Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-09-24 (ITC-9267)
Certification No.	C0270
Sponsor	KYOCERA MITA Corporation
Name of TOE	Data Security Kit (E) Software Type III
Version of TOE	V1.00J
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.
2010-09-28

Takumi Yamasato, 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 3.1 Revision 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2

Evaluation Result: Pass

"Data Security Kit (E) Software Type III V1.00J" 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 "Data Security Kit (E) Software Type III V1.00J" (hereinafter referred to as "the TOE") developed by KYOCERA MITA Corporation, and evaluation of the TOE was finished on 2010-09-15 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 book together. Especially, the TOE security functional requirements, the assurance requirements for TOE and rationale of sufficiency about those are specifically described in ST.

This certification report assumes such as "system administrator in consumer site which the TOE is introduced and used" to be a reader. 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.

1.1 Product Overview

Overview of the TOE function and operational condition are as follows; Refer since Chapter 2 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 Data Security Kit (E) Software Type III V1.00J.

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 it in order to protect against the image data 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 TOE assumes threats and assumptions as described in the following items.

1.1.2.1 Threat and Security Objectives

The TOE provides the following security functions for countermeasure to the respective threats.

- It is assumed the threat is that the HDD inside the MFP is pulled out when operating or after discarding/returning, and the image data temporarily stored in the HDD because of the MFP functions (copy function etc.) is leaked.
  Here the object is the image data (for example, it is the scanned image data using the copy function and will be stored until completion of printing operation.) stored for the MFP functions that is nothing related to user's intention. The image data that the user intentionally stored is not the object.
  To counter this threat, the TOE encrypts the image data and then stores it when storing the image data in the HDD.

- It is assumed the threat is that the HDD inside the MFP is pulled out when operating or after discarding/returning, and the deleted image data is recovered and leaked.
  Here the object will be the case that the stored image data is intentionally deleted by a user and another case that the image data temporarily stored for the MFP functions is automatically deleted.
  To counter this threat, when deleting the image data on the HDD, the TOE overwrites the actual image data area and that disables re-usage of the data. Therefore it protects against the image data leakage.

1.1.2.2 Configuration and Assumptions

It is assumed that the evaluated products are managed under the following configurations and assumptions.

- The TOE is installed to be used for the following MFP manufactured by KYOCERA MITA Corporation:

  > TASKalfa 300i

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

- In this usage environment, it is assumed that the place where the MFP is located can be watched by employees, and actions that can be at least clearly recognized as attacks are prevented. However considering the configuration of the MFP, it is relatively easy to remove the HDD. Thus there is still a possibility not to be able to prevent it.

- When the MFP is connected to the network, it is assumed that it is 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 organization), access to the MFP from the external network is controlled to be restricted.

- It is assumed that the service person is reliable.

1.1.3 Disclaimers

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

1.2 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"[1], "IT Security Certification Procedure"[2] and "Evaluation Facility Approval Procedure"[3]. Evaluation was completed on 2010-09.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] 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.
Those concerns pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM ([10] or [11]).
The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE:	Data Security Kit (E) Software Type III
Version of TOE:	V1.00J
Developer:	KYOCERA MITA Corporation

The condition for being the TOE which has been evaluated and certified is that the license is granted to use 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 is consistent 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 thus 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. Thus to get a confirmation of the correct MFP will also be to get a confirmation of the correct ASIC.

3. Security Policies

This chapter describes how the TOE performs the function as security services in accordance with what kind of policies or rules.

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 is temporarily stored in the HDD as needed. It is called "temporary storage" when the image data is temporarily stored for the MFP functions without users being conscious about it.

When operations of these functions are completed and so the temporary stored image data become unnecessary, it is then automatically deleted.

The TOE also provides function that stores 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 is stored over a long period of time with user's intention, and this should be distinguished from the temporary storage.

The image data stored for a long period of time is not deleted without user's instruction.

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

When deleting the temporary stored image data or the stored image data for a long period of time, the TOE overwrites on the actual image data area so that leakage of the image data is prevented.

(Note)
As long as the stored image data over a long period of time is not deleted, it is not considered as the image data that should be protected against leakage.

3.1 Security Function Policies

The TOE has the security functions that counter the threats as shown in 3.1.1.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes threats as listed in table 3-1, and has the functions to counter the threats.

Table 3-1 Assumed Threats

Identifier	Threat
T.TEMP	**Unauthorized access to the temporary stored data.** Attackers may remove the HDD and be unauthorized to read out and steal the image data temporarily stored in the HDD by using the tools that are easily available.
T.RESIDUAL	**Unauthorized access to the residue data.** Attackers may remove the HDD and be unauthorized to recover, decode, read out and steal the remaining data in the HDD even after deletion of the image data by using the tools that are easily available. (Supplement) Both of the following are the objects for deletion of the image data. - The TOE automatically deletes the temporary stored image data. - The TOE deletes the stored image data for a long period of time by user's instruction.

3.1.1.2 Security Function Policies against Threats

The TOE counters the following security function policies against the threats as presented in the table 3-1.

(1) Countermeasure to threat "T.TEMP"
To counter this threat, the TOE encrypts image data and then stores it when storing the image data in the HDD.

(2) Countermeasure to threat "T.RESIDUAL"
To counter this threat, the TOE overwrites an actual image data area with meaningless data when deleting the image data on the HDD.
Countermeasure to threat "T.TEMP" (as above) counters threat that the temporary stored image data is read out. Thus this threat is countered doubly.

3.1.2 Organizational Security Policy and Security Function Policy

There is no organizational security policy that the TOE supports.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environments required in use of the TOE, as useful information for assumed readers to determine if they use the TOE.

4.1 Usage Assumptions

Assumptions required in using the TOE are shown in table 4-1.
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	**Safe security of the TOE in the operational environment** To protect the hardware inside the MFP from being possibly attacked (i.e. violating the TOE security), it is assumed that the TOE operates in mutually watchable and manageable environment. Regarding the attacking to the hardware, it is assumed that the attacker opens up the MFP to make it connect to devices for analyzing or replacing the MFP board. (Supplement) This indicates that it is used under mutually watchable and in the manageable environment so that actions that are clearly recognized as the attacking such as opening the internal MFP, connecting it to devices and analyzing, or replacing the MFP board, can be prevented. However, to remove the HDD may not be completely prevented by mutual watching, because it is relatively easier than the clearly recognizable attacking as above-mentioned because of configuration of the MFP. Therefore even if the assumption is satisfied, but it is still regarded as the possible attack method and is raised as threat.
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) This is the assumption that the MFP in which the TOE is installed, is connected to the internal network.
A.CE	**The service person reliability** It is assumed that the TOE service person is a reliable person and does not act unfaithfully.

4.2 Environment Assumptions

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

- TASKalfa 300i

It is assumed that the MFPs including the TOE are located in offices managed by organizations such as enterprises and these departments. A typical operational environment of the TOE is as shown in figure 4-1.

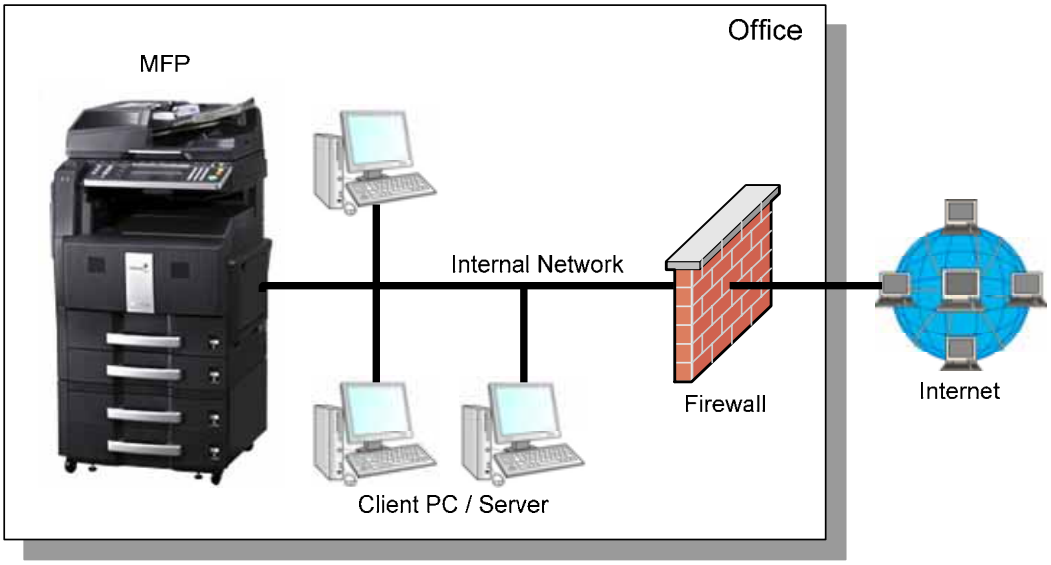

Figure 4-1 Operational Environment of the TOE

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

- Printer driver and TWAIN driver identified by the guidance
- SMTP server, SMB server and FTP server

The firewall is provided to achieve A.NETWORK.

Reliability of the part of the MFP outside the scope of 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 firewall are outside the evaluation scope.(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 MFP.

- The function that encrypts 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 that overwrites 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 image data stored over a long period of time from unauthorized access) however, these functions are not assured by this evaluation.

5. Architectural Information

This chapter describes purposes and relations with respect to the scope of the TOE and main configuration (components).

5.1 TOE boundary and component

TOE is the MFP firmware and ASIC. Main components are constituted as shown in figure 5-1. The part of the MFP except the firmware and ASIC is outside the scope of the TOE.

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 is created by users to utilize the MFP, performance of the overwrite-erase function and the encryption function confirmed for this evaluation are reliable.

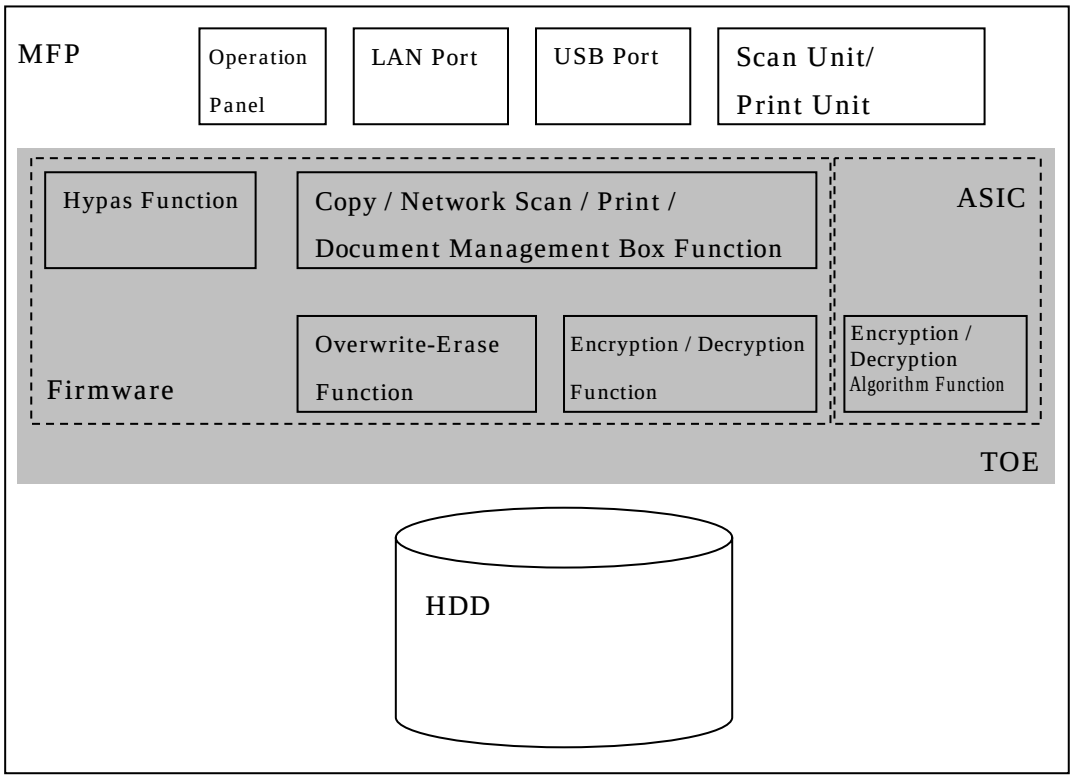

Figure 5-1 TOE Boundary

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.

- Copy/Network Scan/Print/Document Management Box function
  These functions can be used no matter if the license of the Data Security Kit (E) is granted or not. These functions are not the security functions.

  Respective functions of the MFP are provided as follows:

> Copy Function
A function that reads image data from the scanner device, and outputs from the printer unit by inputting or operating from the operation panel.

> Network Scan Function
A function that transmits image data read from the scanner unit, via LAN by inputting or operating from the operation panel.

> Print Function
A function that outputs image data transmitted from server PC or client PC connected over LAN or to USB, from the printer unit by operating from the client PC or serve PC.

> Document Management Box Function
The image data inputted by inputting/operating from the operation panel or operating through the client PC or the server PC connected over LAN or to USB is stored in the HDD for a long period of time. The image data stored in the HDD for a long period of time can be printed out, forwarded to the client PC or the 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 is encrypted, and the data read out from the HDD is decrypted by performing "Encryption/Decryption Function".

When data is deleted on the HDD, "Overwrite-Erase Function" is used. Thus it will be difficult to get back 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 the 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 the 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 the security function.

An area on the HDD where the specified image data exists is overwritten with meaningless data, and that 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 by meaning of protecting the 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, and any operation that would cause the security infringement is not possible.

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 provides interfaces with 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 be able to receive the image data transmitted by using the network scan function.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required full understanding of following documents and compliance with descriptions in order to fulfill the assumptions.

- User Manual

Name	Version	Destination
Data Security Kit (E) Operation Guide	Rev.2 2010.8	Japan
Notice	303MS56320 2010.1	Japan
Data Security Kit (E) Operation Guide Set-Up Edition	303MS56710 2008.12	Japan
TASKalfa 300i Operation Guide	302K556010 First Edition 2009.9	Japan

- Service Manual

Name	Version	Destination
TASKalfa 300i Service Manual	2K5SM001 Rev.1 2010.2	Japan

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 requirements in CC Part 3. Details for evaluation activities are reported 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.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows; Evaluation has started on 2009-09 and concluded by completion the Evaluation Technical Report dated 2010-09 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 2009-12, 2010-01 and 2010-03 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 the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-03.

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 the developer and all concerns were solved eventually.

7.3 IT Product Testing

The evaluator confirmed the validity of the test that the developer had executed. The evaluator executed reappearance tests, additional tests and penetration tests based on vulnerability assessments judged to be necessary from the evidence shown by the process of the evaluation and results by the verification of the developer testing.

7.3.1 Developer Testing

The evaluator evaluated the integrity of developer testing that the developer executed and the test documentation of actual test results. The overview of evaluated developer testing is shown as follows;

1) Developer Test Environment

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

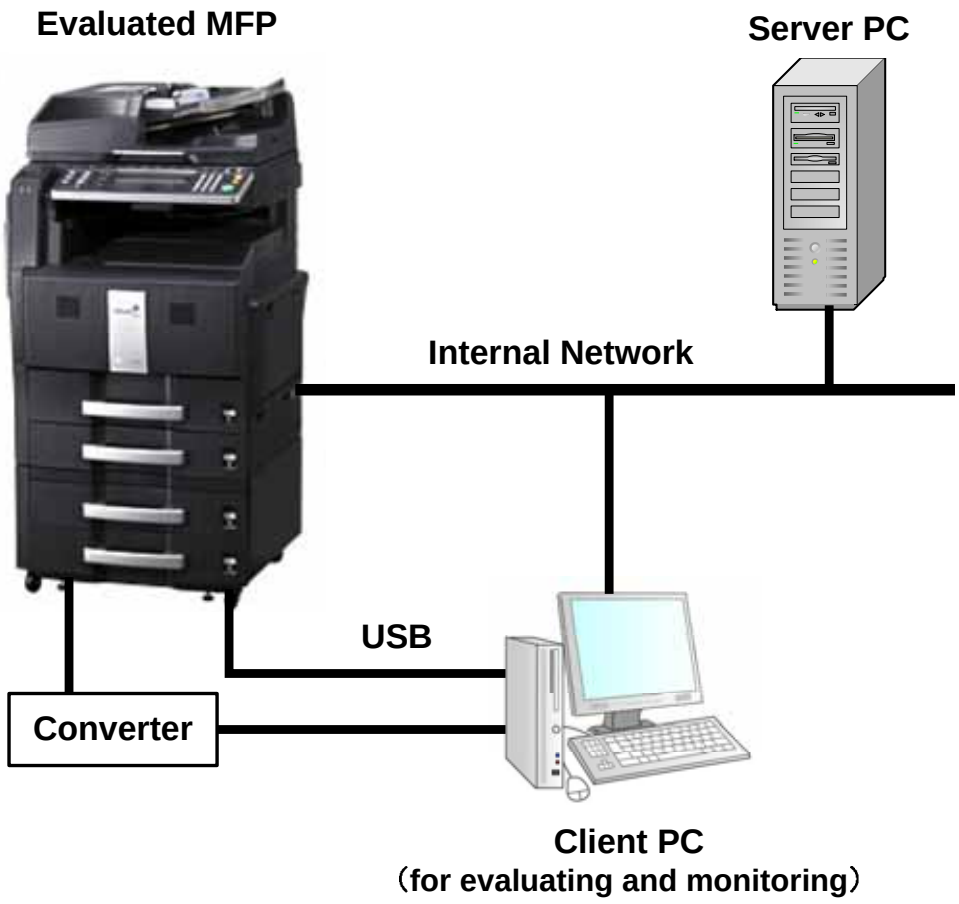

Figure 7-1 Configuration of the developer testing

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

- MFP (Operational Environment of the TOE)
  TASKalfa 300i was used.
  This is consistent with the MFP model identified in the ST.

- Printer Driver and TWAIN Driver (Operational Environment of the TOE)
  The following drivers were used for client PC.
  > Kyocera TASKalfa KX Ver 5.0.2130a
  > Kyocera TWAIN Driver Ver 1.7.1106
  These are consistent with the one identified in the guidance. Also, ST requires the one identified in the guidance. Thus these are consistent with the one identified in ST.

- SMTP server, SMB server and FTP server (Operation 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 ST.

From the above-mentioned, the developer testing was conducted in the same TOE operational Environment as configuration of the TOE identified in the ST.

2) Outline of Developer Testing

The testing performed by the developer is as follows:

a. Test Outline
Outline of the testing performed by the developer is as follows:

<Developer Testing Approach>
Although the function that can be confirmed through an external interface of the TOE (changing an icon relating to the security function displayed on the operation panel etc) was tested by stimulating and observing through the external interface but, 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.

  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.
  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 confirm the data that is 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 recording the content of the appropriate portion in the HDD before and after overwrite-erase operation. Then the developer operates the overwrite-erase to be performed, and observes the recorded log.

<Developer Testing Tools>
The tools used in the developer testing are shown in table 7-1. The evaluator determined these tools would not affect 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 conducted using clear text/coded message and encryption key that are published by the NIST.

Table 7-1 Tools used in 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.

<Implementation of Developer Testing>
Observation results of the external interface as well as of recorded logs were compared to the expected values as shown in the test plan.
Encrypted data obtained by the debug operations, was decoded by using the

software AES, and it was then compared to see consistency with the data before being encrypted.

b. Scope of Test Performed
103 items of testing are performed by the developers.
The coverage analysis was conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis was conducted and examined to testing satisfactorily all the subsystems described in the TOE design and the subsystem interfaces.

c. 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.

7.3.2 Evaluator Independent Testing

The evaluators performed the independent testing using the evidence, which were provided during the evaluation process, in order to revalidate the security functions of the product are securely performed. The following are the overview of the independent testing that the evaluators performed.

1) Evaluator Independent Testing Environment

Configuration of test performed by the evaluator is the same configuration as the developer testing.
Configuration of test performed by the evaluator is the same configuration as the developer test configuration shown in the figure 7-1.
The TOE and environment used in the evaluator independent testing were the same as the one used for the developer testing. Therefore the evaluator independent testing was conducted in the same TOE testing environment as the configuration of the TOE identified in the ST.

2) Overview of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. Viewpoints of the Evaluator Independent Testing
The evaluator devised the evaluator independent testing in the following points of view from the developer testing and the provided evaluation documents.

Sampling of developer testing was conducted as follows.
- Selected all the testing items related to behavior of the subsystem implementing the security functions.
- Regarding an external interface that calls a subsystem implementing the security functions so that it can provide with these security functions, selected any possible external interfaces to make sure not to omit any one of them and to cover differences between the interface providing methods.

Since there was a concern that the overwrite-erase function could be affected by other operations, the evaluator devised the independent testing to obtain assurance that the overwrite-erase function would correctly perform under the different

condition and at the different timing from the developer testing. With regard to buffer overflow prevention mechanism, the evaluator also devised the test conducted by different inputs from the developer testing.

<Viewpoints of the Independent Testing>
1. Confirm that the overwrite-erase function does not perform when parameters related to the temporary stored data are different from the ones used for the developer testing.
2. Confirm that the overwrite-erase function correctly performs when it is interfered with the sleep mode operation.
3. Confirm that the overwrite-erase function correctly performs when it is interfered with usage of the MFP functions.
4. Confirm that the buffer overflow prevention mechanism correctly performs when the independent testing is conducted by providing the different input from the ones inputted in the developer testing.

b. Outline of the Independent Testing
Outline of the independent testing performed by the evaluator is as follows;

<Independent Testing Approach>
The independent testing was conducted using the same approach as the one used in the developer testing.

<Independent Testing Tools>
The tools used in the developer testing as listed in the table 7-1 were used.

<Implementation of the independent testing>
The viewpoints of the independent testing devised by the evaluator and the corresponding testing contents are described in table 7-2.

Table 7-2 the Independent Testing Conducted

Viewpoint of the Independent Testing	Test Outline
1	Confirm that the overwrite-erase function does not operate when using the MFP functions without generating the temporary stored data.
2	Manually switch on the sleep mode during processing of the overwrite-erase, and then confirm if overwrite-erase operation is correctly completed.
3	Operate the copy function during processing of the overwrite-erase, and then confirm if the overwrite-erase is correctly completed.
4	Attempt to print out the image data that will become large size after developing to the original image, and the image data that has the different size of the information from the actual image data size, and then confirm if there is no problem caused.

c. Result
All the evaluator independent testing conducted were correctly completed, and the behavior of the TOE was confirmed. The evaluator confirmed consistencies between all the test results and the expected behaviors.

7.3.3 Evaluator Penetration Testing

The evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern at assumed environment of use and attack level from the evidence provided through the evaluation process. Outlining of the evaluator penetration testing is as follows:

1) Outlining of Evaluator Penetration Testing
The penetration testing performed by the evaluator is as follows;

a. Vulnerability concerned
The evaluator searched the potential vulnerability from the evidence provided and the well-known information, and identified the following vulnerability that requires the penetration testing.

1. When non-assumed port opens, there is a possibility that the port may become a spot of a channel for invasion.
2. When the FTP service is not appropriately configured, there is a possibility of unauthorized access to data.
3. In a state of small remaining capacity in the HDD, there is a possibility that the security functions may incorrectly perform because of the running out of resources or time-out.
4. Consistencies between the job contents may be destroyed by rearranging the order of jobs (using the MFP functions) with respect to the same image data so that there is a possibility that the security functions may incorrectly perform.
5. When the web server function is not appropriately configured, there is a possibility of unauthorized access to data.
6. There is a possibility that the activation information of the security functions may be physically changed to a state of non-activation and be used for a wrong purpose.
7. There is a possibility that the TOE may be changed by using the update function of the firmware.
8. Due to mechanism for domain separation, unauthorized access from HyPAS application to an area where image data is stored can not be done but, assurance has not been fully made if the TOE behaves as expected.
9. There was a concern at the evaluation of initializing the TOE that the security kit does not correctly activate when turning off the power during activation of the security kit.

b. Penetration Test Outline
The evaluator conducted the following penetration testing to determine if there is a possibility of using the potential vulnerability for a wrong purpose.

<Penetration Test Environment>
The penetration test was conducted in the same environment as the developer testing. However, Nmap 5.21 was additionally used for performing port scan.

<Implementation of Vulnerability Testing>
The concerned vulnerability identified by searching the potential vulnerability and the corresponding evaluator penetration test are described in table 7-3. The evaluator conducted the following evaluator penetration test to determine if there is a possibility of using the potential vulnerability for a wrong purpose.

Table 7-3 Penetration Testing Outline

Vulnerability	Test Outline
1	Tests were conducted to confirm if a port that is not mentioned in the specification is opened or not by using the port scan tool.
2	Tests were conducted to confirm that unauthorized access to image data in HDD is not available by connecting to FTP service and attempting to move directory or to obtain files.
3	Tests were conducted to perform many functions and so that makes remaining capacity small in the HDD, and to further perform the MFP functions. Even in such a case, the tests were conducted to confirm that performance of the overwrite-erase is correctly completed.
	Same as the above, tests were conducted to attempt to store image data exceeding the remaining capacity in the HDD in a state of small remaining capacity in the HDD. Even in such a case, the tests were conducted to confirm that the TOE still does not incorrectly activate.
4	Tests were conducted to confirm that rearranging the waiting order of the jobs (using the MFP functions) with respect to the same image data would not cause the incorrect activation of the TOE. Specifically, when the outcome is "print after deletion" after rearranging the job order, this would be a concern.
5	Tests were conducted to confirm that there would not be the directory traversal on the TOE web server functions by inputting that could cause a concern about the directory traversal.
6	Tests were conducted to confirm that even if someone attempt to physically change the activation information of the security functions to a state of non-activation but, unauthorized changes still can not be done.
7	Tests were conducted to prepare the different content of the firmware data from the one officially provided by vendors, and to confirm that even if someone attempt unauthorized update on TOE but, this attempt would still be rejected.
8	Tests were conducted to confirm that even if someone attempt unauthorized access from HyPAS application to an area where image data is stored, however this still can not be done.
9	Tests were conducted to confirm that even if the power is turned off during the activation of the security kit, however the security kit would still continue to correctly activate after the power is again turned on.

c. Result

In the conducted evaluator penetration testing, the exploitable vulnerability that attackers who have the assumed attack potential could not be found.

7.4 Evaluated Configuration

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

There are printer driver, TWAIN driver, SMTP server, SMB server and FTP server as

the assumed software that is installed into client PC or server PC. These were prepared to be consistent with the ones described in ST.

Although it is not clearly described in ST, but it is assumed that Web browser is also installed into client PC or server PC. There is no operation relating to the TOE security functions from a web browser, so only one (Internet Explorer ver 6.0 sp1) was prepared.

7.5 Evaluation Results

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

As a result of the evaluation, the following assurance components were judged, "Passed".

- All assurance components of EAL3 package

In the evaluation, the following were confirmed.

- PP Conformance: none
- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

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

8.1 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 determined the TOE is satisfied the assurance requirements of EAL3 components prescribed in CC Part 3.

8.2 Recommendations

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

9. Annexes

There is no annex.

10. Security Target

Security Target of the TOE [12] is published as follow, separately from this report.

KYOCERA MITA Data Security Kit (E) Software Type III Japan Version Security Target Version 1.10 (August 10, 2010) 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
USB	Universal Serial Bus

The definition of terms used in this report is listed below.

Client PC	It indicates the computers that connect to the network, and utilizes the TOE services (functions) of the TOEs that are connected to the network.
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. The users will have to consciously conduct 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 re-usage of the data.

Temporary storage

Keeping the received image data temporarily on the HDD without outputting it or forwarding it as is, or keeping the image data temporarily on the HDD during the image processing. This is executed automatically during the process of the MFP without the 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 1 September 2006 CCMB-2006-09-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[7] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001 (Japanese Version 2.0, March 2008)

[8] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002 (Japanese Version 2.0, March 2008)

[9] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003 (Japanese Version 2.0, March 2008)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[11] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004 (Japanese Version 2.0, March 2008)

[12] KYOCERA MITA Data Security Kit (E) Software Type III Japan Version Security Target Version 1.10 (August 10, 2010) KYOCERA MITA Corporation

[13] Data Security Kit (E) Software Type III Japan Version Evaluation Technical Report Version 1.1, September 15, 2010, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center