Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2013-09-19 (ITC-3475)
Certification No.	C0446
Sponsor	KYOCERA Document Solutions Inc.
TOE Name	TASKalfa 3010i, TASKalfa 3510i, TASKalfa 3010iG, TASKalfa 3510iG, CS 3010i, CS 3510i, 3060i, 3560i with Data Security Kit (E), FAX System (W)
TOE Version	System: 2NL_2000.C01.201 Panel: 2NP_7000.C01.200 FAX: 3N6_5100.B04.001
PP Conformance	IEEE Std 2600.1™-2009
Assurance Package	EAL3 augmented with ALC_FLR.2
Developer	KYOCERA Document Solutions Inc.
Evaluation Facility	Information Technology Security Center, Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.

2014-10-30

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass

"TASKalfa 3010i, TASKalfa 3510i, TASKalfa 3010iG, TASKalfa 3510iG, CS 3010i, CS 3510i, 3060i, 3560i with Data Security Kit (E), FAX System (W)" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT 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

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "TASKalfa 3010i, TASKalfa 3510i, TASKalfa 3010iG, TASKalfa 3510iG, CS 3010i, CS 3510i, 3060i, 3560i with Data Security Kit (E), FAX System (W), Version System: 2NL_2000.C01.201 Panel: 2NP_7000.C01.200 FAX: 3N6_5100.B04.001" (hereinafter referred to as the "TOE") developed by KYOCERA Document Solutions Inc., and the evaluation of the TOE was finished on 2014-10-27 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, KYOCERA Document Solutions Inc., and provide security information to procurement personnel and consumers who are interested in the TOE.

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

This Certification Report assumes "procurement personnel who purchase the TOE" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

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

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a digital Multi-function Product (hereafter "MFP"), which provides the basic functions such as copy function, scan to send function, print function, FAX function and box function.

In addition to the basic functions of the MFP, the TOE provides security functions to protect document data used in the basic functions and the setting data affecting security, from disclosure and alteration.

For 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 next clause describes the assumed threats and assumptions of the TOE.

1.1.2.1 Threats and Security Objectives

The TOE assumes the following threats and provides the security functions to counter them.

For protected assets such as user document data and the setting data affecting security, there are threats of unauthorized disclosure and alteration caused by unauthorized

operation of the TOE and by unauthorized access to the communication data on the network that the TOE is connected.

The TOE provides the security functions such as identification and authentication, access control and encryption, to prevent those protected assets from unauthorized disclosure and alteration.

1.1.2.2 Configuration and Assumptions

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

The TOE is assumed to be located in an environment where physical components and interfaces of the TOE are protected from the unauthorized access. For the operation of the TOE, the TOE shall be properly configured, maintained, and managed according to the guidance documents.

1.1.3 Disclaimers

The following operation and functions are not included in the assurance provided by this evaluation.

In this evaluation, only the configuration, to which the setting condition shown in "7.5 Evaluated Configuration" is applied, is evaluated as the TOE. If the TOE settings are changed, the configuration will not be assured by this evaluation.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2014-10, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility and evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	TASKalfa 3010i, TASKalfa 3510i, TASKalfa 3010iG, TASKalfa 3510iG, CS 3010i, CS 3510i, 3060i, 3560i with Data Security Kit (E), FAX System (W)
TOE Version:	System: 2NL_2000.C01.201 Panel: 2NP_7000.C01.200 FAX: 3N6_5100.B04.001
Developer:	KYOCERA Document Solutions Inc.

Users can verify that a product is the TOE, which is evaluated and certified, by following means.

Users operate on the operation panel according to the description in the product guidance documents, and confirm the TOE name and version information displayed on the MFP operation panel by comparing them with the following list.

- MFP name: Either of the following
  TASKalfa 3010i, TASKalfa 3510i, TASKalfa 3010iG, TASKalfa 3510iG,
  CS 3010i, CS 3510i, 3060i, 3560i
- Option name: “Data Security Kit (E)” and “FAX System (W)”
- Each version of System, Panel, and FAX

3. Security Policy

This chapter describes security function policies and organizational security policies that the TOE adopts to counter threats.

The TOE provides the basic functions of the MFP such as copy function, scan to send function, print function, FAX function, and box function, and has functions to store user document data in the HDD inside the TOE and to communicate with user clients and various servers via network.

When using those functions, the TOE provides security functions that meet the security functional requirements required by the Protection Profile for MFPs, IEEE Std 2600.1™-2009 [14] (hereinafter referred to as the "PP"). The security functions that the TOE provides include user identification and authentication, access control, encryption of the document data stored in the HDD, overwrite-erase upon deletion of the document data, and encryption communication. Those functions prevent user document data and the setting data affecting security that are protected assets from unauthorized disclosure and alteration of the data.

The TOE assumes the following user roles.

- Normal user
  A user of the basic functions of the MFP, such as copy function, scan to send function, print function, FAX function, and box function that the TOE provides.

- Device Administrator
  A TOE user who has special authority to configure settings of the TOE security functions.

- TOE Owner
  Any person or organizational entity responsible for protecting TOE assets and realizing the security objectives for operational environment of the TOE.

The protected assets of the TOE are also defined as follows.

- User Document Data
  Document data of users.

- User Function Data
  User Function Data are the information relevant to user document data or jobs to be processed by the TOE. For the TOE, job data that are generated when performing the basic functions of the MFP are included.

- TSF Confidential Data
  TSF Confidential Data are the data used for security functions, and whose integrity and confidentiality are required. For the TOE, login user passwords, an encryption key, and audit logs are included.

- TSF Protected Data
  TSF Protected Data are the data used for security functions and whose integrity only is required. For the TOE, various setting values of security functions, such as login user names, job executable authorization, box permission that stores document data, and network setting, excluding TSF Confidential Data, are included.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1, and to meet the organizational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them. These threats are the same as the threats described in the PP.

Table 3-1 Assumed Threats

Identifier	Threat
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons.
T.DOC.ALT	User Document Data may be altered by unauthorized persons.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies. Details of the respective security functions are described in Chapter 5.

1) Countermeasures against the threats "T.DOC.DIS," "T.DOC.ALT," and "T.FUNC.ALT"

These are threats to user data (User Document Data and User Function Data). The TOE counters the threats by the "User Management function," the "Job Authorization function," the "Data Access Control function," the "Overwrite-Erase function," and the "Network Protection function."

The "User Management function" of the TOE is a function that allows only successfully identified and authenticated users to use the TOE.

The "Job Authorization function" of the TOE is a function that checks the executable authorization assigned to the users, and allows only authorized users to use the basic functions, when identified and authenticated users attempt to use the basic functions of

the MFP such as copy function, scan to send function, print function, FAX function, and box function.

The “Data Access Control function” of the TOE is a function that performs access control when users attempt to operate the basic function of the MFP on user data, and allows only authorized users to access to the user data.

The “Overwrite-Erase function” of the TOE is a function that overwrites the area of the HDD where the document data were stored when the document data are deleted. This protects the residual information from being referred to.

The “Network Protection function” of the TOE is a function that uses SSL encryption communication protocol and encrypts the communication data when the TOE communicates with client PCs and various servers.

With the above-described functions, the TOE prevents the user data to be protected from disclosure and alteration caused by unauthorized usage of the TOE or unauthorized access to the communication data.

2) Countermeasures against the threats “T.PROT.ALT,” “T.CONF.DIS,” and “T.CONF.ALT”

These are threats to data used for security functions. The TOE counters the threats by the “User Management function,” the “Security Management function,” and the “Network Protection function.”

The “User Management function” and the “Security Management function” of the TOE are functions that allow only identified and authenticated device administrators to refer to and change the data used for security functions. For normal users, they are allowed to change their login passwords.

The “Network Protection function” of the TOE is a function that uses encryption communication protocol and encrypts the communication data when the TOE communicates with client PCs and various servers.

With the above-described functions, the TOE prevents the data to be protected from disclosure and alteration caused by unauthorized usage of the TOE or unauthorized access to the communication data.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE are shown in Table 3-2. These organizational security policies are the same as the security policies described in the PP, except that P.HDD.ENCRYPTION is added.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.ENCRYPTION	To improve the confidentiality of the documents, User Data and TSF Data stored in HDD will be encrypted by the TOE.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the following security functions to meet the organizational security policies shown in Table 3-2. Details of the respective security functions are described in Chapter 5.

1) Means to support organizational security policy "P.USER.AUTHORIZATION"

   The TOE realizes this policy by the "User Management function" and the "Job Authorization function."

   The "User Management function" of the TOE is a function that allows only successfully identified and authenticated users to use the TOE.

   The "Job Authorization function" is a function that checks the executable authorization assigned to the users, and allows only authorized users to use the basic functions, when identified and authenticated users attempt to use the basic functions of the MFP such as copy function, scan to send function, print function, FAX function, and box function.

2) Means to support organizational security policy "P.SOFTWARE.VERIFICATION"

   The TOE realizes this policy by the "Self-Test function."

The “Self-Test function” of the TOE is a function that verifies whether or not the HDD encryption function using an encryption key correctly performs upon start-up, and that verifies the integrity of TSF executable code upon receipt of an instruction from a device administrator.

3) Means to support organizational security policy “P.AUDIT.LOGGING”

The TOE realizes this policy by the “Audit Log function.”

The “Audit Log function” of the TOE is a function that records security-relevant events as audit logs. Only identified and authenticated device administrators can read out and delete the stored audit logs. However, they cannot modify the audit logs.

4) Means to support organizational security policy “P.INTERFACE.MANAGEMENT”

The TOE realizes this policy by the “User Management function” and the “Network Protection function.”

The “User Management function” of the TOE is a function that allows only successfully identified and authenticated users to use the TOE. When a state in which a user does not perform any operations continues for the specified period of time, the TOE terminates a session.

Regarding the “Network protection function” of the TOE, the data received from the external interfaces of the TOE must be processed by the TOE. This prevents unauthorized forwarding of the data from the external interfaces, including telephone lines, to the internal network.

5) Means to support organizational security policy “P.HDD.ENCRYPTION”

The TOE realizes this policy by the “HDD Encryption function.”

The “HDD Encryption function” of the TOE is a function that encrypts data to be written to the HDD. The encryption algorithm is 256 bits AES.

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 determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. These assumptions are the same as the assumptions described in the PP. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Identifier	Assumptions
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 Environmental Assumptions

The TOE is installed in offices and connected to the internal network, and it is used from client PCs connected to the internal network as well. Figure 4-1 shows the general operational environment of the TOE.

Although it is not shown in Figure 4-1, it is possible to use the print function of the TOE by connecting client PCs to the TOE via USB ports.

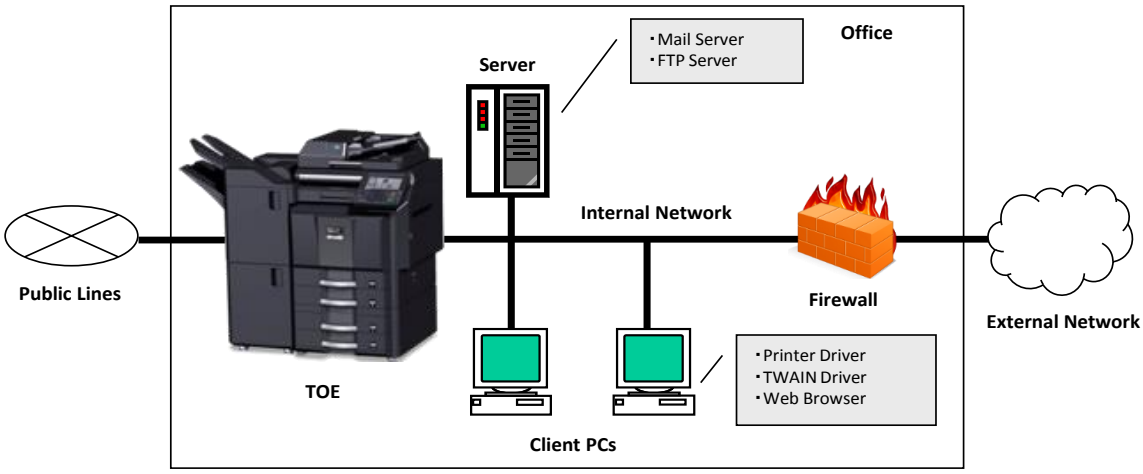

Figure 4-1 Operational environment of the TOE

The following are components, excluding the TOE, in the operational environment of the TOE:

1) Client PC

Client PC is used for users to use the TOE functions via the internal network or USB ports. The following software is necessary.

Type	Name and version
Web Browser	- Microsoft Internet Explorer 9.0
Printer Driver	- KYOCERA Document Solutions Inc. KX Driver
TWAIN Driver (Scan to send function)	- KYOCERA Document Solutions Inc. KYOCERA TWAIN Driver

2) Server (Mail Server)

Mail Server is used for device administrators to read the audit logs of the TOE. The server is also necessary when using the function that sends document data in the TOE by email. The following server is necessary:

- Mail Server: SMTP over SSL (SSL3.0) should be supported

3) Server (FTP Server)

FTP Server is necessary when using the function that sends document data in the TOE by using FTP. The following server is necessary:

- FTP Server: FTP over SSL (SSL3.0) should be supported

Note that the reliability of hardware and cooperating software, excluding the TOE, shown in this configuration is outside the scope of this evaluation. (It is assumed to be trustworthy.)

4.3 Clarification of Scope

The TOE provides the functions that prints the stored document data in the USB memory connected to the TOE, and stores the internal TOE document data into the USB memory. In this evaluation, the USB memory is treated just like a shared folder that enables box permission. Therefore, there is no assurance that other users cannot access to the stored document data in the USB memory by using other interfaces than the operation panel. It is a users' responsibility to take measures against the cases when storing the document data which cannot be shared in the USB memory, or when misplacing the USB memory.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE.

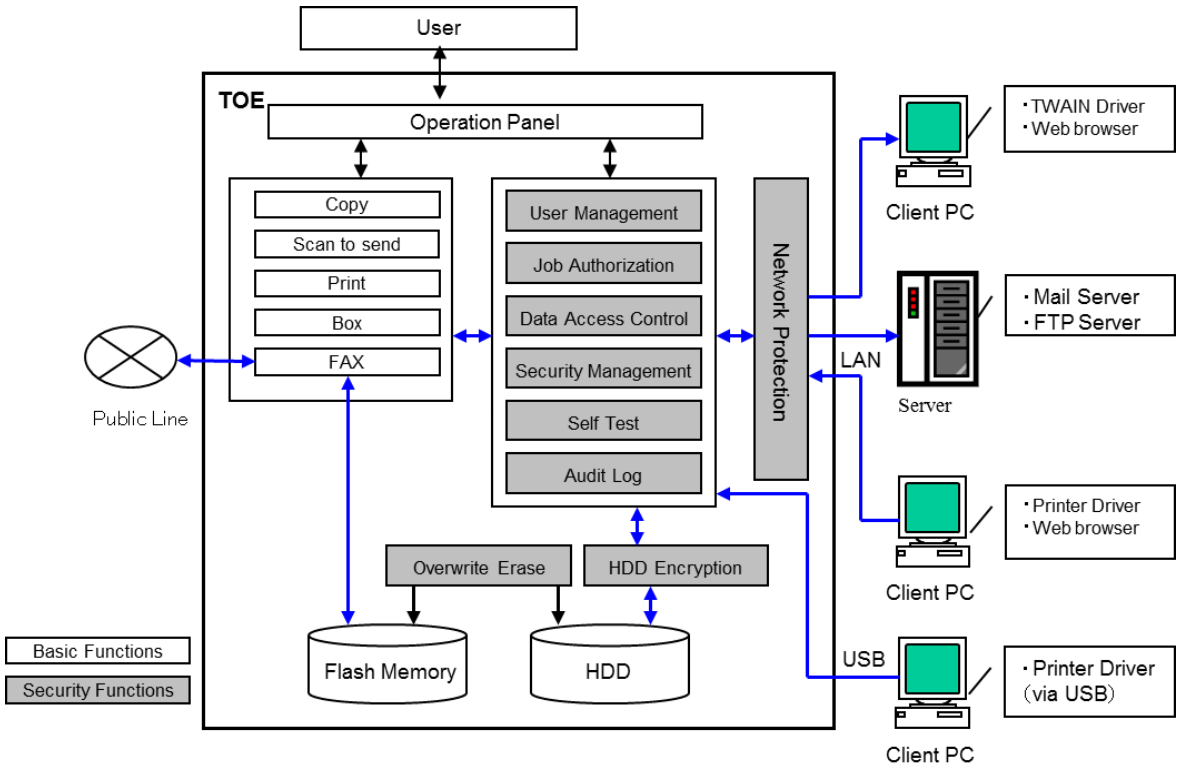

Figure 5-1 TOE Composition

As shown in Figure 5-1, the functions shaded in gray squares indicate security functions. The following describe the security functions of the TOE.

1) User Management function

The User Management function is a function that identifies and authenticates TOE users with their login user names and login user passwords. Identification and authentication are applied to all of the following user interfaces.

- Operation panel
- Client PC (Web browser and printer driver)

In order to enhance the identification and authentication function, the following functions are provided:

- Users are required to use passwords of eight or more characters.
- When the number of consecutive authentication failures reaches the setting value set by the device administrator, the authentication process is suspended.
- If no operation is performed for a certain period of time after a user has been successfully identified and authenticated, the session is terminated.

2) Job Authorization function

The Job Authorization function is a function that restricts only authorized users to use basic functions of the MFP such as copy function, scan to send function, print function, FAX function, and box function.

When a user attempts to use the basic functions of the MFP, the TOE checks executable authorization assigned to the user, and the user is authorized to use only the basic functions.

3) Data Access Control function

The Data Access Control function is a function that restricts the access to document data and job data used in the basic functions of the MFP to only authorized users.

Access Control is performed based on the owner information of document data and job data as well as the information for box permission storing the document data. Users are permitted to access only to the data, which users themselves are the owners, and the document data stored in box permission. Device administrators are allowed to delete all the data and perform operations on all the document data stored in the box.

4) Security Management function

The Security Management function is a function that permits only identified and authenticated device administrators to configure, refer to, and change the setting of the data used for security functions. Note that normal users are allowed to change their own passwords, refer to, and change their own box permissions.

5) Self-Test function

The Self-Test function is a function that performs the following self-tests:

- Upon start-up, the TOE verifies that the HDD Encryption function correctly performs, and the integrity of the encryption key is also verified simultaneously.
- Upon receipt of an instruction from a device administrator, the TOE verifies hash values of the executable module of the security functions.

6) Audit Log function

The Audit Log function is a function that records security-relevant auditable events as audit logs. Only identified and authenticated device administrators can delete and read out the audit logs stored in the TOE via email (send). The audit logs cannot be modified.

7) HDD Encryption function

The HDD Encryption function is a function that encrypts data to be stored in the HDD. The encryption algorithm is 256 bits AES. An encryption key is generated using SHA-256, based on a combination of eight characters and other secret information set by device administrators when the TOE is installed. The same value of the encryption key is generated every time the power is turned on and stored in the volatile memory, whereas it is deleted when the power is turned off.

8) Overwrite-Erase function

The Overwrite-Erase function is a function that overwrites and erases the internal HDD and Flash memory area, where document data were stored, when the document data are deleted. The Overwrite-Erase function is performed at the following timing:

- When document data become unnecessary after a user finishes using basic functions of the MFP. The data, which are temporarily generated in the TOE due to the TOE processing, are also included.
- When document data are deleted upon receipt of an instruction from a user.
- When the power of the MFP is turned on. If the overwrite-erase operation has not been completed when the power is turned off, the operation resumes when the power is turned on.

Device administrators can select a pattern of overwriting data, such as one pass overwrite or three pass overwrite (DoD method). The data is overwritten into the internal HDD or Flash memory without being encrypted.

9) Network Protection function

The Network Protection function is a function that encrypts communication with various servers and client PCs via network using SSL protocol. The Network Protection function also provides a function that prevents unauthorized forwarding of the data from the external interfaces, including public lines, to the internal network via the TOE.

5.2 IT Environment

Audit logs of the TOE can be read out via email (send) by using a mail server.

6. Documentation

The identification of documents attached to the TOE is listed below. There are guidance documents for Japan and for Overseas in regard to the TOE, and one of them is distributed depending on the sales areas.

TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Guidance Documents for Japan

Name	Version
TASKalfa 3010i / TASKalfa 3510i Quick Guide	302NL5612001 First Edition
TASKalfa 3010i / TASKalfa 3510i Safety Guide	302NL5622001 First Edition
TASKalfa 3010i / TASKalfa 3510i Operation Guide	2NLKDJA002 Rev.2
FAX System (W) Operation Guide	3N6KMJA002 Rev.2
Data Security Kit (E) Operation Guide	Rev.8
Command Center RX Operation Guide	Rev.6
TASKalfa 3010i / TASKalfa 3510i Printer Driver User Guide	Rev.1.0
KYOCERA Net Direct Print User Guide	Rev.2.3
Notice	303MS5632002
Data Security Kit (E) Installation Guide	303MS56710-02
FAX System (W) Installation Guide	303N656731-01

Table 6-2 Guidance Documents for Overseas

Name	Version
TASKalfa 3010i / TASKalfa 3510i QUICK GUIDE	302NL5611001 First Edition
TASKalfa 3010i / TASKalfa 3510i Safety Guide	302NL5622001 First Edition
TASKalfa 3010i / TASKalfa 3510i OPERATION GUIDE	2NLKDEN002 Rev.2

Name	Version
FAX System (W) OPERATION GUIDE	3N6KMEN002 Rev.2
Data Security Kit (E) Operation Guide	Rev.6
Command Center RX User Guide	Rev.5
TASKalfa 3010i / TASKalfa 3510i Printer Driver User Guide	Rev.16.13
KYOCERA Net Direct Print User Guide	Rev.3.5
Notice	303MS5632002
Data Security Kit (E) Installation Guide	303MS56710-02
FAX System (W) Installation Guide	303N656731-01

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Information Technology Security Center, Evaluation Department that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which is agreed on mutual recognition with ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

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

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2013-09 and concluded upon completion of the Evaluation Technical Report dated 2014-10. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2013-09, 2013-10, 2014-06 and 2014-07, and examined procedural status of configuration management, delivery, and development security by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2014-04.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and the verification results of the testing performed by the developer, the evaluator performed the reproducibility testing, additional testing, and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer.

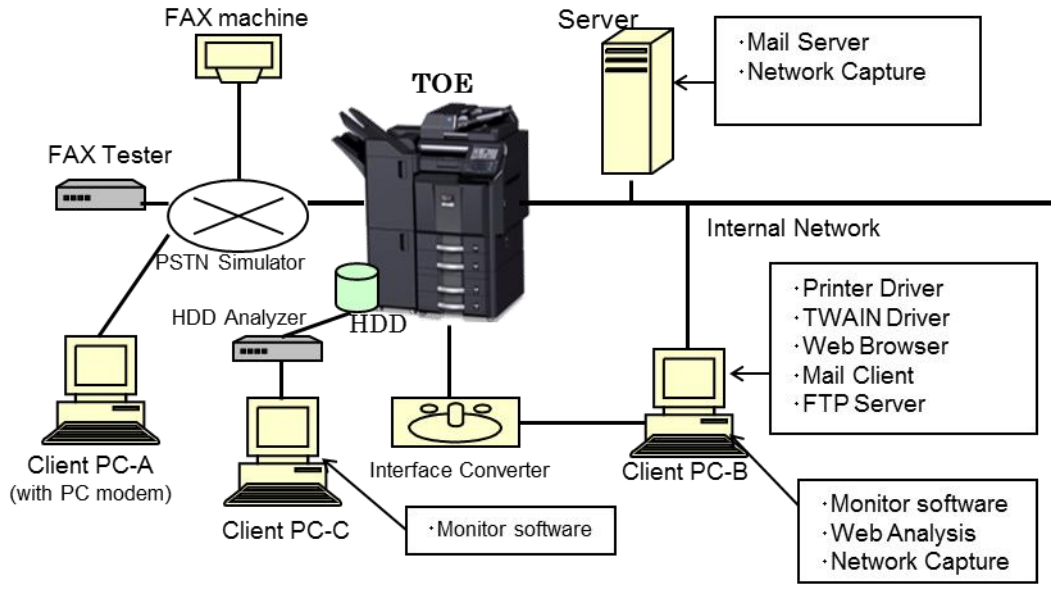

Figure 7-1 Configuration of the Developer Testing

Table 7-1 shows the components of the developer testing.

Table 7-1 Configuration Items for the Developer Testing

Item	Description
TOE	TASKalfa 3010i, TASKalfa 3510i - Data Security Kit (E) and FAX System (W) are installed.
Server (Mail Server)	It is used as a mail server. - PC with Windows Server 2003 SP1 - Mail server: Pmail Server Manager 1.91 *Other than the above-described, the following developer testing tool is installed: - Network Capture Software: WireShark v1.8.10
Client PC-B (It is also used as FTP Server.)	It is used as TOE user client PC and FTP server. - PC with Windows 7 Professional SP1 - Printer Driver: KX Driver v6.1.0826 - TWAIN Driver: KYOCERA TWAIN Driver v2.0.2507 - Web Browser: Internet Explorer 9.0 - Mail Client: Mozilla Thunderbird 24.0 - FTP Server: nekosogiFTPd v2.04+sslmod.dll Ver0.02b *Other than the above-described, the following developer testing tools are installed: - Monitor Software: Tera Term Professional v4.82 - Web Analysis tool: Fiddler v2.4.5.6 - Network Capture Software: WireShark v1.8.10
Interface Converter	A board to connect the developer interface inside the TOE - KYOCERA Document Solutions proprietary board
Client PC-C	It is connected to HDD analyzer and used to monitor data transferred to and from the internal HDD of the TOE. - PC with Windows 7 Professional SP1 - Monitor Software: Tera Term Professional v4.82
HDD Analyzer	A device that analyzes data transferred to and from the internal HDD of the TOE. - SATA Command Monitor
FAX machine	It is used to send and receive FAX transmission to and from the TOE. - ECOSYS M6526cidn (The MFP manufactured by KYOCERA Document Solutions Inc.)

FAX Tester	Super G3 Facsimile Tester corresponding to ITU-T recommendation - Super G3 Facsimile Tester AFT-336N
PSTN Simulator	A device that performs a pseudo operation as public line - X4008 Switch Simulator (AD SYSTEMS)
Client PC-A	It is used to confirm a function to prevent unauthorized access via public line. - PC with Windows 7 Professional SP1

The TOEs used in the developer testing are all MFP models which have names starting with "TASKalfa" and ending with "i," and are the same TOEs as described in TOE identification of Chapter 2.

Table 7-2 shows the relation between MFP models used in the developer testing and other models of the TOE. The products listed in the same row are the same models but have different product names. It is considered that the configuration of the developer testing includes all of the TOEs identified.

Table 7-2 TOE Variation

	MFP used for the developer testing	Series A	Series B	Series C
1	TASKalfa 3010i	TASKalfa 3010iG	CS 3010i	3060i
2	TASKalfa 3510i	TASKalfa 3510iG	CS 3510i	3560i

The developer testing was performed in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of the Developer Testing

A summary of the developer testing is described as follows.

a. Developer Testing Outline

An outline of the developer testing is described as follows.

<Developer Testing Approach>

For the external interfaces of the TOE, the developer confirmed the TOE behavior by using the TOE operation panel, PC, testing tools, and FAX machine. To confirm its behavior, the following approach was used:

- Using the external interfaces provided by the TOE, and confirming responses to the input operations, the TOE behavior, audit logs, and communication data.

- Connecting HDD Analyzer to the internal HDD interfaces of the TOE, and monitoring data to be written to and read out from the HDD, and confirming the behavior of encryption and overwrite-erase.

- With respect to the Self-Test function and the Encryption function such as encryption key generation, which cannot be confirmed through the interfaces provided by the TOE, using the modified firmware to acquire logs in the TOE for the module test, and confirming the log information and memory capacity through the interfaces for developers.

It is confirmed that the encryption algorithm is implemented as specified by comparing the data that were obtained by the above approach, with the known data calculated by a different approach.

<Developer Testing Tools>

Table 7-3 shows the tools used in the developer testing.

Table 7-3 Developer Testing Tools

Tool Name	Outline and Purpose of Use
Network Capture Software (WireShark v1.8.10)	It captures communication data on the internal network. It is used for confirming communication protocols.
Web Analysis Tool (Fiddler v2.4.5.6)	It analyzes communication between Web browser and the TOE to refer to and change the communication data between them.
HDD Analyzer & Monitor Software (Client PC-C)	It captures data traveling through SATA interface of the internal HDD of the TOE. It is used for confirming the encryption of the HDD and overwrite-erase of the data.
Firmware for testing Encryption function	Firmware for testing, which is modified to output information, such as encryption key of the HDD encryption function, as logs. The implementation part of encryption key generation and encryption algorithm is the same as the TOE.
Firmware for testing Self-Test function	Firmware for testing, which is modified to enable developers to specify target of verification for self-tests. The implementation part of self-tests is the same as the TOE.
Interface Converter & Monitor Software (Client PC-B)	By using interfaces for TOE developers, it refers to logs of firmware for testing and performs memory dump, etc.

<Content of the Performed Developer Testing>

By operating basic functions of the MFP and security management functions from various interfaces, it was confirmed that the security functions to be applied to various input parameters behave as specified.

The variations of the input parameters include the rewrite of communication data between Web browser and the TOE, and the data that might cause unauthorized processing such as buffer overflow.

b. Scope of the Performed Developer Testing

The developer testing was performed on 115 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 sufficiently tested.

c. Result

The evaluator confirmed the approach of the performed 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 performed by the developer.

7.4.2 Evaluator Independent Testing

The evaluator performed the sampling testing to reconfirm the execution of security functions by the test items extracted from the developer testing. Additionally, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to ensure that security functions are surely implemented from the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the independent testing performed by the evaluator is the same as that in the developer testing environment shown in Figure 7-1, except for the following:

- Only TASKalfa 3510i was used as the TOE.

The evaluator determined that it is sufficient to test only one model because the difference among TOE models is only printing speed, and the security functions are the same.

The independent testing was performed in the same environment with the TOE configuration identified in this ST.

The components and testing tools used in the independent testing environment were the same as those which were used in the developer testing. Those include what the developer developed by themselves, but their validation confirmation and behavior tests were conducted by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing performed by the evaluator is described as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

<Viewpoints of the Independent Testing>

(1) To confirm the variations of the combination of different input data and operations that are not used by the developer.

(2) To confirm the behavior that was not performed by the developer in the testing.

(3) With sampling testing, to select the testing items of the developer testing from the following viewpoints.

- To confirm all the security functions.
- To confirm all interface types together with the evaluator devised testing.
- To confirm all user roles together with the evaluator devised testing.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The independent testing was performed by the evaluator using the same testing approach as the developer testing.

<Independent Testing Tools>

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

<Content of the Performed Independent Testing>

The evaluator performed 27 items of sampling testing and 13 items of additional independent testing, based on the viewpoints of the independent testing.

Table 7-4 shows viewpoints of the independent testing and the content of the major tests corresponding to them.

Table 7-4 Viewpoints of Independent Testing Performed

Viewpoints	Outline of the Independent Testing
Viewpoint (1)	- Confirm that the TOE behaves as specified using different parameters from those which the developer used, such as modification of password characters, threshold until the account locked, and user authorization. - Perform a combination of operations that the developer has not confirmed, such as modification of box owner and confirmation of access control when storing document, and confirm the TOE behaves as specified.

Viewpoint (2)	- Confirm that the number of authentication failures until the account locked is totaled in case of using different interfaces. - With the Self-Test function, confirm irregular case that the developer has not performed in the testing, such as alteration of hash value.

c. Result

All the independent testing performed by the evaluator 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.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is described as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

(1) There is a concern that the known vulnerability may exist on various interface.

(2) There is a concern that the known vulnerability may exist in the processing of PDF files.

(3) There is a concern that the security functions do not behave correctly when the power is turned off during the TOE operation.

(4) There is a concern that the security functions do not behave correctly by entering control characters, which cannot be entered through Web browser, into the TOE.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing was performed in the same environment as that of the independent testing, except for the additional PC for the penetration testing. Table 7-5 shows details of the tools used in the penetration testing.

Table 7-5 Penetration Testing Tools

Name		Purpose of Use
PC for Penetration Testing		A PC with Windows VISTA Business SP2, which operates the following penetration testing tools.
	Nmap Ver.6.25	A tool to detect available network ports.
	Fiddler V2.4.4.5	It is a tool to mediate the communication between Web browser and Web server (TOE), which refers to and changes the communication data between them.
	Metasploit Version 4.6.2	It is used for creating the testing data to detect vulnerabilities in the PDF files.

<List of the Performed Penetration Testing>

Table 7-6 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-6 Outline of the Penetration Testing

Vulnerability	Outline of the Penetration Testing
Vulnerability (1)	- By using the Nmap for the TOE, it was confirmed that unnecessary network ports are not opened. - It was confirmed that the processing is not executed even if characters including unauthorized script or executable SQL command are entered from the operation panel, printer driver or Web browser. - It was confirmed that identification and authentication as well as access control are not bypassed even if URL of Web browser is directly specified.
Vulnerability (2)	- It was confirmed that the processing is not executed even if PDF files including unauthorized processing are entered into the TOE.
Vulnerability (3)	- It was confirmed that the following security functions behave correctly even if the power is turned off/on during the TOE operation. - Maintaining the number of unsuccessful authentication until the account locked. - Maintaining an account lockout state. - Overwrite-erase process (resumes after the power is turned on.)
Vulnerability (4)	- It was confirmed that the TOE does not malfunction even if the communication data from Web browser to the TOE are rewritten by using Fiddler, and linefeed code is inserted.

c. Result

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

7.5 Evaluated Configuration

The TOE configuration conditions, which are the assumptions of this evaluation, are as described in the guidance documents shown in Chapter 6. Device administrators of the TOE need to configure the TOE settings as described in the guidance documents to enable security functions of the TOE and securely use them. In case that these setting values are changed to the values different from the values specified in the guidance documents, the configuration will not be assured by this evaluation.

It should be noted that the TOE configuration conditions also include the settings that disable the functions provided by the TOE. For example, the following setting values are also included:

- Disabling print protocol, except for IPP
- Disabling SNMP
- Disabling remote diagnostics via public line

7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:

  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A (IEEE Std 2600.1™-2009)

The TOE also conforms to the following SFR packages defined in the above PP.

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
- 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

- Security functional requirements: Common Criteria Part 2 Extended
- 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
- Additional assurance component ALC_FLR.2

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

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendations to be addressed to consumers.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. 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 the submitted Evaluation Technical Report and related evaluation deliverables, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

It should be noted that procurement personnel who are interested in the TOE need to consider whether the scope of the evaluation and the operational requirements of the TOE satisfy the operational conditions that they assume, by referring to the descriptions in “1.1.3 Disclaimers,” “4.3 Clarification of Scope,” and “7.5 Evaluated Configuration.”

For the TOE, the document data can be outputted as printed documents only by the operation from the operation panel, and it cannot be done from the client PCs, including Web browser. It means that the basic approach of the PP is faithfully implemented for ensuring security of output as printed documents.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

TASKalfa 3010i, TASKalfa 3510i Series with Data Security Kit (E), FAX System (W) Security Target, Version 1.31, October 14, 2014, KYOCERA Document Solutions Inc.

11. Glossary

The abbreviations relating to the 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 abbreviation relating to the TOE used in this report is listed below.

MFP	Multi-Function Printer

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

Box:
An area that stores document data in the TOE. As security attributes, it has both box owner and box permission information.

Box function:
A function that stores document data in the internal HDD of the TOE, and reads the data to print and send. The following means of sending are available: FTP Server, Mail Server, Client PC (TWAIN Driver), USB Memory connected to the TOE, and FAX. The Box function can be operated from the operation panel of the TOE or client PCs (Web browser). However, printing document data can be operated only from the operation panel.

Copy function:
A function that reads paper document and prints out the copy by operating from the operation panel.

FAX function:
A function that sends and receives documents by FAX via public line. The sent/received data by FAX are stored in the internal Flash memory of the TOE.

Print function:
A function that prints out document data received by the TOE from client PCs via internal network or USB ports. Once the TOE receives document data, they will be stored in the TOE, and will be outputted upon receipt of printing instructions from the operation panel.

Scan to Send function:
A function that reads paper documents and sends them to FTP Server, Mail Server, Client PC (TWAIN Driver), and USB Memory connected to the TOE, by operating from the operation panel.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2014, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2014, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, April 2013, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] TASKalfa 3010i, TASKalfa 3510i Series with Data Security Kit (E), FAX System (W) Security Target, Version 1.31, October 14, 2014, KYOCERA Document Solutions Inc.

[13] TASKalfa 3010i, TASKalfa 3510i Series with Data Security Kit (E), FAX System (W) Evaluation Technical Report, Version 4.2, October 27, 2014, Information Technology Security Center, Evaluation Department

[14] IEEE Std 2600.1™-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009