



Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-04-17 (ITC-7146)
Certification No.	C0177
Sponsor	SEIKO EPSON CORPORATION
Name of TOE	Japanese name: EpsonNet ID Print Authentication Print Module English name: EpsonNet ID Print Authentication Print Module
Version of TOE	Japanese version: 1.5b English version: 1.5bE
PP Conformance	None
Conformed Claim	EAL2
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.

2008-08-12

Hideji Suzuki, 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

"Japanese name: EpsonNet ID Print Authentication Print Module, version: 1.5b, English name: EpsonNet ID Print Authentication Print Module, version: 1.5bE" 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.....	9
1.3 Conduct of Evaluation.....	11
1.4 Certification	12
1.5 Overview of Report	12
1.5.1 PP Conformance.....	12
1.5.2 EAL	12
1.5.3 SOF	12
1.5.4 Security Functions.....	13
1.5.5 Threat.....	13
1.5.6 Organizational Security Policy.....	13
1.5.7 Configuration Requirements	13
1.5.8 Assumptions for Operational Environment	15
1.5.9 Documents Attached to Product	16
2. Conduct and Results of Evaluation by Evaluation Facility.....	17
2.1 Evaluation Methods	17
2.2 Overview of Evaluation Conducted	17
2.3 Product Testing	17
2.3.1 Developer Testing.....	17
2.3.2 Evaluator Testing.....	19
2.4 Evaluation Result	25
3. Conduct of Certification	26
4. Conclusion.....	27
4.1 Certification Result.....	27
4.2 Recommendations.....	27
5. Glossary	28
6. Bibliography	35

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Japanese name: EpsonNet ID Print Authentication Print Module, version: 1.5b, English name: EpsonNet ID Print Authentication Print Module , version: 1.5bE" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security.

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:	Japanese name: EpsonNet ID Print Authentication Print Module
	English name: EpsonNet ID Print Authentication Print Module
Version:	Japanese version: 1.5b
	English version:1.5bE
Developer:	SEIKO EPSON CORPORATION

1.2.2 Product Overview

This product is a software product that runs on the Java VM, and consists of an accessory application software that runs on the authentication print module Offirio SynergyWare ID Print (worldwide name: EpsonNet Authentication Print) implemented on optional network interface cards with authentication printing function for Seiko Epson printers and multifunction printers (hereinafter collectively referred to as "printers") and on computers that process print requests.

This TOE provides functions to receive print jobs with user ID information and the like corresponding to print data submitted by client PC users for printing, hold them temporarily, and output as prints (hereinafter referred to as "authentication printing") after authenticating the print owner by using an authentication device connected to the network interface card of the printer. This TOE provides the following security functions.

- User identification

- Print-job management
- Printer settings
- Settings management

The following functions are included in this TOE but are not target of the evaluation.

- User identification and authentication at startup of the system configuration tool

1.2.3 Scope of TOE and Overview of Operation

1.2.3.1 Scope of TOE and Operating Environment

This TOE is an accessory application software that runs on the authentication print module Offirio SynergyWare ID Print (worldwide name: EpsonNet Authentication Print) implemented on network cards with authentication printing function and on computers that process print requests, and is made up of three parts, the authentication printing software, the spooler software, and the system configuration tool.

This TOE can be configured in two ways, for printing via a server or for direct printing depending on where the print jobs are held temporarily.

When printing via a server, a server (authentication printing server) is installed to temporarily hold the print jobs created from print requests from client PC users. All print jobs are held on this server, which transfers the print jobs in accordance with the output requests from the printer.

In direct printing, the print jobs created from print requests from client PC users are temporarily held on each client PC, which transfers the print jobs in accordance with the output requests from the printer.

Figure 1-1 shows an overview of the operating environment and Figure 1-2 shows the physical scope for this TOE when printing via a server while Figure 1-3 shows an overview of the operating environment and Figure 1-4 shows the physical scope for this TOE in direct printing.

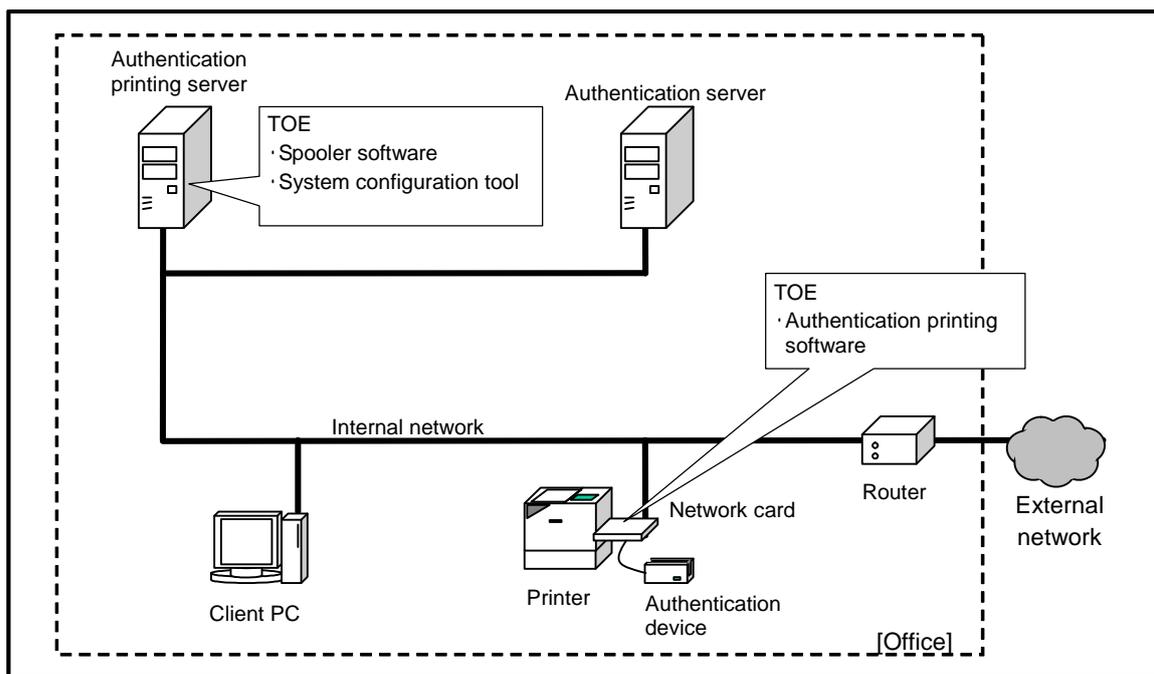


Figure 1-1 Overview of the operating environment of the TOE (printing via a server)

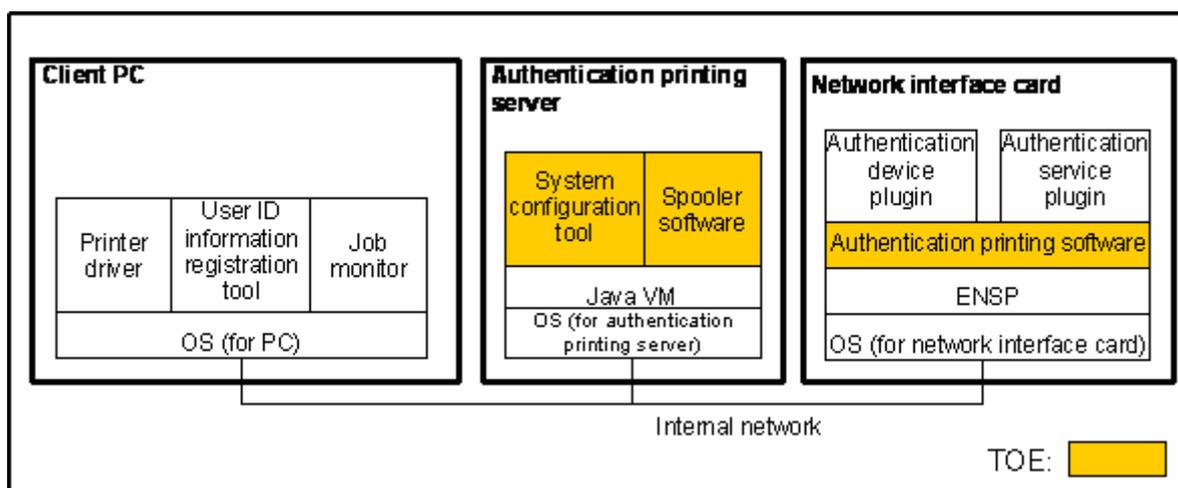


Figure 1-2 Physical scope of the TOE (printing via a server)

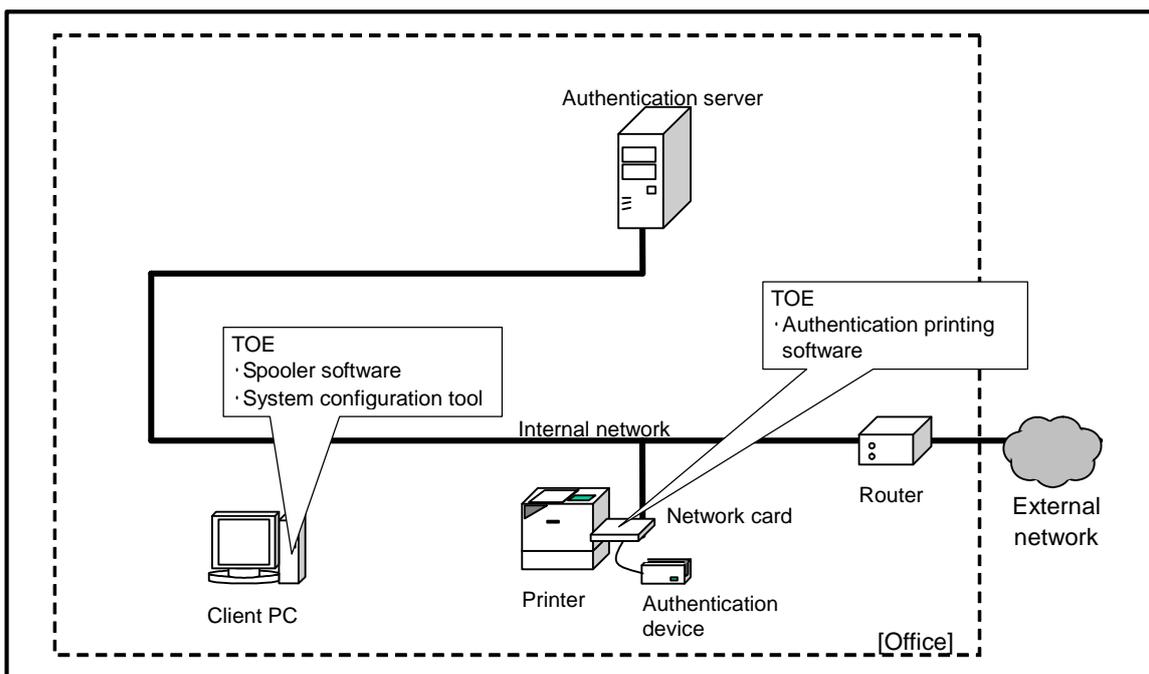


Figure 1-3 Overview of the operating environment of the TOE (direct printing)

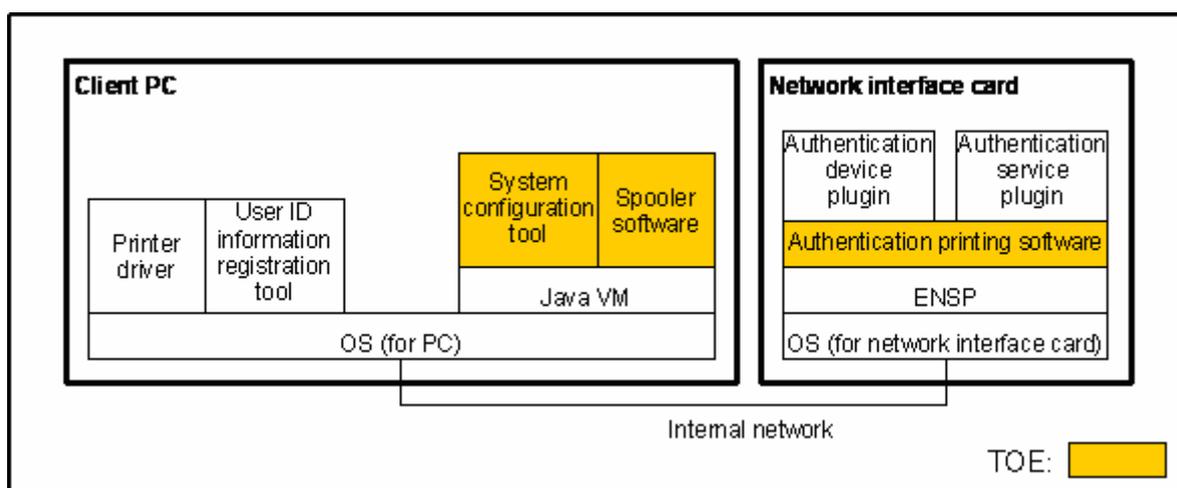


Figure 1-4 Physical scope of the TOE (direct printing)

The roles of each component involved in the operation of this TOE are as follows.

[Client PC] (Installation location of the TOE when direct printing is used)

A computer used by a user for work.

A user submits requests for authentication printing from this computer. Furthermore, a number of application software (printer driver, user ID information registration tool, and job monitor for printing via a server; printer driver, user ID registration tool, and Java VM for direct printing) necessary for using authentication printing are installed on this computer. In direct printing, the spooler software and system configuration tool which are parts of this TOE are installed on this computer to hold print jobs temporarily. When a user submits an authentication printing request, a print job with the user ID information and the like is created from the print data and sent to the spooler software.

There may be one or more client PCs. However, when printing via a server, the maximum number of client PCs that can be connected to one authentication printing server is 50.

[User ID information registration tool] (Outside the scope of the TOE)
Configures and registers user ID information to be added to print jobs.

[Printer driver] (Outside the scope of the TOE)
A driver for creating print jobs and controlling a printer.
Creates print jobs by adding user ID information and printing method information to print data submitted by users, and sends them to the spooler software.
The driver to use must be one corresponding to the used printer.
The printer driver can be installed on the authentication printing server and shared.

[Job monitor] (Outside the scope of the TOE)
An application used by a print owner to delete by him/herself a print job held in the spooler software.
This application is not installed when direct printing is used as print jobs are deleted by using the system configuration tool installed on each client PC.

[Java VM] (Outside the scope of the TOE)
Software for running the spooler software, system configuration tool, and authentication printing software those make up this TOE.

[OS (for computer)] (Outside the scope of the TOE)
Operating system for running the printer driver, user ID information registration tool, and Java VM.

[Authentication printing server] (Installation location of the TOE when printing via a server is used)
A server that holds print jobs created from authentication printing requests submitted by users while they are identified and authenticated.
When printing via a server is used, this computer has the spooler software and system configuration tool which are parts of this TOE installed for holding a number of print jobs temporarily, and the Java VM for running the TOE.
In direct printing, authentication printing server is unnecessary since each client PC serves as authentication printing server.

[Spooler software] (Part of the TOE)
Refers to EpsonNet ID Print Spooler Service.
Holds print job with user ID information and the like and decides whether to send a print job requested by the authentication printing software to the printer or not.

[System configuration tool] (Part of the TOE)
Refers to EpsonNet ID Print System Configuration.
A tool for setting up the authentication printing server and changing the printer setup information.

[OS (for authentication printing server)] (Outside the scope of the TOE)
Operating system for running Java VM on the authentication printing server.

[Network interface card] (Installation location of the TOE)
An optional network interface card with authentication printing function for Seiko Epson printers and multifunction printers. The authentication printing software, which is a component of this TOE, is installed on the network interface card.

[Authentication printing software] (Part of the TOE)

Refers to EpsonNet ID Print AuthBase.

Queries the spooler software whether there is any print job corresponding to a user ID information acquired from the authentication device, and if there is, acquires the corresponding print job(s) and transfers it(them) to the printer. Furthermore, requests the spooler software to delete the corresponding print job(s) when printing finishes.

[ENSP] (Outside the scope of the TOE)

Refers to EpsonNet Service Platform.

A platform for running the authentication printing software. Also includes the Java VM.

[Authentication device plugin] (Outside the scope of the TOE)

A plugin for controlling an authentication device connected to the network interface card.

Processes data entered from the authentication device in accordance with the content of the printer setup information. Where authentication server is not used, the processed data becomes the user ID information. The plugin to use must be one corresponding to the connected authentication device.

[Authentication service plugin] (Outside the scope of the TOE)

Where authentication server is used, a plugin that enables the authentication printing software to communicate with the authentication server and acquire the user ID information.

With data processed by the authentication device plugin, queries the user ID information to the authentication server. The plugin to use must be one corresponding to the used authentication server.

[OS (for network interface card)] (Outside the scope of the TOE)

Operating system for embedded devices for running the various pieces of software implemented on the network interface card.

[Printer] (Outside the scope of the TOE)

A Seiko Epson product to which a network interface card that includes this TOE can be installed.

There may be one or more printers.

[Authentication device] (Outside the scope of the TOE)

A device that connected to a network interface card, identifies and authenticates users. Users are authenticated using an authentication media for magnetic card reader, IC card reader, biometric authentication device, or any other authentication device allocated to each printer for authentication printing. Where appropriate, the authentication server is used to identify the user ID information from the information read from the authentication media.

[Authentication server] (Outside the scope of the TOE)

A server for managing user ID information.

Manages the correspondence between the information read from an authentication media by an authentication device and a user ID information. Authentication server is unnecessary if the user ID information is directly stored in the authentication media read by the authentication device.

[Internal network] (Outside the scope of the TOE)

A network environment separated from external networks by a router and is not subject to attacks from external networks.

[Router] (Outside the scope of the TOE)

A router located between the external and internal networks.

Prevents unauthorized accesses from external networks.

[External network] (Outside the scope of the TOE)

A network environment used by an unspecified number of people such as the Internet.

An environment in which there are people who may perform various malicious acts.

1.2.3.2 TOE Operation Overview

The following describes the way this TOE works together with non-TOE software and the like in the operating environment shown in Figures 1-1 and 1-2 where printing via a server is used, and in the operating environment shown Figures 1-3 and 1-4 where direct printing is used.

[Printing via a server]

- (1) The administrator of this TOE configures the authentication printing server and network interface card using the system configuration tool which is a part of this TOE after authenticating him/herself with a password. Furthermore, the administrator configures the user ID information registration tool, printer driver, and job monitor which are non-TOE software for enabling authentication printing from the client PC.
- (2) Each user submits authentication printing requests from his/her client PC. When a user submits a print request, the print driver in the client PC creates a print job by adding the user ID information that was configured with the user ID information registration tool and the specified printing method to the print data, and sends the print job to the spooler software in the authentication printing server.
- (3) The spooler software in the authentication printing server assigns a job ID to the print job received from the printer driver in the client PC and holds it.
- (4) Each user loads the authentication media he/she has received in advance to the authentication device connected to the network interface card of the printer.
- (5) The network interface card reads the information for identifying the user ID information from the authentication media using the authentication device plugin which is a non-TOE software, and identifies the user ID information in accordance with settings configured in advance. The user ID information can be identified using an authentication server which is outside the scope of the TOE. In that case, the authentication service plugin which is a non-TOE software is used to access the authentication server through the authentication printing software which is a part of the TOE. Thereafter, the authentication printing software in the network interface card sends the identified user ID information to the spooler software in the authentication printing server.
- (6) The spooler software in the authentication printing server sorts out the print jobs with the received user ID information and sends those print jobs to the authentication printing software in the network interface card.
- (7) The authentication printing software in the network interface card sends the received print jobs to the printer that starts printing. For print jobs that finished

printing, the authentication printing software in the network interface card sends requests for deletion to the spooler software in the authentication printing server.

- (8) The spooler software in the authentication printing server deletes the print jobs requested for deletion and completes the sequence of operations.

[Direct printing]

- (1) The administrator of this TOE configures the client PC and network interface card using the system configuration tool which is a part of this TOE after authenticating him/herself with a password. Furthermore, the administrator configures the user ID information registration tool and printer driver which are non-TOE software for enabling authentication printing from the client PC.
- (2) Each user submits authentication printing requests from his/her client PC. When a user submits a print request, the print driver in the client PC creates a print job by adding the user ID information that was configured with the user ID information registration tool and the specified printing method to the print data, and sends the print job to the spooler software in the same client PC.
- (3) The spooler software in the client PC assigns a job ID to the print job received from the printer driver in the client PC and holds it.
- (4) Each user loads the authentication media he/she has received in advance to the authentication device connected to the network interface card of the printer.
- (5) The network interface card reads the information for identifying the user ID information from the authentication media using the authentication device plugin which is a non-TOE software, and identifies the user ID information in accordance with settings configured in advance. The user ID information can be identified using an authentication server which is outside the scope of the TOE. In that case, the authentication service plugin which is a non-TOE software is used to access the authentication server through the authentication printing software which is a part of the TOE.
Thereafter, the authentication printing software in the network interface card sends the identified user ID information to the spooler software in the client PC.
- (6) The spooler software in the client PC sorts out the print jobs with the received user ID information and sends those print jobs to the authentication printing software in the network interface card.
- (7) The authentication printing software in the network interface card sends the received print jobs to the printer that starts printing. For print jobs that finished printing, the authentication printing software in the network interface card sends requests for deletion to the spooler software in the client PC.
- (8) The spooler software in the client PC deletes the print jobs requested for deletion and completes the sequence of operations.

1.2.3.3 User Assumptions

The users and user roles in relation to this TOE are as follows.

[Administrator]

Role: Build the environment of use, configure, and manage the TOE (do installation, initial settings, and settings change according to guidance)

documents).

Privilege: Install, do initial setting, and change settings of the TOE; define the user ID information; configure and operate the authentication server.

Level of trust: Can be trusted.

Knowledge: Has IT and printer knowledge.

[Service staff]

Role: Build the environment of use and configure the TOE (do installation, initial settings, and settings change according to guidance documents) upon request from the administrator.

Privilege: Install, do initial setting, and change settings of the TOE.

Level of trust: Cannot always be trusted. May collect someone else's print by mistake. May perform malicious acts.

Knowledge: Has IT and printer knowledge.

[User]

Role: Use authentication printing implemented with the TOE.

Privilege: Request prints.

Level of trust: Cannot always be trusted. May collect someone else's print by mistake. May perform malicious acts.

Knowledge: Has basic IT knowledge.

[Responsible of the organization]

Role: Appoint administrators.

Privilege: Decide introduction of the TOE.

Level of trust: Can be trusted.

Knowledge: No knowledge level assumed. (IT knowledge not required)

1.2.4 TOE Functionality

Functions included in this TOE can be classified in security functions and non-security functions. Figure 1-5 shows the relationship between the TOE and functions that work together with the TOE. Table 1-1 describes the security functions included in this TOE while Table 1-2 describes the non-security functions included in this TOE (including functions that are not target of the evaluation).

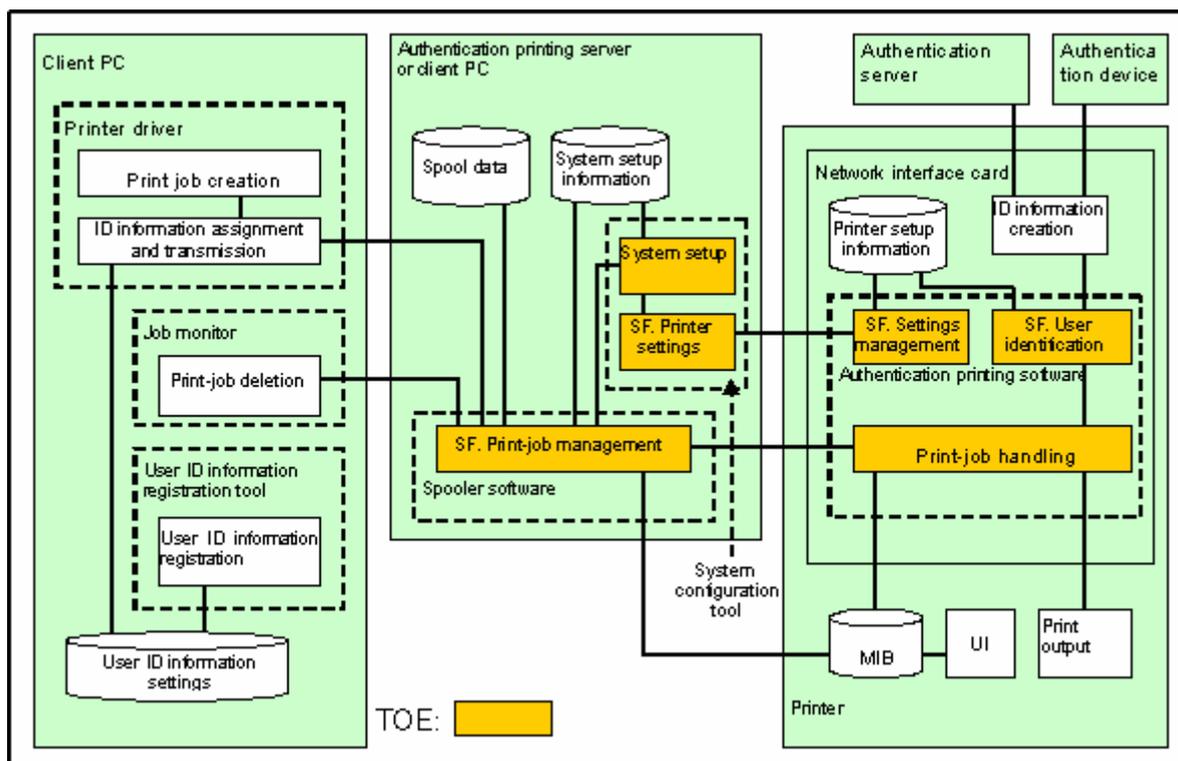


Figure 1-5 Logical scope of the TOE

Table 1-1 Security functions of the TOE

Security function	Overview
User identification (Included in the authentication printing software)	A function that identifies users. <ul style="list-style-type: none"> • Requests creation of user ID information to the ID information creation function which is a non-TOE software in accordance with the authentication device settings and authentication method settings in the printer setup information. • Sends the acquired user ID information to the print-job handling function.
Print-job management (included in the spooler software)	A function that manages spool data. Executes the following operations on the spool data. <ul style="list-style-type: none"> • Assigns job IDs to print jobs with user ID information and the like received from the ID information assignment and transmission function which is a non-TOE software, and holds them as spool data. • Sends the list of job IDs of print jobs with the user ID information specified by the print-job handling function to the print-job handling function. • Transfers the print jobs corresponding to the job ID specified by the print-job handling function to the printer via the print-job handling function.

Printer settings (Included in the system configuration tool)	A function that provides the user interface for accessing the printer setup information. <ul style="list-style-type: none"> • Performs administrator authentication before permitting access to the printer setup information. • Displays the settings screen for changing the printer setup information.
Settings management (Included in the authentication printing software)	A function that manages the printer setup information. <ul style="list-style-type: none"> • Restricts the access to printer setup information to authenticated administrators.

**Table 1-2 Non-security functions of the TOE
(Including functions that are not target of the evaluation)**

Non-security function	Overview
System setup (Included in the system configuration tool)	Performs identification and authentication before the system setup function can be used to configure or change a system setup information. Furthermore, requests deletion of specified print jobs to the print-job management function which is a TOE security function. Invokes the printer settings function which is a TOE security function when the settings of a printer setup information are changed. An identity authentication takes place whenever the system configuration tool is started. However, the function that performs this identity authentication is not a security function.
Print-job handling (Included in the authentication printing software)	Works together with the print-job management function which is a TOE security function to transfer the print jobs of an identified user to the print output function of the printer which is a non-TOE software, and perform the printing.

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 "EpsonNet ID Print Authentication Print Module Security Target Ver1.11" as the basis 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 "EpsonNet ID Print Authentication Print Module 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 2008-07 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 EAL2 conformance.

1.5.3 SOF

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

This TOE is assumed to be used in a general office environment. An office is a space where the number of people entering and leaving the place is limited to those authorized, and the information handled there are classified information of a general company. With regard to the TOE, users, service staff, and third parties are assumed as parties that cannot be trusted. Of these, possible attackers are users and third parties since for service staff, assumption A. Service staff requires the building of an

environment where service staff cannot perform malicious acts. However, attack-ability of users and third parties are of low level. Therefore, SOF-basic is sufficient.

1.5.4 Security Functions

For the security functions of this TOE, see "1.2.4 TOE Functionality".

1.5.5 Threat

This TOE assumes such threats presented in Table 1-3 and provides functions for countermeasure to them.

Table 1-3 Assumed Threats

Identifier	Threat
T. Unauthorized disclosure of prints	A user, a service staff, or a third party other than the print owner wrongfully takes the print data that is output as print and discloses the content without authorization.
T. Tampering of settings	A user, service staff, or third party may disclose print data without authorization by impersonating the administrator and changing the printer setup information.

1.5.6 Organizational Security Policy

There are no organizational security policies required for the use of the TOE.

1.5.7 Configuration Requirements

Of the IT products this TOE needs for operating, Tables 1-4 and 1-5 describe the environment verified in this evaluation.

**Table 1-4 Configuration for printing via a server
(Environment assuming use of English version TOE)**

Printer	AL-C4200 (worldwide printer model, English display)	
Network interface card	Card	C12C824402
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework
Authentication device	pcProx	
Authentication	pcProx card	

media		
Authentication server	Authentication server	LDAP (Active Directory)
	Authentication proxy server	EpsonNet Authentication Server
Authentication printing server	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service
	Java VM	Java SE 6 Update 3
	OS	Windows Server 2003 Enterprise Edition SP2 (32-bit)
Client PC	Printer driver	AL-C4200 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Job monitor	EpsonNet ID Print Job Monitor
	OS	Windows XP Professional SP2 (32-bit)

**Table 1-5 Configuration for direct printing
(Environment assuming use of Japanese version TOE)**

Printer	LP-S6500 (Japanese printer model, kanji display)	
Network interface card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework
Authentication device	PaSoRi and magnetic card reader	
Authentication media	FeliCa card and magnetic card	
Authentication server	Authentication server	LDAP (Active Directory)
	Authentication proxy server	EpsonNet Authentication Proxy for LDAP
Client PC	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service

	Printer driver	LP-S6500 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Java VM	Java SE 6 Update 3
	OS	Windows XP Professional SP2 (32-bit)

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 preconditions are satisfied.

Table 1-6 Assumptions in Use of the TOE

Identifier	Assumptions
A. Administrator	An administrator does not perform malicious acts.
A. Service staff	The administrator shall ensure the service staff does installation, initial settings, or settings change in an environment where he/she cannot perform malicious acts while doing the work.
A. User ID information	The media that contains the user ID information is not available to other users, service staff, or third parties. Furthermore, the user ID information configured in the client PC of a user is not changed fraudulently by other users, service staff, or third parties.
A. Spool data	The spool data is not exposed to unauthorized disclosure by unauthorized access, theft of HDD, or wrongful taking of HDD during a repair.
A. Network	The network environment where the TOE is used satisfies the following requirements. <ul style="list-style-type: none"> • Is not subject to attacks from external networks. • Data flowing through the internal network are not intercepted or tampered. • No network interface cards with authentication printing function outside the control of the administrator are connected. • Where authentication printing server is used, the authentication printing server cannot be spoofed by using the IP address specified by the administrator fraudulently. • Where authentication server is used, the

	authentication server cannot be spoofed by using the IP address specified by the administrator fraudulently.
--	--

1.5.9 Documents Attached to Product

Documents attached to the TOE are as follows.

[Japanese version]

- Offirio SynergyWare ID Print Administrator's Guide, NPD3196-00 (Japanese version only)
- Offirio SynergyWare ID Print User's Guide, NPD3197-00 (Japanese version only)
- PRIFNW7S Readme First, 411139800 (Japanese version only)
- PRIFNW7S/U Setup Guide, 411139701 (Japanese version only)
- Offirio SynergyWare ID Print Updater Application Procedure, NPD3702-00 (Japanese version only)
- PRIFNW7S Firmware Update Procedure, NPD3857-00 (Japanese version only)

[English version]

- EpsonNet Authentication Print Software Administrator's Guide, NPD3647-00
- EpsonNet Authentication Print Software User's Guide, NPD3648-00
- Online Guide Supplement, 411200400
- EpsonNet Authentication Print Network Interface Card User's Guide, NPD3731-00
- How to use EpsonNet Authentication Print Software Updater, NPD3754-00
- How to use EpsonNet Authentication Print Network Interface Card Firmware Updater, NPD3753-00

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 2007-04 and concluded by completion the Evaluation Technical Report dated 2008-07. 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 sites on 2008-03 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation 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 2008-03.

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 review was 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

Tables 1-4 and 1-5 describe the test configuration used by the developer. Table 1-4 describes the environment used for testing printing via a server while Table 1-5 describes that used for testing direct printing. Although the test environments of both printing via a server and direct printing include an authentication server as component, only the interface with the TOE is tested as it is not a mandatory component for the TOE operation.

In addition to the above, the display of messages that depend on the printer hardware was tested in the environment described in Table 2-1.

**Table 2-1 Developer test configuration for printer display confirmation
(direct printing using Japanese version TOE)**

Printer	LP-9400 (Japanese printer model, English display) LP-2500 (Japanese printer model, without LCD) LP-M6000 (Japanese printer model, displays messages stored in the printer unit)	
Network interface card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework
Authentication device	PaSoRi	
Authentication media	FeliCa card	
Authentication server	Authentication server	LDAP (Active Directory)
	Authentication proxy server	EpsonNet Authentication Proxy for LDAP
Client PC	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service
	Printer driver	LP-9400 Printer Driver LP-2500 Printer Driver LP-M6000 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Java VM	Java SE 6 Update 3
	OS	Windows XP Professional SP2 (32-bit)

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

Developer testing was performed using the configurations described in Tables 1-4, 1-5, and 2-1. The developer performed testing at a TOE testing environment identical to the TOE configuration identified in ST.

Adequacy of the selected test configuration is confirmed by the evaluator.

b. Testing Approach

For the testing, the following approach was used.

- (1) Testing started with a print request from a client PC and confirmations were done through operations with and without user intervention, screens, messages, and acquisition of data exchanged along the print output flow following the identity verification by the authentication device connected to the printer.
- (2) Confirmations were done through administrator operations using the system configuration tool, screens, messages, and acquisition of exchanged data.

c. Scope of Testing Performed

Testing was performed on 75 items by the developer.

A coverage analysis was performed and it was verified that the security functions described in the functional specifications as well as the external interfaces are sufficiently tested.

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, 2-3, 2-4, and 2-5 describe the configurations used for testing by the evaluator. Table 2-2 describes the environment in which the evaluator performed sampling tests of developer tests, Table 2-3 describes the environment in which conditions judged necessary by the evaluator were additionally tested, and Tables 2-4 and 2-5 describe the environments in which unauthorized accesses were tested.

**Table 2-2 Evaluator test configuration for independent testing
(printing via a server using Japanese version TOE)**

Printer	LP-M6000 series (Japanese printer model, displays messages stored in the printer unit) printer	
Network interface card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework

Authentication device	PaSoRi	
Authentication media	FeliCa card	
Authentication server	None	
Authentication printing server	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service
	Java VM	Java SE 6 Update 3
	OS	Windows 2000 Server SP4 (32-bit)
Client PC	Printer driver	LP-M6000 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Job monitor	EpsonNet ID Print Job Monitor
	OS	Windows Vista Business Edition (32-bit) Windows Vista Ultimate Edition (32-bit) Windows Vista Enterprise Edition (32-bit) Windows 2000 Professional SP4 (32-bit)

**Table 2-3 Evaluator test configuration for additional testing
(printing via a server using Japanese version TOE)**

Printer	Two LP-M6000 series (Japanese printer model, displays messages stored in the printer unit) printers	
Network interface card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework
Authentication device	Two PaSoRi	
Authentication media	FeliCa card	
Authentication server	None	
Authentication printing server	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service
	Java VM	Java SE 6 Update 3
	OS	Windows 2000 Server SP4 (32-bit)
Client PC	Printer driver	LP-M6000 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Job monitor	EpsonNet ID Print Job Monitor
	OS	Windows Vista Business Edition (32-bit) Windows Vista Ultimate Edition (32-bit)

**Table 2-4 Evaluator test configuration for unauthorized access testing 1
(printing via a server using Japanese version TOE)**

Printer	LP-M6000 series (Japanese printer model, displays messages stored in the printer unit) printer	
Network interface card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework
Authentication device	PaSoRi	
Authentication media	FeliCa card	
Authentication server	None	
Authentication printing server	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service
	Java VM	Java SE 6 Update 3
	OS	Windows Server 2003 SP2 (32-bit) Windows 2000 Server SP4 (32-bit)
Client PC	Printer driver	LP-M6000 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Job monitor	EpsonNet ID Print Job Monitor
	OS	Windows Vista Business Edition (32-bit)

**Table 2-5 Evaluator test configuration for unauthorized access testing 2
(direct printing using Japanese version TOE)**

Printer	LP-S4000 (Japanese printer model, displays messages in English)	
Network interface card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication service plugin	EpsonNet Auth Proxy Plugin
	Authentication device plugin	ENSP Device Control Libraries
	ENSP	ENSP Framework
Authentication device	Two PaSoRi	
Authentication media	FeliCa card	
Authentication server	None	
Client PC	System configuration tool	EpsonNet ID Print System Configuration
	Spooler software	EpsonNet ID Print Spooler Service
	Printer driver	LP-S4000 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	Java VM	Java SE 6 Update 3
	OS	Windows Vista Ultimate Edition (32-bit) Windows Vista Enterprise Edition (32-bit)

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Evaluator testing was performed using the configurations described in Tables 2-2, 2-3, 2-4, and 2-5. The evaluator performed testing at a TOE testing environment with the following components removed from the TOE configuration identified in ST.

- Authentication server

Adequacy of the removed component and selected test configuration is confirmed by the evaluator.

b. Testing Approach

For the testing, the following approach was used.

- (1) Testing started with a print request from a client PC and confirmations were done through operations with and without user intervention, screens, messages, and acquisition of data exchanged along the print output flow following the identity verification by the authentication device connected to the printer.
- (2) Confirmations were done through administrator operations using the system configuration tool, screens, messages, and acquisition of exchanged data.
- (3) Confirmations were done using a vulnerability testing tool (Nessus).

c. Scope of Testing Performed

The evaluator performed 65 tests in total: 20 independent tests, 21 sampling tests of the developer tests, and 24 penetration tests. The following were considered as the selection criteria of the tests.

[Selection criteria of independent tests]

- (1) Include as many TOE security functions as possible in one test.
- (2) By performing a series of tests, test all of the TSFIs used by users.
- (3) By performing a series of tests in order, use all of the TSFs.
- (4) Include direct testing of authentication printing of a print job, which is a characteristic feature of the TOE.
- (5) Use types of printer passwords not covered in the developer testing including testing of SF. Settings management (TSF. Administrator authentication) for the claimed SOF.
- (6) Perform testing of conflicting prints since functional tests by the developer are performed with individual, non-conflicting prints.

[Selection criteria of sampling tests]

- (1) Cover all TSFs and TSFIs.
- (2) Focus on parts where input parameters are easily affected by operations by users who are humans, such as the password input.

[Selection criteria of penetration tests]

- (1) An attack related to a threat (T. Tampering of settings, T. Unauthorized disclosure of prints) for the TOE.
- (2) Direct attack to TOE components such as the system configuration tool, spooler software, and authentication device interface since internal network is protected from interception and tampering according to the assumptions of ST.
- (3) Of the tests by the developer, those considered necessary to be confirmed as vulnerability test.
- (4) Of the vulnerability tests reported in the vulnerability analysis by the developer, those considered necessary to be subject to additional testing from a different point of view by the evaluator.
- (5) Tests that support the strength analysis reported in the functional strength analysis by the developer.
- (6) Acts people with malicious intent may attempt to perform by referring to guidance documents.

d. Result

All performed evaluator testing completed correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior.

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 review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review 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 EAL2 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

User identification information given to the print data with the printer driver on client PC must be unique in the entire user of the product.

When the authentication server is used, TOE is handled assuming that the information registered in the authentication server and the response from the authentication server are justified.

It is limited to the printer equipped with the network card with the authentication device to be able to do the transmission request of the print data to the spooler software installed in client PC or the authentication printing server.

It is necessary to administrate the network to prevent an illegal transmission request of the print data because the spooler software works assuming that the transmission request of the print data from the printer is justified.

5. Glossary

The abbreviations used in this report are as follows.

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 specific abbreviations for the TOE used in this report are as follows.

ENSP	EpsonNet Service Platform
MIB	Management Information Base
OS	Operating System
UI	User Interface

The terms used in this report are as follows.

Administrator	<p>Role: Build the environment of use, configure, and manage the TOE (do installation, initial settings, and settings change according to guidance documents).</p> <p>Privilege: Install, do initial setting, and change settings of the TOE; define the user ID information; configure and operate the authentication server.</p> <p>Level of trust: Can be trusted.</p> <p>Knowledge: Has IT and printer knowledge.</p>
Authentication device	<p>A device that connected to a network interface card, identifies and authenticates users.</p> <p>Users are authenticated using an authentication media for magnetic card reader, IC card reader, biometric authentication device, or any other authentication device allocated to each printer for authentication printing. Where appropriate, the authentication server is used to identify the user ID information from the information read from the authentication media.</p>

Authentication device plugin A plugin for controlling an authentication device connected to the network card. Processes data entered from the authentication device in accordance with the content of the printer setup information. Where authentication server is not used, the processed data becomes the user ID information. The plugin to use must be one corresponding to the connected authentication device.

Authentication printing A method for printing in which the print is output after identifying and authenticating the print owner.

Authentication printing server A server that holds print jobs created from authentication printing requests submitted by users while they are identified and authenticated.

When printing via a server is used, this computer has the spooler software and system configuration tool which are parts of this TOE installed for holding a number of print jobs temporarily, and the Java VM for running the TOE.

In direct printing, authentication printing server is unnecessary since each client PC serves as authentication printing server.

Authentication printing software Refers to EpsonNet ID Print AuthBase. Queries the spooler software whether there is any print job corresponding to a user ID information acquired from the authentication device, and if there is, acquires the corresponding print job(s) and transfers it(them) to the printer. Furthermore, requests the spooler software to delete the corresponding print job(s) when printing finishes.

Authentication server A server for managing user ID information. Manages the correspondence between the information read from an authentication media by an authentication device and a user ID information. Authentication server is unnecessary if the user ID information is directly stored in the authentication media read by the authentication device.

Authentication service plugin Where authentication server is used, a plugin that enables the authentication printing software to communicate with the authentication server and acquire the user ID information. With data processed by the authentication device plugin, queries the user ID information to the authentication server. The plugin to use must be one corresponding to the used authentication server.

Client PC	<p>A computer used by a user for work.</p> <p>A user submits requests for authentication printing from this computer. Furthermore, a number of application software (printer driver, user ID information registration tool, and job monitor for printing via a server; printer driver, user ID registration tool, and Java VM for direct printing) necessary for using authentication printing are installed on this computer. In direct printing, the spooler software and system configuration tool which are parts of this TOE are installed on this computer to hold print jobs temporarily.</p>
Direct printing	<p>A printing method in which the print jobs created from print requests from client PC users are temporarily held on each client PC, which transfers the print jobs in accordance with the output requests from the printer.</p>
ENSP	<p>Abbreviation for EpsonNet Service Platform.</p> <p>A platform for running the authentication printing software. Also includes the Java VM.</p>
External network	<p>A network environment used by an unspecified number of people such as the Internet.</p> <p>An environment in which there are people who may perform various malicious acts.</p>
ID information assignment and transmission function	<p>Adds user ID information to print jobs according to the user ID information settings and sends the print jobs with user ID information to the print-job management function.</p>
ID information creation function	<p>Creates user ID information from the information read from the authentication device in accordance with the content of the printer setup information. Performs either of the following operations depending on the content of the printer setup information.</p> <ul style="list-style-type: none"> • Processes the information read from the authentication device and makes it the user ID information. • Processes the information read from the authentication device and based on that processed information, requests/acquires to/from the authentication server the user ID information.
Internal network	<p>A network environment separated from external networks by a router and is not subject to attacks from external networks.</p>
Java VM	<p>Software for running the spooler software, system configuration tool, and authentication printing software that make up this TOE.</p>
Job ID	<p>A unique integer assigned automatically by the TOE to print jobs for management.</p>

Job monitor	<p>An application used by a print owner to delete by him/herself a print job held in the spooler software.</p> <p>This application is not installed when direct printing is used as print jobs are deleted by using the system configuration tool installed on each client PC.</p>
MIB	<p>Abbreviation for Management Information Base.</p> <p>A database for managing device statuses.</p>
Network interface card	<p>An optional network card with authentication printing functions for Seiko Epson printers and multifunction printers. The authentication printing software, which is a part of this TOE is installed on the network interface card.</p>
Print data	<p>The data a user wants to output using a printer.</p>
Print job	<p>The data created by adding printing method information and user ID information to a print data. The print job is created by a printer driver when a user submits a print request.</p>
Print-job creation function	<p>Creates print jobs by adding information such as the method of printing with a printer to print data submitted by users.</p>
Print-job deletion function	<p>Where printing via a server is used, deletes print jobs spooled in the authentication printing server as spool data. It cannot delete print jobs sent by other client PCs.</p>
Print-job handling function	<p>Works together with the print-job management function which is a TOE security function to transfer the print jobs of an identified user to the print output function of the printer which is a non-TOE software and perform the printing.</p>
Print-job management function	<p>A function that manages spool data. It is included in the spooler function, which is a part of the TOE. Executes the following operations on the spool data.</p> <ul style="list-style-type: none"> • Assigns job IDs to print jobs with user ID information and the like received from the ID information assignment and transmission function which is a non-TOE software, and holds them as spool data. • Sends the list of job IDs of print jobs with the user ID information specified by the print-job handling function to the print-job handling function. • Transfers the print jobs corresponding to the job ID specified by the print-job handling function to the printer via the print-job handling function.
Print output function	<p>Outputs print data included in print jobs received from the print-job handling function as prints.</p>

Printer driver	<p>A driver for creating print jobs and controlling a printer. Creates print jobs by adding user ID information and printing method information to print data submitted by users, and sends them to the spooler software.</p> <p>The driver to use must be one corresponding to the used printer. The printer driver can be installed on the authentication printing server and shared.</p>
Printer password	A password for changing the printer setup information.
Printer settings function	<p>A function that provides the user interface for accessing the printer setup information.</p> <ul style="list-style-type: none"> • Performs administrator authentication before permitting access to the printer setup information. • Displays the settings screen for changing the printer setup information.
Printer setup information	The setting information regarding authentication printing that is stored in the network interface card. The information consists of the authentication device type, authentication method, user ID information creation rules, and printer password.
Printing via a server	A printing method in which a server (authentication printing server) is installed to temporarily hold the print jobs created from print requests from client PC users. All print jobs are held on this server, which transfers the print jobs in accordance with the output requests from the printer.
Responsible of the organization	<p>Role: Appoint administrators.</p> <p>Privilege: Decide introduction of the TOE.</p> <p>Level of trust: Can be trusted.</p> <p>Knowledge: No knowledge level assumed. (IT knowledge not required)</p>
Router	A router located between the external and internal networks. Prevents unauthorized accesses from external networks.
Service staff	<p>Role: Build the environment of use and configure the TOE (do installation, initial settings, and settings change according to guidance documents) upon request from the administrator.</p> <p>Privilege: Install, do initial setting, and change settings of the TOE.</p> <p>Level of trust: Cannot always be trusted. May collect someone else's print by mistake. May perform malicious acts.</p> <p>Knowledge: Has IT and printer knowledge.</p>
Settings management function	<p>A function that manages the printer setup information.</p> <ul style="list-style-type: none"> • Restricts the access to printer setup information to authenticated administrators.

Spool data	The print job temporarily held by the print-job management function.
Spooler software	Refers to EpsonNet ID Print Spooler Service. Holds print job with user ID information and the like and decides whether to send a print job requested by the authentication printing software to the printer or not.
System configuration tool	Refers to EpsonNet ID Print System Configuration. A tool for setting up the authentication printing server and changing the printer setup information.
System setup function	Performs identification and authentication before the system setup function can be used to configure or change a system setup information. Furthermore, requests deletion of specified print jobs to the print-job management function which is a TOE security function. Invokes the printer settings function which is a TOE security function when the settings of a printer setup information are changed.
System setup information	The setting information that decides the behavior of the print-job management function. Includes information regarding the following items. <ul style="list-style-type: none"> • Print job timeout period (print jobs held in the spool data for the period specified here are automatically deleted). • Warm up ON/OFF (If set to ON, the printer is warmed up from the moment a print job is received from the ID information assignment and transmission function)
Third party	Role: Any person other than the responsible of the organization, administrators, users, and service staff whose presence is possible in an office where the TOE is used. In other words, not a user of the authentication printing but a person that can enter/leave the office such as persons of other departments/divisions, delivery persons, cleaning staff, and part-time workers. Privilege: None Level of trust: Same as user. Knowledge: Has basic IT knowledge.
UI	Abbreviation for User Interface. Displays the statuses of printing operations.
User	Role: Use authentication printing implemented with the TOE. Privilege: Request prints. Level of trust: Cannot always be trusted. May collect someone else's print by mistake. May perform malicious acts. Knowledge: Has basic IT knowledge.

User ID information	The information for identifying the user that requested a print. By default, it is the username of the user for logging onto his/her client PC. However, the information used for identifying a user can be changed in accordance with the environment of use.
User ID information settings	The settings regarding the user ID information to be added to print jobs.
User ID information registration function	Registers and changes the information in the user ID information settings which is then used as user ID information.
User ID information registration tool	Configures and registers user ID information to be added to print jobs.
User identification function	<p>A function that identifies users.</p> <ul style="list-style-type: none">• Requests creation of user ID information to the ID information creation function which is a non-TOE software in accordance with the authentication device settings and authentication method settings in the printer setup information.• Sends the acquired user ID information to the print-job handling function.

6. Bibliography

- [1] EpsonNet ID Print Authentication Print Module Security Target Ver1.11 (Jun 24, 2008) 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] EpsonNet ID Print Authentication Print Module Evaluation Technical Report Version 3, Jul 7, 2008, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security.