Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2018-09-27 (ITC-8693)
Certification Identification	JISEC-C0632
Product Name	TOSHIBA e-STUDIO5516AC/6516AC/7516AC all of the above with FAX Unit(GD-1370J/GD-1370NA/GD-1370EU) and FIPS Hard Disk Kit(GE-1230)
Version and Release Numbers	SYS V1.0
Product Manufacturer	TOSHIBA TEC CORPORATION
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)
Name of IT Security Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE has been certified as follows.
2019-03-13

Tatsuro Yano, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

"TOSHIBA e-STUDIO5516AC/6516AC/7516AC all of the above with FAX Unit(GD-1370J/GD-1370NA/GD-1370EU) and FIPS Hard Disk Kit(GE-1230)" 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 "TOSHIBA e-STUDIO5516AC/6516AC/7516AC all of the above with FAX Unit(GD-1370J/GD-1370NA/GD-1370EU) and FIPS Hard Disk Kit(GE-1230), Version SYS V1.0" (hereinafter referred to as the "TOE") developed by TOSHIBA TEC CORPORATION, and the evaluation of the TOE was finished on 2019-01-31 by Information Technology Security Center Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, TOSHIBA TEC CORPORATION, and provide security information to procurement entities and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes procurement entities who purchase this 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 Protection Profile or Assurance Package

The TOE conforms to the following protection profiles [14][15] (hereinafter, referred to as “Conformance PP”).
Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015
(Certification Identification: JISEC-C0553)

1.1.2 TOE and Security Functionality

The TOE is an IT product and a multifunctional digital system (hereinafter referred to as “MFP”) which has the copy, print, scan, and fax functions.
The TOE provides security functions which are required by the Conformance PP that is the protection profile for the MFP, to protect the data handled by the MFP from being disclosed or altered.
Regarding such security functionality, the validity of the design policy and the accuracy of implementation have been evaluated in the scope of the assurance requirements requested by the Conformance PP.
The threats and the assumptions that the TOE assumes are as follows:

1.1.2.1 Threats

The following are assumed as Threats against the TOE.
There is a threat of unauthorized exposure or alteration of the user document data and the data affecting the security functions which are the TOE assets to be protected in TOE operation and access to the network to which the TOE is connected.
There is also a threat of damaging the security functions of the TOE due to the failure of the TOE itself or installation of unauthorized software.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.
It is assumed that the TOE is used in an environment where the LAN is protected from unauthorized physical access and internet.
For the operation of the TOE, the TOE shall be properly configured, managed and maintained according to the guidance documents. Users of the TOE shall be trained to use the TOE safely.

1.1.3 Disclaimers

Operations indicated below are not included in the assurance of this evaluation.

- Operations with the TOE environment described in “4.3 Clarification of Scope” is unsecure.
- Operations of the TOE under the conditions other than the ones described in “7.5 Evaluated Configuration”.

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 in 2019-01, based on functional requirements and assurance requirements of the TOE according to the publicised documents "IT Security Evaluation and Certification Scheme Document"[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 as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure.

The Certification Body confirmed that all the concerns were fully resolved, and 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 and fully concluded certification activities.

2. Identification

The TOE is identified as follows.

TOE Name:	TOSHIBA e-STUDIO5516AC/6516AC/7516AC all of the above with FAX Unit(GD-1370J/GD-1370NA/GD-1370EU) and FIPS Hard Disk Kit(GE-1230)
TOE Version:	SYS V1.0
Developer:	TOSHIBA TEC CORPORATION

The TOE consists of the main body of the MFP and mandatory options. Details of the TOE components are shown in Table 2-1.

Table 2-1 TOE Components

Model Number	Mandatory Options	Sales Area
One of the following models: ・ e-STUDIO5516AC ・ e-STUDIO6516AC ・ e-STUDIO7516AC	GD-1370J and GE-1230	Japan
One of the following models: ・ e-STUDIO5516AC ・ e-STUDIO6516AC ・ e-STUDIO7516AC	GD-1370NA and GE-1230	North America
One of the following models: ・ e-STUDIO5516AC ・ e-STUDIO6516AC ・ e-STUDIO7516AC	GD-1370EU and GE-1230	Europe

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

Users confirm the following information indicated in the body, control panel, and package of the TOE according to the guidance of the product.

・Model Number

The name of the MFP indicated in the main body should be included in "Model Number" in Table 2-1.

・Mandatory options

The name of the options indicated in the package should be the ones indicated in "Mandatory Options" in Table 2-1.

・TOE version

The TOE version displayed on the control panel should match the identification version.

3. Security Policy

The TOE provides the MFP basic functions such as Copy, Print, Scan, and Fax functions. The TOE also has the functions to store user document data inside the TOE and transfer them to and from users' devices and various servers via the network.
The TOE provides the following security functions that satisfy the requirements required by the Conformance PP.

- Function which identifies and authenticates users
- Function which controls access of the users' data
- Function which encrypts and stores users' data and such
- Function which protects users' data on the communication path while using the LAN
- Function which limits the security management to the identified and authorized user
- Function which records the logs of the security-related events
- Function which verifies and installs the update firmware
- Function which verifies that the security function operates normally at startup
- Function which separates the Public Switched Telephone Networks from the LAN

Details of the security functions of the TOE are described in Section 5.1.
Details of the user roles, protected assets, threats, and security policies of the organisation are described in Section 3.1 through Section 3.4.

3.1 User Roles

The TOE assumes the user roles shown in Table 3-1.

Table 3-1 User Roles

Name	Definition
U.NORMAL (a normal user)	A User who has been identified and authenticated and does not have an administrative role.
U.ADMIN (an administrator)	A User who has been identified and authenticated and has an administrative role.

3.2 Protected Assets

The protected assets of the TOE can be grouped into 2 categories as shown in Table 3-2. The User data and TSF data are composed of 2 types of the protected assets as shown in Table 3-3 and Table 3-4 respectively.

Table 3-2 Protected Assets of the TOE

Name	Type	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF.
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF.

Table 3-3 Protected Assets (User Data)

Name	Type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form.
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job.

Table 3-4 Protected Assets (TSF Data)

Name	Type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable.
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE.

3.3 Threats

Table 3-5 shows threats.

Table 3-5 Threats

Name	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 Organisational Security Policy

Table 3-6 shows organisational security policies required for use of the TOE.

Table 3-6 Organisational Security Policies

Name	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.

Name	Definition
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

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. The effective performances of the TOE security functions are not ensured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Name	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2 Environmental Assumptions

The TOE is installed in general offices and connected to the public telephone network and internal LAN of the organisation, and is used from the client PC and various servers connected to the LAN. Figure 4-1 shows the general operational environment as assumptions of the TOE.

Users use the TOE by operating the control panel of the TOE and the PC connected to the LAN.

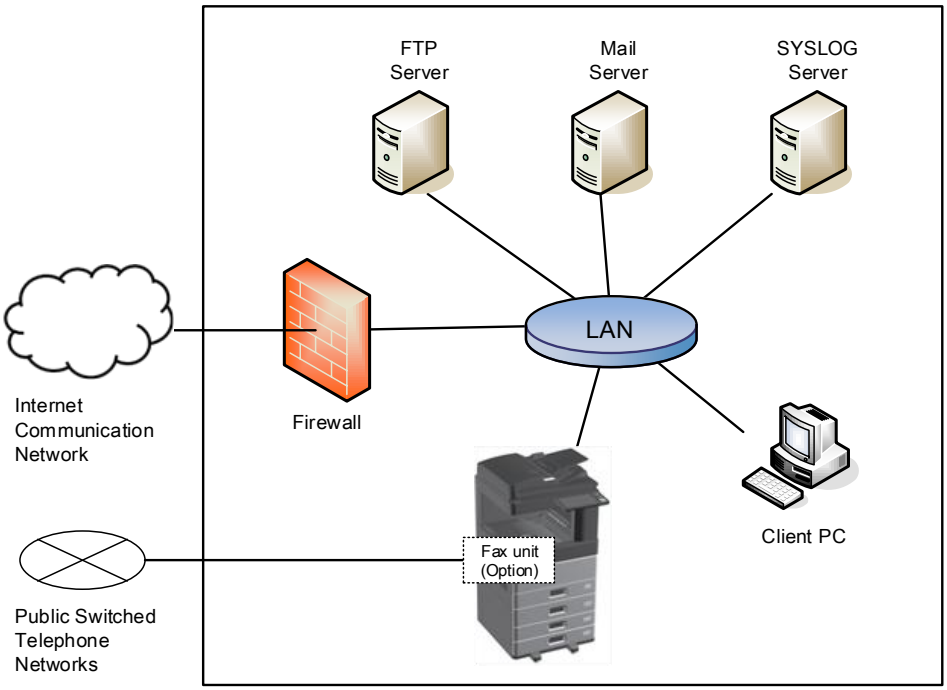

Figure 4-1 Operational Environment of the TOE

The following shows the components under the operational environment of the TOE.

(1) Client PC

The client PC is the general PC used by users.

The following software is required to use the TOE.

・Printer driver

TOSHIBA Universal Printer Driver2 (Version: 7.204.4408.17)

・Web browser

Internet Explorer 11

(2) SYSLOG Server (Audit server)

The SYSLOG server is the audit server which stores the audit log generated by the TOE. It is required to support TLS v1.2 by using the syslog protocol. It is essential to install the SYSLOG server.

(3) Mail Server

The mail server is required when the user document data scanned by the “scan function” is sent as an attachment of an email. The mail server must support TLS v1.2.

(4) FTP Server

The FTP server is required when the user document data scanned by the “scan function” is sent to the specified FTP server. The FTP server must support TLS v1.2.

Reliability of hardware and cooperative software indicated in this structure is not the scope of the evaluation (It should be thoroughly reliable.)

4.3 Clarification of Scope

Secure operation is required so that the communication protocol operates correctly in the client PC and various servers in order to protect the data on the communication path between the TOE and client PC, and the TOE and various servers.

Operators have responsibility for the client PC and various servers to be operated securely.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE. The TOE is the area surrounded by the frame indicated as TOE in Figure 5-1.

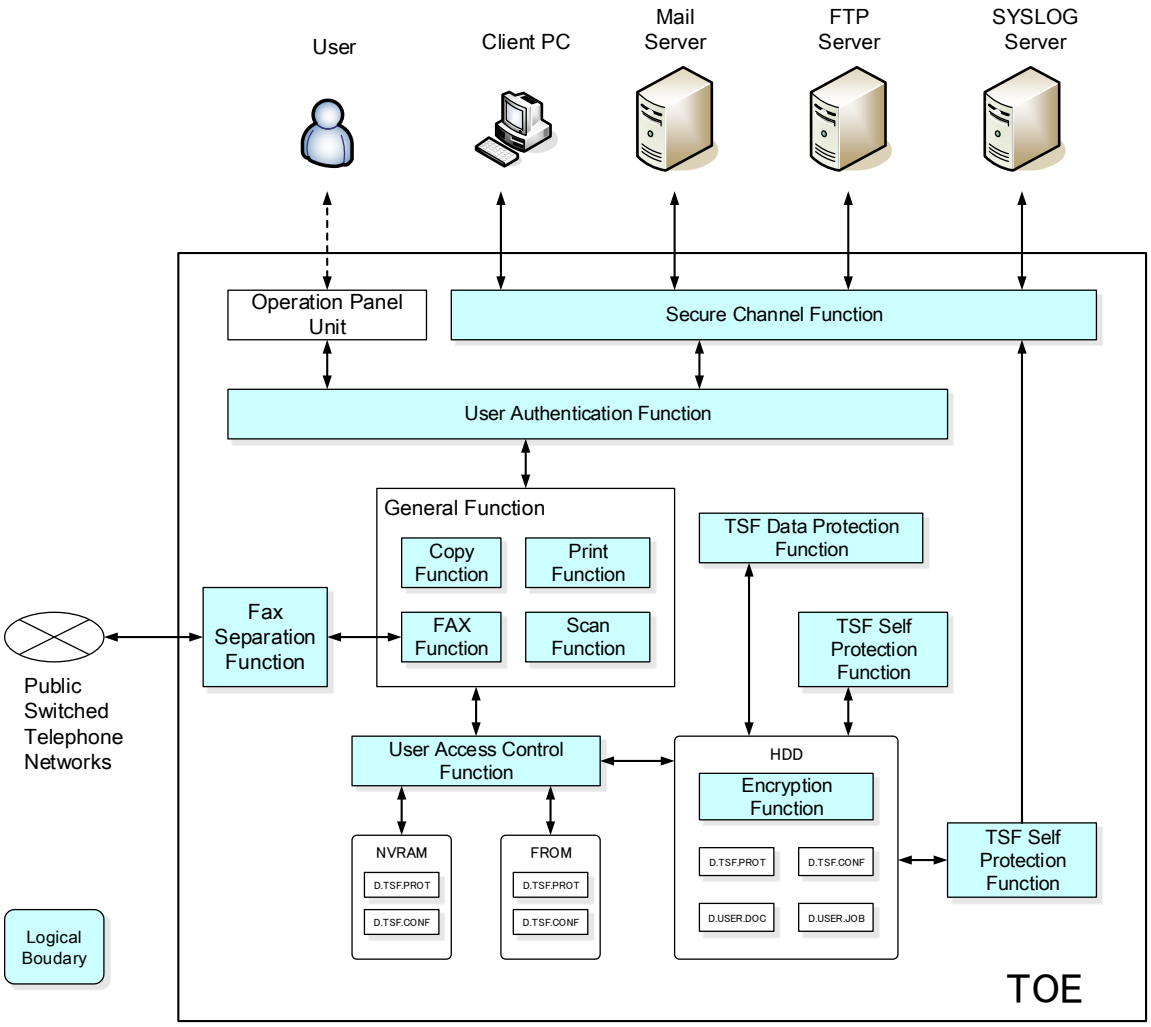

Figure 5-1 TOE Boundary

The TOE functions are composed of the functions surrounded by the colored frame indicated in Figure 5-1.

The security functions are described below. Refer to Chapter 11 for general functions.

5.1.1 Security Functions

(1) User identification and authentication function

This function is the function to identify and authenticate the TOE users by the user ID and login password when the TOE is used from the control panel or web browser of the client PC.

In the case the TOE receives the user document data transmitted from the printer driver of the client PC, the user ID is identified.

(2) User access control function

This function controls access of the user document data when a user operates the user document data by using the general functions of the TOE.

・ Access to the user data is controlled based on the policies defined for each user type such as an owner of the user document data or user role.

(3) Encryption function

This function stores the user document data or such in the self-encryption drive in the TOE. The self-encryption drive has been validated by JCMVP.

(4) Secure channel function

This function protects the user document data or such on the communication path by encrypted communication with TLS v1.2 while using the LAN.

(5) TSF data protection function

This function controls access based on the policies for the TSF data type when operating the TSF data from the control panel or web browser of the client PC.

(6) TSF self-protection function

This function verifies the normal operation of the security functions at startup of the TOE.

・ This function verifies that the security functions operates normally by confirming that there is no damage in firmware.

・ If an error is detected during verification, the TOE stops operation and does not accept any operations.

The TOE verifies firmware for update and enables installation of the normal firmware only.

(7) Audit log function

This function creates a log of events related to use and security of the TOE, and sends it to the SYSLOG server.

(8) Fax separation function

Separate the public line and LAN.

・ Only the Fax transmission operates for communication via the public line in order to protect the LAN from attacks from the public line.

5.2 IT Environment

The TOE communicates with the various servers and client PC through the LAN.

The TOE transmits the created audit data to the audit server. An administrator reads the audit data from the audit server.

The TOE can transmit the scanned user document data to the mail server and FTP server.

6. Documentation

The identification of documents attached to the TOE is listed below. Table 6-1 is for the guidance documents sold outside Japan, and Table 6-2 for those sold in Japan.

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

Table 6-1 Attached Documents (Guidance for English Version)

Document Name	Identification
Quick Start Guide	OME17005000
Safety Information	OME170056A0
Copying Guide	OME170060A0
Scanning Guide	OME170066A0
MFP Management Guide	OME170074A0
Software Installation Guide	OME170072A0
Printing Guide	OME170070A0
TopAccess Guide	OME170076A0
Software Troubleshooting Guide	OME170062A0
Hardware Troubleshooting Guide	OME17005400
High Security Mode Management Guide	OME170078B0
Paper Preparation Guide	OME17005200
Specifications Guide	OME170058A0
Fax Guide　GD-1370	OME170080A0

Table 6-2 Attached Documents (Guidance for Japanese Version)

Document Name	Identification
かんたん操作ガイド	OMJ17004900
安全にお使いいただくために	OMJ17005500
コピーガイド	OMJ170059A0
スキャンガイド	OMJ170065A0
設定管理ガイド	OMJ170073A0
インストールガイド	OMJ170071A0
印刷ガイド	OMJ170069A0
TopAccess ガイド	OMJ170075A0
トラブルシューティングガイド［ソフトウェア編］	OMJ170061A0
トラブルシューティングガイド［ハードウェア編］	OMJ17005300
ハイセキュリティモード管理ガイド	OMJ170077B0
用紙準備ガイド	OMJ17005100
仕様ガイド	OMJ170057A0
ファクスガイド GD-1370J	OMJ170079A0

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Evaluation Department, Information Technology Security Center 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 joins Mutual Recognition Arrangement of 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 on the assurance requirements in the CC Part 3 required by the Conformance PP using the evaluation methods prescribed in the CEM and the assurance activities of the Conformance PP.

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 for each work unit in the CEM and assurance activity of the Conformance PP.

7.3 Overview of Evaluation Activity

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

The evaluation started in 2018-09 and concluded upon completion of the Evaluation Technical Report dated 2019-01.

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.

Furthermore, the evaluator conducted the evaluator testing at the developer site in 2018-11 and 2018-12.

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 those confirmed validity, the evaluator performed the evaluator independent testing and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The TOE does not include the developer testing in the assurance requirements.

7.4.2 Evaluator Independent Testing

The evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to ensure that security functions are certainly implemented from the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained below.

(1) Independent Testing Environment

The configuration of the independent testing conforms to the TOE operation environment shown in Figure 4-1 and the components are as shown in Figure 7-1. There are following differences. However, these configurations are the same as the ones identified by the ST, and it has been evaluated that there are no problems in confirmation of the TOE functions.

- The TOE which was tested by the evaluator is a part of the combinations of the components of the TOE (Refer to Figure 2-1) which was described in Chapter 2, Identification. Though there are following differences depending on the TOE components, they were judged that they do not impact the security functions. The test target was the combination of the TOE components from which it can be confirmed that the following differences do not impact the security functions.
  - Difference of the print speed due to difference of the MFP
  - Difference of the language settings depending on the sales area (Japanese or English)
  - Difference of the fax units (GD-1370J, GD-1370NA or GD-1370EU)
- The firewall which is installed to protect the TOE from unauthorized access from the external network does not exist in the test environment because it does not impact on the TOE operation.
- The telephone line pseudo exchange which can emulate the fax communication protocol which is the same as the public telephone line is used instead of the public telephone line.
- In the TLS test, communication is made between the TOE and the server/client PC via the TLS test tool which was created by the Evaluation agency. The TLS test tool alters the packet data required in the assurance activity of the Conformance PP. It is not used for other tests.

- The program for testing is used which was created by the developer for calling for the encryption module test within the TOE in a part of the tests such as the encryption test. The module called at the test which uses the program for testing is appropriate for the TOE function test because it is the same as that of the TOE module.

Table 7-1 Test Configurations

Configuration item	Detail
TOE	e-STUDIO5516AC ・Language: Japanese ・Option (Fax Unit): GD-1370J ・Option (FIPS hard disk kit): GE-1230 e-STUDIO7516AC ・Language: English ・Option (Fax Unit): GD-1370NA or GD-1370EU ・Option (FIPS hard disk kit): GE-1230
SYSLOG Server	Syslog-ng 3.14.1
Mail Server	Sendmail 8.152
FTP Server	ProFTPD 1.3.6
Client PC	Web browser: ・Internet Explorer 11 ・Google Chrome 63.0.3239.108 (for cipher suite test) Printer driver: ・TOSHIBA Universal Printer Driver2 7.204.4408.17

(2) Summary of Independent Testing

The independent testing conducted by the evaluator is as follows.

a) Independent Testing Viewpoints

The viewpoints for the independent testing that the evaluator designed from the Conformance PP requirements and the provided evaluation documentation are shown below.

<Independent Testing Viewpoints>

1. To confirm the security functions per SFR.
2. To confirm that the encryption implementation is correct.

b) Independent Testing Outline

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

<Independent Testing Approach>

The behaviour of the external interface of the TOE was confirmed by performing entry using the TOE control panel, client PC, and test tools by the following means:

・The external interface of the TOE is used when the behaviour can be confirmed by the external interface of the TOE.

・The logs in the audit server are studied and the network analyzer and program for testing are used when the behaviour cannot be confirmed by the external interface of the TOE.

<Content of the Performed Independent Testing>

The evaluator performed 18 items of the independent testing.

Table 7-2 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 7-2 Performed Independent Testing

Viewpoint	Outline of the Independent Testing
(1)	Confirmation of the security functions ・Confirm that all security functions are as specified in the specifications per SFR by using the assurance activity of the Conformance PP or the test items created from the SFR specifications.
(2)	Confirmation of the encryption implementation ・Confirm the implementation of the following encryption algorithms which are the target of the test by using the program for testing installed in the TOE. - RSA (Key generation, Signature generation/verification) - AES-CBC-128, AES-CBC-256 - SHA1, SHA256, SHA512 - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 - Hash_DRBG, CTR_DRBG - KDF in Counter Mode

c) Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behaviour of the TOE. The evaluator confirmed consistencies between the expected behaviour 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 concern that an unintentionally open network port of the TOE or known vulnerabilities that may exist in the network service are exploited.
2. There is concern that the identification and authentication functions may be bypassed by directly specifying the URL through the web interface of the TOE or known vulnerabilities may exist such as XSS.
3. There is concern that print job operation, buffer overflow, or arbitrary code execution may occur due to wrong print data entered in the TOE.
4. There is concern that the identification and authentication functions may be bypassed by unauthorized entry from the control panel, printer driver or web interface.

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 the independent testing environment by installing the penetration testing tools shown in Table 7-3.

Table 7-3 Penetration Testing Tools

Name	Outline/Purpose
Port scanning tool nmap 7.60	It is used for searching the port.

Name	Outline/Purpose
Vulnerability scanning tool Nessus 6.11.1	It is used for detecting known vulnerabilities.
Web vulnerability scanning tool OWASP ZAP 2.7.0	It is used for detecting general vulnerabilities in the web.
Web application analyzing tool Fiddler 5.0.20173.50948	It is used for acquiring or issuing the communication data exchanged by the web applications.
Printer security testing tool PRET 0.39	It is used for detecting vulnerabilities by using the printer language for the print device.
TCP/UDP data communication tool Netcat 1.12	It is used for detecting vulnerabilities for identification and authentication.
Penetration testing tool Metasploit Framework v4.6.2	It is used for creating a file for unauthorized printing.

< Content of the Performed Penetration Testing >

Table 7-4 shows vulnerabilities concerned and the content of the related penetration testing.

Table 7-4 Outline of the Performed Penetration Testing

Vulnerability	Outline of the Testing
(1)	Confirm that no unexpected port is open and there is no known vulnerability in the available port by using the port scanning tool and vulnerability scanning tool.
(2)	Confirm that there is no known vulnerability in the web interface by using the web vulnerability scanning tool and web application analyzing tool.
(3)	Confirm that no unintended behaviour occurs by using the print data which is intended to generate wrong behaviour.
(4)	Confirm that no wrong behaviour occurs by character strings entered in the identification and authentication function.

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 configuration conditions of the TOE, which are the assumptions of this evaluation, are described in the guidance documents shown in Chapter 6. The security functions of the TOE need to be activated and the TOE needs to be configured as described in the appropriate guidance documents for secure use. If these settings are not in accordance with the description of the guidance documents, such cases are not included in the assurance of this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM and all assurance activities in the Conformance PP as per the Evaluation Technical Report.
In the evaluation, the following were confirmed.

- PP Conformance:
  Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015

  Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

  Temporary treatment regarding FDP_DSK_EXT.1, Guideline for Certification Application with HCD-PP Conformance [16]
- 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 required by the Conformance PP:
ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

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 recommendation to be addressed to consumers.

8. Certification

Based on the evidence submitted by the Evaluation Facility during the evaluation process, the Certification Body has performed certification by checking that the following requirements are satisfied:

1. The submitted documentation was sampled, the content was examined, and the related work units in the CEM and assurance activities of the Conformance PP 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 and the assurance activities of the Conformance PP.

8.1 Certification Result

As a result of verification of the received Evaluation Technical Report and related evaluation documentation, the Certification Body determined that the TOE evaluation satisfies the assurance requirements required by the Conformance PP.

8.2 Recommendations

It should be noted that the procurement personnel who are interested in the TOE need to refer to the descriptions of “4.3 Clarification of Scope” and “7.5 Evaluated Configuration” and to see whether or not the evaluated scope of the TOE and the operational requirements are consistent with the operational conditions that they assume.
The old audit data will be lost in the case the audit data is not sent and the capacity of the storage area inside the TOE becomes full. Thus the operator has to periodically confirm whether the audit data is sent to the SYSLOG server.
As explained in Chapter 2, it is required to confirm the packages of the options in addition to the indicated information of the TOE for confirming TOE identification. Be careful not to throw away the packages because the TOE cannot be identified without them.

9. Annexes

There is no annex.

10. Security Target

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

TOSHIBA e-STUDIO5516AC/6516AC/7516AC Security Target, Version 0.14 (November 27, 2018) TOSHIBA TEC CORPORATION

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
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DRBG	Deterministic Random Bit Genera
FTP	File Transfer Protocol
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
MFP	Multifunction Peripheral
PSTN	Public Switched Telephone Network
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
XSS	Cross Site Scripting

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

Assurance activity	Evaluation operation which has to be operated by the evaluator for conformance to the PP. It is a supplemental to the CEM and described in the Conformance PP for Conformance PP [14].
Copy function	A function to copy and print the scanned paper document data by user's operation from the control panel.

FAX function	A function to transmit/receive document data with the external fax machines which are connected to the public telephone line and compliant with the G3 standard. There are the fax transmission function, which scans the paper document and transmits the scanned data to the external fax machine, and the fax reception function, which prints out the document data received from the external fax machine by user's operation.
Field Replaceable (Unit)	The smallest subassembly that can be swapped in the field to repair a fault.
Hardcopy Device	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones" and other similar products.
JCMVP	It is an abbreviation of Japan Cryptographic Module Validation Program.
Print function	A function to receive the user document data from the printer driver of the client PC via the LAN and prints the data out by user's operation from the control panel.
Scan function	A function to transmit the scanned paper document data to the mail server and FTP server by user's operation from the control panel.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, September 2018, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, September 2018, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version 1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017,CCMB-2017-04-002, (Japanese Version 1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components, Version 3.1 Revision 5, April 2017,CCMB-2017-04-003, (Japanese Version 1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017,CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017,CCMB-2017-04-004, (Japanese Version 1.0, July 2017

[12] TOSHIBA e-STUDIO5516AC/6516AC/7516AC Security Target, Version 0.14, (November 27, 2018), TOSHIBA TEC CORPORATION

[13] TOSHIBA e-STUDIO5516AC/6516AC/7516AC all of the above with FAX Unit(GD-1370J/GD-1370NA/GD-1370EU) and FIPS Hard Disk Kit(GE-1230) Evaluation Technical Report, Version 1.1, January 31, 2019, Information Technology Security Center Evaluation Department

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

[16] Guideline for Certification Application with HCD-PP Conformance, Version 1.4, January 10, 2019, Information-technology Promotion Agency, Japan