Certification Report

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

IT Product (TOE)

Reception Date of Application (Reception Number)	2020-03-11 (ITC-0742)
Certification Identification	JISEC-C0693
Product Name	SHARP BP-30C25 fax option model with BP-FR10U
Version and Release Numbers	0110Uc00
Product Manufacturer	SHARP 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.
2020-12-04

YANO Tatsuro, 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

"SHARP BP-30C25 fax option model with BP-FR10U, Version 0110Uc00" 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 1
1.1 Product Overview 1
1.1.1 Protection Profile or Assurance Package 1
1.1.2 TOE and Security Functionality 1
1.1.2.1 Threats 2
1.1.2.2 Configuration and Assumptions 2
1.1.3 Disclaimers 2
1.2 Conduct of Evaluation 3
1.3 Certification 3
2 Identification 4
3 Security Policy 5
3.1 Users 5
3.2 Assets 5
3.3 Threats 6
3.4 Organisational Security Policy 7
4 Assumptions and Clarification of Scope 8
4.1 Usage Assumptions 8
4.2 Environmental Assumptions 9
4.3 Clarification of Scope 10
5 Architectural Information 11
5.1 TOE Boundary and Components 11
5.1.1 Security Functions 11
5.2 IT Environment 14
6 Documentation 15
7 Evaluation conducted by Evaluation Facility and Results 16
7.1 Evaluation Facility 16
7.2 Evaluation Approach 16
7.3 Overview of Evaluation Activity 16
7.4 IT Product Testing 17
7.4.1 Developer Testing 17
7.4.2 Evaluator Independent Testing 17
7.4.3 Evaluator Penetration Testing 20
7.5 Evaluated Configuration 22
7.6 Evaluation Results 22
7.7 Evaluator Comments/Recommendations 22
8 Certification 23
8.1 Certification Result 23

8.2 Recommendations 23
9 Annexes 24
10 Security Target 24
11 Glossary 25
12 Bibliography 27

1 Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "SHARP BP-30C25 fax option model with BP-FR10U, Version 0110Uc00" (hereinafter referred to as the "TOE") developed by SHARP CORPORATION, and the evaluation of the TOE was finished on 2020-11 by Information Technology Security Center Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, SHARP 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 "general consumers 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 Profile [14][15] (referred to as the "Conformance PP").

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

1.1.2 TOE and Security Functionality

This TOE is an IT product and a digital multifunction device (hereinafter referred to as the "MFD") equipped not only with copy, printer and scanner function, but also with a function to save and retrieve documents (referred to as the "document filing function" in this TOE). This TOE has no fax function.

The TOE provides security functions required by the Conformance PP that is the Protection Profile for the MFD, to prevent unauthorized disclosure and tampering of the data handled by the MFD.

For these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance requirements required by the Conformance PP.

The following show the threats and the assumptions that the TOE assumes:

1.1.2.1 Threats

The TOE presumes the following threats:

There is a threat of unauthorized disclosure or tampering of User Document Data and data relevant to security functions which are the assets to be protected of the TOE by operating the TOE and/or accessing the network to which the TOE is connected.

There is also a threat of compromising security functions of the TOE due to the failure of the TOE itself or by installing unauthorized software.

1.1.2.2 Configuration and Assumptions

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

It is assumed that the TOE is operated in the environment where unauthorized physical access is restricted and it is connected to a LAN separated from the Internet.

The management and maintenance of the TOE under operation shall be appropriately performed by an administrator trusted by the procurement entities in accordance with the guidance documents. In addition, users of the TOE shall be trained to use the TOE securely.

1.1.3 Disclaimers

In this evaluation, the following operations are outside the scope of assurance:

- Operations in the state where the operational environment of the TOE shown in "4.3 Clarification of Scope" is not secure
- TOE's operations under conditions other than those indicated 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 2020-11, 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] and the Observation Reports 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 oversight reviews were also prepared for those concerns found in the certification process.

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: SHARP BP-30C25 fax option model with BP-FR10U
TOE Version: 0110Uc00

The TOE name consists of the MFD main unit and mandatory option. TOE components are shown in Table 2-1.

Table 2-1 TOE Components

Model number of Main unit	Fax	Mandatory option
BP-30C25	none	BP-FR10U

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

The following information indicated on the casing of the TOE and the operation panel should be confirmed in accordance with the description in the product guidance.

・Model number of Main unit

The model number of main unit indicated on the casing shall be the name contained in "Model number of Main unit" of Table 2-1.

・Fax

“NONE” is indicated in the FAX field of the operation panel.

・Mandatory option

The option name indicated on the operation panel shall be the name in "Mandatory option" of Table 2-1.

・TOE version

The TOE version indicated on the operation panel shall match the TOE identification version.

3 Security Policy

The TOE provides MFD basic functions such as copy function, printer function, scanner function and document filing function. It has the functions to store user's document data inside the TOE as well as to communicate with user's terminals and various servers via the network.

The TOE provides the following security functions that satisfy the requirements of the Conformance PP:

- A function to identify and authenticate users
- A function to control access to user data
- A function to encrypt and store user data
- A function to protect user data on the communication paths when using the LAN
- A function to restrict security management to the identified and authenticated users
- A function to log events related to security
- A function to verify and install updated firmware
- A function to verify normal operation of security functions at start-up

Details of the security functions of the TOE are shown in Section 5.1.

Details of the user roles, protected assets, threats, organisational security policy that the TOE assumes are shown in Sections 3.1 to 3.4.

3.1 Users

For use of the TOE, users in Table 3-1 are assumed.

Table 3-1 User Categories

Designation	Category Name	Definition
U.NORMAL	Normal User	A User who has been identified and authenticated and does not have an administrative role
U.ADMIN	Administrator	A User who has been identified and authenticated and has an administrative role

3.2 Assets

Assets to be protected in the TOE can be classified into two categories in Table 3-2. Out of them, Table 3-3 shows user data, and Table 3-4 shows TSF data, each of which consists of two types of assets.

Table 3-2 Asset categories

Designation	Asset category	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 User Data types

Designation	User Data 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 TSF Data types

Designation	TSF Data 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 the threats to be countered by the TOE.

Table 3-5 Threats

Designation	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

Designation	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.
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.

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 whether to use 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 assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Designation	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 an office and connected with the LAN which is the internal network of the organization, and used with a client PC and various servers similarly connected to the LAN.

Figure 4-1 shows the general operational environment as assumptions of the TOE.

Users use the TOE by operating the operation panel of the TOE or a PC connected to the LAN.

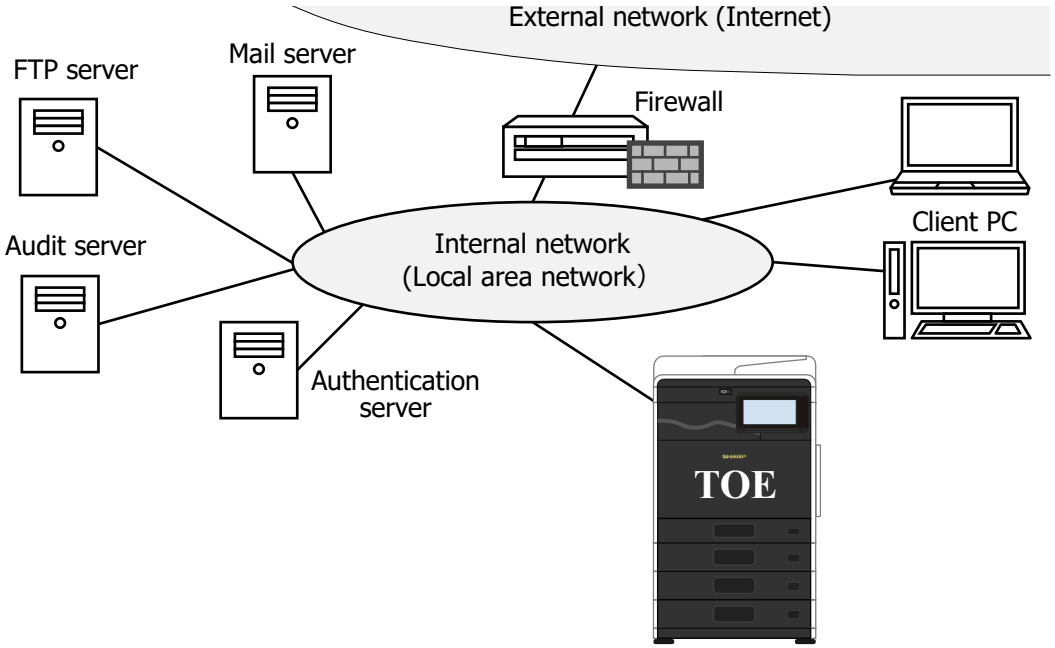

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

(1) Client PC

It is a general PC used by users.
The following software are required for use of the TOE.

・Printer Driver

The name is "SHARP BP-30C25 PCL6 driver".

・Web Browser

(2) Audit Server

It is an audit server to store the audit log generated by the TOE. It must use the syslog protocol and support TLS 1.2. Installation of this server is mandatory.

(3) Authentication Server

In the case of "external authentication method" shown in "Identification and authentication function" in Section 5.1.1, an authentication server which supports TLS 1.2 and of which authentication protocol is LDAP authentication method is required.

(4) Mail Server

It is necessary to send user document data scanned using the "Scanner function" as an E-mail attached file. It must support TLS 1.2.

(5) FTP Server

It is necessary to send user document data scanned using the "Scanner function" to the specified FTP server. It must support TLS 1.2.

It should be noted that the reliability of the hardware and the software other than the TOE shown in this configuration is outside the scope of this evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

In the TOE, a server such as an authentication server may be installed in addition to the audit server that is mandatory to install. In addition, it is necessary to install a firewall to connect to the Internet which is an external network. It is the responsibility for the operators that these servers and firewalls are operated securely.

5 Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE.

The area enclosed by the frame indicated as the "TOE" in Figure 5-1 is the TOE. It does not include Audit server, Mail server, FTP server, Authentication server, Client PC and User.

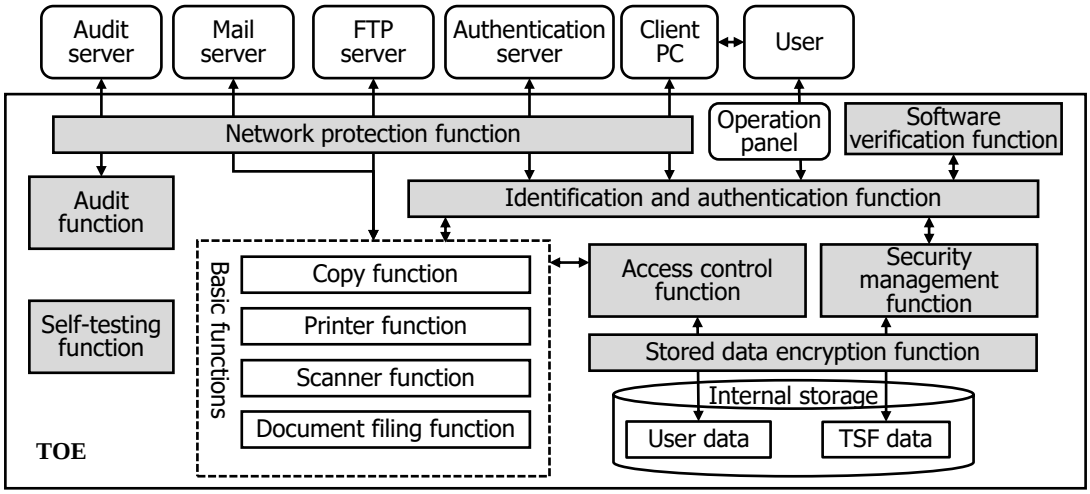

Figure 5-1 TOE boundary

The TOE function consists of security functions (functions shown in colored box) and basic functions (functions shown in white box) in Figure 5-1.

The security functions are described below. For basic functions, see Chapter 11.

5.1.1 Security Functions

(1) Identification and authentication function

It is a function to identify and authenticate users of the TOE by login names and passwords in the operation panel, the web browser of the client PC, and the printer driver.

- It requests a password consisting of upper or lower case letters of the alphabet, numbers, or special characters and having the number of characters set by the administrator or more.

- It supports "internal authentication method" using user information stored in the TOE and "external authentication method" using external authentication server.
- When entering a password, it displays an asterisk instead of the input character.
- It stops accepting authentication for 5 minutes if password authentication has failed consecutively.
- After identification and authentication, the session is terminated if no operation is performed for the time set by the administrator in the case of the operation panel, or for 5 minutes in the case of the web browser.

(2) Access control function

It is a function to control access of user data when manipulating user data with the basic functions of the TOE.

- It controls access to user data based on the policy defined for each type of user such as owner of user data or user role.

(3) Stored data encryption function

It is a function to encrypt and store user data, etc., in the TOE.

- User data and TSF data are encrypted by AES CBC mode with a 256-bit key and stored.
- An encryption key for encrypting user data, etc., is created by a random number generator having sufficient entropy.

(4) Network protection function

It is a function to protect user data on the communication path when using the LAN.

- Encrypted communication by TLS 1.2 is used between the TOE and various servers such as audit server.
- The encryption key used for encrypted communication is created by a random number generator having sufficient entropy.
- In the communication between the client PC and the TOE, IPP over TLS communication is used for the printer driver, and HTTPS communication is used for the web browser.

(5) Security management function

It is a function to restrict the security management of the TOE to the identified and authenticated users.

- Registration / deletion of internal authentication users, change of minimum password length, setting of various servers, overwriting of user data and TSF data, etc., are provided only to users with the administrator role.
- Inquiries about user login names and authority groups of the users themselves, and change of passwords are provided to all internal authentication users.

(6) Audit function

It is a function to log events related to use of the TOE and security.

- In addition to the start and end of the audit, a log of the audit event such as the end of the job and failure of identification and authentication is generated as audit data. In the audit data, the event name, date and time of occurrence, user login name, event result and additional information are recorded.
- The generated audit data is sent to the audit server by using the syslog protocol and TLS 1.2.
- The audit data generated by the TOE is encrypted and stored in the TOE until it is successfully transmitted to the audit server. In the TOE, it is possible to store 40,000 audit data. The audit data generated newly in excess of 40,000 is not stored but is discarded.

(7) Software verification function

It is a function that the TOE verifies the update firmware and enables installation of only legitimate firmware.

- It verifies that it is a legitimate firmware by checking the hash value of the firmware with a digital signature provided at the same time as the firmware and the hash value calculated by the TOE using SHA - 256.
- A user with the administrator role can acquire the version of the firmware.

(8) Self-testing function

It is a function to verify the normal operation of the security functions at the start-up of the TOE.

- Verification that the security functions operate normally is done by the entropy source health test of the random number generator, by the known answer test of the encryption algorithm, and by confirming that the firmware is not corrupted.
- In the verification, if any error is detected in all or in part, the TOE stops the start-up and suspends any operation until the power is turned off.

5.2 IT Environment

The TOE communicates with various servers and client PCs via the LAN.

The TOE sends the generated audit data to the audit server. The administrator reads the audit data from the audit server.

In the case of the external authentication method, the authentication server is used to identify and authenticate users.

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

6 Documentation

The identification of guidance attached to the TOE is shown in Table 6-1.

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

Table 6-1 Attached Documents

Name	Version	Language
Start Guide	TINSM2376QSZZ HH1	English
Quick Start Manual	2020C-EX1	English
User's Manual	2020C-EX1	English
User's Manual (Touch Panel Operation)	2018H-EN1	English
User's Manual (Address Book Registration)	2018H-EN1	English
User's Manual (Web Page Settings)	2018H-EN1	English
Software Setup Guide	2020C-EN1	English
Troubleshooting	2020C-EN1	English
BP-FR10U Data Security Kit Operation Guide	EX1	English
BP-FR10U Data Security Kit Notice	1.0	English
How to set up BP-FR10U to be the "Protection Profile for Hardcopy Devices" compliant	V1.0	English

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 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 2020-03 and concluded upon completion of the Evaluation Technical Report dated 2020-11.

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 evaluators conducted the evaluator testing at the developer site in 2020-07.

Concerns found in evaluation activities were issued as the Observation Reports and reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns in the evaluation process that the Certification Body found were described as the certification oversight reviews, and they were sent to the Evaluation Facility.

The Evaluation Facility and the developer examined them, which was reflected in the Evaluation Technical Report.

7.4 IT Product Testing

As the verification results of the evidence shown in the evaluation process, the evaluators performed the independent testing to ensure that the security functions of the product are accurately implemented and penetration testing based on the vulnerability assessment.

7.4.1 Developer Testing

The developer testing is not included in the assurance requirements of this evaluation.

7.4.2 Evaluator Independent Testing

The evaluators conducted evaluator independent testing (hereinafter referred to as "independent testing") based on the evidence presented during the evaluation to ensure that the security functions of the product are accurately implemented.

The independent testing performed by the evaluators is explained as follows.

(1) Independent Testing Environment

Configurations for the independent testing are based on the operational environment of the TOE shown in Figure 4-1, and the components are as shown in Table 7-1. Although there are differences in the following points, the evaluator also evaluates that these configurations are equivalent to the configuration identified in the ST, and there is no problem in checking the function of this TOE.

- Firewalls installed to protect the TOE against unauthorized access from the external network do not exist in the testing environment because they do not affect the operation of the TOE.
- In the TLS test, communication between the TOE and the server / client PC is performed via the TLS testing tool created by the Evaluation Facility. Since the TLS testing tool only modifies the packet data of the TLS handshake message, it does not affect the functions of the TOE.
- For some tests such as cryptographic tests, the testing firmware created by the developer is used for calling for testing the cryptographic modules in the TOE.

The module called in the test using the testing firmware is the same as the module of the TOE, so it does not affect the functions of the TOE.

Table 7-1 Components of Independent Testing

Configuration Item	Detail
TOE	BP-30C25 (Fax: none) ・Option: BP-FR10U
Audit Server	rsyslog ver.8.24.0
Mail Server	Postfix ver.2.10.1
Authentication Server	openLDAP ver.2.4.44
FTP Server	Microsoft Internet Information Services ver.8.5 9600.16384
Client PC	OS : Windows 8.1 / 10 Web browser: ・Internet Explorer 11 ・Google Chrome 81.0.4044.129 Printer driver: ・SHARP BP-30C25 PCL6 06.00.06.14

(2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

The viewpoints of the independent testing devised by the evaluator based on the requirements of the Conformance PP and on the evaluation documentation submitted for evaluation are shown below.

<Independent Testing Viewpoints>

1. Checking security functions by SFR.
2. Checking if the encryption implementation is correct.

b. Independent Testing Outline

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

<Independent Testing Approach>

For the external interfaces of the TOE, inputs were provided using the TOE operation panel, client PC and testing tools, and the behaviors were observed using the following methods.

- If the behavior can be observed from the external interface of the TOE, the external interface of the TOE is used.

・ If the behavior cannot be observed from the external interface of the TOE, the logs in the audit server are investigated, and network analyzer or testing firmware is used.

<Content of the Performed Independent Testing>

The independent testing was performed on 34 items by the evaluators.

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

Table 7-2 Content of the Performed Independent Testing

Viewpoint	Outline of the Independent Testing
1	Checking security functions ・To confirm for each SFR that all the security functions are as specified by the test items created from the assurance activities of the Conformance PP or the specification of SFR.
2	Checking encryption implementation ・To confirm the implementation of the following encryption algorithm to be tested by the testing firmware installed on the TOE. - RSA (key generation, signature generation/verification) - ECDSA (signature verification) - DSA (signature verification) - AES-CBC-128, AES-CBC-256, AES-ECB-256, AES-GCM-128, AES-GCM-256 - SHA-1, SHA-256, SHA-384, SHA-512 - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 - CTR_DRBG ・The encryption key of the user document data and the user document data encrypted and stored inside the TOE are taken out by the testing firmware and decrypted by the decryption tool to confirm that it is correctly encrypted.

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 evaluators 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 evaluators is explained as follows.

(1) Summary of the Penetration Testing

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

a. Vulnerability of Concern

The evaluators 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 it can be exploited by the fact that the unintended port of the TOE is enabled or a publicly known vulnerability exists in the running network service.
2. In the TOE web interface, there is concern that it can be exploited by the existence of publicly known vulnerabilities, such as bypass of the identification and authentication function by direct designation of URL, and XSS.
3. There is concern that buffer overflow or arbitrary code execution may occur due to unauthorized print data input to the TOE.
4. There is concern that the identification and authentication function may be bypassed due to unauthorized input from the operation panel, printer driver and web interface.
5. When the TOE operates as a TLS client, there may be vulnerabilities in the verification process of the server certificate of the communication destination.

b. Penetration Testing Outline

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

<Penetration Testing Environment>

The following testing tools shown in the Table 7-3 below were added to the environment of the evaluator independent testing to implement.

Table 7-3 Penetration Testing Tools

Tool Name	Outline and Purpose of Use
Port Scan Tool nmap 7.8.0	It is used for searching ports.
Vulnerability Scan Tool Nessus 8.8.0	It is used for detecting publicly known vulnerability.
Web Vulnerability Scan Tool OWASP ZAP 2.8.0 Active scanner rules(beta) v27.0.0 Added	It is used for detecting general vulnerability of web.
Web Application Analysis Tool Fiddler 5.0.20194.41348	It is used for capturing or issuing communication data received or sent by web application.
Printer Security Testing Tool PRET 0.40	It is used for detecting vulnerability of printing device by using printer language.
Penetration Testing Tool Metasploit Framework v5.0.9	It is used for creating unauthorized print files.

<Content of the Performed Penetration Testing>

Table 7-4 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-4 Content of the Performed Penetration Testing

Vulnerability	Penetration Testing Outline
1	It is confirmed that unexpected ports are not open and that there is no publicly known vulnerability in the available ports by using the port scan tool and the vulnerability scan tool.
2	It is confirmed that there is no publicly known vulnerability in the Web interface by using the web vulnerability scan tool and web application analysis tool.
3	It is confirmed that unintended behavior does not occur by using print data in PJL language, TIFF format and PDF format that are intended to generate unauthorized behavior.
4	It is confirmed that no unauthorized behavior occurs due to character strings entered in the identification and authentication function.
5	It is confirmed in the mail processsing that TOE has correctly performed the verification processing of the TLS server certificate.

c. Result

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

7.5 Evaluated Configuration

The requirements of the TOE configurations, which are the assumptions for this evaluation, are as described in the guidance documents listed in Chapter 6. In order to enable the security functions of this TOE and use them securely, the TOE must be set as described in the guidance documents. Different settings are not subject to assurance by this evaluation.

7.6 Evaluation Results

The evaluators 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

  Guideline for Certification Application with HCD-PP Conformance [16]

  - Treatment regarding FCS_RBG_ EXT.1 Test
  - Treatment regarding FCS_TLS_ EXT.1.1 Test

- 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 procurement entities.

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. Contents pointed out in the Observation Reports shall be adequate.
2. Contents pointed out in the Observation Reports shall properly be solved.
3. 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.
4. Rationale of the evaluation verdict by the evaluators presented in the Evaluation Technical Report shall be adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM and the assurance activities of the Conformance PP.

Concerns found in the certification process were prepared as the certification oversight reviews, and they were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

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

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer to "4.3 Clarification of Scope" and "7.5 Evaluated Configuration" to make sure that the scope of the evaluation target and operational requirements of the TOE meet the operational conditions they assume.

If the transmission of the audit data to the audit server fails, the warning messages are displayed on the operation panel and the web page. The TOE tries to retransmit, but the operator needs to be careful about the warning messages.

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.

Title:	SHARP BP-30C25 fax option model with BP-FR10U Security Target
Version:	1.03
Publication Date:	2020-11-02
ST Author:	SHARP 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 Generator
ECB	Electronic Codebook
FTP	File Transfer Protocol
GCM	Galois/ Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL/TLS
IPP	Internet Printing Protocol
LDAP	Lightweight Directory Access Protocol
MFD	Multifunction Device
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TLS	Transport Layer Security
XSS	Cross Site Scripting

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

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.
Copy function	It is a function to copy and print the user document data scanned from paper documents by user's operation from the operation panel.
Scanner function	It is a function to scan paper documents and send the scanned user document data to the mail server and FTP server by user's operation from the operation panel.
Document filing function	It is a function to store the user document data in the internal storage of the TOE at the same time with the copy function, etc., and to print the stored user document data by user's operation from the operation panel or from the client PC via the LAN.
Printer function	It is a function to receive the user document data via the LAN from the printer driver of the client PC and print it by user's operation from the operation panel.
Assurance Activities	Evaluation work that the evaluator must carry out for PP Conformance. It is supplement of the CEM, and it is described in the Conformance PP regarding the Conformance PP [14].

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 Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

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

[6] Common Criteria for Information Technology Security Evaluation Part 3: 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] SHARP BP-30C25 fax option model with BP-FR10U Security Target, Version 1.03, November 02, 2020, SHARP CORPORATION

[13] SHARP CORPORATION SHARP BP-30C25 fax option model with BP-FR10U Evaluation Technical Report, Version 1.3, November 05, 2020, 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 1.7, July 1, 2020, Information-technology Promotion Agency, Japan, JISEC-CERT-2020-A17