Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-11-11 (ITC-0327)
Certification No.	C0309
Sponsor	KYOCERA MITA Corporation
Name of TOE	TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445, DC 2455 Data Security Kit (E)
Version of TOE	V1.00E
PP Conformance	None
Assurance Package	EAL3
Developer	KYOCERA MITA Corporation
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2011-08-31

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center, Technology Headquarters

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 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

"TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445, DC 2455 Data Security Kit (E) V1.00E" 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

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445, DC 2455 Data Security Kit (E) V1.00E" (hereinafter referred to as "the TOE") developed by KYOCERA MITA Corporation, and evaluation of the TOE was finished on 2011-07 by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, KYOCERA MITA Corporation and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the Security Target (hereinafter referred to as "the ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This certification report assumes "system administrators, etc., in consumer site where the TOE is introduced and used" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions is as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

The TOE is the firmware that controls Multi Function Printer (hereinafter referred to as "MFP") and the special custom IC (ASIC) that performs security algorithm after the license is granted to use the Data Security Kit (E) for the MFP having mainly copy function, scan function and print function. The firmware and the ASIC after being granted the license are called the TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445, DC 2455 Data Security Kit (E) V1.00E.

The TOE overwrites an actual image data area when deleting the image data on the HDD and protects the image data against leakage.

The TOE encrypts the image data and then stores them in order to protect the image data against leakage when temporarily storing the image data in the HDD for the MFP functions (copy function etc.).

Regarding these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated in the scope of the assurance package. The threats and assumptions which the TOE assumes are described in the following sections.

1.1.2.1 Threats and Security Objectives

There is no threat that the TOE assumes. To meet the requirements of the organisation to deploy the TOE, it provides security functionality described in 1.1.2.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

- The TOE is installed to be used for the following MFP manufactured by KYOCERA MITA Corporation:
  - > TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i
  - > TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG
  - > CS 3500i, CS 4500i, CS 5500i
  - > CD 1435, CD 1445, CD 1455
  - > DC 2435, DC 2445, DC 2455

- It is assumed that the MFP including the TOE is located in offices managed by organizations such as enterprises or those departments, etc.

- To prevent attacks against the hardware of the MFP, it is placed under the supervision of employees. (Power-off at inappropriate timing is also considered as an attack.)

- When the MFP is connected to the network, it is assumed to be connected to the LAN in the office. Even when the LAN is connected to the external network (the Internet, etc., that is outside of the organisation), access to the MFP from the external network is restricted.

- It is assumed that the service persons in charge are reliable.

1.1.3 Disclaimers

In this evaluation, the assurance is limited to the "overwrite function" and the "encryption function" that become valid after the license is granted to use the Data Security Kit (E) for the MFP.

Although there are functions which are recognized as security function in general even before the license is granted to use the Data Security Kit (E) for the MFP, these functions are not certified by this evaluation.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation and completed on 2011-07 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] and Observation Report prepared by Evaluation Facility and evaluation evidential materials, and confirmed that the

TOE evaluation is conducted in accordance with the prescribed procedure. It is confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]).
The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE:	TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445, DC 2455 Data Security Kit (E)
Version of the TOE:	V1.00E
Developer:	KYOCERA MITA Corporation

The condition for being the evaluated and certified TOE is that the license is granted to use (i.e. activate) the Data Security Kit (E) for the correct MFP and firmware. Users can confirm it by the following methods.

- Confirmation of the MFP
  MFP can be identified by the description on the MFP main body. The confirmation can be made if it corresponds with any of a list of the MFP as described in the guidance. Thus, the MFP can be confirmed as the correct one.

- Confirmation of the Firmware
  The firmware version can be printed out by operating the MFP according to the procedure as described in the guidance. The printed version can be checked with the correct version of the firmware as described in the guidance. Thus, the firmware can be confirmed as the correct one.

- Confirmation if the license of the Data Security Kit (E) is granted to use (i.e. activated)
  The icon displayed on the operation panel when the license is granted, is described in the guidance. It can be checked with the operation panel according to the guidance, and it can be confirmed if the license is granted to use.

(Supplement)
ASIC identification is uniquely fixed when the MFP identification is fixed, since the manufacturing management is maintained. Therefore, a confirmation of the correct MFP also means a confirmation of the correct ASIC.

3. Security Policy

This chapter describes the security function policies and organisation security policies that the TOE adopted to counter threats.

The TOE is the firmware and the ASIC, and performs copy function, scan function and print function by controlling the MFP. When operating these functions, image data are temporarily stored in the HDD as needed. It is called "temporary storage" when the image data are temporarily stored for the MFP functions without users being conscious about it.

When operations of these functions are completed and the temporarily-stored image data become unnecessary, the data will be automatically deleted.

The TOE also provides function to store image data in the HDD for a long period of time by user's instruction. It is called "long-period storage" when the image data are stored over a long period of time with user's intention, and this should be distinguished from the "temporary storage".

The long-period stored image data are not deleted without user's instruction.

When image data are temporarily stored in the HDD for the MFP functions (copy functions etc.), the TOE encrypts the image data and stores them so that the leakage of the image data is prevented.

When deleting the temporarily-stored image data or long-period stored image data, the TOE overwrites on the actual image data area so that the leakage of the image data is prevented.

(Note)
As long as the long-period stored image data are not explicitly deleted, it is not considered as the image data that should be protected against leakage.

3.1 Security Function Policies

The TOE possesses the security functions to meet the organisational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

There is no threat that the TOE assumes.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-1.

Table 3-1 Organisational Security Policies

Identifier	Organisational Security Policy
P.ENCRYPT	**Encryption of the temporarily-stored data** As a request from the organisation, the temporarily-stored data of the HDD shall be encrypted to prevent them from unauthorized reading. (Supplement) To use the temporarily-stored data is legitimate only if the data are decrypted and used by the MFP which has generated the data.
P.OVERWRITE	**Overwrite-erase of the residue data** As a request from the organisation, it shall make it impossible to reuse the residue data of the HDD to prevent them from unauthorized reading.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to meet the Organisational Security Policies shown in Table 3-1.

(1) Complying with the organizational security policy "P. ENCRYPT"
To meet this policy, when saving the image data on the HDD, the TOE encrypts the image data and saves.

(2) Complying with the organizational security policy "P.OVERWRITE"
To meet this policy, when deleting the image data on the HDD, the TOE overwrites with meaningless data to areas where image data exist.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to judge the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.LOCATION	**Ensuring security of the TOE in the operational environment** It is assumed that the MFP is operated under the controlled environment to prevent the security breach of the TOE by the potential attacks to the hardware of MFP. (Supplement) Power-off at inappropriate timing is also considered as an attack.
A.NETWORK	**Safety of the TOE from the external network** It is assumed that the TOE is used by connecting to the internal network that is protected against unauthorized access from the external network. (Supplement) There is an assumption that the MFP in which the TOE is installed, is connected to the internal network.
A.CE	**The reliability of service persons** It is assumed that the service persons in charge of the TOE are reliable and never act unfaithfully.

4.2 Environment Assumptions

The TOE is installed into the following MFPs manufactured by KYOCERA MITA Corporation and used.

- TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i
- TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG
- CS 3500i, CS 4500i, CS 5500i
- CD 1435, CD 1445, CD 1455
- DC 2435, DC 2445, DC 2455

It is assumed that the MFPs including the TOE are located in offices managed by

organizations such as enterprises and those departments. A typical usage environment of the TOE is shown in Figure 4-1.

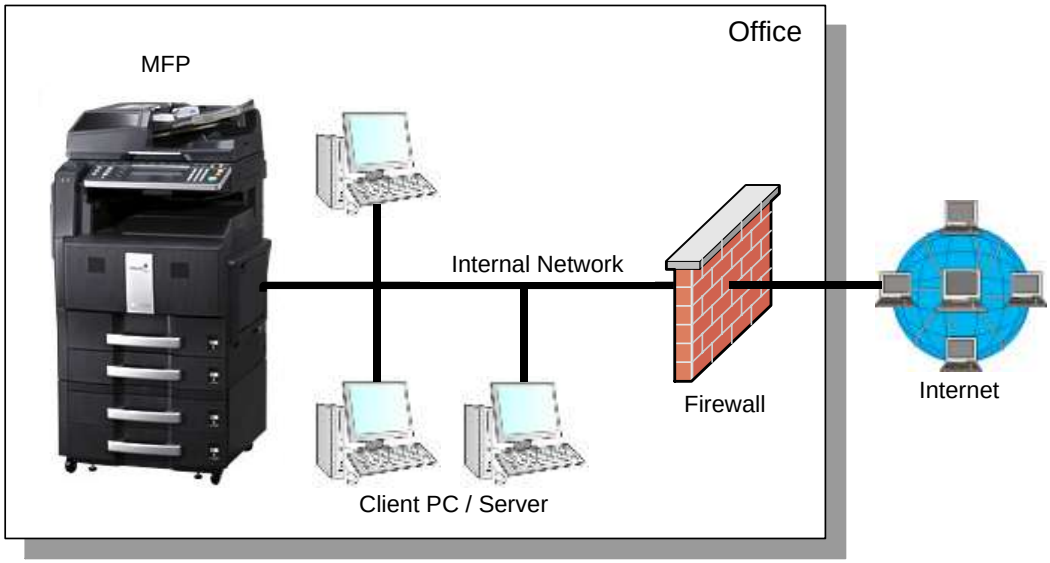

Figure 4-1 Operational Environment of the TOE

Although it is not necessary to connect it to the internal network, in order to use the functions of the MFP that connects to the internal network, the following software is needed for client PC and server. (Which is necessary depends on which function of the MFP is used.)

- Printer driver and TWAIN driver identified in the guidance
- Web browser (Microsoft Internet Explorer 8.0 was assumed in this evaluation)
- SMTP server, SMB server and FTP server

The firewall is provided to achieve A.NETWORK.

The scope of this evaluation does not include the reliabilities of a part of the MFP outside the TOE (the part that excludes the firmware and the ASIC), clients PC and server that connect to the internal network, software that is executed by client PC and server, as well as firewall. (It is assumed that these are reliable enough.)

4.3 Clarification of Scope

What this evaluation assures is limited to the following security functions that become activated by using the Data Security Kit (E) for the MFP.

- The function to encrypt image data when temporarily storing the image data in the HDD for the functions of the MFP (such as the copy function etc.)
- The function to overwrite the actual image data area when deleting the image data on the HDD.

The MFP in which the Data Security Kit (E) is not being granted, also has functions that are generally recognized as security functions (for example, identification/authentication or access control to protect the long-period stored image data from unauthorized access), however, these functions are not assured in this evaluation.

5. Architectural Information

This chapter explains the scope of the TOE and the main configuration (components).

5.1 TOE boundary and component

The TOE is the MFP firmware and ASIC, and main components are constituted as shown in Figure 5-1. The scope of the TOE excludes the part of the MFP except the firmware and ASIC.

The TOE performs MFP control including access control to the HDD. Therefore, the TOE will perform all the controls to the HDD including the following; storage of the image data in the HDD when user utilizes the MFP or deletion of the image data from the HDD. That is, regarding the image data that are created by users to utilize the MFP, the performance of the overwrite-erase function and the encryption function confirmed for this evaluation is reliable.

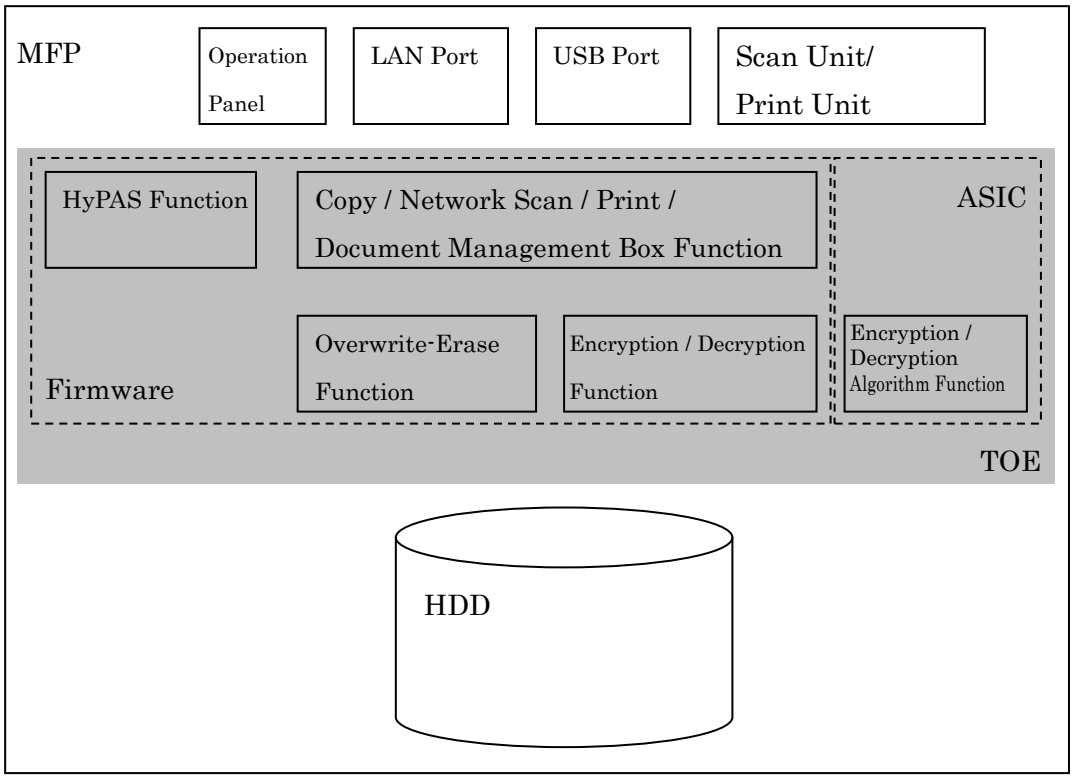

Figure 5.1 TOE boundary

Main components comprising the TOE (Copy Function, Network Scan Function, Print Function, Document Management Box Function, Overwrite-Erase Function, Encryption/Decryption Function, Encryption/Decryption Algorithm Function and HyPAS Function) are explained below.

- Copy/Network Scan/Print/Document Management Box functions

  These functions can be used no matter if the license of the Data Security Kit (E) is granted or not. These functions are not security functions.

  Respective functions of the MFP are provided as follows:

  > Copy Function
  It is a function to read image data from the scanner device, and outputs from the printer unit by inputting or operating from the operation panel.

> Network Scan Function
It is a function to transmit image data via LAN by inputting or operating from the operation panel. The image data have been read from the scanner unit.

> Print Function
It is a function to output the transmitted image data from the printer unit by operating from the client PC or server PC that is connected on the LAN or to USB.

> Document Management Box Function
The inputted image data are stored in the HDD for a long period of time, by inputting/operating from the operation panel or by operating from the client PC or server PC that is connected on the LAN or to USB,. The long-term stored image data can be printed out from the printer unit, forwarded to the client PC or server PC, and deleted.

When these functions are provided, it will be implemented to store image data into the HDD, to read out the image data from the HDD, and to delete the image data on the HDD.

As for reading and writing data on the HDD, the data written into the HDD are encrypted, and the data read out from the HDD are decrypted by performing "Encryption/Decryption Function".

To delete data on the HDD, "Overwrite-Erase Function" is used. Thus, it makes it difficult to recover the deleted data.

- Encryption/Decryption Function

This function will become available after the license is granted to use the Data Security Kit (E), and is a security function.

It is the function that reads and writes image data on the HDD.

When writing into the HDD, encryption is performed by using the AES encryption algorithm based on FIPS PUB 197. When reading out from the HDD, decryption is performed by using the same algorithm.

Encryption/Decryption algorithm is performed by using "Encryption/Decryption Algorithm Function".

- Encryption/Decryption Algorithm Function

This function will become available after the license is granted to use the Data Security Kit (E), and is a security function.
The AES Encryption Algorithm is performed based on FIPS PUB 197.

- Overwrite-Erase Function

This function will become available after the license is granted to use the Data Security Kit (E), and is a security function.

An area on the HDD, where the specified image data exist, is overwritten with meaningless data, which makes it difficult to recover, and the management information of the image data is then deleted.

- HyPAS Function

This function can be used no matter if the Data Security Kit (E) license is granted or not. However, it indirectly contributes to the security function in the sense of protecting a part of the security function.

This function is to install an application in the MFP and to activate it on the MFP. The application installed is not included in the TOE.

Only limited operations are allowed for the application, so any operation that would cause the security infringement is not allowed.

5.2 IT Environment

The TOE is installed in the MFP and performs. The MFP configuration components, especially related to the TOE, are as follows:

- Environment to perform the firmware (CPU or Memory)
- Scanner Unit to optically read image
- Printer Unit to perform printing
- HDD to store image data
- Operation Panel, LAN Port and USB Port that provide interfaces to users, client PC and server PC.

Client PC or server PC are connected via LAN Port or USB Port to be able to use the print function and the document management box function as well as to receive the image data transmitted by the network scan function.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

- User Manual

Name	Version	Destination
Data Security Kit (E) Operation Guide	Rev.3 2011.3	Overseas
Notice	303MS56320 2011.5	Overseas
Data Security Kit (E) Operation Guide Set-up Edition	303MS56710 2008.12	Overseas
3500i/4500i/5500i OPERATION GUIDE	2LHKMEN101 Rev.1 2011.4	Overseas
CD 1435 / DC 2435　CD 1445 / DC 2445 CD 1455 / DC 2455 Operation Guide	2LHUTEN001 Rev.1 2011.4	Overseas

- Service Manual

Name	Version	Destination
TASKalfa 3500i/4500i/5500i SERVICE MANUAL	2LHSM060 2011.3	Overseas

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2010-12 and concluded by completion of the Evaluation Technical Report dated 2011-07. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2011-02, 2011-03 and 2011-05, and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and interviewing staff. A part of the site visit of development and manufacturing sites has not been conducted, because it was judged to be able to reuse the evaluation result of the examined TOE in the past.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2011-05.

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

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had executed. As a result of the evidence shown in the process of the evaluation and those confirmed validity, the evaluator executed the reappearance testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual testing results. It explains the content of the developer testing evaluated by the evaluator as follows.

1) Developer Testing Environment

Configuration of the testing performed by the developer is shown in Figure 7-1.

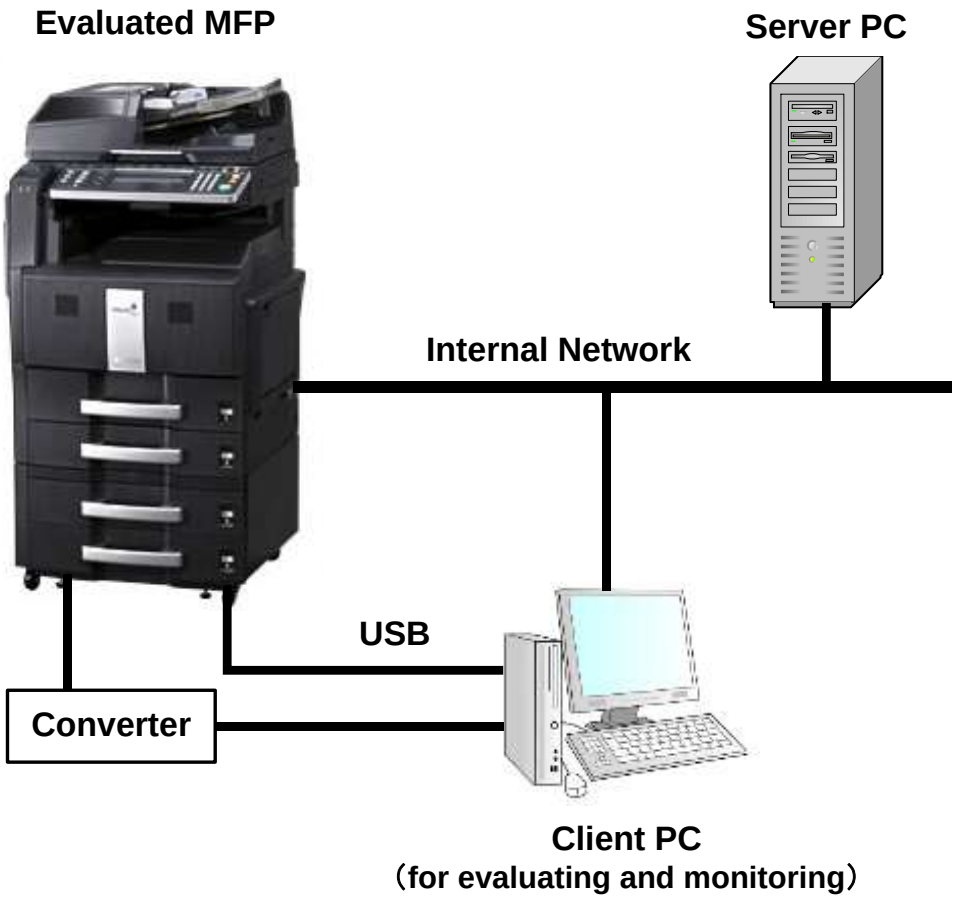

Figure 7-1 Configuration of the Developer Testing

- TOE
  The function that records log for the purpose of the testing was added to the TOE identified in the ST, and this was used for the evaluated MFP.
  The evaluator confirmed that the function added to the TOE would not influence on the behavior of the TOE functions by reviewing source code.

- MFP (Operational Environment of the TOE)
  TASKalfa 5500i was used.
  Although TASKalfa 3500i, TASKalfa 4500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445 and DC 2455 provide the same functions as the ones TASKalfa 5500i provides, these are different models in terms of speed and the number of HDD. By executing the testing with different amount of the print for the speed, the evaluator judged that it is able to cover cases using a model with a different speed. It was also confirmed that the executed testing covered the possible number of HDD. Therefore, all of the models of MFP described in the ST are covered.

- Printer Driver and TWAIN Driver (Operational Environment of the TOE)
  The following drivers were used for client PC.
  > Kyocera TASKalfa 5500i KX Ver. 5.2.1327d
  > Kyocera TWAIN Driver Ver. 1.8.1402
  The evaluator judged that the driver specified in the guidance would operate as well as the driver used in the testing. Because the driver specified in the guidance needs to be used in the ST, all of the drivers shown in the ST are covered.

- Web browser (Operational Environment of the TOE)
  The following was used for client PC.
  > Internet Explorer ver8.0.7600.16385

- SMTP server, SMB server and FTP server (Operational Environment of the TOE)
  The server software corresponding to SMTP, SMB and FTP protocol was used for the server PC. Thus, this is consistent with the one identified in the ST.

As mentioned above, the developer testing was performed in the same TOE operational environment as configuration of the TOE identified in the ST.

2) Summary of Developer Testing

Summary of the developer testing is as follows;

a. Outline of Developer Testing

Outline of the developer testing is as follows.

<Developer Testing Approach>

Although the function that can be confirmed through an external interface of the TOE (such as display on the operation panel relating to the security function) was tested by stimulating and observing through the external interface, the developer could not get enough confirmation by using this method regarding the overwrite-erase function and the encryption function. Therefore, the testing was supplemented by the following method.

- The approach to confirm if the encryption is correctly performed

  To obtain the data encrypted by the TOE function and written to the HDD in a state of the data without being decoded by debug operation.
  To decode the above-obtained data by using the same key as the one used for encryption in accordance with the different software AES from the TOE, and to confirm the data that are consistent with the data before being encrypted.

- The approach to confirm if the overwrite-erase function is correctly performed

  Regarding the additional function to the TOE that records a log, it enables to record the content of the corresponding part of the HDD before and after overwrite-erase operation. Then, the developer operates the overwrite-erase to be performed and observes the recorded log.

<Tools for the Developer Testing>

The tools used in the developer testing are shown in Table 7-1. The evaluator determined these tools would not affect the behavior of the TOE functions.

With regard to converter and cable, the developer confirmed that these tools correctly operate. With regard to the software AES, its reliability is confirmed by the testing performed using clear text/coded message and encryption key that are published by the NIST.

Table 7-1 Tools for Developer Testing

Name of tool	Outline and purpose of use
Converter, Cable	Debugging equipments for developer. It confirms if a log is recorded and implements debugging operation.
Software AES	Software that performs encryption and decryption by using the AES. It is used for confirmation of the encryption function.

<Content of the executed Developer Testing>

Observation results of the external interface as well as of recorded logs were compared to the expected values as shown in the testing plan.
Encrypted data obtained by the debug operations were decoded by using the software AES, and compared with the data before being encrypted to see the consistency.

b. Scope of Execution of the Developer Testing

The developer testing is executed on 111 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been tested enough.

c. Result

The evaluator confirmed an approach of the executed developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach.

The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results executed by the developer.

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the execution of the security function by the test items extracted from the developer testing. The evaluator executed an evaluator independent testing (hereinafter referred to as "the Independent Testing") to reconfirm that security functions are certainly implemented from the evidence shown in the process of the evaluation.

It explains the independent testing executed by the evaluator as follows;

1) Independent Testing Environment

The configuration of the testing executed by the evaluator was the same as the configuration of the developer testing.

Figure 7-1 shows the independent testing configuration executed by the evaluator.
The TOE and environment used in the evaluator independent testing were the same as the ones used for the developer testing. Therefore, the evaluator independent testing was performed in the same TOE testing environment as the configuration of the TOE identified in the ST.

2) Summary of Independent Testing

Summary of the Independent testing is as follows.

a. Viewpoints of Independent Testing

The points of view for the independent testing that the evaluator designed from the developer testing and the provided evaluation evidential materials are shown below.

Sampling of developer testing was performed as follows.

- It shall select all the testing items related to the behavior of the subsystem implementing the security functions.
- Regarding an external interface that calls a subsystem implementing the security functions to provide with these security functions, it shall select any possible external interfaces to make sure not to omit any of them and to cover differences between the interface providing methods.

Independent testing was designed from the viewpoint of eliminating the following concerns.

(1) Strictness is insufficient in the developer testing.
(2) Appropriate implementation of the interface is doubted from the developer testing result.
(3) Because a complex implementation is needed and cost-effectiveness is low in the testing, the testing execution is doubted.

b. Outline of Independent Testing

Outline of the independent testing performed by the evaluator is as follows;

<Independent Testing Approach>

The independent testing was performed using the same approach as the one used in the developer testing.

<Tools for the Independent Testing>

The same tools used in the developer testing as listed in Table 7-1 were used for the independent testing. However, Nmap 4.65.0.0 was additionally used to perform port scan.

<Content of the executed Independent Testing>

Independent testing was executed on 10 items by the evaluator.
As for the independent testing, 10 items were designed from the above-mentioned viewpoint (1); there is no independent testing from the viewpoint (2) and (3) because there was no concern that corresponds to the viewpoint (2) and (3). Table 7-2 shows the outline of the independent testing.

Table 7-2 Performed Independent Testing

Outline of Testing
It is confirmed whether the open port is within the specification with the port scan tool.
It is confirmed that the TOE accepts the data of the print with the FTP server, but it is unable to acquire the file by accessing the function of the FTP server.
It is confirmed not to be able to access to the Web server function of the TOE by illegally going back to the directory.
In order to confirm whether multiple jobs are correctly controlled, it is confirmed that a large amount of overwrite-erase data are accumulated, and the overwrite-erase operates correctly when other jobs are executed at the same time.
In order to confirm whether multiple jobs are correctly controlled, it is confirmed that the overwrite-erase function is completely executed after multiple jobs are simultaneously executed by using multiple TSFIs.
Normal operation of the encryption function and the overwrite-erase function in full HDD is confirmed.
The operation of the input size check for the buffer overflow prevention is confirmed.
Normal operation of the update check function in the firmware update-function is confirmed.
Normal operation of formal software check function is confirmed by downloading applications.
In document data operation job execution from the HyPAS application, normal operation of the security function is confirmed.

c. Result

All the executed independent testing was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

The evaluator devised and executed the necessary evaluator penetration testing (hereinafter referred to as "the penetration testing") for the possibility of exploitable concern at assumed environment of use and attack level. It explains the penetration testing executed by the evaluator as follows.

1) Summary of the Penetration Testing

Summary of the penetration testing executed by the evaluator is as follows.

a. Vulnerability of concern

The evaluator searched into the provided evidence and the public domain information for the potential vulnerabilities, and then identified the following vulnerabilities which require the

penetration testing.

(1) According to information in the guidance, there was a concern that a physical operation which easily enables to return the license of Data Security Kit (E) to the state of inactivating existed.

b. Penetration Testing Outline

The evaluator executed the following penetration testing to identify possibly exploitable vulnerabilities.

< Penetration Testing Environment>

The penetration test was performed in the same environment as the developer testing.

<Content of the executed Penetration Testing>

Table 7-3 shows the vulnerability concerned and the content of related penetration testing.

Table 7-3 Outline of Executed Penetration Testing

Vulnerability	Outline of the penetration testing
(1)	A physical operation with the concern that the license of Data Security Kit (E) returns to the state of inactivating is executed. Even if such an operation is executed, it is confirmed that the leakage of the protected assets does not happen.

c. Result

In the penetration testing conducted by the evaluator, the evaluator could not find any exploitable vulnerability that attackers who have the assumed attack potential could exploit.

7.4 Evaluated Configuration

Multiple models of MFP in the operational environment of the TOE are described in the ST. One of those models was selected for this evaluation. The evaluator determined the validity. (Refer to "7.3.1 Developer Testing".)

As the assumed software that is installed into client PC or server PC, there are printer driver, TWAIN driver, Web browser, SMTP server, SMB server and FTP server. These were prepared to be consistent with the ones described in the ST.

7.5 Evaluation Results

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

In the evaluation, the followings were confirmed.

- PP Conformance: none

- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL3 package

The result of the evaluation is applied to the composed by the corresponding TOE to the identification described in Chapter 2.

7.6 Evaluator Comments/Recommendations

The configuration excluding the fax function and other optional functions was evaluated. Determination for the validity of the security functions is out of this evaluation scope when having the fax function or other optional functions.

8. Certification

The certification body conducted the following certification based on the materials submitted by Evaluation Facility in the 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, the 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.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Report(s) and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 in the CC part 3.

8.2 Recommendations

It should be aware of what is evaluated as the security functions among the functions that the TOE has. For more details, refer to "4.3 Clarification of Scope".

9. Annexes

There is no annex.

10. Security Target

Security Target[12] of the TOE is provided within a separate document of this certification report.

TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i Data Security Kit (E) Overseas Version Security Target Version 0.80 (July 7, 2011) KYOCERA MITA Corporation

11. Glossary

The abbreviations relating to CC 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
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functionality

The abbreviations relating to TOE used in this report are listed below.

AES:	Advanced Encryption Standard
ASIC:	Application Specific Integrated Circuit
HDD:	Hard Disc Drive
MFP:	Multi Function Printer
NIST:	National Institute of Standards and Technology
USB:	Universal Serial Bus

The definitions of terms used in this report are listed below.

Client PC:	As against the TOE which is connected to the network, it indicates the computers on the network to utilize the TOE services (functions).
Image data:	It indicates the image information that is processed inside the MFP when TOE users use copy function, network scan function, print function and document management box function.
Long-period storage:	Keeping the image data on the HDD as users consciously perform the storage operation for this storage. This should be compared to "temporary storage".
Network scan:	A function to transmit the scanned image data or the stored image data in the document management box 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.

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.

Overwrite-erase: This is to overwrite on the actual image data area with meaningless character strings when receiving an instruction for deletion of the stored image data in the HDD, and to delete the management information of the image data after the actual data area is completely erased. Thus, it disables the reuse of data.

Temporary storage: Keeping the received image data temporarily on the HDD as is without outputting or forwarding, or keeping the image data temporarily on the HDD during the image processing. This is executed automatically during the process of the MFP without users being conscious about it. This should be compared to "long-period storage".

12. Bibliography

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

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

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

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001, (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, (Japanese Version 1.0, December 2009)

[12] TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i Data Security Kit (E) Overseas Version Security Target Version 0.80, July 7, 2011, KYOCERA MITA Corporation

[13] TASKalfa 3500i, TASKalfa 4500i, TASKalfa 5500i, TASKalfa 3500iG, TASKalfa 4500iG, TASKalfa 5500iG, CS 3500i, CS 4500i, CS 5500i, CD 1435, CD 1445, CD 1455, DC 2435, DC 2445, DC 2455 Data Security Kit (E) Evaluation Technical Report, Version 2.0, August 22, 2011, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center