



# Certification Report

Koji Nishigaki, Chairman  
Information-technology Promotion Agency, Japan

## Target of Evaluation

Application date/ID	2007-07-18 (ITC-7161)
Certification No.	C0228
Sponsor	SEIKO EPSON CORPORATION
Name of TOE	PP-100N Security control unit
Version of TOE	1.00
PP Conformance	None
Conformed Claim	EAL3
Developer	SEIKO EPSON CORPORATION
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

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

2009-07-27

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

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

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

## Evaluation Result: Pass

"PP-100N Security control unit Version 1.00" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

**Notice:**

This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

**Table of Contents**

---

1. Executive Summary .....	1
1.1 Introduction .....	1
1.2 Evaluated Product .....	1
1.2.1 Name of Product .....	1
1.2.2 Product Overview .....	1
1.2.3 Scope of TOE and Overview of Operation.....	2
1.2.4 TOE Functionality.....	7
1.3 Conduct of Evaluation.....	7
1.4 Certification .....	7
1.5 Overview of Report .....	8
1.5.1 PP Conformance.....	8
1.5.2 EAL .....	8
1.5.3 SOF .....	8
1.5.4 Security Functions.....	8
1.5.5 Threat.....	12
1.5.6 Organisational Security Policy .....	12
1.5.7 Configuration Requirements .....	12
1.5.8 Assumptions for Operational Environment .....	13
1.5.9 Documents Attached to Product .....	13
2. Conduct and Results of Evaluation by Evaluation Facility.....	14
2.1 Evaluation Methods .....	14
2.2 Overview of Evaluation Conducted .....	14
2.3 Product Testing .....	14
2.3.1 Developer Testing.....	14
2.3.2 Evaluator Testing.....	17
2.4 Evaluation Result .....	18
3. Conduct of Certification .....	19
4. Conclusion.....	20
4.1 Certification Result.....	20
4.2 Recommendations.....	20
5. Glossary .....	21
6. Bibliography .....	24

## 1. Executive Summary

### 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "PP-100N Security control unit" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, SEIKO EPSON CORPORATION.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

### 1.2 Evaluated Product

#### 1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product: PP-100N Security control unit  
Version: 1.00  
Developer: SEIKO EPSON CORPORATION

#### 1.2.2 Product Overview

The TOE is a security control unit that consists of software and hardware, and provided as a security package for PP-100N. The PP-100N is a disc publisher which writes electronic information acquired over a network on discs such as CD-Rs or DVD-Rs and prints images on the discs.

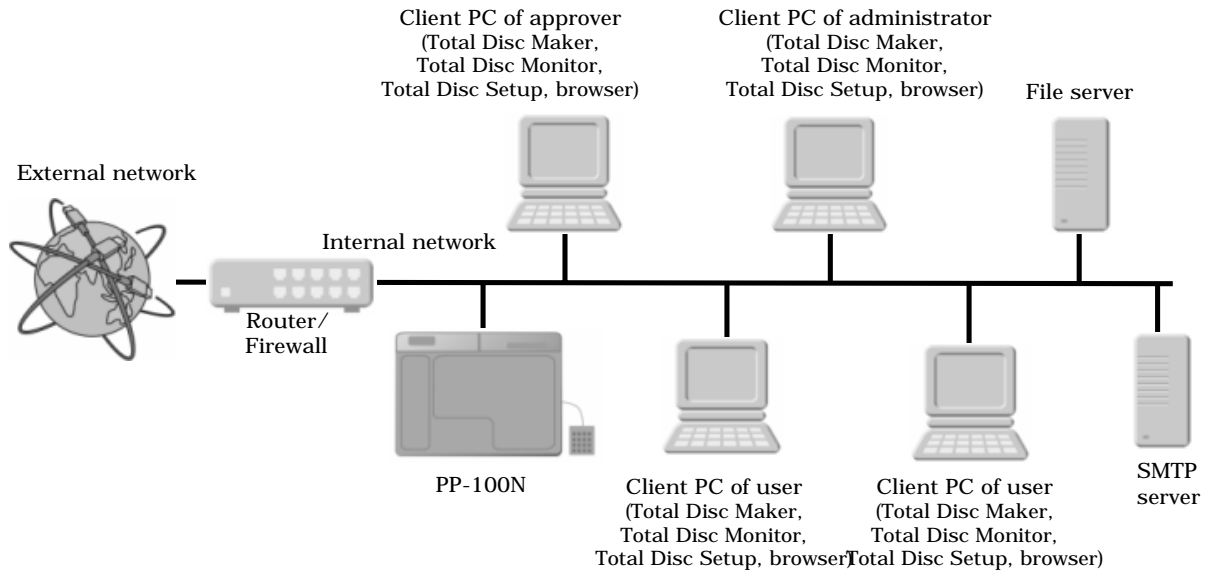
The TOE provides the following security functions in order to prevent published discs from being taken out by anyone except the user who published the discs.

- Identify Authentication function
- Controlled Distribution function
- Electronic Lock Open function
- Warning function
- Setting Data Control function

1.2.3 Scope of TOE and Overview of Operation

(1) TOE Operating Environment

Figure 1-1 shows a typical environment in which this TOE is used, and Table 1-1 lists the parties/persons involved with this TOE.



**Figure 1-1: Typical TOE Environment**

**Table 1-1: Parties involved with TOE Environment**

Responsible of the organization	This person appoints an administrator and approver.
Users	The following persons who are allowed to publish discs using PP-100N. In other words, a collective term for the administrator, approver, and the person in charge of publishing discs.
Administrator	A person who manages the usage of PP-100N. Reliable person who never tries malicious attempts.
Approver	A person authorized to approve disc publishing application submitted by persons in charge of the job. Reliable person who never tries malicious attempts.
Publisher (person in charge of publishing discs)	A person only authorized to publish discs. There is a possibility that the person will try malicious attempts against TOE operations.
Service person	SEIKO EPSON company member, overseas subsidiary company member, or service contractor member who takes charge in repairing and maintaining PP-100N. There is a possibility that the service person will try malicious attempts against TOE operations.
Third party	Any persons other than above. There is a possibility that the person will try malicious attempts against TOE operations.

As shown in Figure 1-1, PP-100N with TOE is assumed to be connected to the internal network protected by a firewall or other security device/software against unauthorized access from external network. The system elements other than the TOE are the client PCs (for administrators, approvers and publishers), file server where disc images files are stored, network related server (SMTP server in Figure 1-1) which is placed depending on the operational environment of the internal network. On each client PC, special applications, such as Total Disc Maker, supplied with PP-100N are installed for operating/monitoring the TOE. The PP-100N user should purchase the security pack sold separately, and using an activation key included in the pack, activate TOE security function (set PP-100N to security mode).

The following explains the overview of PP-100N disc publishing process. The process consists of two phases, the first one is "publishing discs" (from the user starts publishing the discs until the discs are published and stored in PP-100N), and the second one is "taking out the discs" (the user takes out the discs from PP-100N).

## [Publishing discs]

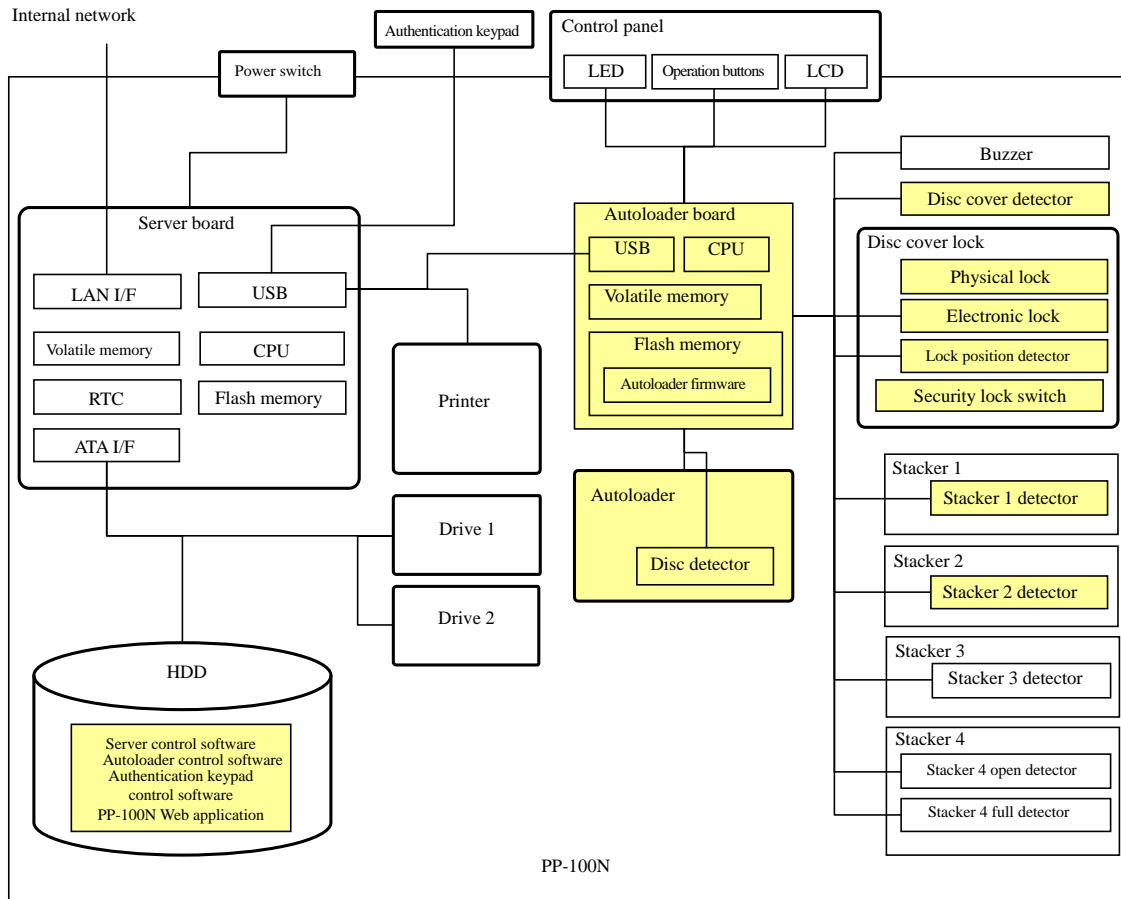
- The user creates a disc image file and label data file using the application (Total Disc Maker) on the client PC
- The user starts publishing the discs using the application (Total Disc Maker) on the client PC. The disc image files and label data files are sent to PP-100N and stored as spool data on PP-100N hard disc drive.  
(When the disc publishing process is started, the TOE creates the new job information and starts to manage the job.)
- A request for disc publishing approval is sent from the user to the approver, and the approver permits PP-100N to process the disc publishing job from the approver's client PC.
- PP-100N performs the disc publishing process (writing the disc image file, label printing), and stores the published discs in Stacker 2 that is predetermined to be used for storing published discs.

## [Taking out the discs]

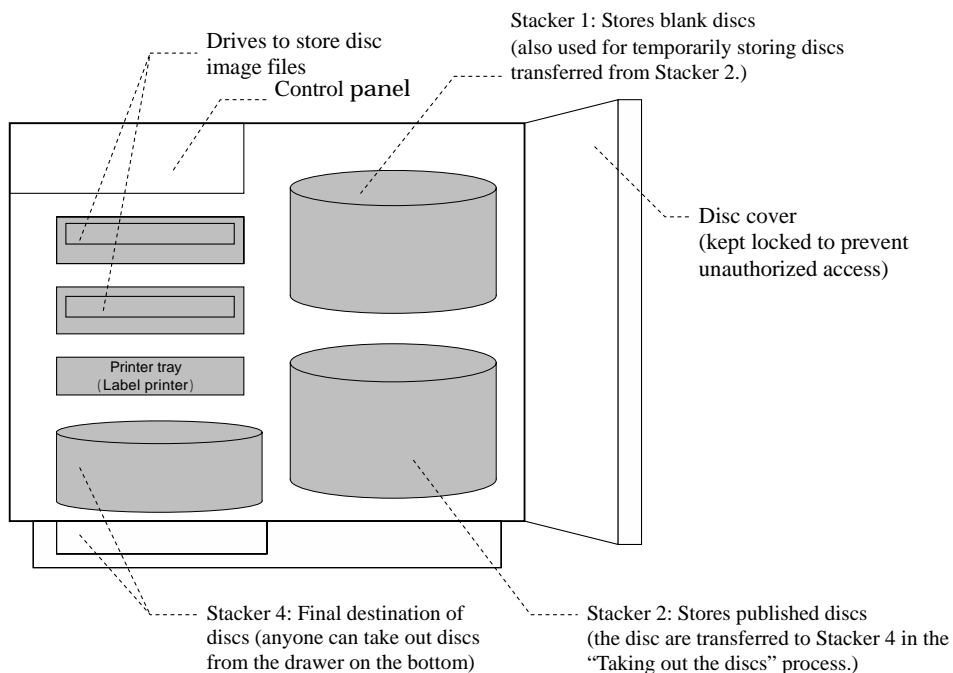
- The user who published the discs starts to operate PP-100N control panel to take out the discs, and enters his/her user identifier and password.
- After the identify authentication is successfully completed, the published discs are transferred from Stacker 2 to Stacker 4 by the autoloader.  
(When more than one disc exists, which are published by the authenticated user, all the discs are transferred to Stacker 4, however, if there is a disc which needs to be stored separately and temporarily, the disc is stored in Stacker 1.)
- The user opens Stacker 4 to take out the discs.  
(Only the discs in Stacker 4 can be taken out.)

## (2) TOE Configuration and Operation Overview

Figure 1-2 shows PP-100N internal configuration block diagram, and Figure 1-3 shows PP-100N internal image. The yellow boxes in Figure 1-2 indicate the components included in this TOE, and the components are listed in Table 1-2.



**Figure 1-2: PP-100N Internal Configuration (TOE is in yellow boxes)**



**Figure 1-3: PP-100N Internal Image**

**Table 1-2: TOE Components List**

Autoloader board	A board consists of CPU for hardware control, flash memory and such, and controls TOE hardware.
Autoloader	A robotic arm that moves being controlled by the autoloader board to transfer each disc to a requested location (Stacker 1, Stacker 2, Stacker 4, printer tray or drive).
Disc detector	A detector to detect whether the autoloader is holding a disc or not. This is also used to check the remaining discs in Stacker 1 and 2.
Disc cover detector	A detector to detect opening/closing status of the disc cover.
Physical lock	A disc cover lock which can be opened using a physical key. The key is kept safely by the administrator.
Electronic lock	A disc cover lock which can be deactivated electronically by the software control.
Lock position detector	A detector to detect opening/closing of the disc cover lock and on/off of the security lock switch.
Security lock switch	A switch to turn the disc cover lock function on or off. The disc cover is kept unlocked all the time when the switch is off, therefore, it is kept on in this TOE operation.
Stacker 1 detector	A detector to detect removing/reattaching status of a stacker from/to Stacker 1.
Stacker 2 detector	A detector to detect removing/reattaching status of a stacker from/to Stacker 2.
PP-100N Web application	Application to communicate with the client PC.
Autoloader control software	Library and firmware to control the autoloader.
Server control software	Software to make total control over PP-100N. It is embedded in the server board and runs under OS embedded in the board.
Authentication keypad control software	Library to control the authentication keypad.

As shown in Figure 1-2 and Table 1-2, TOE consists of hardware and software. In addition to the TOE, as indicated in Figure 1-3, PP-100N consists of disc cover, drives to write disc image files, label printer and printer tray, stackers to store the discs (Stacker 1, Stacker 2 and Stacker 4. Stacker 3 is not used), control panel, other hardware such as the control boards, OS, database, software to control the hardware.

This TOE handles the published discs as assets and the security function prevents the discs from being taken out by unauthorized persons. The assets, "published discs", are protected from when writing disc image file and printing label image are finished (then the discs are transferred to Stacker 2) until the discs are ejected to Stacker 4. (The TOE security function does not protect disc image files temporarily stored as a spool data on the internal hard disc drive.)

#### 1.2.4 TOE Functionality

The main purpose of this TOE is to provide security functions to protect discs published by the product (hereinafter called "PP-100N") on which the TOE is installed. The security functions prevent the published discs from being taken out by anyone except the user who published the discs. Refer to "1.5.4 Security Functions" for the details of the security functions.

#### 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "SEIKO EPSON PP-100N Security control unit Security Target" as the basic design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "PP-100N Security control unit Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

#### 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification

review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2009-07 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

## 1.5 Overview of Report

### 1.5.1 PP Conformance

There is no PP to be conformed.

### 1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

### 1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.

This TOE is designed under the premise that PP-100N is used in a general office environment which is not subjected to unauthorized access from external networks. Under the supervision of the administrator, there is really very little chance that someone attempts complicated attacks to the TOE by directly accessing the TOE or through the internal network. Therefore, assuming the attack level is "low level" is reasonable, and "SOF-basic" that is strong enough against the low level attacks is sufficient as the minimum strength of function.

### 1.5.4 Security Functions

Security functions of the TOE are as follows:

#### (1) Controlled Distribution function

This function provides access control so that published discs cannot be taken out by anyone other than the user who created discs. The access control is performed as follows.

- This function is started by the request from the user to take out the discs (the user presses the EJECT button on the PP-100N control panel).
- The TOE activates the Identify Authentication [Panel] function to identify the user. (The process is terminated if the authentication fails.)
- The TOE searches the job information associated with the authenticated user identifier [Panel], and when it finds that the discs published by the user exist in PP-100N, the TOE checks the disc position using the job information and the disc position information. (If the job information is not found, this function is terminated.)
- The TOE moves the autoloader to transfer the discs from Stacker 2 to Stacker 4. (If any other discs exist on the target discs, the non-target discs are temporary transferred to Stacker 1.)
- The disc position information controlled by TOE is updated to "discs taken-out" status.

#### (2) Electronic Lock Open function

This function controls on/off of the electronic lock so that only the administrator is allowed to open the disc cover.

- The administrator selects the menu for deactivating the electronic lock on the control panel of PP-100N.
- The TOE activates the Identify Authentication [Panel] function to identify the user.
- If the user is identified as the administrator, the TOE deactivates the electronic lock.
- If the disc cover is not opened within a predetermined time period (5 seconds or longer) after the lock is deactivated, the TOE activates the electronic lock.

### (3) Identify Authentication function

This function allows to identify and authenticate TOE users. According to the interface, the following three functions are provided; Identify Authentication [Web\_app] function, Identify Authentication [Cli\_app] function and Identify Authentication [Panel] function.

#### [Identify Authentication [Web\_app] function]

- This function identifies and authenticates the user who accesses to various setting functions provided by TOE (refer to "(5) Setting Data Control function for the details) via a browser.
- When the PP-100N Web application is started, a user identify authentication screen is displayed. The user is required to enter his/her user identifier [Appli] and password [Appli].
- The TOE compares the entered user identifier [Appli] and password [Appli] with registered user information, and determines that the user is authenticated when a match is detected. If no match is found, the TOE prompts the user to reenter the identification [Appli] and password [Appli].
- When the TOE failed the user identify authentication three times in a row during a given time, the TOE locks the user account to prevent the user from logging in using the PP-100N Web application. The TOE automatically unlocks the user account after six hours for an administrator, and after one hour for the other users.

#### [Identify Authentication [Cli\_app] function]

- This function identifies an authorized user who accesses to the TOE using the Total Disc Maker or Total Disc Monitor.
- When the TOE detects an access from Total Disc Maker or Total Disc Monitor, a user identify authentication screen is displayed. The user is required to enter his/her user identifier [Appli] and password [Appli].
- The TOE compares the entered user identifier [Appli] and password [Appli] with registered user information, and determines that the user is authenticated when a match is detected. If no match is found, the TOE prompts the user to reenter the identification [Appli] and password [Appli].
- When the TOE failed the user identify authentication three times in a row during a given time, the TOE locks the user account to prevent the user from logging in using Total Disc Maker or Total Disc Monitor. The TOE automatically unlocks the user account after six hours for an administrator, and after one hour for the other users.

#### [Identify Authentication [Panel] function]

- This function identifies an authorized user who accesses to the TOE using the control panel of PP-100N.
- This function is activated when a user is operating the control panel and the user identity authentication is required.
- A screen to enter the user identifier [Panel] and password [Panel] is displayed. The user is required to enter his/her user identifier [Panel] and password [Panel].
- The TOE compares the entered user identifier [Panel] and password [Panel] with registered user information, and determines that the user is authenticated when a match is detected. If no match is found, the TOE prompts the user to reenter the identification [Panel] and password [Panel].
- When the TOE failed the user identify authentication three times in a row during a

given time, the TOE locks the user account to prevent the user from logging in using the control panel. The TOE automatically unlocks the user account after six hours for an administrator, and after one hour for the other users.

- The TOE makes the LCD to display the same number of "\*" (asterisks) as the entered characters.

#### (4) Warning function

This function warns the administrator of security problems using the following methods.

- Sounds a buzzer
- Turns on the ERROR LED
- Displays a solution on the LCD

In the following cases, there is a high possibility that a security problem is arising.

##### (a) When turning off the power

The following status is found in job information during the power-off process.

- Published discs exist in Stacker 2
- Processing jobs exist

When either one of the above is detected, the TOE stops the power-off process and warns the administrator of security problems.

##### (b) When the disc cover is open

When the TOE detects that the cover is kept open for 60 seconds, the TOE warns the administrator of security problems.

##### (c) When the disc cover is closed

If the status below is continued for more than 10 seconds when the disc cover is closed, the TOE warns the administrator of security problems.

- The cover is not physically locked
- The security lock switch is off

##### (d) When feeding discs

Alerts the administrator that the autoloader drops a disc during its disc feeding operation.

##### (e) When removing Stacker 2

When the Stacker 2, where the published discs are stored, is removed and reattached, the TOE checks the presence or absence of discs in Stacker 2 and alerts the administrator if any disc presents. (This is to prevent mismatch between actual disc position and the disc position information managed by the TOE. The mismatch, which will cause incorrect disc ejection control, can occur if the user, for example, puts wrong discs in Stacker 2 before reattaching it.)

#### (5) Setting Data Control function

This function provides access control over the TSF data such as setting information and job information so that each user is allowed to access or operate the data within his/her authority predetermined by user type (administrator, approver or publisher). Prior to the access to the TSF data, user authentication by Identify Authentication [Web\_app] is performed when the user connects to the TOE using the browser on the client PC. The user authority by user type (user role) is fixed and cannot be changed. The following table lists the available user operations by user type (role). (listing only operations aiming at direct access to TSF data.)

**Table 1-3: Available User Operations by User Role**

Role	TSF data	Available user operations
Administrator	User information	Viewing, adding, deleting, and changing user information
	Setting information	Changing security mode status Viewing and changing time setting information Viewing and changing network setting information
	Job information	Viewing, deleting, and changing job information
Approver	User information	Changing the user's password
Publisher	User information	Changing the user's password

The TSF data (user information, job information) in Table 1-3 mainly consists of the following.

**[User information]**

User identifier [Appli], password [Appli]: User identifier and password to use for identify authentication activated from the client application and such.

User identifier [Panel], password [Panel]: User identifier and password to use for identify authentication activated from the control panel of PP-100N.

Privilege: User role (administrator, approver, publisher).

**[Job information]**

Job ID: Identifier for each job

User identifier: User identifier associated with the job

Status: Current job status information

Disc position information: Disc position in stackers for each job

## 1.5.5 Threat

This TOE assumes such threats presented in Table 1-4 and provides functions for countermeasure to them.

**Table 1-4 Assumed Threats**

Identifier	Threat
T.Taking out of discs	Anyone except the user who published the discs may pretend to be the user or the administrator, and take out published discs and leak the disc data.
T.Disc cover unlocked	When the disc cover is unlocked by the mistake of the administrator, anyone except the user who published the discs may take out the discs and leak the disc data.
T.Dropping of discs	When the autoloader drops published discs during transferring, the published discs may go into Stacker 4. In such case, anyone except the user who published the discs may take out the discs and leak the disc data.
T.Misplacement of discs	When published discs are ejected due to the disc misplacement to Stacker 2 by the administrator or the service person, anyone except the user who published the discs may take out the discs and leak the disc data.  * The matter of concern is that PP-100N is controlled to eject incorrect discs due to a mismatch between actual discs stored in Stacker 2 and the disc position information managed by the TOE.

## 1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-5.

**Table 1-5 Organisational Security Policy**

Identifier	Organisational Security Policy
P.Published discs	PP-100N is not stopped with published discs remained inside it.

## 1.5.7 Configuration Requirements

The client PC on which the following browser can activate is necessary for the TOE operations. The client applications (Total Disc Maker, Total Disc Monitor) must be installed to the client PC.

Browser (one of the following):

Microsoft Internet Explorer 6

Microsoft Internet Explorer 7

## 1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-6. The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 1-6 Assumptions in Use of the TOE

Identifier	Assumptions
A.Approver	An approver is a reliable person who never tries malicious attempts against TOE operations.
A.Administrator	An administrator is a reliable person who never tries malicious attempts against TOE operations.
A.Password	The user password is not leaked to anyone except the user. The password is not easily guessed and must be changed on a regular basis.
A.Operation status management	The administrator monitors the PP-100N's operation status to prevent the followings from occurring. <ul style="list-style-type: none"> <li>- Destroying PP-100N</li> <li>- Unlocking of the disc cover by anyone except the administrator</li> </ul>
A.Security mode	The administrator connects the authentication keypad to PP-100N included in the security pack, and makes security mode setup for the PP-100N.
A.Network	The network environment satisfies the following requirements. <ul style="list-style-type: none"> <li>- TOE is not subjected to attacks from external networks.</li> <li>- The internal network where the TOE devices are connected is protected from being bugged.</li> </ul>

## 1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

Document name	Identifier
PP-100N Security Administrator's Guide	M00012700
PP-100N Security User's Guide	M00012000

## 2. Conduct and Results of Evaluation by Evaluation Facility

### 2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

### 2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on 2007-08 and concluded by completion the Evaluation Technical Report dated 2009-07. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2009-01, 2009-03, and 2009-06 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-04.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification reviews were sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

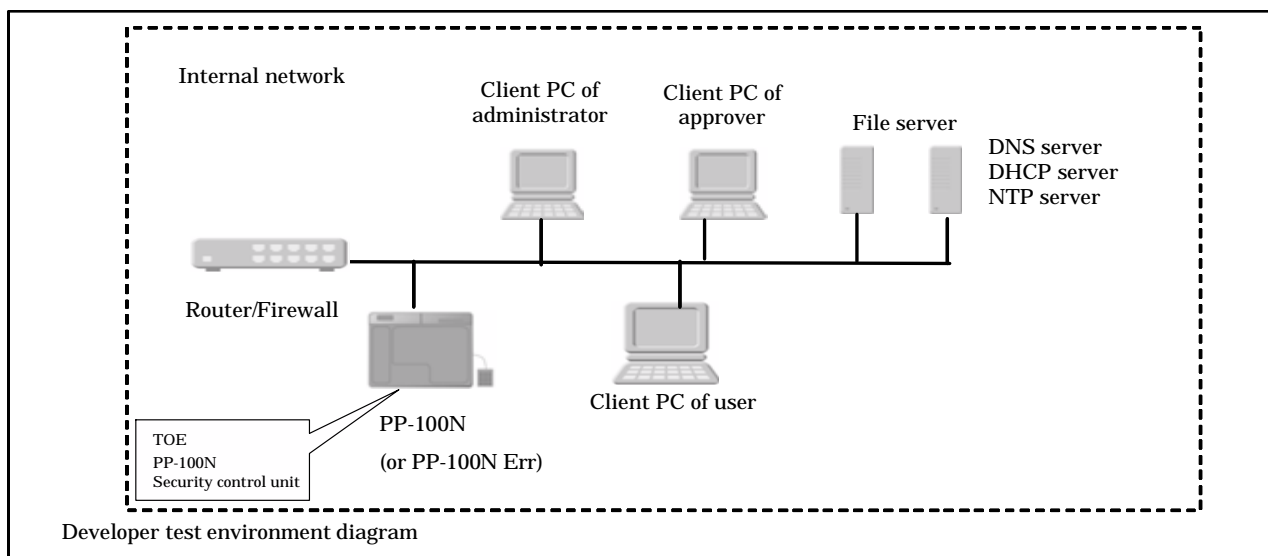
### 2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

#### 2.3.1 Developer Testing

##### 1) Developer Test Environment

Test configuration performed by the developer is shown in the Figure 2-1.



**Figure 2-1: Developer Test Configuration Diagram**

**Table 2-1: Developer Test Configuration**

Component	Description
PP-100N	PP-100N on which TOE as a security control unit is installed. TOE version: 1.00
PP-100N_Err	PP-100N specially modified for error test (with the disc cover removed). TOE version: 1.00
Client PC	Client PCs for administrator, approver, and user. The client application such as Total Disc Maker and the following OS and browser are installed. OS: Windows XP Professional SP3 Windows Vista Ultimate SP1 Browser: Internet Explorer6,7
File server	A server machine on which disc image files are stored. This server is prepared as necessary. Under this test environment, a PC with the following OS is used as the file server. OS: Windows Server 2003

DNS server DHCP server NTP server	The servers which are installed depending on the network environment. Under this test environment, a PC with the following OS is used as the server.  OS:  Windows Server 2003
Router/Firewall	A router/firewall for communication control of internal network. The test environment is not connected to external network, therefore, the firewall function is not used.

## 2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follows:

### a. Test configuration

As indicated in Figure 2-1 and Table 2-1, the developer testing was performed in the same environment as the TOE environment whose components are identified by the ST.

### b. Testing Approach

For the testing, the following approach was used.

Operate the user interface (control panel, client applications) which are used for actual operation, and check the following security function behavior.

- Ejection of published discs created by TOE, physical operation such as disc cover lock operation
- Operation of operation screens (LCD on the PP-100N, display on the client PC), and message displays
- Error notification by buzzer, the ERROR LED, and error messages

Using PP-100N specially modified for the test (the disc cover is removed, so called PP-100N\_Err in the list), check the following security function behavior when a direct access to inside the PP-100N is performed (such as holding the autoloader by hand when the autoloader is moving, knocking the discs off the autoloader when the autoloader transferring the discs).

- Operation of operation screens (LCD on the PP-100N, display on the client PC), and message displays
- Error notification by buzzer, the ERROR LED, and error messages

### c. Scope of Testing Performed

Testing was performed on 1,071 items by the developer. Each item is further classified by normal operations, abnormal operations, or parameters. The coverage analysis on the test items has verified that all the security functions and external interfaces described in the functional specification were fully tested. And by depth analysis, it has also verified that all the subsystems and subsystem interfaces described in the higher-level design were fully checked.

d. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The evaluator confirmed that the developer testing approach and tested items were legitimate and that the approach and results of actual tests matched those described in the test plan.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Tables 2-2 and Figure 2-2 describe the configurations used for testing by the evaluator. (Table 2-2 shows only the items different from the developer test.).

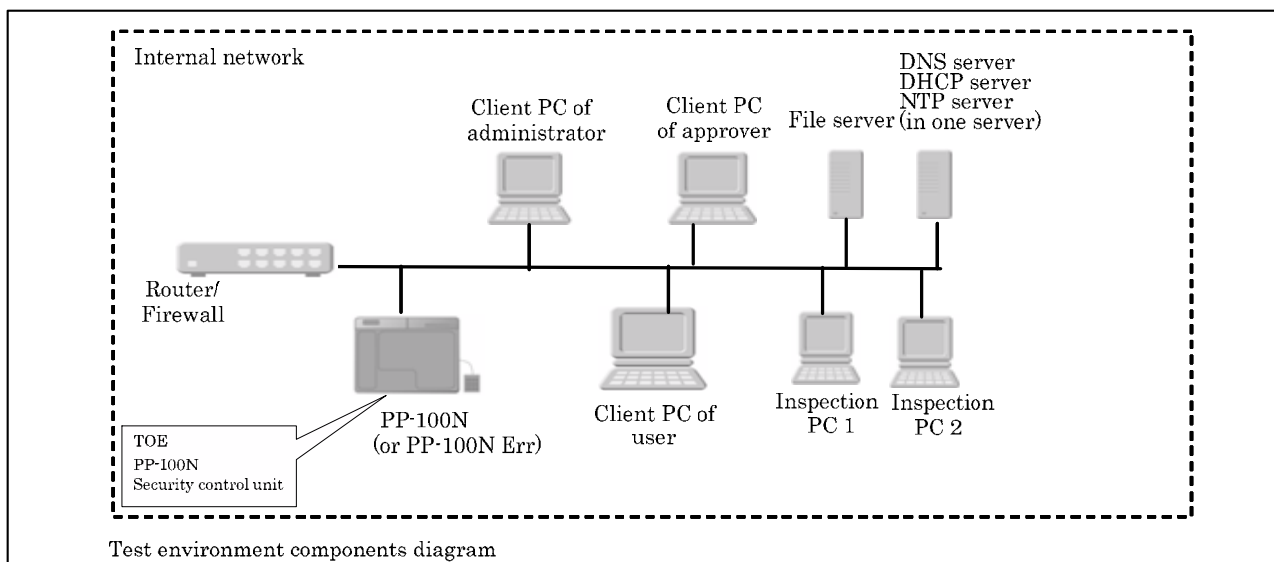


Figure 2-2: Evaluator Test Configuration Diagram

Table 2-2: Evaluator Test Configuration

Component	Description
Inspection PC 1 Inspection PC 2	Both inspection PCs are Windows XP SP2 computers with network terminal, and used for vulnerability test. The security scanner software and various tools are installed.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follows:

a. Test configuration

As indicated in Figure 2-2 and Table 2-2, the evaluator testing environment is the same as the developer testing environment shown in Figure 2-1 except for the inspection PCs. The inspection PCs are used only for checking packet data

on the network and sending data to the TOE, therefore, it is verified by the evaluator that adding them to the TOE environment does not make any differences from the original TOE environment whose components are identified by the ST.

#### b. Testing Approach

For the testing, the following approach was used.

The same test methods used for the developer test.

Check the security function behavior by directly accessing TSFI from the inspection PC using HTTP or such protocols, and checking the information sent from the TOE by return.

#### c. Scope of Testing Performed

The evaluator performed 321 tests in total: five independent tests, 309 sampling tests of the developer tests, and seven penetration tests. Each item is, in the same way as the developer testing, further classified by normal operations, abnormal operations, or parameters.

The following were considered as the selection criteria of the tests.

All the TOE security functions are covered.

In the developer testing, the followings are considered as the lack of the testing environment.

- Testing on the assumption of simultaneous connection or operation by multiple users
- Use of combinations of various parameters that are assumed operations at power-off or such

Testing for concerns found by the vulnerability analysis

- Availability of bypassing the security function when an unexpected usage of TSFI such as a direct access from other than the client application is attempted.
- Presence or absence of residual vulnerability of the network interface which is in the public domain.
- Influence on the security functions exerted by a hardware failure or any other physical failure.

#### d. Result

All of the evaluator testing items completed and the evaluator confirmed that all of the test results satisfied the expected behavior. Regarding the influence on the security functions exerted by a failure of hardware included in this TOE, the developer analyzed failure rate and serviceable life of the hardware, and concluded that normal operation of the product can be guaranteed during its product lifetime, and the evaluator confirmed the validity of the conclusion.

### 2.4 Evaluation Result

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

### 3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification reviews, which were sent to evaluation facility.

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

## 4. Conclusion

### 4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

### 4.2 Recommendations

In order to ensure the security provided by the TOE security functions (especially, the warning function), the administrator should always monitor the TOE and quickly deal with errors notified by the TOE. Note that the security cannot be ensured unless the administrator plays the role correctly.

## 5. Glossary

The abbreviations 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
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The glossaries used in this report are listed below.

JOB:	A disc publishing work unit of PP-100N.
LCD:	A display to show operation menu or warning messages.
LED:	A light-emitting diode to show the status of PP-100N as follows. <ul style="list-style-type: none"> <li>- POWER LED: shows power on/off, and printer cleaning status</li> <li>- BUSY LED: shows that disc publication (burning/printing) is in progress</li> <li>- ERROR LED: lights when an error occurs</li> </ul>
Total Disc Maker:	An application that is installed on a client PC. This allows the user to select files to be written to discs and to create label print data.
Total Disc Monitor:	An application that is installed on a client PC. This allows the user to check a job status, pause/resume a job, and cancel a job.
Published disc:	A disc to/on which electronic information has been written and an image has been printed.
Stacker:	A container that stacks discs to store them.
Stacker 1:	A detachable stacker for loading blank discs. In Security Mode, this is used to temporarily store discs.

Stacker 2:	A detachable stacker to store published discs.
Stacker 3:	An extra stacker to store published discs. Used when Stacker 2 becomes full. Mounted on Stacker 4. This is not used in Security Mode.
Stacker 4:	A stacker to store published discs that should be ejected by the pre-approved user. The user can take out the discs in Stacker 4 by opening the drawer on the bottom of PP-100N.
Spool data:	Disc image files or label data files temporarily stored on the hard disc of PP-100N until they are recorded or printed on discs.
Security mode:	<p>PP-100N offers two modes; Security mode and non-security mode. In the Security mode, the following functions indispensable for the security work.</p> <ul style="list-style-type: none"> <li>- Identify Authentication function</li> <li>- Controlled Distribution function</li> <li>- Electronic Lock Open function</li> <li>- Warning function</li> <li>- Setting Data Control function</li> </ul> <p>This ST describes the specifications of the Security mode.</p>
Control panel:	User interface consists of LCD, LED, and operation buttons.
Disc:	Disc-shaped storage medium such as a CD-R and DVD-R.
Disc image file:	A data file to be recorded on the recording surface of the disc.
Disc cover:	<p>A cover on the front of PP-100N. Usually, it is locked physically or electronically by the disc cover lock and can be opened by deactivating the lock. When it opens, the user can access the following.</p> <ul style="list-style-type: none"> <li>- Stacker 1</li> <li>- Stacker 2</li> <li>- Drive</li> <li>- Printer</li> <li>- Security lock switch</li> </ul> <p>(A switch to turn the disc cover lock function on or off.)</p>
Disc cover lock:	A lock for the disc cover. There are two types of lock; electronic key that can be activated/deactivated using software and physical key. Using either one of the two, the disc cover can be opened. The disc cover is automatically locked as soon as it is closed.
Drive:	A disc drive to write a disc image file on the recording

surface of a disc. PP-100N is equipped with two disc drives.

Security pack:	These are needed to use PP-100N in the Security mode. <ul style="list-style-type: none"><li>- PP-100N Security Administrator's Guide</li><li>- PP-100N Security User's Guide</li><li>- PP-100N security activation key sheet</li></ul>
Authentication keypad:	A USB keypad used for identity authentication to operate PP-100N. This keypad is an optional and not included in the PP-100N kit, but necessary to operate TOE. This should be prepared and connected to PP-100N by the administrator.
Buzzer:	A device to notify the user with sounds in the event of a PP-100N failure.
Blank disc:	A disc that stores no data.
Printer:	An apparatus to print images on the label surface of discs.
Printer tray:	A tray to put a disc to print on its label surface.
Label data file:	A print data file to be printed on the label surface of the disc.

## 6. Bibliography

- [1] SEIKO EPSON PP-100N Security control unit Security Target Version 2.0 (July 3,2009) SEIKO EPSON CORPORATION
- [2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01
- [3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02
- [4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03
- [5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001
- [6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002
- [7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003
- [8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)
- [9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)
- [10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)
- [11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- [12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- [14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004
- [15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)
- [16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

- [17] PP-100N Evaluation Technical Report Version 1.0, July 9, 2009,  
Mizuho Information & Research Institute, Inc. Center for Evaluation of  
Information Security