Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-08-29 (ITC-7167)
Certification No.	C0149
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japanese Name: magicolor 8650 Control Software English Name: magicolor 8650 Control Software
Version of TOE	A02E0Y0-0100-GP0-12
PP Conformance	None
Conformed Claim	EAL3
Developer	Konica Minolta Business Technologies, Inc.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2008-03-26

Hideji Suzuki, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"Japanese Name: magicolor 8650 Control Software English Name: magicolor 8650 Control Software" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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 "Japanese Name:magicolor 8650 Control Software English Name:magicolor 8650 Control Software Version: A02E0Y0-0100-GP0-12" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (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:	Japanese name:magicolor 8650 Seigyo Software English name:magicolor 8650 Control Software
Version:	A02E0Y0-0100-GP0-12
Developer:	Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

This TOE is the embedded software that is installed on the Konica Minolta Business Technologies, Inc. network printer (magicolor 8650) (Hereinafter referred to as"printer").

This TOE offers the protection from exposure of the highly confidential document stored in the printer. Moreover, TOE can encrypt the image data written in HDD for the danger of taking HDD that is the medium that stores the image data in printer out illegally by installing the encryption board which is the option parts of printer. Besides, TOE has the deletion method to follow various overwrite deletion standards. It deletes all the data of HDD completely and it contributes to the prevention of the divulging information of the organization that uses printer by using the method at the time of abandonment or the lease returns.

1.2.3 Scope of TOE and Overview of Operation

This TOE exists on the flash memory on the printer controller, which built in the body of the printer, and is loaded on the RAM. Figure 1-1 shows the relationship between this TOE and the printer. Shaded region on the figure 1-1 indicates the TOE and "*" shows the option parts of printer.

Flash memory is the storage medium that stores the object code of the printer Control Software that is TOE. It also stores the message data of each country's language to display the response accessed through the panel and network, OS (VxWorks), and so on.

NVRAM is the nonvolatile memory that stores various setting values needed for the operation of the printer used for processing of TOE. On the encryption board, the hardware-based cryptographic function, which is the integrated circuit for encryption, is installed in order to encipher all data to be written in HDD.

HDD is utilized besides the image data is stored as a file, temporarily image data with such as extension conversion. As a feature function, the security function (HDD lock function) is installed, being possible to set the password and not being possible to read and write unless it agrees to the password.

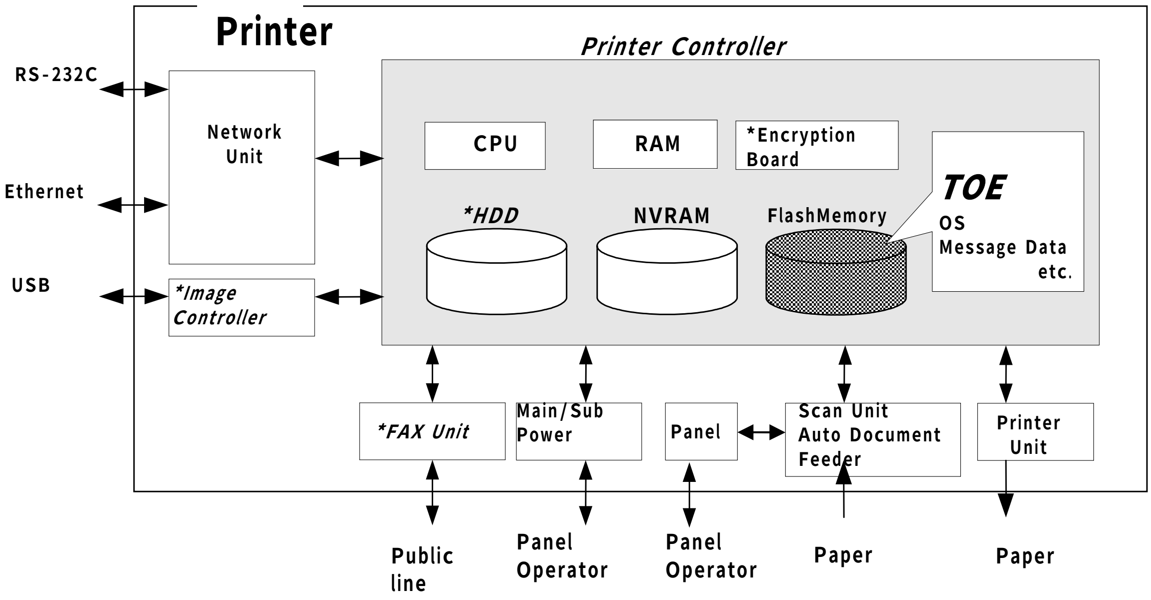

Figure 1-1: Hardware structure that relates to TOE

Next, the logical structure of this TOE is shown. Network printer includes the function that is not associated with the security directly such as basic function, user choice function, and remote diagnosis function other than the function that is indicated in “1.2.4 TOE functionality”.

Basic function is a print function and TOE performs the core control in the operation of these functions.

Remote diagnosis function is used for managing the operation status of printer, and the device information like the number of prints by using the methods for the connection, such as the modem connection via a RS-232C and the E-Mail, etc, and communicating with the support center of printer produced by Konica Minolta business technologies, Inc.

Printer user who can use these functions uses each function that TOE provides, via the panel or the network.

The roles of the person that relate to the use of the printer are defined as follows.

1) User

Printer user (In general, the employee in the office is assumed.)

2) Administrator

Printer's user who carries out the management of the operation of printer. An administrator performs the operation management of printer and the management of user. (In general, it is assumed that the person elected from the employees in the office plays this role.)

3) Service Engineer

A user who performs management of maintenance for the printer. Service Engineer performs the repair and adjustment of printer. (In general, the person in charge at the sales companies that performs the maintenance service of printer and is in cooperation with Konica Minolta Business Technologies, Inc. is assumed.)

4) Person in charge at the Organization that uses the printer

A person in charge at the organization that manages the office where the printer is installed. This person assigns an administrator who carries out the management of the operation of the printer.

5) Person in charge at the Organization that manages the Maintenance of the printer

A person in charge at the organization that carries out management of the maintenance for the printer. This person assigns service engineers who perform the maintenance management for the printer.

Besides this, though not a user of TOE, a person who goes in and out in the office are assumed as an accessible person to TOE.

1.2.4 TOE Functionality

This TOE has the following functions.

1) Secure Print Function

When the secure print password is received with the printing data, the image data is stored as the standby status. And the print command and password input from the panel allows printing.

2) User Box Function

The directory named a use box can be created as an area to store the image file in HDD. Three types of user box exist; the first is the personal user box which a user possesses, the second is the public user box which the registered user making a group within a certain number uses jointly and the third is the group box which the users belong to same account uses jointly. As for the personal user box, the operation is limited only for the user who owns it, the public user box performs access control by sharing a password set to the user box among users and group box, the operation is limited only for the user who the use of the account is permitted. This TOE treats the processing related to public user box as an object of a security function in user box function.

TOE processes the operation for an operation requests that is transmitted from the panel or the network unit through a network from a client PC.

3) Administrator Function

TOE provides the functions such as the management of the user boxes, the management of various settings of the network and image quality, and the management of user information at the time of machine authentication in the administrator mode that only authenticated administrator can operate. Also, it offers the operation setting function related to the behavior of the other function. It deletes the various setting values and the data stored by user.

4) Service Engineer Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate.

5) Encryption key generation function

When the encryption board, an optional product, is installed in printer controller, the encoding and decoding is processed on the encryption board due to the reading and writing data in HDD. (TOE does not process the encryption and description itself.)

The operation setting of this function is performed by the administrator function. When it operates, TOE generates the encryption key by the encryption passphrase that was entered on the panel.

6) HDD Lock Function

HDD has the HDD lock function as measure against the illegal taking out, when the password is set. The access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the printer. (Even if HDD is taken out, it is impossible to use it excluding the printer that the concerned HDD installed.)

7) Remote diagnostic function

Making use of several connected systems such as E-mail, and a modem connection through a RS-232C, in communication with support center of printer produced by Konica Minolta Business Technologies Inc., it manages the state condition of printer and the machinery information such as count of printing. In addition, if necessary, appropriate service (shipment of an additional toner, the account claim, dispatch of the service engineer due to the failure diagnosis, etc.) is provided.

8) Updating function of TOE

TOE facilitated with the function to update itself. As for the update means, there are the methods executing in remote diagnostic function: a TOE update function via Internet, an update function from client PC, and a method that performs the connection of the Compact Flash memory medium.

9) Encryption Communication Function

TOE can encrypt the data transmitted from PC to Printer by using SSL/TLS.

10) Setup function

It offers the function to setup by using the installed software dedicated to perform on PC with connecting to client PC through Ethernet. Dedicated installed software is used by service engineer and so it's not offered to a user.

11) Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, there is the reset function of the network setting and the update function of TOE through the network, but the use of these functions is prohibited

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 "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[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 "magicolor 8650 Control Software Security Target" 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 B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) 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] or [13]) as its rationale. Such evaluation procedure and its result are presented in “magicolor 8650 Control Software Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

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 concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report on February 2008 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 assumes the use in the general office environment that is protected from the attack of the external network. The access via the panel or the internal network to TOE is under the management by the administrator and does not assume the complex attack. Therefore, it is reasonable to assume the attacking ability to attacker is “low-level”.

Thus, it is adequate with the SOF-Basic.

1.5.4 Security Functions

Security functions of the TOE are as follows.

1) F.ADMIN (Administrator Function)

F.ADMIN is a series of security function that administrator operates, such as an administrator identification authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box.

a. Administrator Identification and Authentication Function

It identifies and authenticates the accessing user as the administrator in response to the access to the administrator mode.

b. Function offered in Administrator Mode

When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user. And the following operations and the use of the functions are permitted.

(1) Change of the administrator password

When a user is re-authenticated as an administrator by the panel, and the new password satisfied the quality, the password is changed.

It resets the number of authentication failure when succeeding in the re-authentication.

It returns "*" for each character as feedback for the entered administrator password in the re-authentication by the access from the panel.

When the authentication failure that becomes 1-3 times at total in each authentication function by using the administrator password is detected, it logoffs the administrator mode accessing from the panel, and locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)

F.RESET works and the lock release function of the administrator authentication function in F.SERVICE is carried out, and the lock of authentication function is released.

(2) User Box Settings

It registers as public user box by setting the user attributes to the unregistered user box ID. It performs the setting and change of the user box password, and the change of the user attributes of the user box. User box password is set with 8 digits by using ASCII code (0x20~0x7E) (A total of 95 characters are selectable.)Also, it shall not be composed of one kind of character.

(3) Release of Lock

It resets (0 clear) the number of each secure prints, each user boxes and SNMP password. If access locked exists, the lock is released.

(4) Setting of unauthorized access detection threshold

The unauthorized access detection threshold in the authentication operation prohibition function is set in the range for 1-3 times.

(5) Setting and execution of all area overwrite deletion function

The deletion method shown in the table 1-1 is selected first, and then the overwrite deletion at the data area of HDD and NVRAM. (Perform F.OVERWRITE-ALL.)

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	Random numbers -> Random numbers -> 0x00
Mode:3	0x00 -> 0xFF -> Random numbers -> Verification
Mode:4	Random numbers -> 0x00 -> 0xFF
Mode:5	0x00 -> 0xFF -> 0x00 -> 0xFF
Mode:6	0x00 -> 0xFF -> 0x00 -> 0xFF -> 0x00 -> 0xFF -> Random numbers
Mode:7	0x00 -> 0xFF -> 0x00 -> 0xFF -> 0x00 -> 0xFF -> 0xAA
Mode:8	0x00 -> 0xFF -> 0x00 -> 0xFF -> 0x00 -> 0xFF -> 0xAA -> Verification

(6) Network Settings

A setup operation of the following setting data is performed.

- A series of setup data that relates to printer address (IP address, NetBIOS Name, AppleTalk Printer Name, etc.)

(7) Execution of back-up and restoration function

All the setting data stored in NVRAM and HDD is backed-up and re-stored except the administrator password and the CE password.

(8) Operation setting function of HDD lock function

When turning HDD lock function ON from OFF, it verifies that the newly set HDD lock password satisfies the following qualities.

Change the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.

HDD lock password is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D)(A total of 83 characters are selectable)

Return "*" for each character as feedback for the entered HDD lock password in verification.

Also, it shall not be composed of one kind of character.

(9) Operation setting of encryption function

When turning the encryption function ON from OFF, it verifies that the encryption passphrase newly set satisfies the qualities, and F.CRYPT is performed.

Change the encryption passphrase. By using the encryption passphrase currently set, when it is re-authenticated as an administrator, and the new encryption passphrase satisfies the quality, it is changed and F.CRYPT is performed.

Encryption passphrase is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D)(A total of 83 characters are selectable)

Also, it shall not be composed of one kind of character, and it must differ from the current password.

Return "*" for each character as feedback for the entered encryption passphrase in verification.

(10) Function related to Enhanced Security function

- Function to set valid or invalid of Enhanced Security function
- The settings of enhanced security function are invalidated by executing the overwrite deletion of all area.

- Along with the execution of this logical format which is the function to re-write system file of OS in HDD, the setting of Enhanced Security function is invalidated.
- The setting of the Enhanced Security function is invalidated by nullifying HDD installation setting.

(11) Change of SNMP password

Change the SNMP passwords (Privacy password and Authentication password), and verify the quality of new password.

(12) Setting of SNMP password authentication function

The authentication method in the SNMP passwords authentication function is set to “Only Authentication password” or the “Authentication password and Privacy password.”

(13) Setting of Administrator Authentication Lock Time

Set the administrator authentication lock time between 5 - 60 minutes.

(14) Setting of Trusted Channel function

Set the setting data of the Trusted Channel function by SSL/TLS.

2) F.ADMIN-SNMP (SNMP Administrator Function)

F.ADMIN-SNMP is a security function, which identifies and authenticates the administrator in the access through the network by using SNMP from PC, and then permits the operation of a setting function of the network only to the administrator whose identification and authentication was succeeded.

a. Identification and authentication function by SNMP password

It identifies and authenticates by the SNMP password, that the user who accesses the MIB object through the network with the use of SNMP is an administrator.

b. Management function using SNMP

When it is identified and authenticated that the user is an administrator by the SNMP password, the access to the MIB object is permitted, and then the operation of the setting data shown as followings is permitted to be done.

(1) Network Settings

A series of setting data that relates to printer address (IP address, NetBIOS name, AppleTalk printer name, etc.

(2) Change of SNMP password

SNMP password (Privacy password, Authentication password) is changed. It verifies that SNMP password newly set is 8 digits or more by using ASCII code (0x21-0x7E, except 0x5C).

(3) Setting of SNMP password authentication function

The authentication method in the SNMP password authentication function is set to “Only Authentication password” or the “Authentication password and Privacy password.”

3) F.SERVICE (Service mode function)

This is a series of security function that the service engineer operates, such as the service engineer identification authentication function in service mode accessing from the panel, and a security management function that includes a change in the CE password and the administrator password.

a. Service engineer identification authentication function

It identifies and authenticates the accessing user as the service engineer in response to the access request to the service mode from the panel.

b. Function offered in service mode

When a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the access request to the service mode, the use of the following functions is permitted.

(1) Change of CE password

When a user is re-authentication as a service engineer and the new password satisfies the quality, it is changed.

CE password is composed of 8-digits by using ASCII code.(0x21 to 0x7E, except 0x22 and 0x2B)Also, it shall not be composed of all the same character. Reset the number of authentication failure when succeeding in the re-authentication.

Return “*” for each character as feedback for the entered CE password.

When the authentication failure that becomes 1-3 times at total in each authentication function by using the CE password is detected, it logoffs the service mode accessed from the panel, and locks all the authentication functions to use the CE password. (The access to the service mode is refused.)

(2) Change of administrator password

Change the administrator password. It verifies that the administrator password newly set satisfies the following qualities.

- It is composed of 8 digits by using ASCII code (0x21 - 0x7E, except 0x22 and 0x2B). Also, it shall not be composed of one kind of character.
- It shall not be matched with the current value.

(3) Function that relates to Enhanced Security function

The following functions are offered.

- HDD logical format function

  The function to re-write system file of OS in HDD. The setting of the Enhanced Security function is invalidated along with the execution of this logical format.
- HDD physical format function

  The function to rewrite the entire disk in HDD with a regulated pattern including the signal rows such as the track and sector information. The setting of the Enhanced Security function is invalidated along with the execution of this Physical format.
- HDD installation setting function

  The function to make the installed HDD effective. The setting of the Enhanced Security function is invalidated by nullifying this HDD installation setting.
- Initialization function

  Function to reset every setting value written in NVRAM to the factory default. The setting of the Enhanced Security function is invalidated by executing this initialization function.

(4) Function that relates to password initialization function

The following functions are offered.

- Initialization function

  Function to reset various setting values written in NVRAM to the factory default.
- HDD physical format function

  The function to rewrite the entire disk in HDD with a regulated pattern including the signal rows such as the track and sector information.

(5) Release of the lock of the Administrator authentication function

Resets (0 clear) the number of authentication failure for the Administrator. If access is locked, the lock is released.

(6) Setting of the CE authentication lock time

Set the CE authentication Lock Time between 5 - 60 minutes.

(7) Operation Setting function of Setup function

Set whether the Setup function is used or not.

4) F.BOX (Public User Box Function)

This is a series of security function related to the public user box, such as the authentication to the user who is permitted the utilization of the user box in the access to the pubic box, and the access control function to permit various operations of the concerned user box and the user box file after the authentication.

a. Registration of user box by user operation

By selecting the user attribute to the “Public” to the non-registration user box ID selected, this registers a pubic user box.

b. Public User Box Function

(1) Authentication function in access to a public user box

For the access request for each public user box, the user who accesses is authenticated that it is a user permitted the use of a public user box concerned respectively. When the authentication failure that becomes the 1-3 times in total is detected for the public user box concerned, the authentication function to the public user box concerned is locked. The administrator specifies the failure count threshold by the unauthorized access detection threshold setting function. The lock of the authentication function is released by the lock release function to the public user box of F.ADMIN executed.

(2) Access control to a user box and a user box file in a public user box

The task to act for the user is related the "User Box ID" of the user box as a user box attribute. This task is permitted the user box file, which have a corresponding user box attribute to the user box attribute of the subject attribute, to do the printing, the movement to other user boxes, and the copy operations to other user boxes.

(3) Change of a public user box password

Change the user box password of the public user box. When the user box password newly set satisfies the regulated qualities, it is changed.

5) F.PRINT (Secure Print Function)

F.PRINT is a series of security function related to the secure print such as the access control function that allows the printing the secure print file after authenticating if a user is the authorized user to use the secure print file for the access to the secure print file from the panel.

a. Authentication function by the secure print password

For the access request for each secure print file, the user who access is authenticated that it is a user permitted the use of a secure print file concerned.

The secure print authentication mechanism by the separate session information is not needed because it becomes only an access from the panel in the case of the secure print.

Return “*" for each character as feedback for the entered secure print password.

Resets the number of authentication failure when succeeding in the authentication. The access from the panel is not accepted for 5 seconds when the authentication is failed. When the authentication failure that becomes the 1-3 times in total for the secure print file concerned is detected, the authentication function to the secure print file is locked.

The administrator specifies the failure count threshold by the unauthorized access detection threshold setting function. The lock is released by the lock release function to the secure print file of F.ADMIN executed.

b. Access control function to secure print file

The secure print file access control operates when it is authenticated.

The task to act for the user who is identified and authenticated has the secure print internal control ID of the authenticated secure print file for the file attribute.

This task is permitted the printing to the secure print file with a corresponding file attribute to the file attribute of this task.

c. Registration function of a secure print file

For the registration request of the secure print file, the registration of the secure print password with the concerned secure print file.

(1) Registration of the secure print password

It verifies that the registered security print password satisfies the quality of the specified password.

(2) Giving of the secure print internal control ID

For the registration request of secure print file, when the verification of the secure print password is completed, the secure print internal control ID uniquely identified is set to the concerned secure print file.

6) F.OVERWRITE-ALL (All area overwrite deletion function)

F.OVERWRITE-ALL executes the overwrite deletion in the data area of HDD and initializes the setting value of the password that is set to NVRAM as well.

The deletion methods such as the data written in HDD and the written count is executed according to the deletion method of all area overwrite deletion function set in F.ADMIN. The HDD lock password and the encryption passphrase cannot be used for being turned off the operation setting of the HDD lock function and the encryption function. The setting of the Enhanced Security function becomes invalid in the execution of this function.

7) F.CRYPTO (Encryption key generation function)

This generates the encryption key to encrypt all data written in HDD by using KonicaMinolta HDD encryption key generation algorithm (SHA-1) that is regulated by the KonicaMinolta encryption specification standard. KonicaMinolta HDD encryption key generation algorithm (SHA-1) is the algorithm to generate the encryption key by using the SHA-1 regulated by FIPS 180-1.

When the encryption passphrase is decided in the encryption functional operation setting to which the access is restricted in F.ADMIN, the encryption key of 128bit length is generated from the encryption passphrase by applying the SHA-1 algorithm.

8) F.HDD (HDD verification function)

This is a check function to permit reading from and writing in the HDD only when it is verified that the illegal HDD is not installed and is confirmed validity when the HDD lock password is set to HDD.

When the HDD lock password is set to HDD, the status of HDD is confirmed in the HDD operation verifying at the time of TOE starting. As a result of status check, when the HDD lock password certainly being set is returned as the result of status confirmation, the access to HDD is permitted. If the HDD lock password not being set is returned, the access to HDD is refused because of an illegitimate possibility.

9) F.RESET (Authentication Failure Count Reset Function)

This is a function to release the lock by resetting the authentication failure count when the account locks in the administrator authentication and CE authentication.

The administrator authentication function lock release is executed by turning OFF and ON of the main power supply, and the lock is released after the administrator authentication lock release time. The CE certificates function lock release is executed by the specific operation, and the lock is released after CE certificates lock release time.

10) F.TRUSTED-PASS (Trusted Channel Function)

This is a function that generates and achieves the Trusted Channel by using SSL or TSL protocol when transmitting and receiving the following image file between PC and Printer.

- Image file that is stored as a user box file (upload from PC to Printer)
- Image file that is stored as Secure Print file (upload from PC to Printer)

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.DISCARD-Printer	- When the leaser returned or the discarded printer were collected, secure print file, a user box file, on memory image file, the stored image file, the remaining image file, the image-related file and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD in Printer.
T.BRING-OUT-STORAGE	- A secure print file, a user box file, a on memory image file, a stored image file, a remaining image file, an image-related file and the setup various passwords can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in Printer. - A person or a user with malicious intent illegally replaces as HDD in Printer. In the replaced HDD, new files of the secure print file, a user box file, on memory image file, a stored image file, a remaining image file, an image related file, a transmission address data file and set various passwords are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.
T.ACCESS-PUBLIC-BOX	- Exposure of the user box file when a person or the user with malicious intent accesses the public user box which is not permitted to use, and prints and removes and copies to the other user box the user box file.
T.ACCESS-SECURE-PRINT	- Exposure of the secure print file when a person or the user with malicious intent prints the secure print file which is not permitted to use.
T.ACCESS-NET-SETTING	- Malicious person or user changes the network setting which set in Printer to identify Printer itself where TOE installed, by setting to the value of the entity such as another illegal

	Printer from the value of Printer (NetBIOS name, AppleTalk printer name, IP address, etc) that TOE is originally installed, so that secure print file is exposed.
T.ACCESS-SETTING	- The possibility of leaking user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.
T.BACKUP-RESTORE	- The user box file and the secure print file can leak by malicious person or user using the backup function and the restoration function illegally. Also, highly confidential data such as password can be exposed and each setting values are falsified.
T.DISCARD-Printer	- When the leaser returned or the discarded printer were collected, secure print file, a user box file, on memory image file, the stored image file, the remaining image file, the image-related file and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD in Printer.
T.BRING-OUT-STORAGE	- A secure print file, a user box file, a on memory image file, a stored image file, a remaining image file, an image-related file and the setup various passwords can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in Printer. - A person or a user with malicious intent illegally replaces as HDD in Printer. In the replaced HDD, new files of the secure print file, a user box file, on memory image file, a stored image file, a remaining image file, an image related file, a transmission address data file and set various passwords are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.

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	Organisational Security Policy
P.COMMUNICATION-DATA	The highly confidential image file (Secure Print file, User box file) which transmitted or received between IT equipments is communicated via trusted pass to the correct destination, or has to be encrypted.

1.5.7 Configuration Requirements

The TOE operates on the magicolor 8650 which is the network printer provided by the Konica Minolta Business Technologies, Inc. The Encryption board is option parts and is not equipped as a standard. When the encryption board is not installed, the function that relates to the encryption cannot be used.

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	- Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.SERVICE	- Service engineers, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.NETWORK	- The intra-office LAN where the printer with the TOE will be installed is not intercepted. - When the intra-office LAN where the printer with the TOE will be installed is connected to an external network, access from the external network to the printer is not allowed.
A.SECRET	- Each password and encryption passphrase does not leak from each user in the use of TOE.
A.SETTING	- Printer with the TOE is used after enabling the enhanced security function.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

<Document for administrator / general user>

1) magicolor 8650 User’s Guide Security Operations (Ver. 1.00)(Japanese)
2) magicolor 8650 User’s Guide (Security Operations) (Ver.1.00) (English)

<Document for service engineer>

1) magicolor 8650 Service Manual Security Function (Ver.1.00) (Japanese)
2) magicolor 8650 Service Manual Security Function (Ver.1.00) (English)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM 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.

2.2 Overview of Evaluation Conducted

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

Evaluation has started from August, 2008 and concluded by completion the Evaluation Technical Report on February 2008. 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 December 2007 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 September 2007.

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

As for concerns 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

Figure 2-1 shows the test configurations used by the developer.

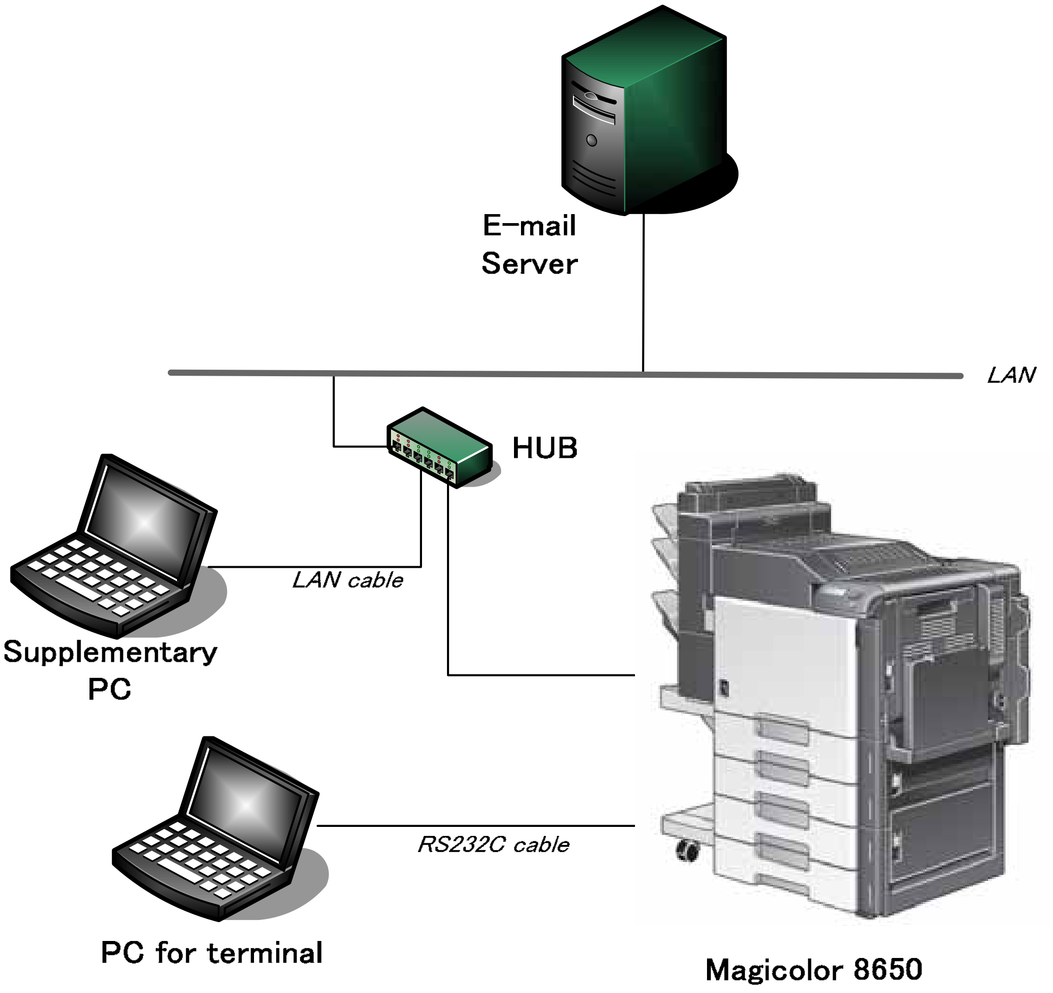

Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

The configurations of the tests performed by the developer are shown in Figure 2-1. Developer testing is 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) About the behavior of TSF related to the operation panel, confirm the behavior of the security function by the observing the operation for the operation panel and the display of the operation panel.

(2) About the behavior of TSF related to the power supply OFF and ON, confirm the operational change of the result after having turned off the

power supply of MFP and on with the operation panel (or through Network).

(3) About the behavior of TSF related to a network, confirm the behavior of the security function by observing the operation on the PC screen and by transmitting and receiving the test data of each protocol with connection to TOE from an application of PSWC, etc. or from a test tool using various protocols.

(4) About the behavior of the function related to the Enhanced Security Function (HDD logical format function, HDD physical format function, HDD installation setting function, Initialization function), confirm that these functions are restricted to a service engineer and an administrator (some of the functions). Also, after executing these functions, it is confirmed in the test process that the panel display of the icon which shows the Enhanced Security Setting ON disappears and that the value which each function makes applicable to initialization in an initialization state.

(5) In the developer testing, the change of the setting value, authentication method and the check of the access control to the security function are confirmed the output message, etc by using the external interface (the operation panel, the power supply OFF and ON and a network) by visual check.

- As for the security function that cannot be verified by using these external interfaces, confirm that the behavior is proper by performing the individual test approach.

c. Scope of Testing Performed

Testing is performed about 87 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

The evaluator used test configuration that are identical to those used by the developer.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The configuration of the tests performed by the evaluator is shown in figure 2-1. The evaluator tests were performed in TOE test environment identical to the TOE configuration identified by ST.

b. Testing Approach

For the testing, the following approach was used.

(1) About the behavior of TSF related to the operation panel, confirm the behavior of the security function by the observing the operation for the operation panel and the display of the operation panel.

(2) About the behavior of TSF related to the power supply OFF and ON, confirm the operational change of the result after having turned off the power supply of MFP and on with the operation panel (or through Network).

(3) About the behavior of TSF related to a network, confirm the behavior of the security function by connecting to TOE from PSWC or a test tool using various protocols, by operating and observing on the WEB screen for PSWC, and by transmitting and receiving the test data of each protocol.

(4) About the behavior of the function related to the Enhanced Security Function (HDD logical format function, HDD physical format function, HDD installation setting function, Initialization function), confirm that these functions are restricted to a service engineer and an administrator (some of the functions), and that the panel display of the icon which shows the Enhanced Security Setting ON is disappeared and the value which each function makes applicable to initialization is in an initialization state after executing these functions.

(5) In the developer testing, the change of the setting value, authentication method and the check of the access control to the security function are confirmed the output message, etc by using the external interface (the operation panel, the power supply OFF and ON and a network) by visual check.

(6) As for the security function that cannot be verified by using these external interfaces, confirm that the behavior is proper by performing the individual test approach.

c. Scope of Testing Performed

The evaluator performed 50 tests in total: 29 independent test and 21 sampled developer tests. As the selection criteria of the test, followings take into account.

(1) Security function that is suspected to operate along the specifications by the developer test.

(2) At the start of TSFI (operation panel, network, (PSWC, TCP, Socket OpenAPI and SNMP, etc.)), confirm the behavior by the difference of password enter method in the probabilistic / permutational mechanism test.

(3) Security function set as the object of strength of function

(4) All subsystems that offer the security function (SS-Panel, SS-CommonAPI, SS-Image, SS-PCPrint, SSPSWC, SSMIB, SS-OpenAPI, SS-TCPSocket and SS-MIO) are objects to test it without deflection in a subsystem.

d. Result

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

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM 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.

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

The Certification Body confirmed such concerns 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 abbreviations peculiar to TOE used in this report are listed below.

DNS	Domain Name System
FTP	File Transfer Protocol
HDD	Hard Disk Drive
IP	Internet Protocol
LAN	Local Area Network
MFP	Multiple Function Peripheral
NVRAM	Non-Volatile Random Access Memory
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
USB	Universal Serial Bus

The glossaries used in this report are listed below.

CE password
Kind of password collating when entering the service mode

Printer Address
Generation terms, such as an IP address of Printer set up by the network setting function in administrator maintenance mode from the operation panel of Printer.

Printer Controller
Controller that controls all the operation of Printer including the operation control process received from the network or the Printer panel and the management of image data. TOE is the software that operates on that controller.

Account Lock
Unable to perform continuous password authentication when the operation of password authentication is failed consecutively, or its situation.

Service Mode
Operation panel screen area which can operate MFP function that is prepared for the service engineer.

Service Engineer
A user who performs the management of maintenance for the printer. Performs the repair and adjustment of Printer. In general, it is the person in charge at the sales companies or agencies that performs the maintenance service of MFP and that is in cooperation with Konica Minolta Business Technologies, Inc.

Remaining Image File
File that remains in the HDD data area. It is the image file that cannot be deleted by general deletion operation.

Secure Print
This is the printing method that restricts by the password authentication. Specify the password by the printer driver and printing by Printer is allowed only when that password is authenticated.

Flash Memory
Memory device that performs the high speed and high integration of EEPROM and carried the batch deletion mechanism.

User Box
Directory that is created in the HDD area in order to store the image files in the MFP.

6. Bibliography

[1] magicolor 8650 Control Software Security Target Version 1.06 (January 18th, 2008) KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] magicolor 8650 Control Software Evaluation Technical Report, February 26th, 2008, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security