Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	September 29, 2004 (ITC-4035)
Certification No.	C0035
Sponsor	KYOCERA MITA Corporation
Name of TOE	Data Security Kit(B) Software
Version of TOE	V1.10E
PP Conformance	None
Conformed Claim	EAL3
TOE Developer	KYOCERA MITA Corporation
Evaluation Facility	Japan Electronics & Information Technology Industries Association, Information Technology Security Center

This is to report that the evaluation result for the above TOE is certified as follows.
November 2, 2005

Haruki Tabuchi, 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 (as of 15 February 2002)

Evaluation Result: Pass

"Data Security Kit(B) Software V1.10E" 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 “Data Security Kit(B) Software V1.10E” (hereinafter referred to as “the TOE”) conducted by Japan Electronics & Information Technology Industries Association, Information Technology Security Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, KYOCERA MITA Corporation .

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:	Data Security Kit(B) Software
Version:	V1.10E
Developer:	KYOCERA MITA Corporation

1.2.2 Product Overview

TOE is a software module product that provides security functions for “KM-8030/KM-6030, CS-8030/CS-6030,” the MFPs of KYOCERA MITA Corporation. This TOE will be installed on MFPs that are to be utilized in offices and schools, and will be utilized for the purpose of protecting image data remaining on the HDDs from unjust exposure, after various copying (duplication), printing (paper output), and network scanning (electronization) processings, by providing an HDD overwriting function.

1.2.3 Scope of TOE and Overview of Operation

(1) Environment for TOE use

TOE installed MFPs will be used in offices and schools where various documents are handled, and they will be connected to the internal network (LAN). They can also be used by being connected to local ports (parallel port, USB port, serial port), for printer output. The environment for MFP use is indicated in Figure 1-1.

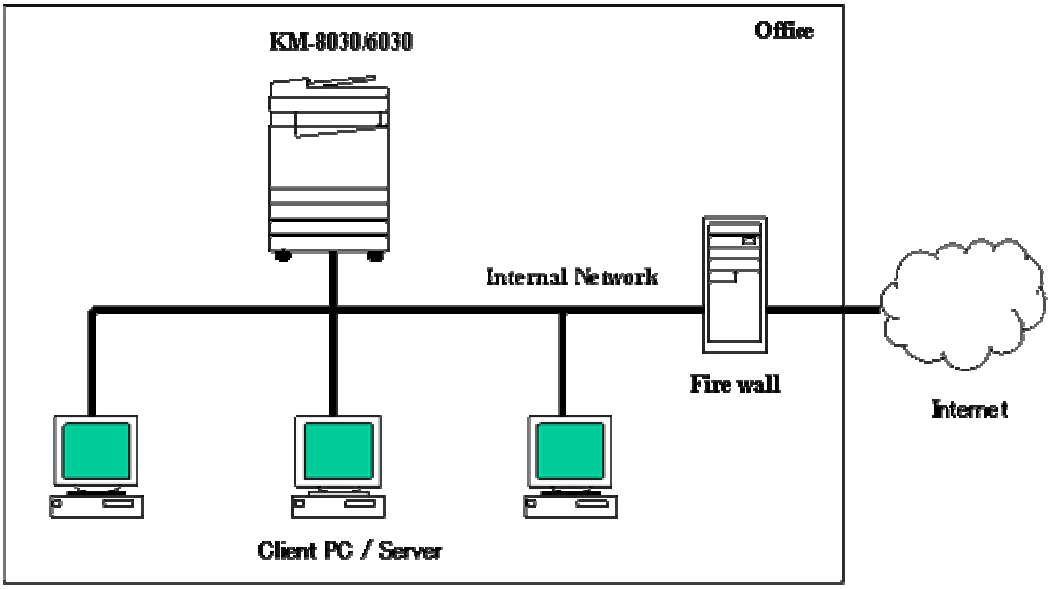

Figure 1-1 MFP operating environment

(2) Scope of TOE and overview of operations

The hardware configuration of TOE is indicated in Figure 1-2. The TOE refers to the software in the MAIN ROM and PRINTER ROM, which are on the main board and printer board, respectively.

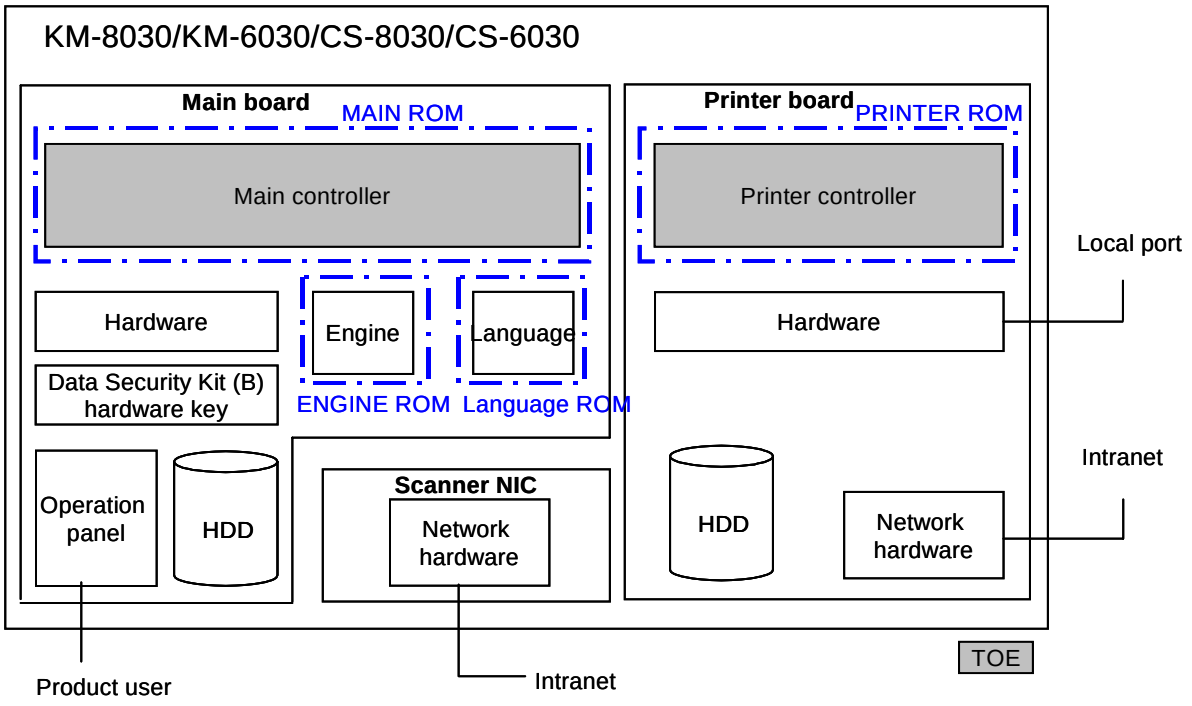

Figure 1-2 TOE hardware configuration

The configuration of software modules included in TOE is indicated in Table 1-1.

Table 1-1 Software modules that constitute the TOE

Name of ROM	Type	Notes
MAIN ROM	Main controller	-
	Copier module	-
	Scanner module	-
	Network module	-
	Library common for both the copier and network scanner	The HDD Overwrite Function and the administrator authenticating function are included in it
PRINTER ROM	Printer controller	-
	Printer module	-
	Network module	-
	Library for the printer	The HDD Overwrite Function is included in it
	Network service	-

A logical configuration of the TOE is indicated in Figure 1-3. The TOE has not only security functions, but also ordinary MFP functions such as copying functions. The following functions are included within the logical configuration of TOE.

- HDD Overwrite Function (Security function)
  There is an HDD overwriting function in addition to the conventional logical delete processing, with a purpose of improving safety furthermore. When using the copier function, network scanner function, or the printer function, and then deleting the image data stored in the HDD, meaningless character strings are overwritten onto the actual data area after those image data are logically deleted, to completely erase the actual data area.
  There is a 3-time Overwrite method and a Once Overwrite method, for the overwriting method.
- Administrator authenticating function (Security function)
  It identifies and authenticates a TOE machine administrator, with the TOE administrator management code inputted from the operation panel. An identified and authenticated TOE machine administrator can execute an "HDD formatting function" that overwrites the whole area of the HDD, and can change the HDD overwriting function between the 3-time Overwrite method and Once Overwrite method. The 3-time Overwrite method is the initial

default, and it should be set when more importance is to be attached to safety than processing efficiency. The 1-time Overwrite method should be set when more importance is to be attached to efficiency. Either of the methods will always be set, and the default setting is the 3-time Overwrite method.

- Copier function

  The copying of the originals read in from the scanner is conducted by the TOE users. (Ordinary copying) When this ordinary copying is executed, the image data is spool-stored onto the HDD of the main board, and will be deleted when the output has been completed. This copier function also includes a document management function. There is a Shared Data Box, Synergy Print Box, and a Form Box for the document management function. Each of the boxes exists onto the HDD of the main board. After the processing, the image data will be deleted.

- Network scanner function

  TOE users can transmit the image data of originals read in from the scanner, to the client PCs. There is PC transmission that transmits them via the LAN, and e-mail transmission that sends them via e-mails. The originals set on the MFP can be captured into a client PC by operations from the client PC, utilizing applications that support TWAIN. When using the network scanner function, the image data is spool-stored onto the HDD of the main board, and will be deleted when the transmission has been completed.

- Printer function

  Image data transmitted from the printer driver are outputted to the papers, by the TOE users (ordinary printing). There are outputs via the LAN, and outputs via the local port. The printer function also has the following expanded functions, besides the function to simply output data. When using ordinary printing, the image data is temporarily spool-stored onto the HDD of the main board, and will be deleted when the output has been completed. When using the extended functions, the image data is stored on the HDDs of the printer boards or the main board, and will be deleted after the processing is finished.

- Job management function

  It is a function included in the copier and printer functions. The jobs/printing-jobs stored on the HDD are administered by each of the functions. It is possible to edit, output, or delete the jobs/printing-jobs. It can be operated from the operation panel, or from utilities in the client PC.

The hardware key for the Data Security Kit (B) will be necessary to activate the TOE. If the Data Security Kit (B) hardware key is removed during operation, the security function will not become invalid, but the MFP itself will become unoperatable.

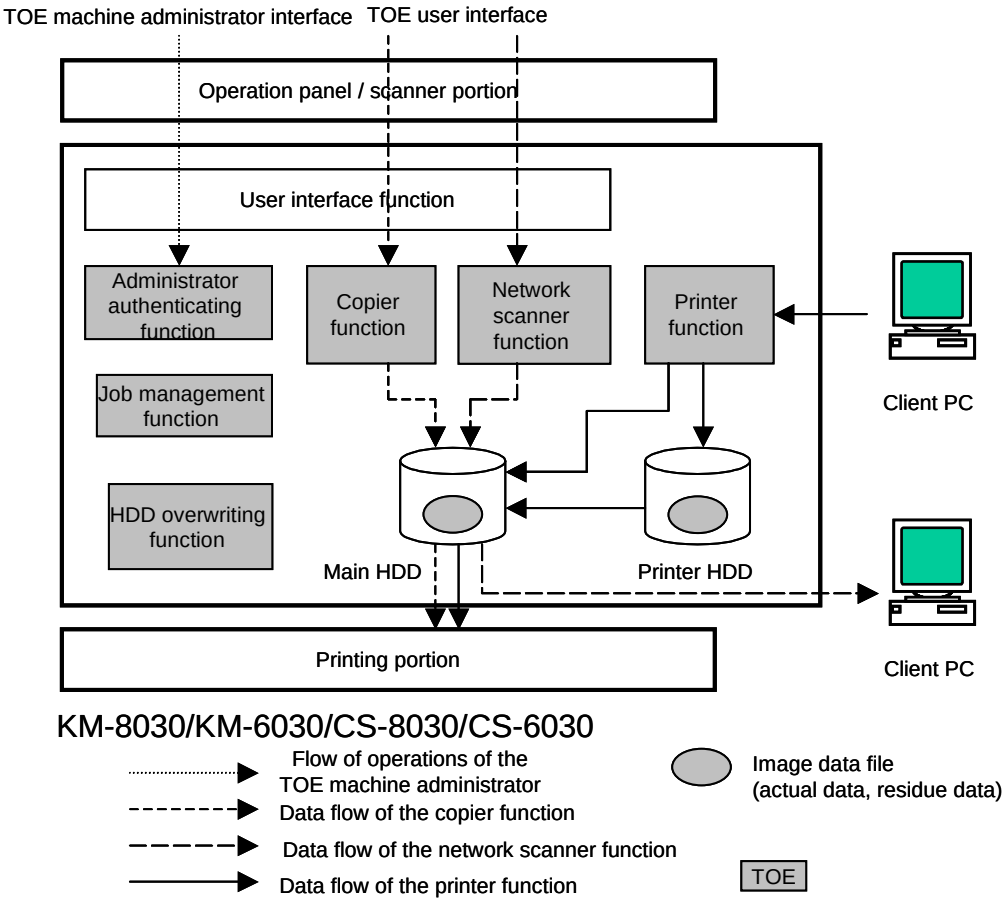

Fig. 1-3 Logical configuration of TOE

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 “KYOCERA MITA Data Security Kit(B) Overseas version Security Target Version 0.15” 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 “Data Security Kit(B) Software Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”)[21]. 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].

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 dated October, 2005 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.
Although it is also assumed that this TOE will be utilized by being installed on MFPs at offices and schools, and connected to the LAN or local ports, residue data within the MFPs cannot be read out from the network, via the LAN/local-ports. And since the MFPs will be installed at places where room entrance/exit management is executed, there will not be any unspecified large number of attackers, including attackers with a medium level or more attacking force, in the operating environment of the TOE. For this reason, the attacking force will be "low-level," and the level of the minimum strength of function that can deal with this should be satisfied by a "SOF-basic."

1.5.4 Security Functions

Security functions of the TOE are as follow.

- HDD Overwrite Funciton SPF.AGAIN

The HDD overwriting function is a function that overwrites all the actual data area of data stored on the HDD, not only deleting the management information of that data logically.
There are the following two methods for overwriting, and only TOE machine administrators can change it.

- 3-time Overwrite
  Random data (1), random data (2), and then NULL (0x00) data will be written in sequence, to all the actual data area of the data to be overwritten.
- Once Overwrite
  NULL (0x00) data is written to all the actual data area of the data to be overwritten.

The HDD overwriting function is executed independently for each of the HDDs of the main and printer boards. However, the setting of either of the overwriting methods, and the execution of the HDD formatting function, which is described below, will be conducted in unification for the HDDs of the main and printer boards, without distinguishing between them.
The HDD overwriting function can be executed in either of the following timings.

・When a job is deleted by an output, power off, or a deleting operation
・When an HDD formatting function is executed by the TOE machine administrator

Note: In overwriting upon power off, the erase-processing is actually conducted when the power is turned on the next time. This HDD overwriting function is always called out in above-mentioned timings, and executed without taking bypasses.

a) Overwriting function for the HDD on the main board
The overwriting function for each of the jobs stored in the image data files of the HDD on the main board goes as follows:

・A function to completely erase the data spool-stored on the HDD
・A function to completely erase the data stored on the HDD for a long period, by deleting operations of TOE users.

b) Overwriting function for the HDD on the printer board
The overwriting functions for each of the jobs stored in the image data files of the HDD on the printer board goes as follows:

・A function to completely erase the data stored on the HDD for a long period, by deleting operations of TOE users.
・A function in which data stored on the HDD for a long period is completely erased by an output
・A function in which data stored on the HDD for a long period is completely erased by a power off

c) HDD formatting function
A function to completely erase data stored on the HDDs of the main and printer boards, when the TOE machine administrator executes this function.

・It overwrites all the areas of the HDDs on the main and printer boards.

●Administrator authenticating function　SPF.ADMIN

The administrator authenticating function is a function to securely identify and authenticate TOE machine administrators.
When a function that requires TOE machine administrator authority is accessed, the accessing person is identified whether he/she is a TOE machine administrator, and then the TOE administrator management code is required to be inputted, and the accessing person is to input the TOE administrator management code from the operation panel. Access will be granted if the inputted TOE administrator management code matches, but will not be granted unless it matches. Dummy characters (*) with the same length as the inputted characters will be displayed on the operation panel, during the authentication.

The metric for the TOE administrator management code is constituted by numbers (0 to 9), with a fixed length of 8 figures. This administrator authenticating function is always called out when a function that requires TOE machine administrator authority is accessed, and executed without taking bypasses.

The TOE administrator management code setting is stored at a certain place, and although there is a default setting for when a machine is to be installed, it is made so that it can only be changed by the TOE machine administrator. When changing the TOE administrator management code, inputs other than numbers will not be accepted, and it will not be changed if it is shorter than 8 figures long.

The authorities given to a TOE machine administrator are the following.

- Changing the setting for the overwriting method (3-time Overwrite method / Once Overwrite method)
- Executing the HDD formatting function
- Changing the TOE administrator management code

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.AGAIN	Malicious TOE users connecting illegal decoding apparatuses to the HDDs, or taking out the HDDs, to browse/output the residue data kept on the HDDs. Or to browse/output the residue data on the HDDs that have not been overwritten completely because the MFP power has gone off during overwriting.

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.METHOD	The 3-time Overwrite method or the Once Overwrite method should be applied when overwriting an HDD, taking into consideration the balance between safety and efficiency.

1.5.7 Configuration Requirements

This product is provided as software modules for “KM-8030/KM-6030 and CS-8030/CS-6030,” the MFPs of KYOCERA MITA Corporation. The software modules are included within the Main ROM and Printer ROM of KM-8030/KM-6030 and CS-8030/CS-6030.

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.PHYSICAL	MFPs with TOE installed should be installed at physically protected places, where only people associated with the TOE are able to use it.
A.ADMIN	The TOE machine administrator should be a reliable person, and someone who will not do anything dishonest.
A.CE	The person in charge of service of the TOE should not do anything dishonest.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- Data Security Kit (B) Operation Guide
  Version : Revision 1.0 2005.6 303J056013

- INSTALLATION GUIDE for Data Security Kit (B)
  Version : 2005.2 303J056710

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 October, 2004 and concluded by completion the Evaluation Technical Report dated October, 2005. 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, 2004, January, 2005 and July, 2005 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 December, 2004 and August, 2005.

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

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

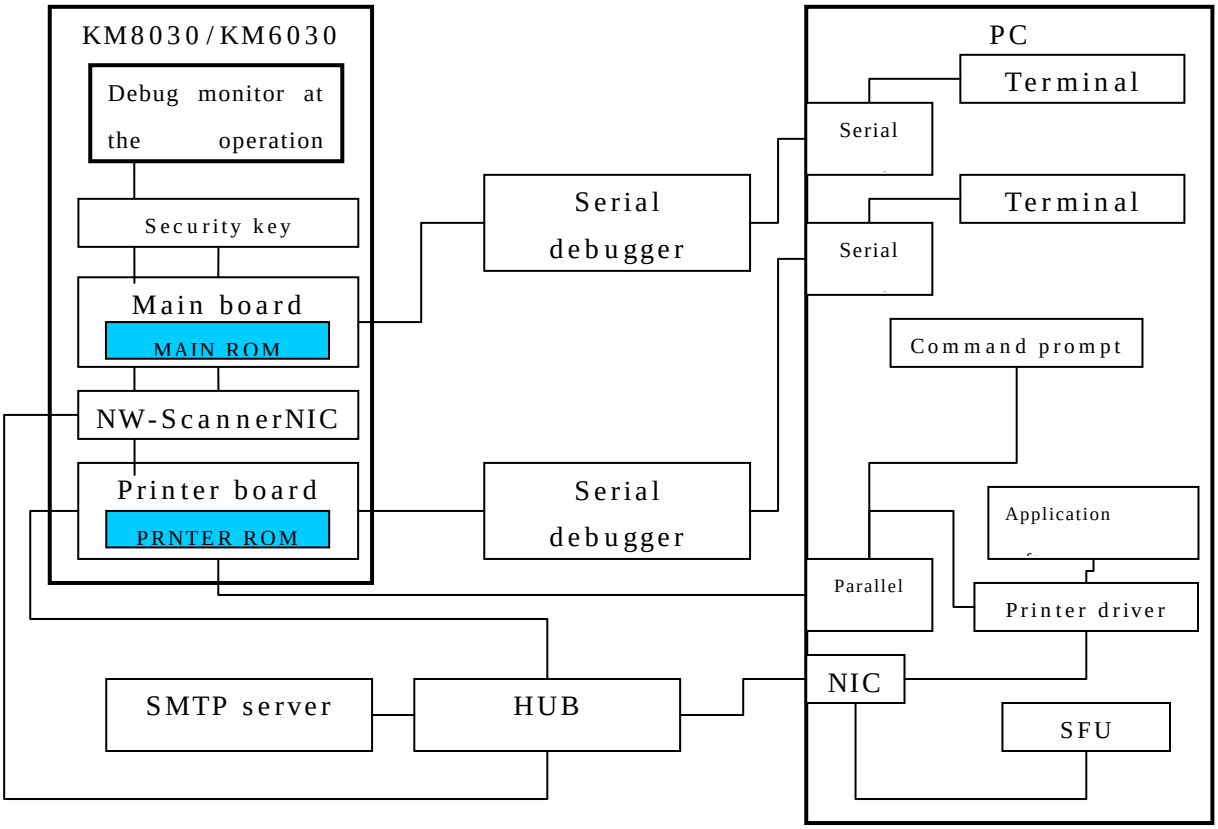

Figure 2-1 Configuration of developer and evaluator testing

TOE: KYOCERA MITA Data Security Kit(B) Software	The TOE refers to the software in the Main ROM and Printer ROM, which are on the main board and printer board, respectively. (Indicated in blue in the figure)
Main board	A board in which the following subsystems operate: MMI, Job management, printer control, image input/output control, file management
Printer board	A board in which the following subsystem operates: Printer
Security key	A board that enables the security functions by connecting to the main board.
PC	OS: Windows 95 or later, RAM: 128MB or more
HUB	Used for constructing a local network, to use the printer printing or network scanner via the LAN from PC.
SMTP server	A server for using the e-mail transmission function of the network scanner.
Debug monitor at the operation section	It can display debugging information on the LCD of the operation section by pressing specific keys simultaneously at the operation section.
Serial debugger board (MAIN/PRT)	There are boards for the main board and printer board. They are connected via terminal software and serial port, and are capable of log output and memory dump, etc. to the connected board. It is also possible to set breakpoints for the printer.

Terminal Software	Terminal software of, for example, Hyper Terminal, which is used for checking logs and setting breakpoints.
Command prompt	MS-DOS command prompt for transferring the prescribe command to the printer board via parallel port.
Printer driver	Necessary for printer printing.
SFU	Scanner File Utility. A software for receiving data files of the network scanner.
Application software	Such as Word/Excel, used for testing the printer printing.

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. There are two kinds of test environments, as shown below:

(1) Test that uses external interfaces

This is in the same configuration as the environment in which users actually use. It is not connected to the debugger (PC) via the Serial debugger board. The results are confirmed by a display on the operation panel or LCD, error sound and printing output from the MFPs.

(2) Test that uses internal interfaces

Connecting the Serial debugger boards respectively to the main board and printer board, the results are confirmed by outputting logs, such as the security function status, requests or details of notices between subsystems, and the counter value to the debugger (PC) via the serial cable. This function is implemented with the compile switch for testing only. Users cannot actually use it as the compile switch is invalidated. In some tests, the results are confirmed by using the debug monitor that displays debugging information on LCD, with the memory dump function for testing incorporated in the TOE.

c. Scope of Testing Performed

Testing is performed 45 function test items (FT Test) and 145 subsystem test items (JT Test) 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

The same testing approaches as those of the developer testing were used.

c. Scope of Testing Performed

The evaluator performed a total of 54 test items, 14 test items uniquely devised by the evaluator and 40 test items by sampling the developer testing.

(1) The tests uniquely devised by the evaluator are considered for the following matters:
- Test on residue data, which has not been conducted by the developer
- Passive test on changes of the administrator management code
- Testing all the security functions

(2) The sampling tests of the developer testing were selected to consider the following:
- Behavior test (FT Test) that is not described in the ST, among the test items covering the two security functions
- Behavior test (FT Test) of the security functions, with or without the hardware keyboard (security hardware keyboard)
- Items that test the main part of each security function (JT Test) from the test items covering each of the subsystems
- Items for observing the expected, typical behavior of the security functions (JT Test)

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.

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

The protection asset of TOE is residue data. TOE does not protect the original file or the data which changes to residue data. This certification report advises the sponsor telling a user the cautions on the security about use of a product.

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.

Spool-storage:	Keeping the received image data temporarily on the HDD, without outputting it or forwarding it as is. This is executed automatically during the process of the MFP, without the user being conscious about it. This should be compared to long period storage.
Long period storage:	Keeping the received image data on the HDD for a long period. The users will have to consciously conduct the storage or reading operations for this storage. This should be compared to spool-storage.
Client PC:	It indicates the computers that connect to the network, and utilize the TOE services (functions) of the TOEs that are connected to the network.
Network scanner:	A function to transmit the scanned originals as image data, to the client PCs. There is PC transmission that transmits them via the LAN, e-mail transmission that transmits them via e-mails, and a TWAIN function that captures images of the originals by operations from the client PC.
PC transmission:	This is a processing in which the scanned images are compressed into file formats specified by the user, and transmitted to the utilities of the specified client PC.
E-mail transmission:	This is a processing in which the scanned images are compressed into file formats specified by the user, and transmitted to pre-registered e-mail servers, according to the SMTP protocol.

TWAIN :	This is a processing in which the originals set on the MFP are captured into the client PCs by operations from the client PC, utilizing TWAIN compatible applications.
Job:	A unit for one processing of the copier, printer, or network scanner functions. Image data of the originals are also included in this job.
Printing job:	Jobs that are processed as printer functions, among the various jobs.
Actual data area:	An area within the image data where data composing the actual image is recorded. When an image data is logically deleted, this area will still remain. This remaining area will be called "residue data."
residue data:	This is an area where image data remains, after deleting the image data of a actual data area logically.
Operation panel:	This is installed on the uppermost part of the MFP, and is constituted by a liquid crystal panel. It is an external interface, and users can utilize the TOE via this operation panel.
NIC:	It is an abbreviation for "Network Interface Card." It is an expansion card for connecting the TOE to the internal network
Forms:	This indicates the combining-source images that will become the source images for the function to superimpose images (combining of the images). Originals that have been read in can be superimposed and copied onto forms.

6. Bibliography

[1] KYOCERA MITA Data Security Kit(B) Overseas version Security Target Version 0.15 (October 21, 2005) KYOCERA MITA Corporation

[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 (as of February 2002)

[21] KYOCERA MITA Data Security Kit(B) Software Overseas version Evaluation Technical Report Version 2.3, October 25, 2005, Japan Electronics & Information Technology Industries Association, Information Technology Security Center.