	FIA_UID.2	✔					
	FIA_UAU.2	✔					
	FIA_UAU.7	✔					
	FIA_AFL.1	✔					
	FIA_SOS.1[1]	✔	✔				
	FIA_SOS.1[2]		✔	✔			
	FDP_SOS.1		✔				
	FDP_ACC.1[1]				✔		
	FDP_ACC.1[2]		✔				
	FDP_ACF.1[1]				✔		
	FDP_ACF.1[2]		✔				
	FAU_GEN.1					✔	
	FAU_STG.1					✔	
	FAU_STG.4					✔	
	FAU_SAR.1					✔	
	FAU_SAR.2					✔	
	FMT_MTD.1[1]			✔			
	FMT_MTD.1[2]			✔			
	FMT_MTD.1[3]		✔				

	FMT_MTD.1[4]	✔					
	FMT_MTD.1[5]		✔				
	FMT_MSA.1		✔				
	FMT_MSA.3		✔				
	FMT_SMR.1	✔	✔	✔	✔		
	FMT_MOF.1	✔	✔	✔	✔	✔	
	FPT_RVM.1	✔	✔	✔	✔	✔	
	FMT_SMF.1	✔	✔	✔	✔		
	FPT_STM.1					✔	
	FDP_MTD.1		✔				
Security functional requirement for IT environment	FIA_UID.2[E]						✔
	FIA.UAU.2[E]						✔

The following shows the rationale for Table 8.2 Correspondence between Security Objectives Policies and IT Security Functional Requirements.

O.IA：Identification and authentication when using

By identifying and authorizing to be the CE in FIA_UID.2 and FIA_UAU.2 respectively, being the operation of valid CE can be confirmed.

By identifying and authorizing to be the administrator in FIA_UID.2 and FIA_UAU.2 respectively, being the operation of valid administrator can be confirmed.

By identifying and authorizing to be the general user who owns his/her BOX in FIA_UID.2 and FIA_UAU.2 respectively, being the operation of valid general user who owns his/her BOX can be confirmed.

In case of the unsuccessful identification and authentication of administrator, CE, and general user who owns his/her BOX, the next authentication trial keeps the administrator, CE, and general user who owns his/her BOX wait for five seconds in FIA_AFL.1, in order to delay the time when the invalid user is successfully identified and authenticated as the administrator, CE, and general user who owns User BOX. The dummy characters (*) corresponding to the number of password characters entered in the password entry area are displayed in FIA_UAU.7 to conceal the password.

In FMT_MTD.1[4], the valid general user who owns the authenticated User BOX is permitted him/her to change the User BOX password of his/her BOX. The change of password makes lower the possibility that the User BOX password entered by the invalid user matches.

When the User BOX password is changed, the User BOX password is checked whether it obeys

the password rules regulated in FIA_SOS.1[1].

The management of password is specified in FMT_SMF.1. The general user who owns the targeted User BOX is maintained in FMT_SMR.1. Their functions are not bypassed with FPT_ RVM.1 and the state of operating are effectively ready in FMT_MOF.1.

Therefore, O.IA can be realized by the correspondent security functional requirements.

O.MANAGE：Provision of the management function

The User BOX is created by registering the User BOX identifier by the administrator in FDP_ ACC.1[2], FDP_ACF.1[2], FMT_MSA.3, and FMT_MSA.1. At the beginning, the use of User BOX is limited because the User BOX password that no one can use is set, however, it becomes possible to use when FMT_MTD.1[3] permits the administrator to change the User BOX password. Thereafter the general user becomes the owner of User BOX by knowing the User BOX identifier of this User BOX. When the User BOX password is registered, it is checked whether it obeys the password rules specified in FIA_SOS.1[1].

FDP_MTD.1 provides the administrator with the function to change and manage the HDD lock password of HDD1 and HDD2, therefore, the unauthorized access of HDD1 and HDD2 can be prevented. This password is checked whether it obeys the rule specified in FDP_SOS.1.

FMT_MTD.1[5] permits the administrator to change his/her own password, therefore, the administrator becomes possible to change his/her own password every a suitable period. When the password of administrator is changed, the password is checked whether it obeys the password rules specified in FIA_SOS.1[2]. The change of password makes lower the possibility that the administrator password entered by the general user matches.

The management of User BOX identifier, User BOX password, HDD1 and HDD2 lock password, is specified in FMT_SMF.1. The administrator, CE, and the general user who owns the targeted User BOX are maintained in FMT_SMR.1. Their functions are not bypassed with FPT_RVM.1.The administrator is permitted to startup and terminate the security function in FMT_MOF.1.

Therefore, O.MANAGE can be realized by the correspondent security functional requirements.

O.CE：Provision of the CE function

The CE can register the administrator password in FMT_MTD.1[1]. By registering the administrator password, the administrator can be registered in the TOE and can start the operation as administrator. The CE can change his/her own password in FMT_MTD.1[2], therefore, the CE becomes possible to change the CE and administrator passwords every a suitable period. The change of password makes lower the possibility that the CE and administrator passwords entered by the general user matches, because the CE and administrator passwords are checked whether they obeys the rule specified in FIA_SOS.1[2].

The management of CE password and administrator password is specified in FMT_SMF.1. The administrator and CE are maintained in FMT_SMR.1. Their functions are not bypassed with FPT_ RVM.1 and the state of operating effectively is ready in FMT_MOF.1.

Therefore, O.CE can be realized by the correspondent security functional requirements.

O.DATAACCESS:**Access limit to the document data**

The access control to User BOX is realized using FDP_ACC.1[1] and FDP_ACF.1[1]. O.DATAACCESS permits the user reception function (subject) to operate for reading the document data in the User BOX owned by the valid general user who owns User BOX. As above mentioned, only the general user who owns the User BOX becomes possible to operate the document data in the User BOX.

The general user who owns the targeted User BOX is maintained in FMT_SMR.1. The management of User BOX identifier is specified in FMT_SMF.1. Their functions are not bypassed with FPT_ RVM.1 and the state of operating is effectively ready in FMT_MOF.1.

Therefore, O.DATAACCESS can be realized by the correspondent security functional requirements.

O.AUDIT:**Record of the audit information**

The necessary audit information is recorded in FAU_GEN.1, with the reliable time stamp in FPT_STM.1. In auditable events, all the events regarding the explicit unauthorized access to “asset to be protected” are selected and the equivalents to “selection: minimum” in FAU_GEN.1 is included. However, the following items that are selected in the minimum are not included.

- FPT_STM.1 : It is not necessary because there is no the function for “change of time”.
- FMT_SMR.1 : It is not necessary because the roles of administrator and CE are fixed.

The audit information is also recorded for “success” in identification and authentication. Therefore, all the events related to access control to “asset to be protected” are recorded.

The area of audit storage is protected in FAU_STG.1. When the area of audit storage is exhausted, overwriting of audit record is executed for the used area of audit information in FAU_ STG.4. The capture of audit information is not bypassed with FPT_ RVM.1 and the state of operating is effectively ready in FMT_MOF.1. As above mentioned, the necessary audit information is stored.

Reading out the audit data by anyone except the administrator is prohibited in FAU_SAR.2. The provision in a form that can interpret the audit record is realized in FAU_SAR.1. As above mentioned, the audit of audit record becomes possible.

Therefore, O.AUDIT can be realized by the correspondent security functional requirements.

OE.HDD：Protection of the HDD

FDP_UID.2[E] and FDP_UAU.2[E] permit the access for only the TOE that HDD1 and HDD2 are successfully identified and authenticated. It prevents the HDD1 and HDD2 from the unauthorized access.

Therefore, OE.HDD can be realized by the correspondent security functional requirements.

8.2.1.3. Adequateness for supporting of security functional requirements - FDP_MTD.1 and FDP_SOS.1 by assurance requirement

FDP_MTD.1 executes only changing “TSF data” of FMT_MTD.1 to “administrator data” and means the same as FMT_MTD.1 “control the security function”. FDP_SOS.1 executes only changing “secret” of FIA_SOS.1 to “secret for IT environment” and means the same as FIA_SOS.1 “validation of secret”.

Therefore, they can apply to the same assurance requirement with FMT_MTD.1 and FIA_SOS.1, namely the present assurance requirement.

8.2.2. TOE Security Functional Requirements Dependency

All of the necessary dependent relationship of TOE security functional requirements is fulfilled as shown in Table 8.3 Dependence Relationship of TOE Security Functional Requirements.

Table 8.3 Dependence Relationship of TOE Security Functional Requirements

No	TOE security functional requirement	Lower level	Dependent	Reference No	Notes
1	FIA_UID.2	FIA_UID.1	None		
2	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	1	As the mediate action of FIA_UID.1 is unnecessary, FIA_UID.2 is used.
3	FIA_UAU.7	None	FIA_UAU.1	2	As the mediate action of FIA_UAU.1 is unnecessary, FIA_UAU.2 is used.
4	FIA_AFL.1	None	FIA_UAU.1	2	As the mediate action of FIA_UAU.1 is unnecessary, FIA_UAU.2 is used.
5	FIA_SOS.1[1]	None	None		
6	FIA_SOS.1[2]	None	None		

7	FDP_SOS.1	None	None		
8	FDP_ACC.1[1]	None	FDP_ACF.1	10	
9	FDP_ACC.1[2]	None	FDP_ACF.1	11	
10	FDP_ACF.1[1]	None	FDP_ACC.1 FMT_MSA.3	8 11	FMT_MSA.3 is fulfilled with dependent relationship of FDP_ACF.1[2] that is access control for the identical object.
11	FDP_ACF.1[2]	None	FDP_ACC.1 FMT_MSA.3	9 23	
12	FAU_GEN.1	None	FPT_STM.1	28	
13	FAU_STG.1	None	FAU_GEN.1	12	
14	FAU_STG.4	FAU_STG.3	FAU_STG.1	13	
15	FAU_SAR.1	None	FAU_GEN.1	12	
16	FAU_SAR.2	None	FAU_SAR.1	15	
17	FMT_MTD.1[1]	None	FMT_SMR.1 FMT_SMF.1	26 25	
18	FMT_MTD.1[2]	None	FMT_SMR.1 FMT_SMF.1	26 25	
19	FMT_MTD.1[3]	None	FMT_SMR.1 FMT_SMF.1	26 25	
20	FMT_MTD.1[4]	None	FMT_SMR.1 FMT_SMF.1	26 25	
21	FMT_MTD.1[5]	None	FMT_SMR.1 FMT_SMF.1	26 25	
22	FMT_MSA.1	None	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	9 26 25	
23	FMT_MSA.3	None	FMT_MSA.1 FMT_SMR.1	22 26	
24	FMT_MOF.1	None	FMT_SMR.1 FMT_SMF.1	26 25	
25	FMT_SMF.1	None	None		
26	FMT_SMR.1	None	FIA_UID.1	2	As the mediate action of

					FIA_UAU.1 is unnecessary, FIA_UAU.2 is used.
27	FPT_RVM.1	None	None		
28	FPT_STM.1	None	None		
29	FDP_MTD.1	None	FMT_SMR.1 FMT_SMF.1	26 25	
30	FIA_UID.2[E]	FIA_UID.1	None		
31	FIA_UAU.2[E]	FIA_UAU.1	FIA_UID.1[E]	30	As the mediate action of FIA_UID.1 is unnecessary, FIA_UID.2 is used.

8.2.3. TOE Security Functional Requirements Interaction

No	TOE security functional requirement	Function that provides defense	
		Detour	Deactivation
1	FIA_UID.2	FPT_RVM.1	FMT_MOF.1
2	FIA_UAU.2	FPT_RVM.1	FMT_MOF.1
3	FIA_UAU.7	FPT_RVM.1	FMT_MOF.1
4	FIA_AFL.1	FPT_RVM.1	FMT_MOF.1
5	FIA_SOS.1[1]	None	FMT_MOF.1
6	FIA_SOS.1[2]	None	FMT_MOF.1
7	FDP_SOS.1	None	FMT_MOF.1
8	FDP_ACC.1[1]	FPT_RVM.1	FMT_MOF.1
9	FDP_ACC.1[2]	FPT_RVM.1	FMT_MOF.1
10	FDP_ACF.1[1]	FPT_RVM.1	FMT_MOF.1
11	FDP_ACF.1[2]	FPT_RVM.1	FMT_MOF.1
12	FAU_GEN.1	FPT_RVM.1	FMT_MOF.1
13	FAU_STG.1	FPT_RVM.1	FMT_MOF.1
14	FAU_STG.4	FPT_RVM.1	FMT_MOF.1
15	FAU_SAR.1	FPT_RVM.1	FMT_MOF.1
16	FAU_SAR.2	FPT_RVM.1	FMT_MOF.1
17	FMT_MTD.1[1]	FPT_RVM.1	FMT_MOF.1
18	FMT_MTD.1[2]	FPT_RVM.1	FMT_MOF.1
19	FMT_MTD.1[3]	FPT_RVM.1	FMT_MOF.1

20	FMT_MTD.1[4]	FPT_RVM.1	FMT_MOF.1
21	FMT_MTD.1[5]	FPT_RVM.1	FMT_MOF.1
22	FMT_MSA.1	FPT_RVM.1	FMT_MOF.1
23	FMT_MSA.3	FPT_RVM.1	FMT_MOF.1
24	FMT_MOF.1	FPT_RVM.1	
25	FMT_SMF.1	None	FMT_MOF.1
26	FMT_SMR.1	None	FMT_MOF.1
27	FPT_RVM.1		FMT_MOF.1
28	FPT_STM.1	None	None
29	FDP_MTD.1	FPT_RVM.1	FMT_MOF.1

<Detour> FPT_RVM.1

When the management function and CE function of the TOE is used, the administrator and CE execute the identification and authentication (FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1).

The document data of User BOX is accessed according to the access control (FDP_ACC.1[1] [2] and FDP_ACF.1[1][2]).

The audit data is always captured. (FAU_GEN.1 and FAU_STG.4)

Only the administrator can refer the audit data.(FAU_SAR.1, FAU_SAR.2, and FAU_STG.1)

Only the user who is applicable to each data can operate the miscellaneous TSF data and administrator data.(FAU_SAR.2, FMT_MTD.1[1]-[5], FMT_MSA.1, FMT_MSA.3, FMT_ MOF.1, and FDP_MTD.1)

The detour is prevented because the avobe mentioned matters are certainly executed in FPT_ RVM.1.

<Deactivation> FMT_MOF.1

The prevention of deactivation in TSF is realized by making the security reinforcement mode to be valid in FMT_MOF.1.

<Falsification>

In this TOE, the access control is only for the User BOX of HDD1.
The unauthorized subject does not exist because the access control to User BOX is limited to the process through the operation panel. Therefore, FPT_SEP.1 is unnecessary because there is no room for the unauthorized subject to enter.

8.2.4. Consistency of Security Function Strength to Security Objectives Policies

This TOE assumes the attack capability of general user to be low level in “2. TOE Description”,

and describes “operate from the operation panel” or “connect unauthorized reading device with HDD” in “3. TOE Security Environment”, namely, the especially highly skilled attacker is not assumed. And it assumes to be operated under the adequate security condition in terms of the physical and human. Therefore, in “5.3. Security Strength”, the security strength claims SOF-Basic that can adequately resist for attacking from the threat agent with the attack capability of low level.

The following shows the operational measures to make this TOE operate in safety.

- The TOE shall be installed in the area where only the product-related person can operate.
- The TOE shall be monitored by the administrator, and as the room TOE installed shall be bolted when the administrator shall be absent, the general user can not enter the room except the administrator.
- The administrator shall set the environment that the data will not disclose from the internal network.
- The administrator shall execute for the general user the instruction and enlightenment to maintain a secure condition of the TOE.
- The responsible person shall appoint and manage a person who does not carry out an illegal act as an administrator.
- The responsible person or administrator shall close the maintenance contract with the CE. It shall be specified a statement that the CE will not carry out an illegal act.

Therefore, the following person is specified as the threat agent.

Attack capability : Low level

As above mentioned, SOF-Basic is proper and consistent as the minimum function strength to security objectives policies because the adequate resistance is taken for the threat agent with the above mentioned attack capacity.

8.2.5. Assurance Requirement Rationale

This TOE is a product of commercial use, and requests the specifications of function and external interface for the TOE, result of developer test, analysis of developer for obvious vulnerability, and analysis of function strength in order to resist the threat with attack capability of low level. Therefore, the level of evaluation assurance is proper for EAL3.

8.3. TOE Summary Specification Rationale

8.3.1. Conformity of Security Functional Requirements to TOE Summary Specification

Table 8.4 shows the relationship of security functional requirements conformed to TOE summary specification.

Table 8.4 Correspondence between IT Security Functions and Security Functional Requirements

IT security function / TOE security functional requirement	IA.ADM_ADD	IA.ADM_AUTH	IA.CE_AUTH	IA.PASS	ACL.USR	AUD.LOG	AUD.MNG	MNG.MODE	MNG.ADM	MNG.HDD
FIA_UID.2		✔	✔		✔					
FIA_UAU.2		✔	✔		✔					
FIA_UAU.7		✔	✔		✔					
FIA_AFL.1		✔	✔		✔					
FIA_SOS.1[1]				✔					✔	
FIA_SOS.1[2]	✔			✔						
FDP_SOS.1										✔
FDP_ACC.1[1]					✔					
FDP_ACC.1[2]									✔	
FDP_ACF.1[1]					✔					
FDP_ACF.1[2]									✔	
FAU_GEN.1						✔				
FAU_STG.1									✔	
FAU_STG.4							✔			
FAU_SAR.1									✔	
FAU_SAR.2									✔	
FMT_MTD.1[1]	✔			✔						

FMT_MTD.1[2]				✔						
FMT_MTD.1[3]				✔						
FMT_MTD.1[4]				✔						
FMT_MTD.1[5]				✔						
FMT_MSA.1									✔	
FMT_MSA.3									✔	
FMT_MOF.1								✔		
FMT_SMF.1	✔			✔					✔	
FMT_SMR.1	✔			✔					✔	
FPT_RVM.1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
FPT_STM.1						✔				
FDP_MTD.1										✔

The following shows the rationale for Table 8.4.

FIA_UID.2

For administrator, the identification of administrator is executed in IA.ADM_AUTH. For CE, the identification of CE is executed in IA.CE_AUTH. For general user who owns User BOX, the identification of general user who owns User BOX is executed in ACL.USR.

Therefore, FIA_UID.2 is realized by implementing IA.ADM_AUTH, IA.CE_AUTH, and ACL.USR.

FIA_UAU.2

For administrator, the authentication of administrator is executed in IA.ADM_AUTH. For CE, the authentication of CE is executed in IA.CE_AUTH. For general user who owns User BOX, the authentication of general user who owns User BOX is executed in ACL.USR.

Therefore, FIA_UAU.2 is realized by implementing IA.ADM_AUTH, IA.CE_AUTH, and ACL.USR.

FIA_UAU.7

When entering the password for the authentication of administrator, CE, and general user who owns User BOX, the entered password is displayed as dummy characters (*) corresponding to the number of characters in IA.ADM_AUTH, IA.CE_AUTH, and ACL.USR respectively.

Therefore, FIA_UAU.7 is realized by implementing IA.ADM_AUTH, IA.CE_AUTH, and ACL.USR.

FIA_SOS.1[1]

For the registration and the change of User BOX password, whether the password is within the coverage of permitted value along the password rules is judged in MNG.ADM and IA.PASS respectively.

Therefore, FIA_SOS.1[1] is realized by implementing MNG.ADM and IA.PASS.

FIA_SOS.1[2]

For the registration of administrator password and the change of administrator/CE password, whether the password is within the coverage of permitted value along the password rules is judged in IA.ADM_ADD and IA.PASS respectively.

Therefore, FIA_SOS.1[2] is realized by implementing IA.ADM_ADD and IA.PASS.

FDP_SOS.1

For the registration of HDD password, FDP_SOS.1 judges whether the password is within the coverage of permitted value along the password rules in MNG_HDD.

Therefore, FDP_SOS.1 is realized by implementing MNG_HDD.

FIA_AFL.1

In case of the unsuccessful authentication, for the administrator, CE, and general user who owns User BOX, the next authentication trial is not executed for five seconds in IA.ADM_AUTH, IA.CE_AUTH, and ACL.USR, to the administrator, CE, and general user who owns User BOX respectively.

Therefore, FIA_AFL.1 is realized by implementing IA.ADM_AUTH, IA.CE_AUTH, and ACL.USR.

FDP_ACC.1[1]

ACL.USR executes to read out the document data according to Access control policy 1.

Therefore, FDP_ACC.1[1] is realized by implementing ACL.USR.

FDP_ACC.1[2]

MNG.ADM creates the User BOX according to Access control policy 2.

Therefore, FDP_ACC.1[2] is realized by implementing MNG.ADM.

FDP_ACF.1[1]

ACL.USR executes to read out the document data according to Access control policy 1.

Therefore, FDP_ACF.1[1] is realized by implementing ACL.USR.

FDP_ACF.1[2]

MNG.ADM creates the User BOX according to Access control policy 2.

Therefore, FDP_ACF.1[2] is realized by implementing MNG.ADM.

FAU_GEN.1

The audit information regarding the operation of security function is recorded in AUD.LOG.

Therefore, FAU_GEN.1 is realized by implementing AUD.LOG.

FAU_STG.1

The function to enable only the administrator to access the data in audit storage area is implemented in MNG.ADM.

Therefore, FAU_STG.1 is realized by implementing MNG.ADM.

FAU_STG.4

When the audit storage area is exhausted, the audit information is overwritten on the used storage area in AUD.MNG.

Therefore, FAU_STG.4 is realized by implementing AUD.MNG.

FAU_SAR.1

The administrator becomes possible to refer the audit record in MNG_ADM.

Therefore, FAU_SAR.1 is realized by implementing MNG_ADM.

FAU_SAR.2

Enabling only the administrator to refer the audit record is set in MNG.ADM.

Therefore, FAU_SAR.2 is realized by implementing MNG.ADM.

FMT_MTD.1[1]

The registration of administrator password is permitted In IA.ADM_ADD and the change of administrator password is executed in IA.PASS by only the CE.

Therefore, FMT_MTD.1[1] is realized by implementing IA.ADM_ADD and IA.PASS.

FMT_MTD.1[2]

In IA.PASS, the change of CE password is permitted and executed by only the CE.

Therefore, FMT_MTD.1[2] is realized by implementing IA.PASS.

FMT_MTD.1[3]

In MNG.ADM, the change of use BOX password is permitted and executed by only the administrator.

Therefore, FMT_MTD.1[3] is realized by implementing MNG.ADM.

FMT_MTD.1[4]

In IA.PASS, the change of User BOX password is permitted and executed by only the general user who owns User BOX.

Therefore, FMT_MTD.1[4] is realized by implementing IA.PASS.

FMT_MTD.1[5]

In IA.PASS, the change of administrator password is permitted and executed by the administrator.

Therefore, FMT_MTD.1[5] is realized by implementing IA.PASS.

FMT_MSA.1

In MNG.ADM, the registration of User BOX identifier is permitted and executed to create the User BOX by only the administrator.

Therefore, FMT_MSA.1 is realized by implementing MNG.ADM.

FMT_MSA.3

In MNG.ADM, the registration of User BOX identifier and the setting of User BOX password to the User BOX, needed for the initialization of User BOX, are permitted and executed by the administrator. The User BOX is created at first in the limited state that nobody can register the User BOX identifier, then the state that the general user can use it by setting the User BOX password.

Therefore, FMT_MSA.3 is realized by implementing MNG.ADM.

FMT_MOF.1

Setting the validity of security functions regulated in this ST is permitted and executed by the administrator in MNG.MODE.

Therefore, FMT_MOF.1 is realized by implementing MNG.MODE.

FMT_SMF.1

The function to manage the administrator password is implemented in IA.ADM_ADD. The function to manage the administrator, CE, and User BOX passwords is implemented in IA.PASS. The function to manage the User BOX is implemented in MNG.ADM.

Therefore, FMT_SMF.1 is realized by implementing IA.ADM_ADD, IA.PASS, and MNG.ADM.

FMT_SMR.1

The maintenance of role is realized by realizing the registration of User BOX identifier and User BOX password, and the change of CE, administrator, and User BOX passwords. The registration of administrator, the registration of general user who owns User BOX, and the change of administrator, CE, User BOX passwords, are implemented in IA.ADM_ADD, MNG.ADM, and IA.PASS respectively. Therefore, FMT_SMR.1 is realized by implementing IA.ADM_ADD, IA.PASS, and MNG.ADM.

FPT_STM.1

The function to create the audit record is realized in AUD.LOG. Therefore, FPT_STM.1 is realized by implementing AUD.LOG.

FDP_MTD.1

The function to enter the HDD lock password is realized in MNG_HDD. Therefore, FDP_MTD.1 is realized by implementing MNG_HDD.

8.3.2. Security Function Strength Rationale

As described in “6.2 Security Function Strength”, SOF-Basic is claimed in the password mechanism of the identification and authentication function (IA.ADM_AUTH, IA_CE_AUTH, ACL_USR, IA_ADM_ADD, and IA.PASS) and management support function (MNG.ADM and MNG_HDD). As described in “5.3 Security Strength”, the minimum function strength claims SOF-Basic to security functional requirements and it is consistent with SOF-Basic claimed in “6.2 Security Function Strength”.

8.3.3. Assurance Measures Rationale

The assurance measures are corresponded to all of the TOE security assurance requirements needed in EAL3 “6.3 Assurance Measures”. The all evidence that TOE security assurance requirements regulated by this ST is covered by the related rules shown in the assurance measures.

Therefore, TOE security assurance requirements in EAL3 can be realized.

8.4. PP Claim Rationale

There is no applicable PP in this ST.