Certification Report

SAITO Yutaka, Commissioner
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2024-01-26 (ITC-4873)
Certification Identification	JISEC-C0832
Product Name	EPSON LM-C400/AM-C550/AM-C400 with FAX
Version and Release Numbers	1.00
Product Manufacturer	SEIKO EPSON CORPORATION
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)
Assurance Package	EAL2 Augmented by ALC_FLR.2
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.

2024-11-19

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

"EPSON LM-C400/AM-C550/AM-C400 with FAX Version 1.00" 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 "EPSON LM-C400/AM-C550/AM-C400 with FAX Version 1.00" (hereinafter referred to as the "TOE") developed by SEIKO EPSON CORPORATION, and the evaluation of the TOE was completed on 2024-10-23 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, SEIKO EPSON CORPORATION, and provide security information to procurement entities 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") 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 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 Protection Profile or Assurance Package

The TOE conforms to the following Protection Profile [14][15] (hereinafter referred to as the "Conformance PP").

U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

Assurance Package of the TOE is EAL2 augmented by ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a Multi-Function Peripheral (hereinafter referred to as the "MFP") which provides the functions of print, scan, copy, fax, and document storage and retrieval.

The TOE provides security functions required by the Conformance PP to protect document data and setting data processed by the TOE.

For these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package.

Threats and assumptions assumed for the TOE are described in the following sections.

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 the documents that the TOE handles and the setting information relevant to the security functions, there are threats of disclosure and tampering caused by unauthorized access to both the TOE and the communication data on the network.

The TOE provides the security functions to prevent those protected assets from unauthorized disclosure and tampering.

1.1.2.2 Configuration and Assumptions

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

1.1.3 Disclaimers

The following operations are not ensured by this evaluation:

- An environment different from that described in "4.2 Environmental Assumptions"

- TOE with settings different from those 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 2024-10, based on functional requirements and assurance requirements of the TOE according to the publicized 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 prepared for those concerns found in the certification process. The Certification Body confirmed that those concerns pointed out by the Certification Body 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:	EPSON LM-C400/AM-C550/AM-C400 with FAX
TOE Version:	1.00

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

Users confirm the following information displayed on the printed status sheet and the label of the FAX board as described in the guidance document.

- MFP main unit: One of the following:

(For Japan) EPSON LM-C400
(For other countries) EPSON AM-C550, EPSON AM-C400

- Hardware version: "A"

- Firmware version: "GL27NC"

- FAX board: Either of the following:

(For Japan) "Super G3/G3 Multi Fax Board / PR3FB0"
(For other countries) "Super G3/G3 Multi Fax Board / PR3FB1"

3. Security Policy

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

The TOE provides the security functions to counter the unauthorized access to protected assets such as the stored documents in the TOE, and to protect the communication data on the network.

For each setting that is relevant to the above security functions, only administrator is permitted to set configurations in order to prevent the deactivation and unauthorized use of the security functions.

The following user roles are assumed in the use of the TOE:

- Normal user
  A user who is allowed to use basic functions provided by the TOE.

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

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

- User Document Data
  Document Data of users.

- User Function Data
  The information about a user's document or job to be processed by the TOE.

- TSF Confidential Data
  The data used for security functions whose integrity and confidentiality are required. In the TOE, they correspond to user passwords, passwords for accessing external servers, and audit logs, etc.

- TSF Protected Data
  The data used for security functions whose integrity only are required. In the TOE, they correspond to the user ID of the user, user authority information, time setting information, and network setting information, etc.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.1.1, and to satisfy the organizational security policies shown in Section 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 ones written in the conforming 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. The details of each security function 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), and the TOE counters these threats using the "User Identification and Authentication Function," the "Access Control Function for TOE Function," the "Document Access Control Function," the "Residual Data Overwrite Function," and the "Network Protection Function."

The "User Identification and Authentication Function" permits only the users who succeeded at the identification and authentication to use the TOE.

The " Access Control Function for TOE Function" and the "Document Access Control Function" are used when an identified and authenticated user uses basic MFP functions such as the print function, scan function, copy function, or FAX function, etc. With these functions, the authority assigned to the user is checked, only the authorized user is permitted to use the function, and access control to the document data on which the function is to be carried out is also performed, and only users with access authority are permitted to access the document data.

The "Residual Data Overwrite Function" overwrites and erases deleted documents and temporarily stored documents from the storage device such as the HDD to prevent unauthorized access to residual information.

The "Network Protection Function" provides an encrypted communication function when communicating between the TOE and various servers and client PCs, and protects communication data.

With the above functions, the TOE prevents the user data to be protected from unauthorized disclosure and alteration by unauthorized use of the TOE and 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 the data used in the security functions (TSF Confidential Data and TSF Protected Data), and the TOE counters these threats with the "User Identification and Authentication Function," the "Security Management Function," and the "Network

Protection Function."

The "User Identification and Authentication Function" and the "Security Management Function" perform access control on these data according to the role of the user in order to prevent unauthorized access beyond the user's authority to data used in the security functions.

The "Network Protection Function" provides an encrypted communication function when communicating between the TOE and various servers and client PCs, and protects communication data.

With the above functions, the TOE prevents the user data to be protected from unauthorized disclosure and alteration by unauthorized use of the TOE and 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 for the TOE are shown in Table 3-2. These organizational security policies are the same as the ones written in the conforming PP.

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.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the following security functions to satisfy the organizational security policies shown in Table 3-2. The details of each security function are described in Chapter 5.

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

The TOE implements this policy by the "User Identification and Authentication Function" and the "Access Control Function for TOE Function."

The "User Identification and Authentication Function" permits only the users who succeeded in the identification and authentication to use the TOE.

The "Access Control Function for TOE Function" is used when an identified and authenticated user uses basic MFP functions such as the print function, scan function, copy function, or FAX function, etc. The authority assigned to the user is checked, and only the authorized user is permitted to use the function.

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

The TOE implements this policy by the "Self-Test Function."

The "Self-Test Function" verifies the integrity of the execution code of the security function at startup of the MFP.

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

The TOE implements this policy by "Audit Log Function."

The "Audit Log Function" records the events relevant to security functions as the audit log. The audit log stored in the TOE can be read out only by the identified and authenticated administrator.

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

The TOE implements this policy by the "User Identification and Authentication Function" and the "Network Protection Function."

The "User Identification and Authentication Function" permits only the users who succeeded at the identification and authentication to use the TOE. It also terminates the session after a certain time of no operation by user.

The "Network Protection Function" provides a function of limiting data transfer between a wired LAN and a telephone line, and prevents unauthorized data transfer.

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 ones written in the conforming PP. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumption
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 a general office and connected to a LAN, and it is used from client PCs connected to the LAN. Figure 4-1 shows the general operational environment of the TOE.

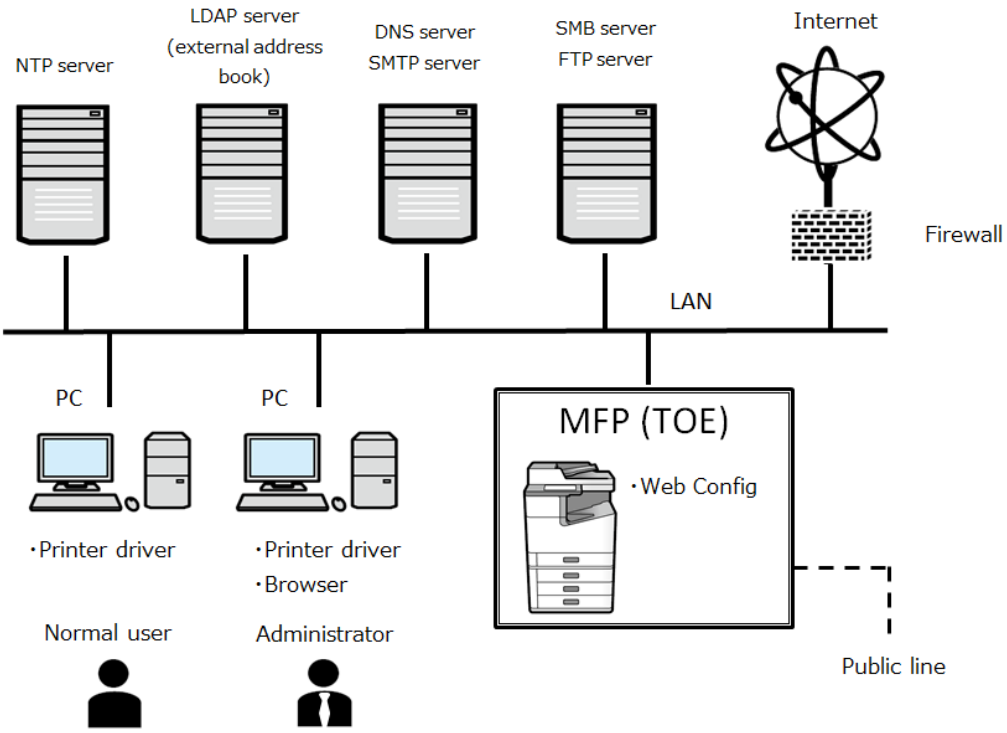

Figure 4-1 Operational Environment of the TOE

As shown in Figure 4-1, the TOE is assumed to be used in an environment such as offices, etc. where office documents are handled. The TOE is connected to the LAN and telephone line.

Various server computers such as an LDAP server, SMB server, and FTP server, etc. are connected to the LAN, and communicate with the TOE for documents and for collection of various information, etc. Also, a firewall is installed to protect the LAN and the TOE from threats from external networks such as the internet. The server software used in this evaluation is shown in Table 4-2.

The operation of the TOE may use the TOE's own operation panel or a client PC connected to the LAN. The software shown in Table 4-3 is installed on the client PC.

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. It is assumed to be trustworthy.

Table 4-2 Server Software Used in This Evaluation

Software	Name and version
DNS server	Microsoft Windows Server 2016 Standard
FTP server	Microsoft Windows Server 2016 Standard
LDAP server	Microsoft Windows Server 2016 Standard
NTP server	Microsoft Windows Server 2016 Standard
SMB server	Microsoft Windows Server 2016 Standard
SMTP server	hMailServer 5.6.7-B2425

Table 4-3 Software of Client PC

Software	Name and version
Printer driver	For Microsoft Windows Japanese version: Epson Printing System(J) Version 3.00.00 English version: Epson Printing System(A) Version 3.01.00
Browser	Microsoft Edge 122

4.3 Clarification of Scope

The evaluated security functions of the TOE have the following constraints:

1) IPsec for IPv6

In this evaluation, only IPv4 is evaluated for the IPsec protocol. IPsec for IPv6 has not been evaluated and is not subject to assurance.

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 TOE is the entire MFP product including the FAX board.

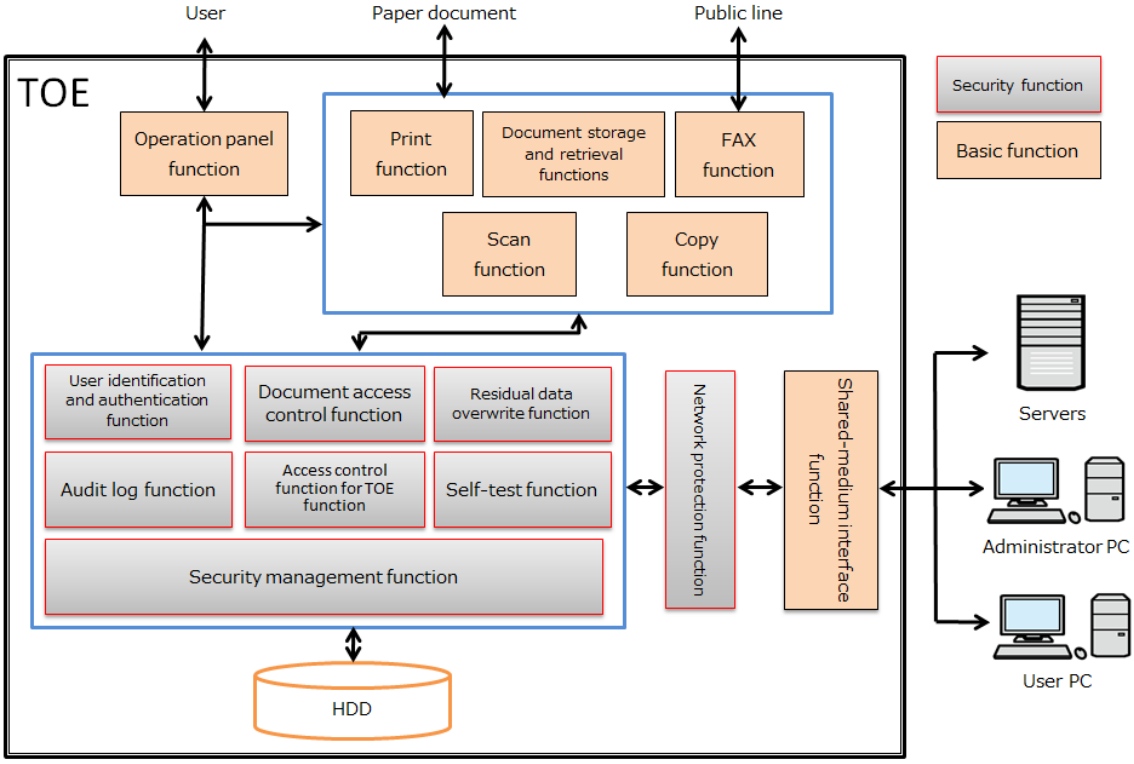

Figure 5.1 Composition of the TOE

The TOE functions consist of security functions and other basic MFP functions. The security functions of the TOE are described below. For the basic MFP functions, see the glossary.

1) User Identification and Authentication Function

This function identifies and authenticates a user by confirming that the entered user ID and password match the user ID and password managed inside the TOE. This function is applied at the time of the following operations:

- Logon from the operation panel

- Administrator logon from a client PC (browser)

- Sending a print job from a client PC (printer driver)

Also, in order to secure necessary authentication strength, the following functions are provided:

- If authentication fails, put the account in the locked state for a certain period of time.

- When setting a password, it is required to be of at least a certain quality in terms of length (number of digits) and character types.

- If there is no operation for a certain period of time after logon, the session is terminated.

When the validity of the password is confirmed, the use authority of the TOE prescribed in advance for each role of the user is assigned, and use of the TOE is permitted. The roles specified by the TOE are normal users and administrator.

2) Access Control Function for TOE Function

This function restricts the use of basic MFP functions such as print, scan, copy, and FAX.

When the user uses a basic MFP function, whether or not to operate the function is determined with reference to the usage authority for basic functions set for each user.

3) Document Access Control Function

In response to a processing request from a user, this function implements access control for the document data and job based on the user ID of the user and the authority for each role. The user ID of the user who performed the operation is associated with the print job input via the network and the document data saved in the TOE, and when the processing request is received from the user, the function controls permission or rejection based on the user's user ID and their operation authority. When the user is an administrator, deletion of all document data and jobs is permitted.

4) Residual Data Overwrite Function

This function overwrites deleted documents and temporarily saved documents with a specific value (0x00) in order to completely erase them from devices such as HDDs which are used as storage areas, making it impossible to access the residual data.

5) Network Protection Function

This function provides the following two functions for the purpose of protecting communication data, etc. when the TOE communicates with the outside.

- When the TOE communicates with various servers and client PCs via the LAN, IPsec which is a cryptographic communication protocol is applied to prevent communication data from being leaked or tampered.

- Provides a function of limiting data transfer between a wired LAN and a telephone line, and prevents unauthorized data transfer.

6) Security Management Function

This function prevents unauthorized access beyond authority by performing access control according to the role of the user for data used in security functions such as user information and various setting information.

7) Self-Test Function

This function verifies the hash value of the firmware at startup of the TOE main body and verifies the integrity of the execution code of the security functions.

8) Audit Log Function

This function is the function to record the audit events relevant to security functions as the audit log. Only the identified and authenticated administrator can download the audit log stored in the TOE to client PCs. The audit log cannot be modified.

5.2 IT Environment

The TOE is connected to the LAN and communicates with server computers, such as an FTP server, an SMB server, and an LDAP server, as well as with client PCs. The TOE communicates with fax devices via telephone line.

Client PCs connected via the LAN use the TOE via a printer driver or a browser.

The server computer and the client PCs necessary for the operation of the TOE must be prepared at the responsibility of the user.

6. Documentation

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

(Japanese)

Name[1]	Version
User's Guide	NPD7236-00 JA
Supplemental Security Guide	NPD7435-01 JA
Before Use	4145053-01

(English)

Name	Version
User's Guide	NPD7235-00 EN
Supplemental Security Guide	NPD7435-01 EN
Before Use	4145053-01

[1] The guidance name listed in Table 6-1 is the translation of Japanese name.

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

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 started in 2024-01 and concluded upon completion of the Evaluation Technical Report dated 2024-10. 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 examined the implementation of the requirements for each work unit of configuration management and delivery by visiting the development site in 2023-07. 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 in 2024-05 and 2024-10.

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

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As the verification results of the evidence shown in the process of the evaluation and 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 had 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, and Table 7-1 shows the main configuration items.

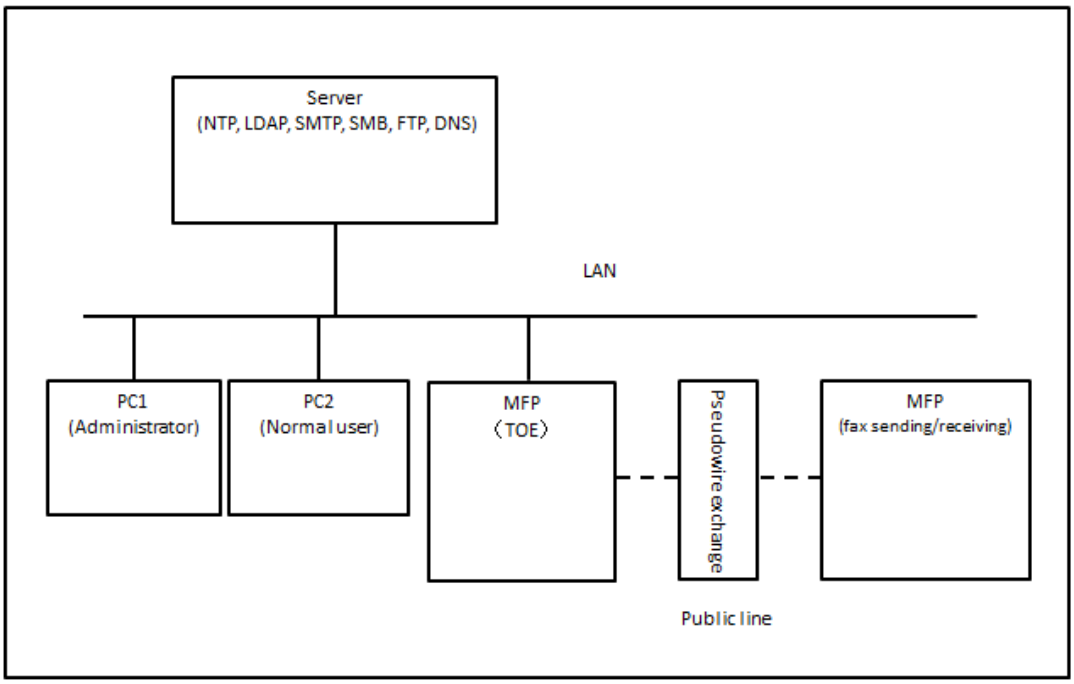

Figure 7-1 Configuration of the Developer Testing

Table 7-1 Configuration Items

Configuration Item	Description
TOE	EPSON LM-C400 with FAX 1.00 EPSON AM-C400 with FAX 1.00 EPSON AM-C550 with FAX 1.00
NTP server	Microsoft Windows Server 2016 Standard
LDAP server	Microsoft Windows Server 2016 Standard (Manage the address book and use it when addressing FAX data)
SMTP server	hMailServer 5.6.7 - Build 2425
SMB server	Microsoft Windows Server 2016 Standard
FTP server	Microsoft Windows Server 2016 Standard
DNS server	Microsoft Windows Server 2016 R2 Standard
MFP (for FAX sending/receiving)	WF-C5890
Pseudo-wire exchange	EXCEL-N012 (Nishiyama)
PC1, PC2	OS: Windows 10 Browser: Microsoft Edge 122 Printer driver: Japanese version: Epson Printing system(J) Version 3.00.00 English version: Epson Printing system(A) Version 3.01.00

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 as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>
In addition to the method of stimulating the external interface (operation panel, LAN interface, etc.) assumed in the usual TOE usage and visually observing the result, the developer testing also includes using the generated audit log and the development interface to confirm the internal status and confirming the communication protocol between the client PC and various servers and the TOE by packet capture.

<Content of the Performed Developer Testing>

The expected values of testing results described in testing specifications which are provided in advance by the developer were compared to the values of the actual developer testing results described in the testing result reports which are also provided by the developer. As a result, it was found that the values of the actual testing results are in conformity to those of the expected testing results.

b. Scope of the Performed Developer Testing

The developer testing was performed on 49 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.

c. Result

The evaluator confirmed an 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 sample testing to reconfirm the implementation of security functions of the product using the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further confidence that security functions are certainly implemented, based on 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 conducted by the evaluator is the same as the configuration of the developer testing shown in Figure 7-1, except for the following:

- The following two models were used as the TOE.
  EPSON LM-C400 with FAX 1.00
  EPSON AM-C550 with FAX 1.00

The evaluator judged that the difference between the TOE models is the printing speed and the target market, and that testing of the above two models is sufficient taking these differences into consideration.

The components of the independent testing environment and the test tools includes those used for the developer testing and those developed independently by the developers, and the evaluator conducted their validity confirmation and operation testing.

2) Summary of the Independent Testing

A summary of the independent testing is 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) For operations that seem to be deficient in developer testing in terms of coverage because there are many kinds of input parameters, add variations such as combinations of parameters.

(2) For execution timing of several TSFs and combination of execution, the testing items to which conditions are added are performed.

(3) The testing items are selected in the sampling testing from the following viewpoints:

- The testing items are selected to include all of TSFs and TSFIs in terms of completeness.
- The testing items are selected to cover the different testing approaches and testing environments.
- The testing items involving TSFI that meet many of the SFRs are mainly selected in order to conduct tests efficiently.

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 with the same testing approach as the developer testing.

<Content of the Performed Independent Testing>
Based on the viewpoints of the independent testing, 9 items for the independent testing and 36 items for the sampling testing were performed.

The main contents of the independent testing corresponding to the viewpoints are shown in Table 7-2.

Table 7-2 Content of the Performed Independent Testing

Viewpoint	Outline of the Independent Testing
(1)	- Confirm that the quality check at the time of setting a password is carried out according to the specification by increasing the variations of the input password. - Change the setting parameters of the communication protocol with the outside and confirm that it behaves as specified.

(2)	- Confirm that the behavior when an account is deleted, or authorization is changed while logged on is as specified. - Confirm that access control is performed according to the specification for operation from multiple interfaces.

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 below.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is 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) Unauthorized access to the TOE may be caused by unintentional network port interfaces.

(2) Security functions may be bypassed in case of entering data, for interfaces, which have the values and formats that are unintended by the TOE.

(3) Security functions may be bypassed by operating the TOE overloaded.

(4) By turning off the power at an unexpected timing, the correct operation of the security function may be infringed.

b. Penetration Testing Outline

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

<Penetration Testing Environment>
The penetration testing environment is identical with those of the developer testing shown in Figure 7-1, and evaluator independent testing.

Table 7-3 shows key tools used in the penetration testing.

Table 7-3 Penetration Testing Tools

Components	Overview
Nessus Version 10.5.5	Vulnerability Scanning Tool (The vulnerability database is the latest as of May 7, 2024)
Nikto Version 2.5.0	Vulnerability Scanning Tool for Web (The vulnerability database is the latest as of May 7, 2024)
Fiddler v5.0.20211.51073	Inspection tool of Web vulnerabilities with Proxy traffic
Burp Suite Community Edition 2021.5.1	Inspection tool of Web vulnerabilities with Proxy traffic
OWASP ZAP Version 2.14.0	Inspection tool of Web vulnerabilities with Proxy traffic (The vulnerability database is the latest as of May 7, 2024)
Nmap Version 7.93	Port Scanning Tool
PRET Version 0.40	PJL, Postscript Testing Tool

<Content of the Performed Penetration Testing>

Table 7-4 shows contents of the penetration testing corresponding to the vulnerabilities of concern.

Table 7-4 Content of the Performed Penetration Testing

Vulnerability	Penetration Testing Outline
(1)	- Confirmed that the unintended network ports were not opened using the port scanning tool and the vulnerability scanning tool. - Confirmed that there are no vulnerabilities to unauthorized inputs for available ports.
(2)	- Confirmed that there are no known vulnerabilities in the Web interface that accesses the TOE using the vulnerability inspection tool. - Confirmed that the security functions are not bypassed by the specified URL at the time of connecting to the TOE via a Web browser.

	- Confirmed that there is no implementation vulnerability related to PJL or PostScript using the testing tool. - Confirmed that unexpected behavior is not observed even if the TOE received FAX data that may cause illegal processing.
(3)	- Confirmed that the TOE is not in a non-secure state in the resource exhaustion state.
(4)	- Performed a power supply operation in a situation different from that during normal operation such as during TOE startup processing, and confirmed that the TOE is not in a non-secure state.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerability 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. In order to use the TOE securely as ensured by the evaluation, TOE administrator must configure the TOE as described in the appropriate guidance documents. If these setting values are changed to different values from those described in 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 by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:
  U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

  The TOE also conforms to the following SFR packages defined in the above PP:
  - 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
  - 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
  - 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
  - 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
  - 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment B
  - 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

- 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 EAL2 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 recommendation to be addressed to procurement entities.

8. Certification

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

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 shall be evaluated as presented in the Evaluation Technical Report.

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

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those 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 submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented by ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Users of the TOE should refer to "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" and exercise caution regarding whether the scope of evaluation of the TOE and operational requirements can be handled in the actual TOE operational environment.

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.

EPSON LM-C400/AM-C550/AM-C400 with FAX Security Target, Rev.02, August 1, 2024, SEIKO EPSON 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
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

HDD	Hard Disk Drive
MFP	Multi-Function Peripheral

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

Basic MFP functions	The basic functions as an MFP, consisting of the following functions: Print function (print document data received from a client PC), scan function, copy function, FAX function, document storage and retrieval function (function to save and retrieve digital documents sent and received by the FAX function)
FTP server	A server for sending and receiving files using FTP (File Transfer Protocol). Used for transfer of scan data that the TOE created using the scan function and received FAX data.
LDAP server	A server that provides directory services using LDAP (Light Directory Access Protocol). The TOE refers to the address book managed by the LDAP server and uses it for the destination of fax transmission.
SMB server	A server for file sharing, printer sharing, etc. using SMB (Server Message Block). Used for transfer of scan data that the TOE created using the scan function and received FAX data.
SMTP server	A server for transmitting emails using SMTP (Simple Mail Transfer Protocol). Used when the TOE sends an email of scanned data created using the scan function.
Web Config	An MFP built-in function that performs various settings (print setting, network setting, user restriction setting, administrator password setting, etc.) by accessing via the browser.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, December 2023, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, December 2023, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, 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] EPSON LM-C400/AM-C550/AM-C400 with FAX Security Target, Rev.02, August 1, 2024, SEIKO EPSON CORPORATION

[13] EPSON LM-C400/AM-C550/AM-C40 with FAX 1.00 Evaluation Technical Report, Version 1.1, October 23, 2024, Information Technology Security Center, Evaluation Department

[14] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

[15] CCEVS Policy Letter #20, 15 November 2010, National Information Assurance Partnership