Certification Report

Target of Evaluation

Application date/ID	April 1, 2004 (ITC-4025)
Certification No.	C0017
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japan: #4036 Multi-Function Peripheral Zentai Seigyo Software Overseas: #4036 Multi Function Peripheral Control Software
Version of TOE	Macro System Controller : 4036-10G0-18-00 Network Module : 4036-A0G0-04-00
PP Conformance	None
Conformed Claim	EAL3
TOE Developer	Konica Minolta Business Technologies, Inc.
Evaluation Facility	Japan Electronics and Information Technology Industries Association, Information Technology Security Center

This is to report that the evaluation result for the above TOE is certified as follows.
September 15, 2004

TABUCHI Haruki, Technical Manager
Information Security Certification Office
IT Security Center
Information-Technology Promotion Agency, Japan

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the “General Requirements for IT Security Evaluation Facility”.

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations-0210

Evaluation Result: Pass

"Japan: #4036 Multi Function Peripheral Zentai Seigyo Control Software, Overseas: #4036 Multi Function Peripheral Control Software" has been evaluated in accordance with the provision of the "General Rules for IT Product Security Certification" by Information-Technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “Japan: #4036 Multi Function Peripheral Zentai Seigyo Software, Overseas: #4036 Multi Function Peripheral Control Software” (hereinafter referred to as “the TOE”) conducted by Japan Electronics and Information Technology Industries Association, Information Technology Security Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Konica Minolta Business Technologies, Inc..

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	Japan: #4036 Multi-Function Peripheral Zentai Seigyo Software
	Overseas: #4036 Multi Function Peripheral Control Software
Version:	Macro System Controller : 4036-10G0-18-00
	Network Module : 4036-A0G0-04-00
Developer:	Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

The #4036 Multi Function Peripheral (MFP) is Konica Minolta Business Technologies, Inc. digital MFP comprising copier, printer, and scanner functions that can be selected and/or combined by the user. This product (Japan: #4036 Multi Function Peripheral Zentail Seigyo Software, Overseas: #4036 Multi Function Peripheral Control Software are identical products although the name is different) consists of two components in the control software installed in the MFP: the Macro System Controller and the Network Module. The Macro System Controller is a software component that implements operational control processing from the MFP operation panel, job resource management, job sequence control processing, and other functions. The Network Module is a software component that implements operational control processing from the client PC. The security functions of this product protect against the exposure of the highly confidential documents that is spooled in the MFP when using certain specific functions of the MFP. The certain specific functions are as follows

- Secure Print Function

  This function allows a password to be set on the client PC and sent to the MFP as print data in the print standby state. This function will then only print that data when a password is entered from the MFP operating panel and the passwords match.

- Box Functions

  This function controls access to a “box” that is set up as a temporary storage area for scan data.

- Memory Recall Off Copy Function

  Normally, when a document is copied, the copy data is retained after printing so that the document can be printed again. This function automatically deletes that data after printing.

Figure 1-1 shows the environment in which the MFP is expected to be used.

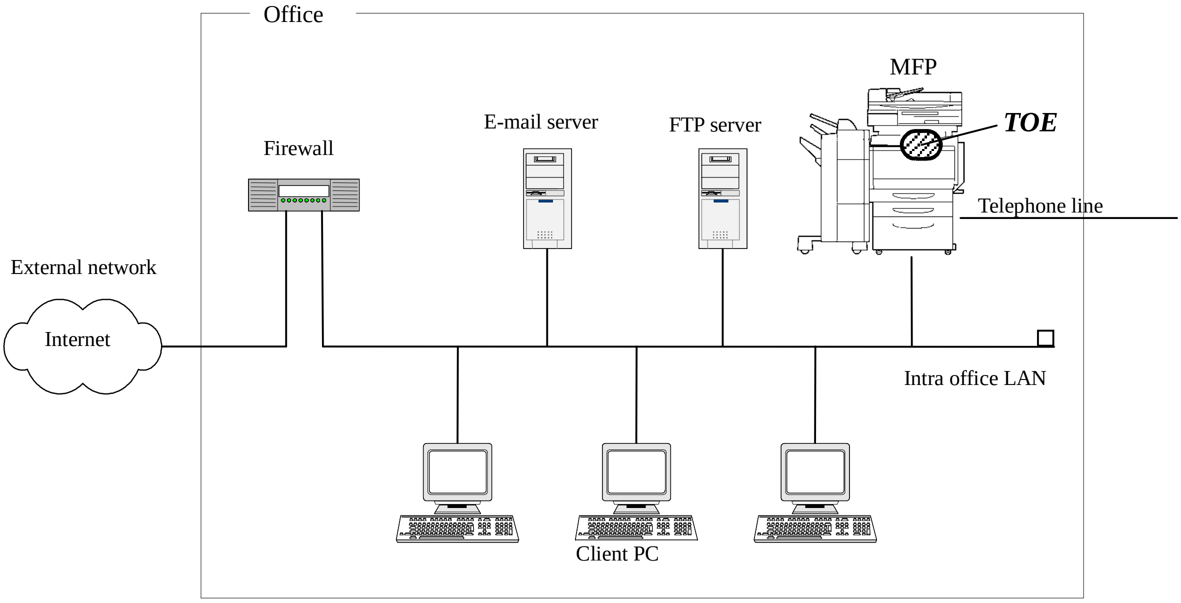

Figure 1-1 Example of Expected MFP Usage Environment

As shown in the figure above, the MFP is installed in a general office. An operations control system that allows only personnel concerned with use, operation, and maintenance of the MFP, is implemented in the office. An intra-office LAN is present as the office internal network. The MFP connects to the client PCs via the intra-office LAN, and had mutual data communication. If email and/or FTP servers are connected to the intra-office LAN, the MFP will also be capable of using them for data communication. If the intra-office LAN is connected to an external network, techniques such as connection through a firewall will be adopted and appropriate settings made to block access requests to the MFP from the external network. Furthermore, the intra-office LAN will be equipped with a network environment such that data communication between the MFP and the client PCs cannot be tapped or intercepted by the usage of switching hub etc. and the office operation. The MFP is connected to a telephone line for communication with the support center that performs maintenance for the MFP.

Also, the installed hard disk drive provides a HDD lock function (detects unsuccessful attempts at password entry and that locks the password function after a fixed number of unsuccessful password matches). This protects against unauthorized access and assures confidentiality even if the hard disk drive is stolen.

1.2.3 Scope of TOE and Overview of Operation

The "Macro System Controller" and the "Network Module", which are the TOE, run under the OS (VxWorks) that runs on the MFP controller inside the MFP itself and are integrated with the other MFP control software components. Figure 1-2 shows the structure of these MFP control software components. The physical area of the TOE is shown by the shaded area in the figure.

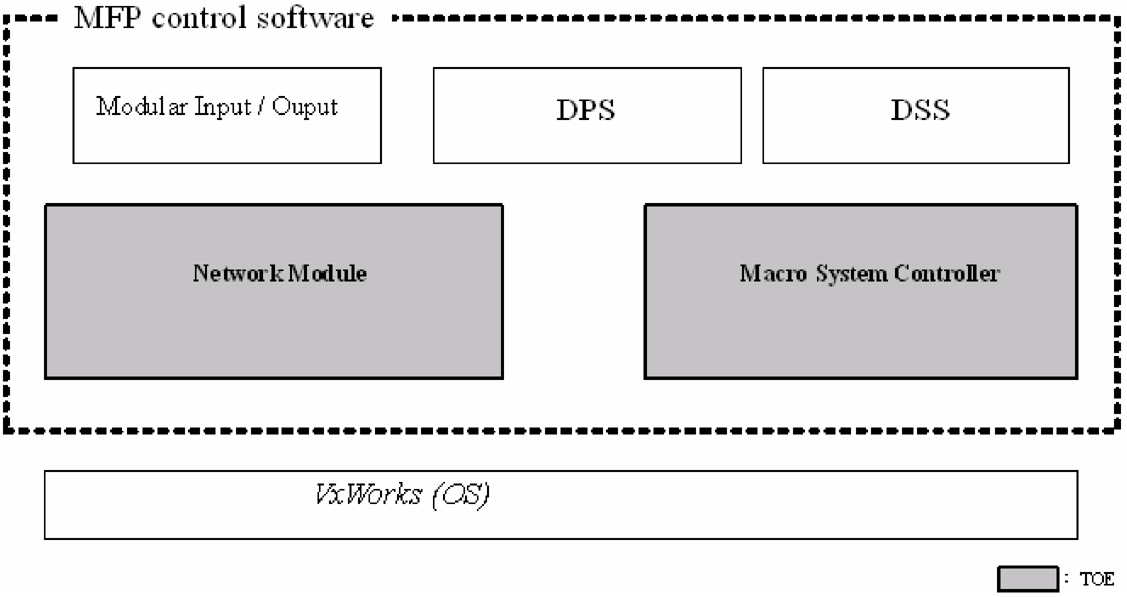

Figure 1-2 Structure of the MFP Control Software Components

The following describes an overview of the operations for which the TOE is responsible.

- Macro System Controller (MSC)

  This module registers the acquired image data as a job and manages job resources, startup, and sequencing. This module processes the information input with the LCD, LED, keys, and other controls on the MFP operations panel, and sends notifications to other components according to that processing. This module also processes messages from other software components and sends notifications to those other software components. It also displays information on the MFP operations panel.

- Network Module (NM)

This module is a software component that performs processing and control operations after data received by the “Modular Input Output” from the network for operation requests from client PCs. This module requests the processing to “VxWorks” and the “Macro System Controller” according to the process. This module also receives data processed by “VxWorks” and the “Macro System Controller” and requests the processing to the “Modular Input Output”.

The “Macro System Controller” and the “Network Module”, which are the TOE, are related to the other MFP control software components and operating system as shown in figure 1-3.

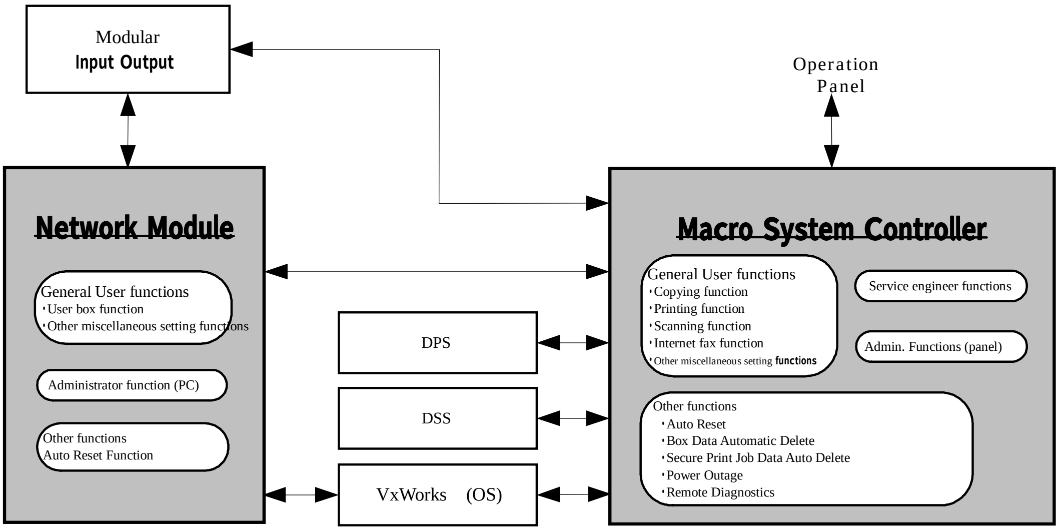

Figure 1-3 MFP Control Software Components Related to TOE Operation and Processing

1.2.4 TOE Functionality

General users and administrators use the variety of functions provided by the MFP in which the TOE is loaded from either a client PC or the operation panel of the MFP. Service engineers can use the service engineer functions from the operation panel of the MFP. The following sections describe the general user functions used by general users and administrators, the administrator functions (administrator functions (panel) and administrator functions (PC)) used in administrator mode that can only be used by administrators, and the service engineer functions provided for service engineers. Note that "general users" refers to MFP users who have permission to enter the room in the office where the MFP is installed.

1.2.4.1 General User Functions

(1) Copy Function

The function is invoked from the MFP operations panel and first acquire image data in volatile memory by scanning the document and then print that image data.

1. Memory Recall Copy

   This is a copy function that, when a copy operation is performed, retains the copy job information data as a printable job after printing has completed, thus allowing the same job to be reprinted as many times as desired.

2. Memory Recall Off Copy

   This is a copy function that automatically deletes the copy job information data after printing has completed. This function can be used in two ways; either the user can explicitly specify automatic deletion or the administrator can set up automatic deletion that does not depend on user settings.

3. Scan to Memory (Copy function)

   This is a function that activates the print standby state when a copy is performed with scan to memory selected. This function is used when it prints a job together with other jobs by the Job Bind Function (described later). Note that no special access restrictions are implemented for operations that would result in printing a job that has been set to the print standby state.

(2) Print Function

Users can print from the MFP by using a printer driver on a client PC to send the print data to the MFP. The MFP stores the data in volatile memory and prints that data. The print functions support the following printing methods.

1. Normal Print

   This printing function prints the print data received and stored in the MFP memory without modification.

2. Reprint

   When "Reprint" is specified on the client PC, this printing function saves the print data in memory even after printing of that data has completed. This allows that data to be reprinted, or for the user to modify the print quality or other settings and to reprint the data as many times as desired. There are no special access restrictions implemented for these print execution operations.

3. Secure Print

When printing highly confidential documents, the user can specify “Secure” in the printer driver on the client PC. The user then specifies a password and sends the print data to the MFP. When this print data is received at the TOE, it is registered as secure print job data and enters the print standby state. The TOE compares the password entered at the MFP operations panel with the password in the secure print job information and, if the passwords match, clears the print standby state and prints the data. The information data for a secure print job is automatically deleted when printing completes.

4. HDD Storage Print

This function saves the print job information data on the MFP hard disk. This data can be printed from the MFP operations panel. There are no special access restrictions implemented for these print execution operations.

(3) Job Bind Function

This function allows the user to select jobs in the print standby state that were created by the Memory Recall Copy or Reprint Function, to specify a sequence, and to print those jobs as a single job. The TOE accepts and processes the job selection and print execution operations for this Job Bind Function.

(4) Scan Function

The scan function is executed from the MFP operations panel and acquires an image of a document as data. The MFP provides methods for sending by email or FTP the image data stored in volatile memory, and these methods can be used in conjunction with the scan function. The scan data can also be stored in a “box” in the hard disk installed in the MFP without transmitting that data outside the MFP.

(5) Internet Fax Function

This function receives and prints Internet faxes (email with an attached image in a stipulated format). This function can also transmit image data acquired by the MFP scanning function as email with an attachment in the stipulated compressed image format as Internet faxes.

(6) Box Function

This function allows the user to create (and specify names and passwords for) “boxes” on the hard disk from a web browser running on a client PC. These boxes are storage areas for scanned image data. The box function provides the following operations from the client PC browser on boxes that hold image data (“box data”).

- Download box data to the client PC
- Delete box data
- Delete boxes
- Change box settings (change of the box name or password)

The following operations are also provided from the MFP operations panel on scanned data stored in boxes.

- E-mail transmission of box data to a client PC

- FTP transmission of box data to a client PC
- Change the name of a box data
- Delete box data

In addition, the following operations for boxes are provided from client PCs using a dedicated application (box utility).

- Preview (display) box data
- List (with thumbnails) box data
- Download box data to the client PC
- Change the name of a box data
- Delete box data

(7) Other Setting Functions

In addition to the functions described in items (1) to (6) above, the MFP also provides other functions that can be used by general users, including functions used from the MFP operations panel for paper selection, image quality selection, and magnification to be used in printing. Other functions accessible using a web-browser on a client PC include functions for viewing the MFP system status (device configuration, overview), viewing the status of jobs on the MFP, and the transmission method for the scan function and setting of destination etc.

1.2.4.2 Administrator Functions

The TOE provides management functions (administrator functions) that can be used in administrator mode, which is only accessible by administrators, for supervising the general user functions. The following are descriptions for two categories: the administrator functions (panel) that can be accessed from the MFP operations panel, and the administrator functions (PC) that can be accessed from the client PC. This section also describes the administrator functions (box utility), which are the administrator functions that can be accessed from the box utility, which is a dedicated application that runs on a client PC.

(1) Panel Administrator Functions

- Function to change the administrator mode password
- Function to set the operation of the unauthorized access lock functions
- Access Lock Release Function (This function clears to 0 the unauthorized access detection count values for secure printing and box function.)
- Function to set the operation of the Auto Reset Function (see section 1.2.4.4 later in this document)
- Function to set the operation of the HDD lock function
- Function to set the SMTP and FTP servers
- Function to set the Memory Recall Settings Data
- Function to set various administrator settings (secure print job information data storage period settings, network settings, copy count limit settings, date and time

settings, and other settings)

(2) PC Administrator Functions

- Function to delete box data
- Function to delete boxes
- Function to change box settings (change of the box name or password)
- Function to set the operation of the Auto Reset Function
- Function to set the SMTP and FTP servers
- Function to set the Memory Recall Settings Data
- Function to set various administrator settings (box data storage period settings, secure print job data storage period settings, network settings, copy count limit settings, date and time settings, and other settings)

(3) Box Utility Administrator Functions

- Function to backup box data
- Function to restore box data from backup

1.2.4.3 Service Engineer Functions

The TOE also provides management functions (service engineer functions) for general user function and administrator functions in service mode that can only be operated by a service engineer from the operations panel of the MFP. These functions are listed below.

- Function to display the ROM version
- Function to initialize the administrator mode password
- Function to change the service code (the service engineer password)
- Function to set various service engineer settings (operation setting function for each setting function provided for general users, counter settings for the number of pages to be printed, verification of functions and operations, sensor checks, HDD installation settings, HDD formatting, and other functions)

1.2.4.4 Other Functions

In addition to the functions that are operated by direct operation by general users, administrators, and service engineers, there are also functions that the TOE operates autonomously according to the settings of each user. This section describes a few representative examples of these functions.

(1) Auto Reset Function

This function automatically resets the MFP to its basic screen when the state in which no operations are invoked continues and a set period elapses. This operation occurs during access from the MFP operations panel and during access from client PCs in administrator mode. The administrator sets the time until this function activates (the Auto Reset Setting Data).

(2) Box Data Automatic Deletion Function

This function deletes box data for which the set storage period has elapsed. The administrator sets the data storage period.

(3) Secure Print Automatic Deletion Function

This function deletes secure print job data for which the set storage period has elapsed. The administrator sets the data storage period.

(4) Power Save Function

Following functions automatically adjust the print engine fuser heater temperature and reduce power consumption when the state in which no operations are invoked continues and a set period elapses. When this function operates, jobs registered in the print standby state are deleted. General users can set the time until this function operates.

- Preheat function: Lowers the print engine fuser heater temperature.
- Sleep function: Turns off the print engine fuser heater.

(5) Remote Diagnostic Functions

These functions accept access requests from the support center and transmit information including the number of times problems occurred in the MFP, values that indicate the degree of depletion of consumable items, and the print count value to the support center. These functions also automatically access the support center and transmit MFP failure status information when certain failures (major faults) occur. These functions use both email and the telephone line to send and receive data.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as “Guidance for IT Security Certification Application, etc.”[2], “General Requirements for IT Security Evaluation Facility”[3] and “General Requirements for Sponsors and Registrants of IT Security Certification”[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined “#4036 Multi Function Peripheral Control Software Security Target Version 1.07” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in “#4036 Multi Function Peripheral Control Software Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”)[22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations[20] and [21].

1.4 Certificate of Evaluation

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those problems found in the certification process. Evaluation is completed with the Evaluation Technical Report dated August, 2004 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function.
This TOE is operated under conditions where adequate physical and personnel security conditions are assured. Therefore the threat agent can be specified as low-level personnel. Accordingly, the “SOF-basic,” which is a level that can counteract against a low-level attack potential can fulfill the condition.

1.5.4 Security Functions

Security functions of the TOE are as follow.

(1) Security Functions for General User Function

- Remaining Copy Data Protection Function provided by the Memory Recall Off Setting

  This function automatically deletes the copy job information and data acquired by using the copy function when the memory recall copy function is turned off in the administrator functions.

- Identification and Authentication Function to allow a general user access to a secure print job

  This function identifies and authenticates a general user as the valid user of the secure print job information data when a user prints that secure print job information data. If authentication fails three times, this function locks the corresponding secure print job information data and access is denied. If authentication succeeds, printing of the corresponding secure print job information data is started.

- Box Creation Function

  General users use this function to specify a name and create a box.

- Identification and Authentication, and Access Control Function to allow a general user access to a box

  This function identifies and authenticates a general user as the valid user of a user box when the user accesses the corresponding user box. If authentication fails three times, this function locks the corresponding user box and access is denied.

  If authentication succeeds, downloading of all of the box data in the box is allowed. (Note that this security function does not apply to user boxes that are specified to be "Public.")

- Box management functions for general users for whom access is allowed

  This function is used to change the settings (name and password) of a box by a general user who is the valid user of the corresponding box.

(2) Security functions for the administrator function

- Identification and Authentication Function to allow access to administrator mode

  - This function identifies and authenticates an administrator when accessing administrator mode from either the MFP operations panel or a web browser on a client PC. If authentication fails three times, this function locks and access is denied.

- This function authenticates an administrator when executing the box data backup function or restore function using the box utility from a client PC. If authentication fails three times, this function locks and access is denied.

➢ Security related functions in administrator mode

The following functions can be operated from the MFP operations panel in administrator mode.

- Function to change the administrator mode password
- Function to set the operation of the unauthorized access lock functions
- Access Lock Release Function
- Function to set the operation of the Auto Reset Function
- Function to set the SMTP and FTP servers
- Function to set the Memory Recall Settings Data

The following functions can be operated from a client PC in administrator mode.

- Function to change box settings (modify the box name or password)
- Function to set the operation of the Auto Reset Function
- Function to set the SMTP and FTP servers
- Function to set the Memory Recall Settings Data

(3) Security functions for the service engineer functions

➢ Identification and authentication function to allow access to service mode

This function authenticates and identifies the user as a service engineer when accessing service mode. If authentication fails three times, this function locks the system and access is denied.

➢ Security related functions in the service engineer functions

The following functions can be operated in service mode.

- Function to initialize the administrator mode password
- Function to change the service code

(4) Security functions for other functions

➢ Auto Reset Function

This function cancels access permission if a fixed period elapses with no operation being performed. (The MFP operations panel returns to the basic screen or, if connecting from a client PC, the connection is terminated.) This function is effective as a supplemental security function for cases where the operator leaves their station inadvertently during administrator mode access.

1.5.5 Threat

This TOE assumes such threats presented in Table 1-1 and provides functions for countermeasure to them.

Table 1-1 Assumed Threats

Identifier	Threat
T.ACCESS-SECURE-PRINT	Unauthorized operation of secure print job data: Unauthorized exposure of secure print job information data when a malicious general user accesses secure print job information data from the MFP operations panel and prints another general user’s secure print job data.
T.ACCESS-BOX	Unauthorized operation of box data: ・ Unauthorized disclosure of box data when a malicious general user accesses a created box from a client PC and downloads, previews, or views as thumbnails box data of a box used by another general user. ・ Unauthorized disclosure of box data when a malicious general user accesses a created box from the MFP operations panel and transmits by email or FTP box data of a box used by another general user. ・ Unauthorized disclosure of box data when a malicious general user accesses a created box from a client PC and backs up that box data. Unauthorized falsification of box data when a malicious general user restores backed up box data from a client PC.
T.ACCESS-COPY-DATA	Unauthorized operation of remaining copy job information data: Unauthorized disclosure of copy job information data when a malicious general user accesses and reprints copy job information data from the MFP operations panel.
T.SEND-BOX-DATA	Transmission of box data to a recipient that was not expected: ・ Transmission of box data to recipients not intended by the general user and disclosure of box data when a malicious general user changes the SMTP or FTP server settings used by the MFP by accessing those settings from the MFP operations panel. Transmission and of box data to recipients not intended by the general user and disclosure of box data when a malicious general user changes the SMTP or FTP server settings used by the MFP by accessing those settings from a client PC.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-2.

Table 1-2 Organisational Security Policy

Identifier	Organizational Security Policy
P.BEHAVIOR-FUNCTION	Functions to set the operation of the security functions: ・ For operational convenience, it is possible to disable the unauthorized access prevention functions in a secure environment. ・ For operational convenience, it is possible to operate the memory recall copy function in a secure environment.

1.5.7 Configuration Requirements

The present TOE is a software product installed in #4036 Multi Function Peripheral, which is provided by Konica Minolta Business Technologies, Inc.
#4036 Multi Function Peripheral is a Multi Function Peripheral provided to consumers as under the product names ”bizhub C350”, “CF2203”, and “8022”.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	Personnel conditions for administrators: Administrators must be persons who bear no malice related to the work they are allowed to perform in carrying out their duties.
A.AUTH	Operation conditions for Password: Passwords used during use of the TOE must be managed so that they are not leaked or revealed by anyone who has one or more of these passwords.
A.HDD	Requirements on the hardware environment in which the MFP is used: ・ Only HDD that have a lock function can be used in an MFP that includes this TOE. ・ Passwords used with the HDD lock function must not be leaked or revealed by anyone who has one or more of these passwords.
A.NETWORK	Network connection conditions for MFP: ・ The organization that uses an MFP that includes this TOE must construct a network environment for the intra-office LAN that cannot be tapped or intercepted. ・ If the intra-office LAN in which an MFP that includes this TOE is used is connected to an external network, it must be impossible to access the MFP from the external network.
A.PHYSICAL	MFP installation conditions: ・ An MFP that includes this TOE must be installed in a location that is physically protected so that only general users, administrators, and service engineers can enter.
A.SERVICE	Personnel conditions for Service engineer:

	Service engineers must be persons who bear no malice related to the work they are allowed to perform in carrying out their duties related to TOE installation or MFP maintenance.
A.SETTING	Operational setting conditions on the security function: Users of this TOE must use the TOE in the state where the unauthorized access prevention function is operating.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- Japanese Version

  <Document for Service engineer>

  - bizhub C350 Service Manual [Security Functions], Version 1.30, June 2004
  - Installation Checklist, Version 1.04

  <Document for Administrator and general user>

  - bizhub C350 User's Guide [Security Functions], Version 1.05, May 2004

- Overseas Version

  <Document for Service engineer>

  - bizhub C350/CF2203/8022 Service Manual [Security Functions], Version 1.10, June 2004
  - Installation Checklist, Version 1.04

  <Document for Administrator and general user>

  - bizhub C350 User's Guide [Security Functions], Version 1.05, June 2004
  - CF2203 User's Guide [Security Functions], Version 1.05, June 2004
  - 8022 User's Guide [Security Functions], Version 1.05, June 2004

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM Part 2.

2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on April, 2004 and concluded by completion the Evaluation Technical Report dated August, 2004. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on June, 2004 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on June, 2004.

Problems found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These problems were reviewed by developer and all problems were solved eventually.

As for problem indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the developer is showed in the Table 2-1.

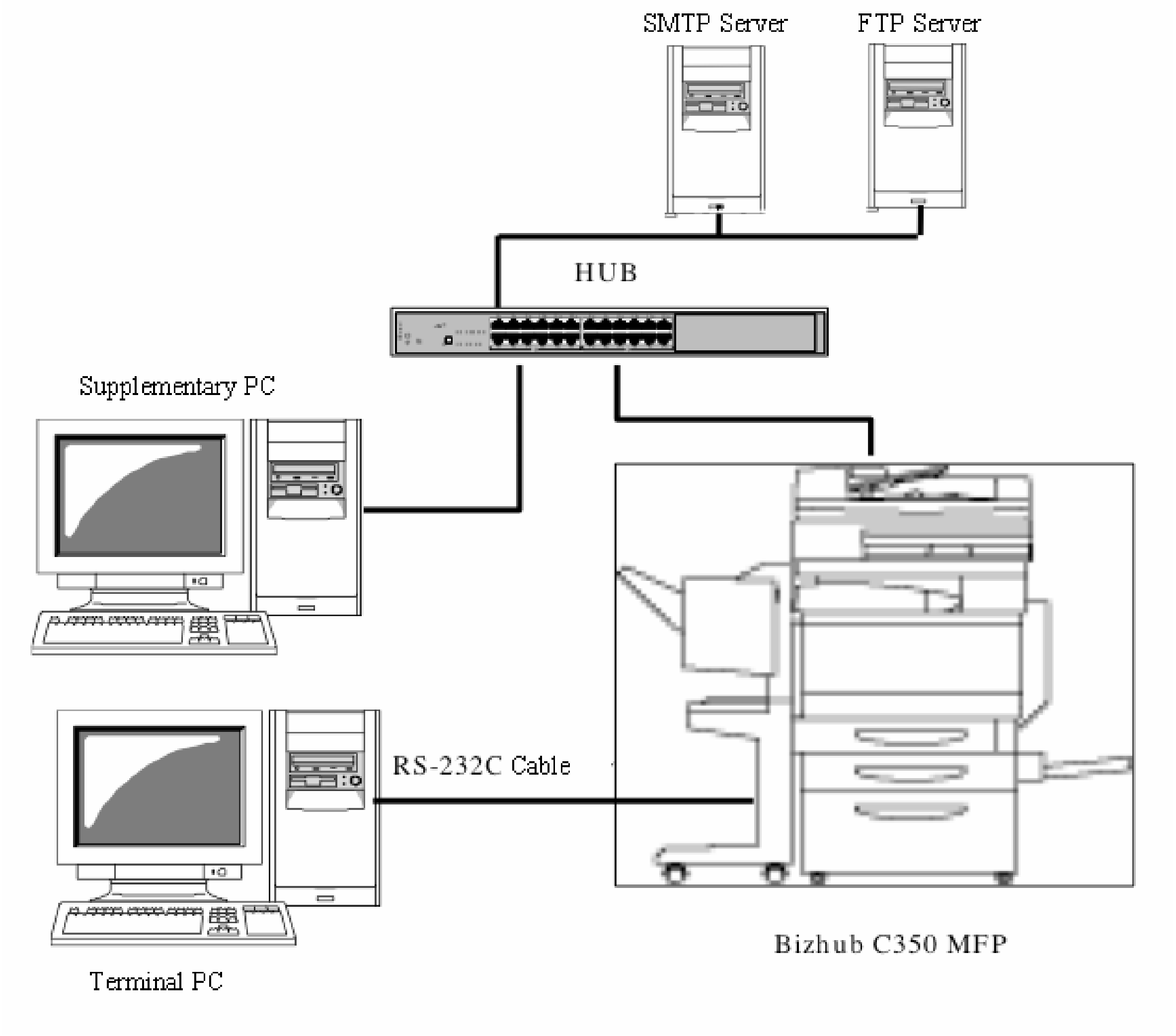

Figure 2-1 Configuration of Developer Test System

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

Test configuration performed by the developer is showed in the Figure 2-1. Developer testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

(1) Test items were set so that they covered all security functions (the security functions for the general user functions, the security functions for the administrator functions, the security functions for the service engineer functions, and the Auto Reset Function).

(2) The behavior of the external interface was checked visually by applying stimuli

(parameters) from the external interface by operating the MFP from the MFP operations panel or from a client PC.

(3) To improve the reliability of the test results, in addition to visual observation of the behavior of the external interface, the test results were verified from the debugging output (log output) for aspects of the interface whose results cannot be verified visually.

c. Scope of Testing Performed

Testing is performed about 29 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

d. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator is showed in the Figure 2-1. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

(1) Test items were set so that they covered all security functions.

(2) The behavior of the external interface was checked visually by applying stimuli (parameters) from the external interface by operating the MFP from the MFP operations panel or from a client PC.

(3) To improve the reliability of the test results, in addition to visual observation of the behavior of the external interface, the test results were verified from the

debugging output (log output) for aspects of the interface whose results cannot be verified visually.

c. Scope of Testing Performed

Total of 32 items of testing; namely 3 items from testing devised by the evaluator and 29 items from testing from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

(1) For the testing devised by the evaluator, the results of developer testing to doubt that a security function operates as specified.

(2) All tests related to security functions performed by the developer were selected as the sampled tests.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Problems found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such problems pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The glossaries used in this report are listed below.

Secure Print: A form of printing when printing from a client PC. When a password is set by the printer driver on a client PC, and printing data is transmitted to MFP, the printing is not executed but rather is queued in standby condition at the MFP. When a set password is entered at the MFP, the standby condition is cancelled and printing is executed.

Secure print job information data:
Print data received by the MFP for secure print. This ST handles this as a protected asset.

Job ID: A control number assigned at the MFP to all jobs in a series, starting with secure print jobs.

Box: A directory set as a storage area in the MFP for scanned image data when the HDD is loaded. Individual users can set the name and password only from a client PC. The box indicated as “Public” is shared, so a password cannot be set. A name change cannot be carried out either.

Box Identifier: A name set to the box.

Box Data: Image data stored in the box. The ST handles this as a protective asset.

Box Password: A password set for the individual box. 95 ASCII codes can be used.

Box Utility: A dedicated application for accessing boxes from a client PC. Using this application enables preview display, box data back up by administrator operation, and the restore operation.

Memory Recall Copy/Memory Recall Off Copy:
The Copy Function that is always available for reprint after executing printing of a copy is called Memory Recall Copy. On the other hand, the function automatically deleting image data of a scanned document after printing is called Memory Recall Off Copy.

Copy Job Information Data File:
Image data scanned into the MFP for use by the Copy Function. This ST handles copy job information data set by Memory Recall Off as protected assets.

Memory Recall Setting Data:
Data sets active/inactive status for Memory Recall Copy. Administrators make this setting. When this data is set to OFF, the Memory Recall On Copy/Memory Recall Off Copy selection function offered to the user is no longer offered to the general user. When a copy is executed, the Copy Function operates as Memory Recall Off Copy that automatically deletes the image data of the scanned documents after printing.

SMTP Server Setting Data File:
Setting information data files that are related to SMTP server installed in the required MFP environment for transmission of Box data as e-mail. Registration in MFP is required, and secondary asset classification is used for protection of Box data.

FTP Server Setting Data File:
Setting information data files that are related to FTP server installed in the required MFP environment for transmission of Box data to the FTP server. Registration in MFP is required, and secondary asset classification is used for protection of Box data.

Administrator Mode:
Functions that are provided for authenticated administrators only.

Administrator Mode Password:
Passwords set for the administrator mode. Eight-digit numbers can be set.

Service Mode: Functions that are provided for authenticated service engineers only.

Service Code: Passwords that are set for the service mode. Eight-digit numbers and “*” and “#” can be used.

Unauthorized Access Lock Function:

A function for which the operation setting is managed by the administrator. When this function is valid, the box authentication function operates and a series of unsuccessful authentication attempts is detected for each of the authentication functions for the administrator function, secure Print Function and Box Function, and depending on the number of unsuccessful authentications, it locks each authentication function.

Unauthorized Box Access Detection Count value:

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the box authentication function while the Unauthorized Access Lock Function is operating.

Unauthorized Secure Print Access Detection Count value:

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the secure print authentication function while the Unauthorized Access Lock Function is operating.

Unauthorized Administrator Mode Access Detection Count value:

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the administrator authentication function while the Unauthorized Access Lock Function is operating.

Unauthorized Service Engineer Access Detection Count value:

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the service engineer authentication function. Unlike other unauthorized access detection count values, it does not rely on the operational setting of the Unauthorized Access Lock Function.

Access Lock Release Function:

A function that clears the unauthorized access detection count value for a box and the unauthorized access detection count value for secure print to zero. When the authentication function for a box and secure print are locked, execution of this function unlocks them.

HDD Lock Function:

Security function that is implemented in the HDD used by MFP. A password for accessing the HDD (HDD lock password) can be set, and when this function is used, the authentication function using the HDD lock password operates. Access is not allowed unless the HDD is verified as the MFP. In addition, if the prescribed number of unsuccessful attempts is detected, the authentication function is locked thereafter, and access is completely prohibited.

Auto Reset Function:

This function returns to the basic screen at starting of power if access is by the MFP operation panel, when no operation has been detected within the prescribed period. The function intercepts the connection if it’s an access to administrator mode from a client PC.

Auto Reset Operational Settings Data:

Time data-enabling setting of Auto Reset Function operations. Can be set to “No limit” or in 1 min increments from 1 to 9 minutes. For administrator mode access from a client PC, operations by time are shown in Table 1.

6. Bibliography

[1] #4036 Multi Function Peripheral Control Software Security Target Version 1.07 August 5, 2004) Konica Minolta Business Technologies, Inc.

[2] Guidance for IT Security Certification Application, etc. April 2004, Information-Technology Promotion Agency, ITQM-23 (Revised on November 5, 2004)

[3] General Requirements for IT Security Evaluation Facility, April 2004, Information-Technology Promotion Agency, ITQM-07

[4] General Requirements for Sponsors and Registrants of IT Security Certification, April 2004, Information-Technology Promotion Agency, ITQM-08 (Revised on November 5, 2004)

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)

[11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model JIS

[12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999 - Information technology - Security techniques – Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model

[15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999

[18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999 (Translation Version 1.0 February 2001)

[19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation

[20] CCIMB Interpretations-0210 (February 2002)

[21] CCIMB Interpretations-0210 (February 2002) (Translation Version 1.0 October 2002)

[22] #4036 Multi Function Peripheral Control Software Evaluation Technical Report Version 1.02, August 27, 2004, Japan Electronics and Information Technology Industries Association, Information Technology Security Center