EPSON
EXCEED YOUR VISION

EpsonNet ID Print Authentication Print Module Security Target

Version 1.11

2008-06-24
SEIKO EPSON CORPORATION

This document is a translation of the evaluated and certified security target written in Japanese.

Revision History

Ver.	Revision date	Description	Revised part	Drawn	Approved
1.1	2007/04/06	First issued	All	Mokuya	-
1.2	2007/05/16	Deleted “2.6.3 Usage” and “2.6.4 Operating Procedure”. Updated to reflect review feedback.	Chapters 2, 3, 4, 8	Mokuya	Aoki
		Corrected other errors such as clerical errors.	All		
		Added approval column.	Revision History		
1.3	2007/06/18	Deleted functional requirement FMT_MOF.1. Updated to reflect review feedback.	All	Mokuya	Aoki
1.4	2007/08/06	Changed name of worldwide product. Changed TOE version.	Chapter 1	Mokuya	Aoki
		Added compatible printer models.	Chapter 2		
		Corrected other errors such as clerical errors pointed out in the review feedback.	All		
1.5	2007/09/07	Revised wording of assumptions.	Chapters 3, 4, 6	Mokuya	Aoki
		Corrected names of documents listed in the assurance measures.	Chapter 6		
1.6	2007/09/13	Corrected errors.	All	Mokuya	Aoki
1.7	2007/09/26	Corrected assurance measures.	Chapter 6	Mokuya	Aoki
		Corrected description of mutual support.	Chapter 8		
1.8	2007/10/29	Corrected clerical errors. Corrected errors pointed out in the review feedback.	All	Mokuya	Aoki
		Corrected claimed strength of function.	Chapter 6		
1.9	2008/02/06	Revised sentences regarding trademarks and product names.	1.5, 2.1.3	Mokuya	Aoki
		Added documents to assurance measures.	6.2		
		Corrected minimum strength of function and claimed strength of function.	5.1.3, 6.1.2		
		Revised wording of assumptions and objectives.	3.1, 4.2		
		Added defeat prevention to mutual support.	8.2.4		
		Corrected other errors such as clerical errors.	All		
1.10	2008/03/18	Added and corrected documents listed in assurance measures.	6.2	Mokuya	Aoki
		Added “security attribute of security functional requirement”.	8.2.5		
		Corrected description on adequacy of the minimum strength of function.	8.2.6		
1.11	2008/06/24	Added description on Java VM. Corrected other clerical errors. Added “2.7 Evaluation Configuration”.	Chapters 1, 2	Mokuya	Aoki

Table of Contents

1. INTRODUCTION

This chapter gives an overview of the Security Target (ST), and includes the ST identification information, overview of the ST, Common Criteria (CC) conformance, and terminology.

1.1. ST Identification

The identification information for this ST is as follows.

ST Title		: EpsonNet ID Print Authentication Print Module Security Target
ST Version		: 1.11
Publication Date		: 2008/6/24
Author		: Business System Department, Business Products Operations Division, SEIKO EPSON CORPORATION
TOE Title	Japanese name	: EpsonNet ID Print Authentication Print Module
	English name	: EpsonNet ID Print Authentication Print Module
TOE Version	Japanese version	: 1.5b
	English version	: 1.5bE
Evaluation Assurance Level		: EAL2
Keywords		: Seiko Epson, Epson, Laser Printer, Printer, Multifunction printer, Authentication printing, Authentication
CC Version		: Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 Interpretations-0512

1.2. ST Overview

This ST describes the security specifications of the authentication print module Offirio SynergyWare ID Print (worldwide name: EpsonNet Authentication Print) implemented on optional network interface cards (hereinafter referred to as “network cards”) with authentication printing function for Epson printers and multifunction printers (hereinafter collectively referred to as “printers”). The TOE is a software product that runs on the Java VM and consists of a piece of software embedded into the network card’s ROM and an accessory application software that runs on PCs.

This TOE provides a function that outputs the print data submitted by a user as prints after authenticating the print owner by using an authentication device connected to the printer. In this way, it is possible to prevent unauthorized disclosure of print data during the interval from print request to print collection by the print owner.

1.3. CC Conformance Claim

This ST conforms to the following evaluation standards for information security (CC).

- Functional requirements: CC Part 2
- Assurance requirements: CC Part 3
- Evaluation Assurance Level: EAL2
- There is no PP to be conformed.

1.4. Terminology and Acronyms

The terms and acronyms used in this ST are as follows.

Term	Description
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.
Printer password	A password for changing the printer setup information.
Authentication printing	A method for printing in which the print is output after identifying and authenticating the print owner.
Print request	The action through which a user submits a request from a client PC to a printer for printing using authentication printing.
Print output	The operation by which a printer outputs print data submitted by a user as prints.
Print data	The data a user wants to output using a printer.
Print job	The data created by adding printing method and user ID information to a print data. The print job is created by a printer driver when a user submits a print request.
Printing method	The information regarding the method of printing the print data such as print paper size, printing direction, etc.
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 recording media	An authentication media containing ID or biometric information to be read by an authentication device.
Network interface card	A network interface card that adds network connectivity to a printer or multifunctional printer.

Acronym	Description
CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.5. Trademarks

The following products are mentioned in this ST using abbreviated names instead of the formal names.

Formal name	Abbreviated name
Microsoft® Windows® 2000 Operating System	Windows 2000
Microsoft® Windows® XP Operating System	Windows XP
Microsoft® Windows Server® 2003 Operating System	Windows Server 2003
Microsoft® Windows Vista® Operating System	Windows Vista
Java™ Platform Standard Edition 6	Java SE 6

Microsoft, Windows, Windows Server, and Windows Vista are registered trademarks of Microsoft Corporation in the United States of America and other countries.

Furthermore, in this ST, when referring to a specific edition or family of a product mentioned above, the edition or family reference is appended to the abbreviated name as “Windows 2000 Server” or “Windows Vista Business”. In addition, when naming a specific Service Pack (hereinafter abbreviated as “SP”) applicable to a product, the SP reference is appended to the abbreviated name as “Windows 2000 SP 4".

Java and Java-related trademarks and logos are registered trademarks of Sun Microsystems, Inc. in the United States of America and other countries.

All other company names or product names mentioned herein are trademarks or registered trademarks of their respective owners.

2. TOE DESCRIPTION

This chapter describes the TOE, and includes the type of product the TOE is, explanation of the TOE, parties, protected assets, physical configurations, logical configurations, and usage.

2.1. TOE Overview

2.1.1. Type of Product

This TOE is a software product intended for printers connected to a network environment such as a corporate LAN that runs on the Java VM and provides functions for outputting prints of print data in the presence of the user who submitted the print request, after identifying him/her.

This TOE is provided as an optional network card for printers and corresponding accessory application software.

2.1.2. Intended Use

This TOE is used to prevent leakage of printed data by preventing prints output by a printer from being taken away by other than the user that submitted the print request.

In a general office with printers connected to the corporate LAN, it is possible for prints to be left on the printer's output tray for long time, or prints of multiple users to be piled up. In such situation, the content of the print data may be leaked if other than the user who requested the print collects the print left on the output tray. Actually, most print data leakages from printers are caused by theft of prints left on the output tray.

This TOE protects print data from threats such as the one described above.

2.1.3. Environment of Use

This TOE is assumed to be used in a general office environment where a few printers connected to the corporate LAN are used by multiple users. In other words, an environment where printers connected to a LAN environment receives print requests from client PCs of users also connected to the LAN.

This TOE realizes a function that instead of immediately sending to a printer the print jobs created from the print requests submitted by users, holds the print jobs temporarily after adding user ID information for identifying the users who submitted the requests. Thereafter, when a user loads a media with his/her user information to the authentication device connected to the printer, identifies the user from the information sent by the authentication device, and of the print jobs it holds, sends to the printer only those corresponding to the identified user. The information to use as user ID information can be configured in accordance with the environment. That is, any information that can uniquely identify a user of this TOE, such as employee number or login ID for a computer can be used directly. Furthermore, in an environment where employee numbers are managed centrally using a directory service or database, the information in that server can be used directly.

This TOE supports the following two configurations depending on where the print Jobs are temporarily held.

1) Printing via a server

In this configuration, a server is installed for centrally holding all the print jobs created from the print requests submitted by users. Figure 1 shows a diagram of a typical environment using this configuration. For a description of each of the components illustrated in the diagram, see

Table 1. In this figure, the authentication printing server serves as the server where the print jobs are temporarily held.

As indicated in the figure, the TOE is a software included in the network card and the authentication printing server.

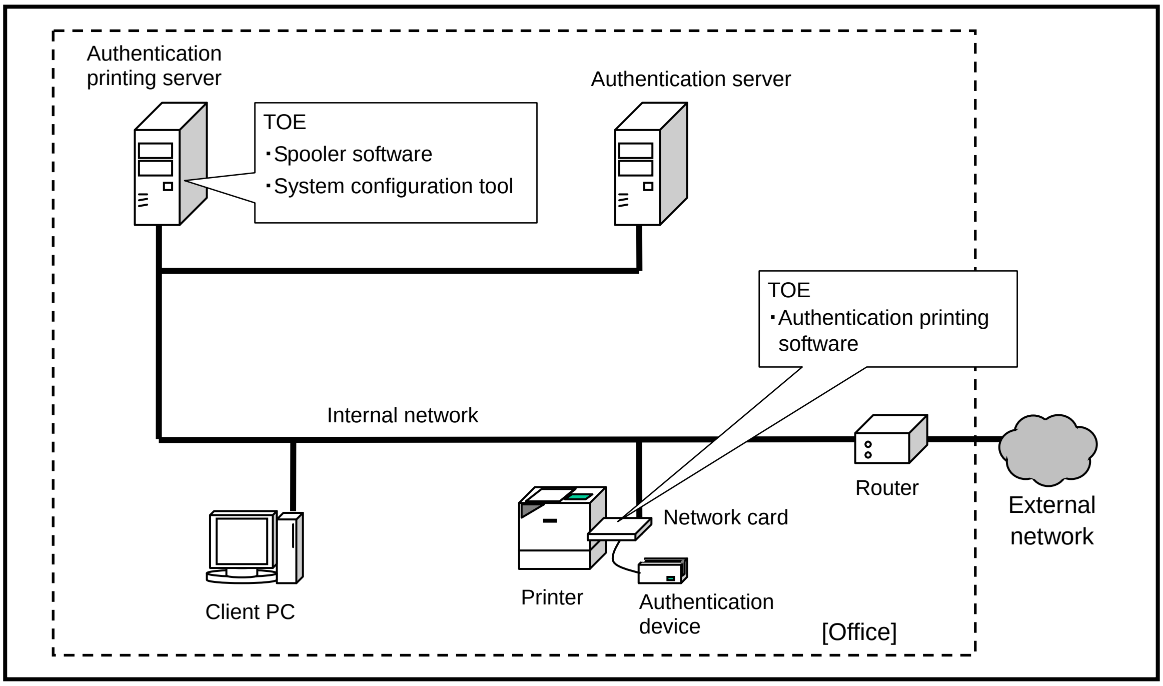

Figure 1: Environment of use (printing via a server)

2) Direct printing

In this configuration, the client PC of a user temporarily holds the print jobs created from the print requests submitted by that user. In this configuration, no authentication printing server is necessary. Figure 2 shows a diagram when this configuration is used. For a description of the components illustrated in this diagram, see also

Table 1.

As indicated in the figure, the TOE is a software included in the network card and the client PC. The part of the TOE software for client PCs must be installed on all client PCs when there are two or more client PCs.

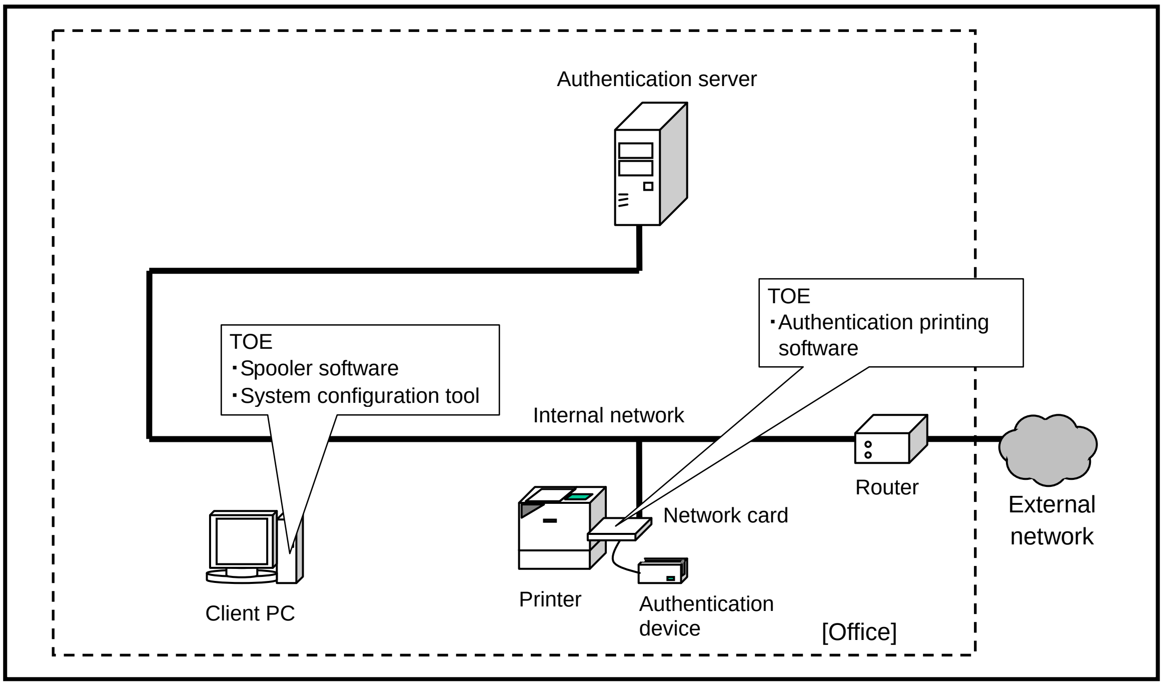

Figure 2: Environment of use (direct printing)

Table 1: Components of the environment of use

Component	Description
Client PC	A computer used by a user for work. A user submits requests for authentication printing from this computer. The computer has installed a number of applications that are necessary for using the authentication printing. The computer must be supported by the following Java VM: • Java SE 6 Update 3 or later In the figure, only one client PC is connected. However, an environment with multiple client PCs is also possible. (One authentication printing server supports up to 50 client PCs)
Printer	A Seiko Epson product to which a network card that includes the TOE can be installed. Product refers to printers and multifunction printers (listed in Table 2) to which a network card including the TOE can be installed. In the figure, there is only one printer connected. However, an environment with multiple printers is also possible.
Network card	An optional network interface card with authentication printing function for Seiko Epson printers and multifunction printers. The TOE is implemented as part of the software installed on this network card. The supported network cards are as follows. • Network card supplied with PRIFNW7S (Japanese version [Destination: Japan]) • Network card supplied with C12C824402 (English version [Destination: worldwide]) * C12C824402 is the English version of PRIFNW7S and uses the same hardware as PRIFNW7S.
Authentication device	A device that connected to a network card, identifies and authenticates users. Authenticates the user and reads his/her ID information. An authentication device such as a magnetic card reader, IC card reader, and biometric authentication device that uses an authentication media.

Authentication printing server (Figure 1 only)	A server PC that holds print jobs created from authentication printing requests submitted by users while they are identified and authenticated. The computer must be supported by the following Java VM: • Java SE 6 Update 3 or later The TOE is an application software installed on this computer. However, in direct printing, authentication printing server is unnecessary since each client PC serves as authentication printing server.
Authentication server	A server for managing user ID information. A server such as the directory server is used.
Router	A router located between the external and internal networks. Prevents unauthorized accesses from external networks.
Internal network	A network environment separated from external networks by a router and is not subject to attacks from external networks.
External network	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.
Office	An area where users use the authentication printing implemented with the TOE. A general office environment is assumed.

*: The applications necessary for using the authentication printing can be installed on client PCs running the following OSs. Furthermore, these OSs are supported by Java VM.
Windows 2000 Server (SP4 or later)
Windows 2000 Professional (SP4 or later)
Windows Server 2003 (SP2 or later)
Windows XP Professional (SP2 or later)
Windows Vista Ultimate (Including future SPs)
Windows Vista Business (Including future SPs)
Windows Vista Enterprise (Including future SPs)
(64-bit editions are not supported)

*: The applications necessary for using the authentication printing can be installed on authentication printing servers running the following OSs. Furthermore, these OSs are supported by Java VM.
Windows 2000 Server (SP4 or later)
Windows Server 2003 (SP2 or later)
(64-bit editions are not supported)

*: Authentication server and external networks may not exist depending on the environment.

Table 2: List of supported models

Japanese models	Worldwide models
LP-S6500 series, LP-S7000 series, LP-9800C series, LP-9200C series, LP-9000C series, LP-8800C series, LP-7000C series, LP-S4500 series, LP-9200B series, LP-9100 series, LP-7900 series, LP-8900 series, LP-9000B series, LP-9400 series, LP-2500 series, LP-M6500 series, LP-M9800 series, LP-S3000 series, LP-S4000 series, LP-M6000 series (*1) *1: Except when the “user identification function” implemented on the LP-M6000 unit is used.	AcuLaser C3800 series, AcuLaser C2600 series, AcuLaser C4200 series, AcuLaser C9100 series, AcuLaser 2600 series, EPL-N2550 series, EPL-N3000 series, AcuLaser M4000 series

*: Drivers other than ESC/Page drivers such as PostScript drivers are not supported by any of the series.

The process flow, in brief, when this TOE is used is as follows.

First, each user submits print requests from his/her client PC. The print job that is created from this print request is then temporarily held in the authentication printing server (when printing via a server) or in the client PC (in direct printing) after adding the user ID information of the user that submitted the print request (print owner).

Next, the print owner loads his/her user information to the authentication device connected to the network card of the printer, which is outside the scope of the TOE. The authentication device sends the read information to the TOE. Then, the TOE identifies the print owner from the information it received from the authentication device.

The TOE makes the printer output the print jobs with the user ID information of the identified print owner.

2.2. Parties Involved with TOE

This section describes the parties that may be involved with the TOE.

Table 3: Parties involved with TOE

Party	Description	
Administrator	[Role]	Build the environment of use, configure, and manage (*1) the TOE.

	[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.
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)
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.
Service staff	[Role]	Build the environment of use and configure (*1) the TOE upon request from the administrator.
	[Privilege]	Install, do initial setting, and change settings of the TOE.
	[Level of trust]	Same as user.
	[Knowledge]	Has IT and printer knowledge.
Third party	[Role]	Any person other than the above 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.

*1: Refers to installation, initial setting, and settings change of the TOE according to guidance documents.

2.3. Physical Configuration

2.3.1. Hardware Configuration

This TOE is a software that runs on a network card and an authentication printing server or client PC. Therefore, the scope of this TOE from the physical configuration point of view is the software implemented on the ROM of a network card, and the software installed on the hard disk of an authentication printing server or client PC.

Figure 3 and Figure 4 show the positional relationship between the hardware configuration and the implemented software when the TOE is used. In addition, Table 4 describes each piece of software illustrated in the figure.

For the authentication printing server, client PC, printer, network card, authentication server, and authentication device, see “

Table 1: Components of the environment of **use**" as the same descriptions apply.

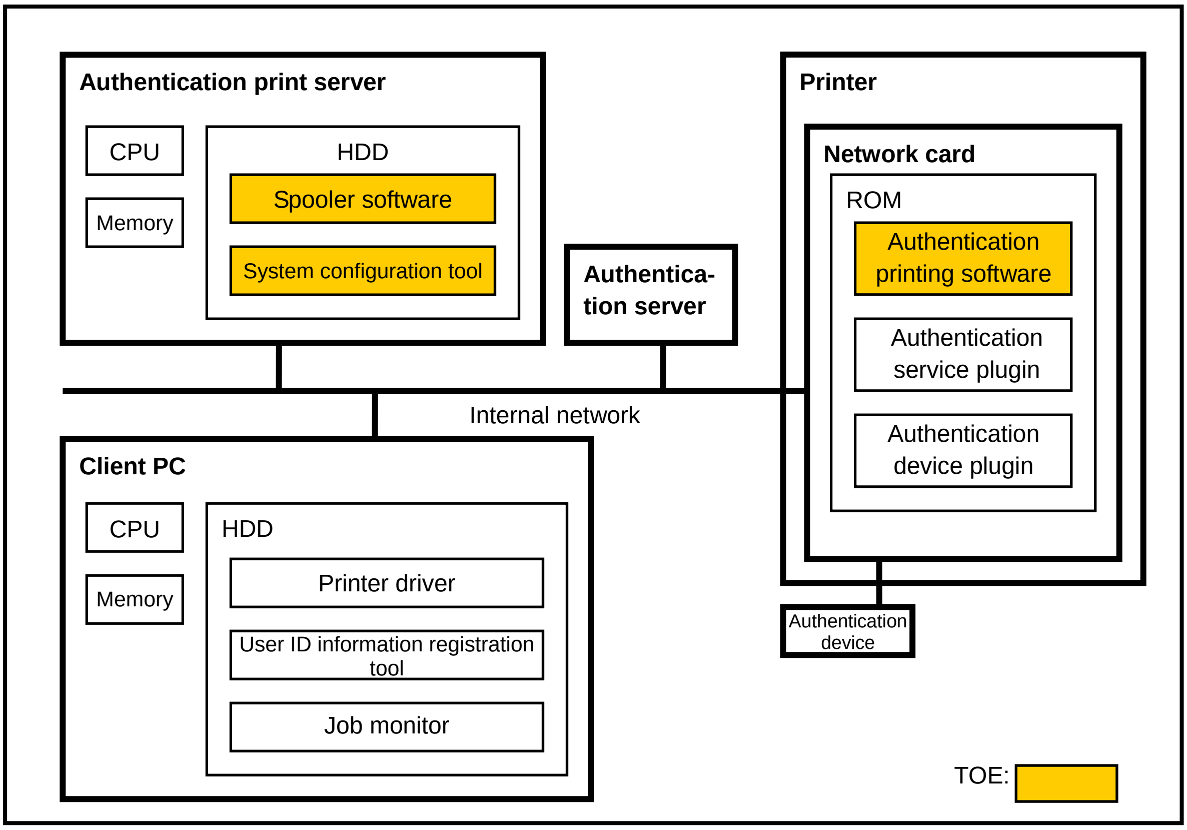
Authentication print server
CPU
Memory
HDD
Spooler software
System configuration tool
Authentica-tion server
Printer
Network card
ROM
Authentication printing software
Authentication service plugin
Authentication device plugin
Internal network
Client PC
CPU
Memory
HDD
Printer driver
User ID information registration tool
Job monitor
Authentication device
TOE:

Figure 3: Hardware configuration of the TOE (printing via a server)

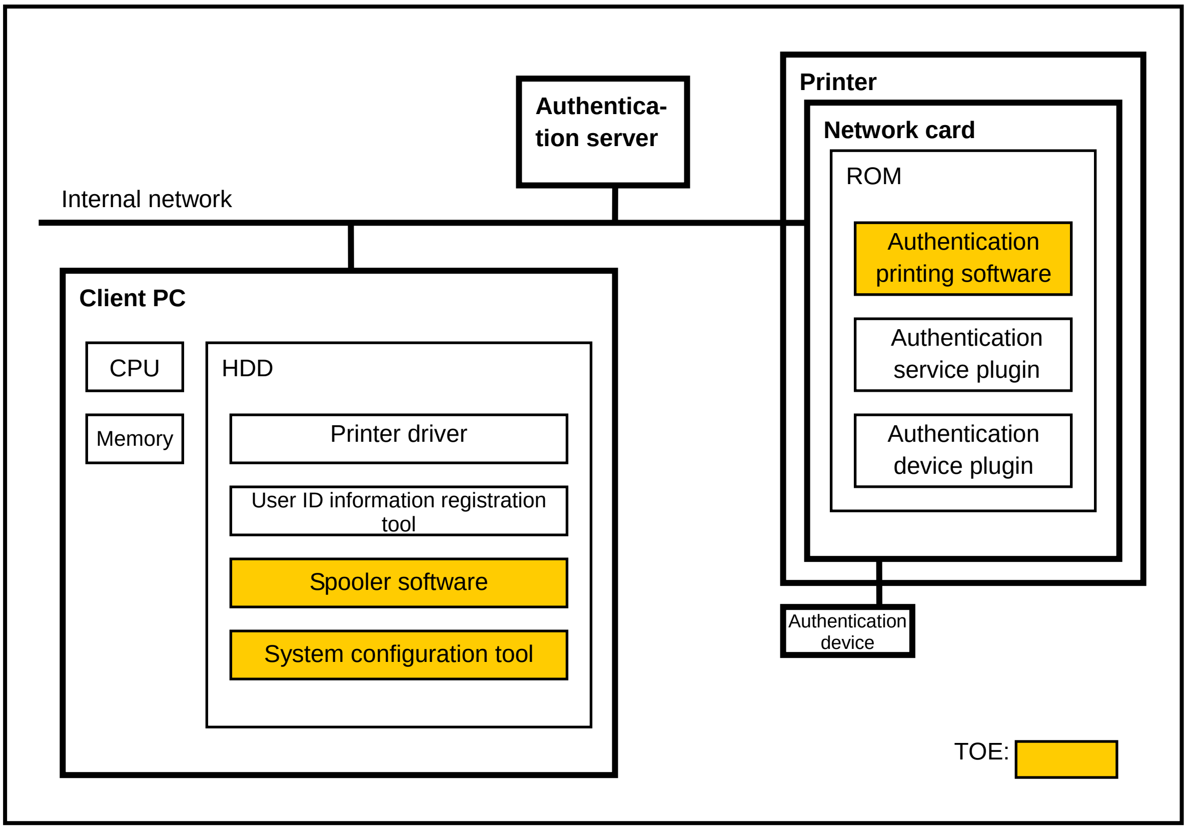
Authentica-
tion server
Printer
Network card
ROM
Authentication printing software
Authentication service plugin
Authentication device plugin
Internal network
Client PC
CPU
Memory
HDD
Printer driver
User ID information registration tool
Spooler software
System configuration tool
Authentication device
TOE:

Figure 4: Hardware configuration of the TOE (direct printing)

2.3.2. Software Configuration

Each piece of software illustrated in Figure 3 and Figure 4 actually runs on a platform such as the Java VM or the OS. Figure 5 and Figure 6 show the software configuration for the purpose of clarifying the scope of the TOE from the software configuration point of view.

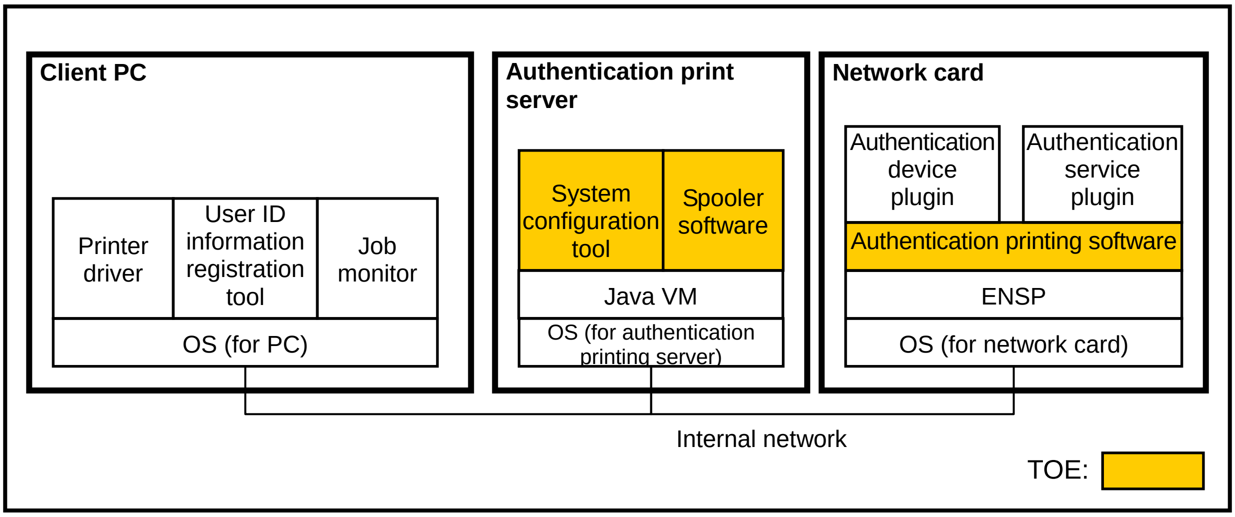
Client PC
Printer driver
User ID information registration tool
Job monitor
OS (for PC)
Authentication print server
System configuration tool
Spooler software
Java VM
OS (for authentication printing server)
Network card
Authentication device plugin
Authentication service plugin
Authentication printing software
ENSP
OS (for network card)
Internal network
TOE:

Figure 5: Software configuration of the TOE (printing via a server)

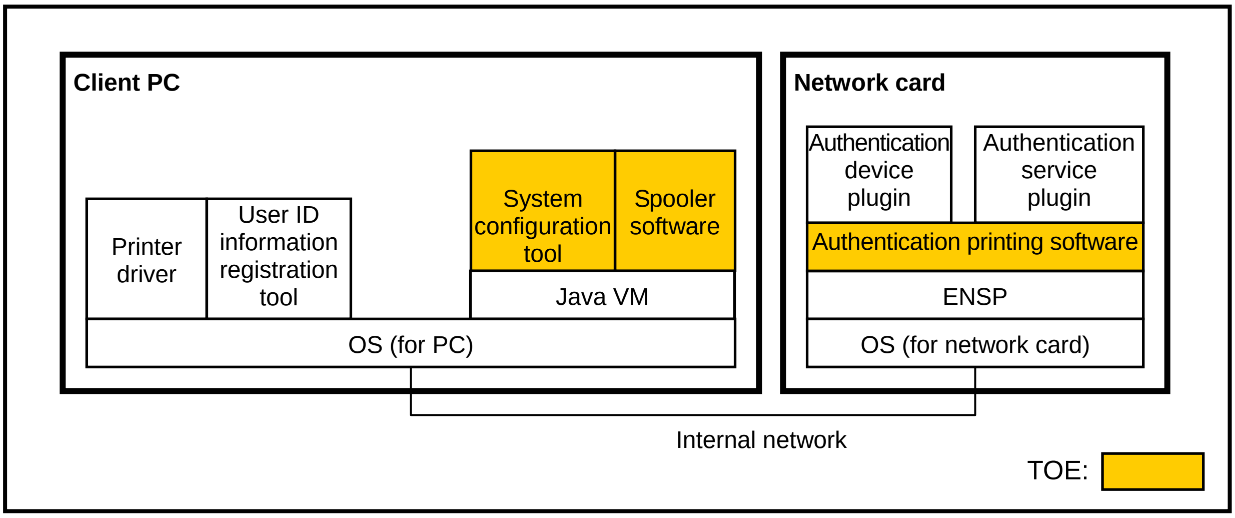
Client PC
Printer driver
User ID information registration tool
System configuration tool
Spooler software
Java VM
OS (for PC)
Network card
Authentication device plugin
Authentication service plugin
Authentication printing software
ENSP
OS (for network card)
Internal network
TOE: 🟨

Figure 6: Software configuration of the TOE (direct printing)

2.3.3. Software Components

Table 4 describes the software components of the TOE.

Table 4: Software components

Component	Description
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 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.
Authentication printing software	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	EpsonNet Service Platform. A platform for running the authentication printing software.
Java VM	Software for running the spooler software and system configuration tool.
OS (for network card)	Operating system for embedded devices for running the various pieces of software implemented on the network card.
OS (for PC)	Operating system for running the Java VM.
OS (for authentication printing server)	Operating system for running the Java VM.
Spooler software	EpsonNet ID Print Spooler Service. Holds print job with user ID information and decides whether to send a print job requested by the authentication printing software to the printer or not.
System configuration tool	EpsonNet ID Print System Configuration. A tool for setting up the authentication printing server and changing the printer setup information.
Printer driver	A driver for creating print jobs and controlling a printer. Creates print jobs by adding user ID information and other 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. In the figure, the printer driver is shown as located in the “client PC”. However, it may also be installed on the “authentication printing server” and shared.
Job monitor	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.
User ID information registration tool	Configures and registers user ID information to be added to print jobs.

2.3.4. Physical Scope and Boundary of the TOE

The physical scope of the TOE includes the software indicated in the table below.

Table 5: Physical scope of the TOE and name of the software

TOE	Name of the software	
	Japanese version	English version
Authentication printing software	EpsonNet ID Print AuthBase	EpsonNet ID Print AuthBase
Spooler software	EpsonNet ID Print Spooler Service	EpsonNet ID Print Spooler Service
System configuration tool	EpsonNet ID Print System Configuration	EpsonNet ID Print System Configuration

2.4. Logical Configuration

2.4.1. Logical Configuration

Figure 7 shows the logical configuration of the TOE. The TOE consists of each function so specified in the figure.

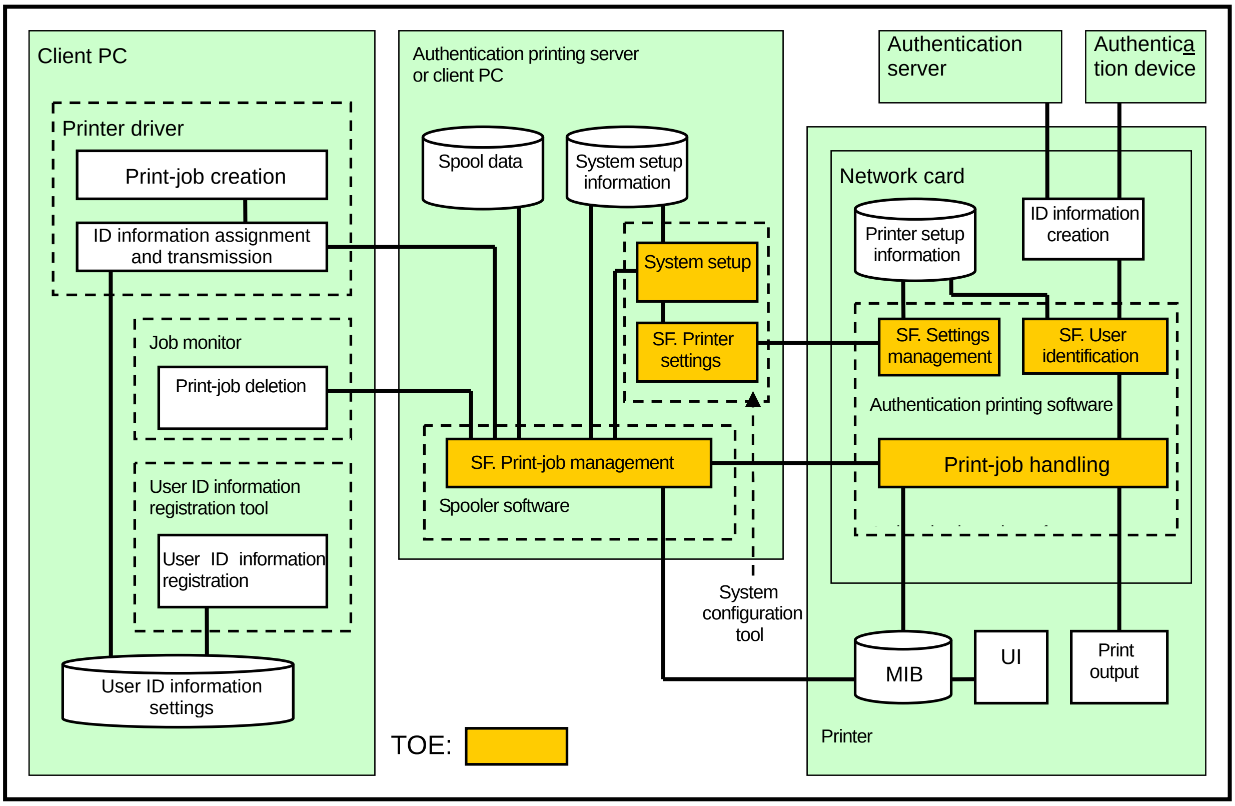

Figure 7: Logical configuration of the TOE

2.4.2. Logical Components

Table 6 describes the logical components of the TOE.

Table 6: List of logical components

Component	Description
Print-job creation function	Creates print jobs by adding information such as the method of printing with a printer to print data submitted by users.
ID information assignment and transmission function	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 SF. Print-job management function.
User ID information registration function	Registers and changes the information in the user ID information settings which is then used as user ID information.
Print-job deletion function	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.
User ID information settings	The settings regarding the user ID information to be added to print jobs.
SF. Print-job management function	Manages the spool data.
System setup function	Configures and changes the system setup information. Furthermore, requests deletion of specified print jobs to the SF. Print-job management function. Invokes the SF. Printer settings function when the settings of a printer setup information are changed. This function is implemented by the system configuration tool. 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.
SF. Printer settings function	Works together with the settings management function in the network card to configure and change the printer setup information. Requests input of printer password for administrator authentication before moving to the screen for changing the printer setup information.
Spool data	The print job temporarily held by the SF. Print-job management function.

System setup information	The setting information that decides the behavior of the SF. Print-job management function. Includes information regarding the following items. • 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)
ID information creation function	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. • 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.
SF. User identification function	Requests the creation of the user ID information to the ID information creation function according to the authentication device and authentication method settings in the printer setup information. Thereafter, sends the acquired user ID information to the print-job handling function.
SF. Settings management function	Manages the printer setup information.
Print-job handling function	Works together with the SF. Print-job management function to transfer the print jobs of an identified user to the print output function of the printer.
Printer setup information	The setting information regarding the following items related to authentication printing. • Authentication device settings (authentication device designation and settings specific to the authentication device) • Authentication method setting (use or not an authentication server) • User ID information creation rule • Printer password
Print output function	Outputs print data included in print jobs received from the print-job handling function as prints.
UI	Displays the statuses of printing operations.

MIB	Management Information Base. A database for managing device statuses.

2.4.3. Logical Scope and Boundary of the TOE

The logical scope of the TOE consists of each function mentioned below.

Table 7: Logical scope of the TOE

Software including the function	Function
Authentication printing software	SF. User identification function
	SF. Settings management function
	Print-job handling function
Spooler software	SF. Print-job management function
System configuration tool	SF. Printer settings function
	System setup function

2.5. Protected Assets

Most of the leakages involving printers in an office are caused by prints left at the printer by the print owner and taken away by third parties, with or without intention.

This is because in an environment where a few printers are used by many users, a user cannot control the flow of his/her print data once the print request is submitted from his/her client PC and print data is output to the printer directly.

This TOE temporarily holds print jobs created from the print requests submitted by users after adding the user ID information, and by a function that only responds to output requests from printers that have the same user ID information, protects the print data from queries with different user ID information.

The figures below show the print data flow in each of the configurations, when printing via a server and in direct printing. In either case, the protected asset is the print data from the time it is held in the spooler until it is collected by the print owner as prints.

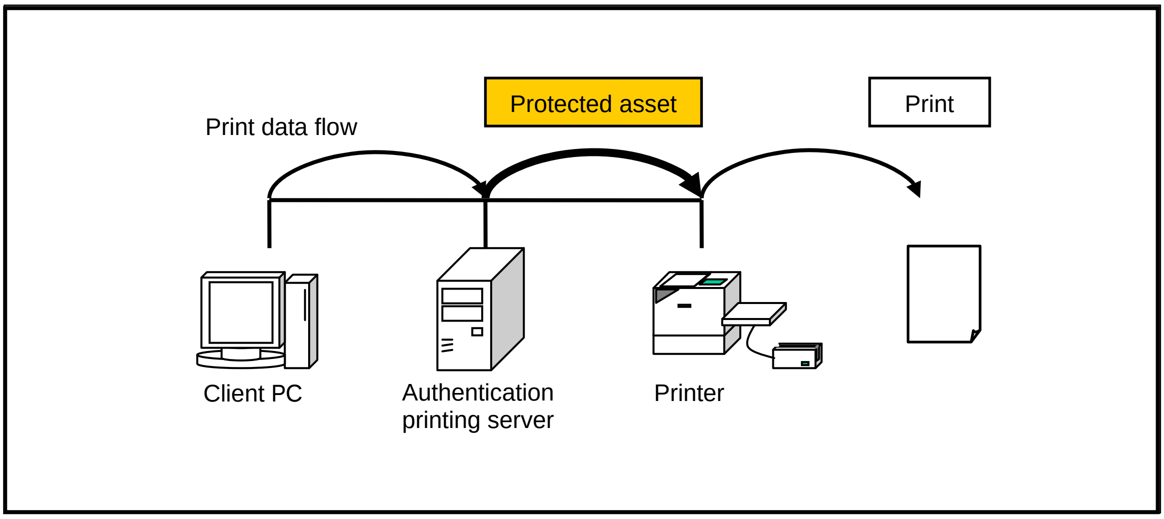

Figure 8: Protected asset (printing via a server)

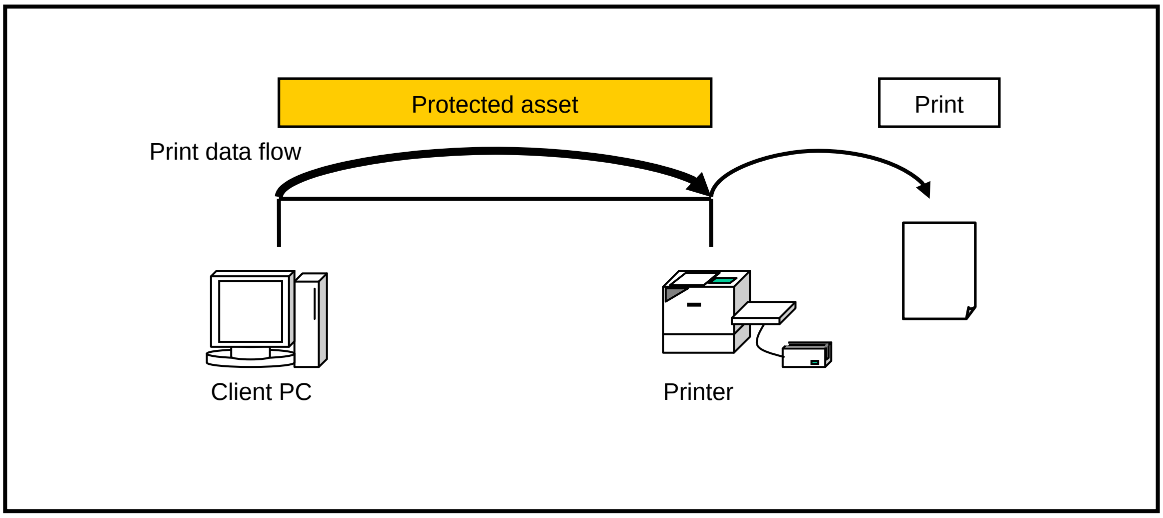

Figure 9: Protected asset (direct printing)

Print data refers to the data a user submitted for printing. During printing, the data that flows through the internal network is the print job which is the unit of processing in printing. The print data is included in the print job. Figure 10 shows the range of print data that is protected.

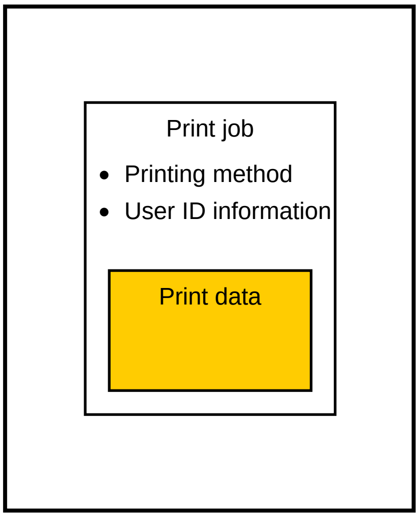

Figure 10: Print data range

2.6. TOE Functionality

2.6.1. TOE Functions

The following describes each of the functions provided by the TOE.

2.6.1.1. Security Functions

SF. User identification function

A function that identifies users.

- Requests creation of user ID information to the ID information creation function 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.

SF. Print-job management function

A function that manages spool data. Executes the following operations on the spool data.

- Assigns job IDs to print jobs with user ID information 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 IDs specified by the print-job handling function to the printer via the print-job handling function.

SF. Printer settings function

A function that provides the user interface (UI) for accessing the printer setup information.

- Performs administrator authentication before permitting access to the printer setup information.
- Displays the settings screen for changing the printer setup information.

SF. Settings management function

A function that manages the printer setup information.

- Restricts the access to printer setup information to authenticated administrators.

2.6.1.2. Non-security Functions

Print-job handling function

Works together with the SF. Print-job management function to transfer the print jobs of an identified user to the printer.

- Receives a user ID information from SF. User identification function.
- Queries to SF. Print-job management function the job ID list of print jobs corresponding to the user ID information.
- Queries to SF. Print-job management function print jobs included in the job ID list received from SF. Print-job management function.
- Transfers the print jobs received from SF. Print-job management function to the print output function of the printer.
- Monitors the MIB and acquires the printer status as well as the print output progress status.
- Displays successful or failed identification as well as printing status on the printer UI via MIB.
- Requests deletion of the print job for which printing is finished to SF. Print job management function.

System setup function

A function for changing settings in the system setup information. This function is not a TSF.

2.6.2. Non-TOE Functions

This TOE does not provide the following functions.

- The function for adding user ID information to print jobs.

2.7. Evaluation Configuration

The TOE can be used in either Figure 1: Environment of use (printing via a server) or Figure 2: Environment of use (direct printing) configured with multiple printers, authentication devices, and other components selected arbitrarily from those described in

Table 1: Components of the environment of use and Table 2: List of supported models.
Since the TOE is not affected by a difference in the components used, the following typical configurations are used for evaluation.
(1) Evaluation configuration for printing via a server

Printer	AL-C4200	
Network 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 media	pcProx card	
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)

(2) Evaluation configuration for direct printing

Printer	LP-S6500	
Network card	Card	PRIFNW7S
	Authentication printing software	EpsonNet ID Print AuthBase
	Authentication printing 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
	Java VM	Java SE 6 Update 3
	Printer driver	LP-S6500 Printer Driver
	User ID information registration tool	EpsonNet ID Print User ID Register
	OS	Windows XP Professional SP2 (32-bit)

3. TOE SECURITY ENVIRONMENT

This chapter describes the security environment for the TOE, and includes the assumptions, threats, and organizational security policies.

3.1. Assumptions

The assumptions are as follows. Note that an assumption without designation of whether it applies to printing via a server or direct printing is common and applies to both.

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.

- Is not subject to attacks from external networks.
- Data flowing through the internal network are not intercepted or tampered.
- No network 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.

3.2. Threats

The possible threats are as follows.

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.

Table 8 shows the settings in the printer setup information and the values or contents specified by the administrator at TOE installation that may lead to this threat if changed.

Table 8: Settings and contents of the printer setup information

Setting in printer setup information	Value or content
Authentication device designation	Specifies the authentication device to use
User ID information creation rule	Setting value that uniquely identifies a user
Authentication method setting (use or not an authentication server)	Setting value in accordance with the environment of use
Printer password	Value difficult to guess

3.3. Organizational Security Policies

There are no organizational security policies.

4. SECURITY OBJECTIVES

This chapter describes the security objectives, and includes the security objectives for the TOE and for the environment.

4.1. Security Objectives for the TOE

The security objectives for the TOE are as follows.

O. User identification before printing

The TOE shall identify the user before outputting a print.

O. Print job control

The TOE shall output the prints requested by a print owner only to the print owner.

O. Administrator authentication

The TOE shall authenticate the administrator before an administrator configures the printer setup information.

O. Printer setup information

The TOE shall permit configuration of printer setup information only to the administrator.

4.2. Security Objectives for the Environment

The security objectives for the TOE are as follows. Note that a security objective without designation of whether it applies to printing via a server or direct printing is common and applies to both.

OE. Administrator

The responsible of the organization introducing the TOE shall select as administrator an individual that can be trusted and does not perform malicious acts.

OE. Work of service staff

The administrator shall be present when a service staff does installation, initial setting, or settings change so that he/she cannot perform malicious acts.

OE. User ID information management

The administrator shall perform the following as user ID information management.

- Manage the media with user ID information so that it is not used by other than the intended user.
- Instruct the user so that the media with user ID information is not used by other than the

intended user.

Users shall perform the following as user ID information management.

- Manage the media with user ID information as instructed by the administrator so that it cannot be used by other than him/her.
- Manage the OS account on his/her client PC so that the user ID information configured there is not changed fraudulently.

OE. Authentication printing server

Where printing via a server is used, the administrator shall protect the spool data on the authentication printing server from unauthorized disclosures by unauthorized accesses and wrongful taking of the HDD by taking the following measures.

- Protect the authentication printing server HDD so that it is not taken out wrongfully and the spool data held on it disclosed without authorization.
- When the authentication printing server needs to be handled by other than the administrator such as when it is sent out for repair, the remaining print jobs shall be deleted completely.
- Manage the OS accounts on the authentication printing server with Administrator privileges so that they are not leaked to users, service staff, or third parties and prevent spool data from being read by people using the OS accounts on the authentication printing server with Administrator privileges fraudulently.

OE. Client PC

Where direct printing is used, users shall protect the spool data on his/her client PC from unauthorized disclosures by unauthorized accesses and wrongful taking of the HDD by taking the following measures.

- Protect the client PC HDD so that it is not taken out wrongfully and the spool data held on it disclosed without authorization.
- When the client PC needs to be handled by other than the user him/herself such as when it is sent out for repair, the remaining print jobs shall be deleted completely.
- Manage the OS account on the client PC so that other users, service staff, of third parties cannot impersonate him/her and use his/her OS account on the client PC fraudulently to read spool data.

OE. Network

The administrator shall block attacks to the TOE from external networks, and protect the information that flows through the internal network from unauthorized disclosure and tampering.

The administrator shall manage the network cards with authentication printing function connected to the internal network so that no network cards with authentication printing function outside his/her control are connected to the internal network.

Where authentication printing server is used, the administrator shall manage the IP address of the authentication printing server connected to the internal network so that it is not used fraudulently to spoof the authentication printing server.

Where authentication server is used, administrators shall manage the IP address of the authentication server connected to the internal network so that it is not used fraudulently to spoof the authentication server.

OE. Printer password management

The administrator shall change the default printer password to a password that is difficult to guess and manage it so that it is not leaked to others.

OI. User ID information assignment

The printer driver shall add the user ID information of the relevant user to print jobs of print requests submitted by a user.

5. IT SECURITY REQUIREMENTS

This chapter describes the IT security requirements, and includes the security requirements for the TOE and for the IT environment.

5.1. TOE Security Requirements

This section describes the TOE security requirements, and includes the TOE security functional requirements, the TOE security assurance requirements, and the minimum strength of function.

5.1.1. TOE Security Functional Requirements

The TOE security functional requirements are as follows.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

[Assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

Subject: User process

Information: Print job

Operation: Send or hold

[Assignment: *information flow control SFP*]

Print job control

Dependencies: FDP_IFF.1 Simple security attribute

FDP_IFF.1 Simple security attribute

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

[Assignment: *information flow control SFP*]

Print job control

[Assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

Subject: User process

Security attribute: User ID information

Information: Print job

Security attribute: Job ID, user ID information

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

[Assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

A job ID list of print jobs with user ID information that matches that of the user process is created, and the print jobs with job IDs that match that in the job ID list are sent to the print output function of the printer.

Where there are no print jobs with matching user ID information, print job sending is put on hold.

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

[Assignment: *additional information flow control SFP rules*]

None

FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].

[Assignment: *list of additional SFP capabilities*]

None

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

[Assignment: *rules, based on security attributes, that explicitly authorise information flows*]

None

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

[Assignment: *rules, based on security attributes, that explicitly deny information flows*]

None

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[Assignment: *list of security attributes*]

User ID information

Dependencies: No dependencies.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[Assignment*: a defined quality metric*]

A combination of 5 to 10 letters and numbers.

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[Refinement] (*Detail for the underlined portion)

User: Administrator

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[Assignment: *list of feedback*]

The same number of characters such as "*" as the number of characters in the input string.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

[Refinement] (*Detail for the underlined portion)

User: User (The user described in "2.2 Parties Involved with TOE")

Dependencies: No dependencies.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

[Assignment: *list of user security attributes*]

User ID information

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

[Assignment: *rules for the initial association of attributes*]

None.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[Assignment: *rules for the changing of attributes*]

None.

Dependencies: FIA_ATD.1 User attribute definition

FMT_MSA.3 (1) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[Selection, choose one of: *restrictive, permissive, [assignment: other property]*]

[Assignment*:* other property]

Other property: Automatically assigned unique integer

[Assignment: *access control SFP, information flow control SFP*]

Print job control

[Refinement]

Security attributes: Job ID (*Detail for the underlined portion)

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[Assignment: *the authorised identified roles*]

None.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[Assignment: *list of TSF data*]

Authentication device designation

User ID information creation rule

Authentication method (use or not an authentication server)

Printer password

[Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

Modify

[Assignment: *the authorised identified roles*]

Administrator

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*].

[Assignment: *list of security management functions to be provided by the TSF*]

Function for managing the management items indicated in Table 9.

Dependencies: No dependencies.

Table 9: List of security management functions

Functional requirement	Management requirement in FMT	Management item
FDP_IFC.1	There are no management activities foreseen.	None
FDP_IFF.1	Managing the attributes used to make explicit access based decisions.	None
FIA_ATD.1	a) If so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.	None
FIA_SOS.1	The management of the metric used to verify the secrets.	None
FIA_UAU.2	Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	Printer password management (FMT_MTD.1)
FIA_UAU.7	There are no management activities foreseen.	None
FIA_USB.1	a) An authorised administrator can define default subject security attributes. b) An authorised administrator can change subject security attributes.	None
FIA_UID.2	The management of the user identities.	None
FMT_MSA.3(1)	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP.	None
FMT_MTD.1	Managing the group of roles that can interact with the TSF data.	None
FMT_SMF.1	There are no management activities foreseen.	None
FMT_SMR.1	a) Managing the group of users that are part of a role.	None
FPT_RVM.1	There are no management activities foreseen.	None
FPT_SEP.1	There are no management activities foreseen.	None

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*].

[Assignment: *the authorised identified roles*]

Administrator

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.1.2. TOE Security Assurance Requirements

The TOE security assurance requirements are as follows.

Table 10: TOE security assurance requirements

Assurance class	Assurance component	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.1.3. Minimum Strength of Function

The minimum strength of function for this TOE is SOF-basic. The target TOE security functional requirements are as follows.

- FIA_UAU.2

5.2. Security Requirements for the IT Environment

The security requirements for the IT environment are as follows.

FMT_MSA.3 (2) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[Selection, choose one of: *restrictive, permissive, [assignment: other property]*]

[Assignment: other property]: User ID information

[Assignment: *access control SFP, information flow control SFP*]

Print job control

[Refinement] (*Detail for the underlined portion)

Security attribute: User ID information

TSF: Printer driver

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[Assignment: *the authorised identified roles*]

None

[Refinement] (*Detail for the underlined portion)

TSF: Printer driver

Dependencies FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

6. TOE SUMMARY SPECIFICATION

This chapter describes the TOE summary specification, and includes the TOE security functions and assurance measures.

6.1. TOE Security Functions

This section describes the TOE security functions, and includes the TOE security functions, the security mechanisms, and the claimed strength of function.

6.1.1. TOE Security Functions

The TOE security functions are as follows.

Table 11: Correspondences between TOE security functions and TOE security functional requirements

	FDP_IFC.1	FDP_IFF.1	FIA_SOS.1	FIA_ATD.1	FIA_UAU.2	FIA_UAU.7	FIA_UID.2	FIA_USB.1	FMT_MSA.3(1)	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1
SF. User identification function				○			○	○					○	○
SF. Print-job management function	○	○							○				○	○
SF. Settings management function					○					○	○	○	○	○
SF. Printer settings function			○			○							○	○

SF. User identification function

This function identifies users.

The TOE requests the user ID information of the print owner to ID creation function before outputting a print [FIA_UID.2]. Furthermore, the TOE associates the user ID information to the subject that acts on behalf of the print owner and maintains that association [FIA_USB.1, FIA_ATD.1].

This function is always executed before the flow control by the SF. Print-job management function [FPT_RVM.1]. Moreover, this function is executed in a memory space separated from that of other processes [FPT_SEP.1].

SF. Print-job management function

This function transfers to the print output function of the printer only the print jobs that correspond to the user ID information.

The TOE receives print jobs with the user ID information the printer driver added.

The TOE assigns job IDs to the received print jobs and holds them. The job IDs assigned here are unique integers assigned by the TOE automatically [FMT_MSA.3(1)].

The TOE, upon receiving a user ID information from SF. User identification function, performs the following flow control on the print jobs it holds in accordance with the print job control SFP [FDP_IFC.1, FDP_IFF.1].

- Creates a job ID list of print jobs with user ID information that matches the received user ID information from the print jobs that are held. (List is used on the assumption that there might be multiple print jobs)
- Transfers the print jobs corresponding to the job IDs in the created list to the print output function of the printer.
- When there are no print jobs with user ID information that matches the received user ID information, print job sending is put on hold.

These functions are always executed during the TSF operation [FPT_RVM.1]. Moreover, these functions are executed in a memory space separated from that of other processes [FPT_SEP.1].

SF. Settings management function

This function limits the ability of changing the TOE security functions behavior and the printer setup information to authorized administrators.

The TOE authenticates the administrator by requesting the printer password before permitting access to the printer setup information.

The TOE maintains the administrator role. Furthermore, the TOE maintains the authenticated subject associated with the administrator role while the screen for editing the printer setup information is displayed. [FMT_SMR.1, FMT_SMF.1]

In this way, only the administrator is permitted to change the following settings or contents.

- Authentication device settings [FMT_MTD.1]
- Authentication method settings (use or not an authentication server) [FMT_MTD.1]
- Printer password change [FMT_MTD.1]
- User ID information creation rule [FMT_MTD.1]

These functions are always executed during the TSF operation [FPT_RVM.1]. Moreover, these functions are executed in a memory space separated from that of other processes [FPT_SEP.1].

SF. Printer settings function

This function displays the printer password input screen for authenticating the administrator when he/she attempts to access the printer setup information as well as the screen for editing the printer setup information.

On the printer password input screen, the TOE displays characters such as "*" instead of the input password so that it cannot be read at a glance and prevent the password from being leaked [FIA_UAU.7].

Furthermore, at printer password change, the TOE rejects any attempt to set a printer password that is not from 5 to 10 characters long and is not a combination of numbers and letters to prevent the setting of a password that can be easily guessed [FIA_SOS.1].

These functions are always executed when printer password is input or changed [FPT_RVM.1]. Moreover, these functions are executed in a memory space separated from that of other processes [FPT_SEP.1].

6.1.2. Claimed Strength of Function

Of the TOE security functions, the correspondences between those that are unencrypted and based on probabilistic or permutational mechanism and the claimed strength of function is described in Table 12.

Table 12: Strength of function

TOE security function	Claimed strength of function
SF. Settings management function (authentication mechanism based on password)	SOF-basic

6.2. Assurance Measures

The documentation provided to support the assurance requirements are as follows.

Table 13: List of assurance measures

Assurance class	Assurance component	Document name and TOE
ACM (Configuration management)	ACM_CAP.2	• EpsonNet ID Print Configuration Management Plan • EpsonNet ID Print Configuration List • EpsonNet ID Print Version Management Table • EpsonNet ID Print Install Configuration
ADO (Delivery and	ADO_DEL.1	• PRIFNW7S/C12C824402 Delivery Procedure Manual • EpsonNet ID Print Web Delivery Procedure Manual

operation)	ADO_IGS.1	• PRIFNW7S Readme First (Japanese version only) • PRIFNW7S/U Setup Guide (Japanese version only) • Offirio SynergyWare ID Print Administrator’s Guide (Japanese version only) • Online Guide Supplement • EpsonNet Authentication Print Network Interface Card User's Guide • EpsonNet Authentication Print Software Administrator's Guide • Offirio SynergyWare ID Print Updater Application Procedure (Japanese version only) • How to use EpsonNet Authentication Print Software Updater • PRIFNW7S Firmware Update Procedure (Japanese version only) • How to use EpsonNet Authentication Print Network Interface Card Firmware Updater
ADV (Development)	ADV_FSP.1	• EpsonNet ID Print Functional Specifications
	ADV_HLD.1	• EpsonNet ID Print High-Level Design
	ADV_RCR.1	• EpsonNet ID Print Expression Compliance Analysis
AGD (Guidance documents)	AGD_ADM.1	• Offirio SynergyWare ID Print Administrator’s Guide (Japanese version only) • EpsonNet Authentication Print Software Administrator's Guide
	AGD_USR.1	• Offirio SynergyWare ID Print User’s Guide (Japanese version only) • EpsonNet Authentication Print Software User's Guide
ATE (Tests)	ATE_COV.1	• EpsonNet ID Print Test Specifications and Report • EpsonNet ID Print Test Coverage
	ATE_FUN.1	• EpsonNet ID Print Test Specifications and Report
	ATE_IND.2	• EpsonNet ID Print Test Specifications and Report
AVA (Vulnerability assessment)	AVA_SOF.1	• EpsonNet ID Print Functional Strength Analysis
	AVA_VLA.1	• EpsonNet ID Print Vulnerability Analysis

7. PP CLAIMS

This ST does not claim conformance to any PP.

8. RATIONALE

This chapter describes the rationale, and includes rationale for the security objectives, security requirements, TOE summary specification, and PP claims.

8.1. Security Objectives Rationale

This section describes the rationale for the security objectives, and includes the needs and sufficiency of the security objectives.

8.1.1. Needs of Security Objectives

Table 14 shows the correspondences between the security objectives and the TOE security environment. As shown by the table, all security objectives have at least one corresponding TOE security environment. Therefore, the need of all of the security objectives is satisfied.

Table 14: Correspondences between TOE security environment and security objectives

	A. Administrator	A. Service staff	A. User ID information	A. Spool data	A. Network	T. Unauthorized disclosure of prints	T. Tampering of settings
O. User identification before printing						○	
O. Print job control						○	
O. Administrator authentication							○
O. Printer setup information							○
OE. Administrator	○						
OE. Work of service staff		○					
OE. User ID information management			○				
OE. Authentication printing server				○			
OE. Network					○		
OE. Printer password management							○
OE. Client PC				○			

OI. User ID information assignment						○	

8.1.2. Sufficiency of Security Objectives

A. Administrator

This requirement assumes the administrator does not perform malicious acts.

According to OE. Administrator, the responsible of the organization selects as administrator an individual that can be trusted and does not perform malicious acts.

In this way, A. Administrator can be realized.

A. Service staff

This requirement assumes the administrator ensures the service staff does installation, initial settings, or settings change in an environment where he/she cannot perform malicious acts while doing the work.

According to OE. Work of service staff, the administrator is present while the service staff is doing these works so that he/she cannot perform malicious acts.

In this way, A. Service staff can be realized.

A. User ID information

This requirement assumes the media with user ID information is not available to other users, service staff, or third parties, and that the user ID information configured in the client PC of a user is not changed fraudulently by other users, service staff, or third parties.

According to OE. User ID information management, the administrator manages the media with user ID information strictly so that it is not used by other than the intended user as well as instructs the user on the management of the media with user ID information. Furthermore, the user manages the media with user ID information as instructed by the administrator so that it is not used by other than him/herself as well as manage the OS account on his/her client PC so that the user ID information configured there is not changed fraudulently.

In this way, A. User ID information can be realized as neither the media with user ID information can be used by other users, service staff, or third parties nor the user ID information configured in the user’s client PC can be changed fraudulently.

A. Spool data

This requirement assumes the spool data is not exposed to unauthorized disclosure by unauthorized access, theft of HDD, or wrongful taking of HDD during a repair.

Where printing via a server is used, the following is performed according to OE. Authentication printing server.

- The administrator protects the authentication printing server HDD so that it is not taken out wrongfully and the spool data held on it disclosed without authorization.
- When the authentication printing server needs to be handled by other than the administrator such as when it is sent out for repair, the administrator deletes the remaining print jobs completely.
- The administrator manages the “OS accounts configured in the authentication printing server” with Administrator privileges so that they are not leaked to users, service staff, or third parties.

Furthermore, where direct printing is used, the following is performed according to OE. Client PC.

- The user protects the client PC HDD so that it is not stolen and the spool data held on it disclosed without authorization.
- When the client PC needs to be handled by other than the user him/herself such as when it is sent out for repair, the user deletes the remaining print jobs completely.
- The user manages the “OS accounts configured in the client PC” so that they are not leaked to other users, service staff, or third parties.

In this way, A. Spool data can be realized.

A. Network

This requirement assumes the following with respect to the network environment where the TOE is used.

- Is not subject to attacks from external networks.
- Data flowing through the internal network are not intercepted or tampered.
- No network 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.

The following is performed according to OE. Network.

- The administrator blocks attacks to the TOE from external networks and protects the information that flows through the internal network from unauthorized disclosure and tampering.
- The administrator manages the network cards with authentication printing function connected to the internal network so that no network cards with authentication printing function outside his/her control are connected to the internal network.
- Where authentication printing server is used, the administrator manages the IP address so that the IP address of the authentication printing server connected to the internal network is

not used fraudulently to spoof the authentication printing server.

- Where authentication server is used, the administrator manages the IP address so that the IP address of the authentication server connected to the internal network is not used fraudulently to spoof the authentication server.

In this way, A. Network can be realized.

T. Unauthorized disclosure of prints

This threat assumes that a user, a service staff, or a third party other than the print owner wrongfully takes the print data that is output as prints and discloses the content without authorization.

To counter this threat, it is necessary that the print data not be output as prints to other than the print owner. This TOE is used when the print owner wants to protect the data from unauthorized disclosures. Therefore, it is clear that this threat cannot take place if prints are output in the print owner's presence.

According to OI. User ID information assignment, the printer driver adds the print owner's user ID information to the print job.

According to O. User identification before printing, the TOE identifies the user.

Furthermore, according to O. Print job control, the TOE outputs the prints requested by the print owner only to the print owner. It is clear that the print owner will immediately collect the output prints.

Therefore, this threat can be countered as prints will not be available to users other than the print owner, service staff, and third parties.

T. Tampering of settings

This threat assumes a user, service staff, or third party discloses print data without authorization by impersonating the administrator and changing the printer setup information.

To counter this threat, it is necessary to permit the access to printer setup information only to the administrator.

The TOE, after authenticating the administrator according to O. Administrator authentication, permits access to the printer setup information only to the authorized administrator according to O. Printer setup information.

Furthermore, according to OE. Printer password management, the administrator changes the default printer password to a password difficult to guess and manage it so that it is not leaked to others.

Therefore, this threat can be countered as users, service staff, and third parties cannot change the printer setup information.

8.2. Security Requirements Rationale

This section describes the rationale for the security requirements, and includes the needs and sufficiency of the security functional requirements, the adequacy of the security functional requirements dependencies, the mutual support structure of the security functional requirements, the adequacy of the minimum strength of function, the adequacy of the evaluation assurance level, and the needs of the security assurance requirements.

8.2.1. Needs of Security Functional Requirements

The table below shows the correspondences between TOE security functional requirements and TOE security objectives.

As shown by the table, all TOE security functional requirements have at least one corresponding TOE security objective. Therefore, the need of all of the TOE security functional requirements is satisfied.

Table 15: Correspondences between security objectives and security functional requirements

	O. User identification before printing	O. Print job control	O. Administrator authentication	O. Printer setup information
FDP_IFC.1		○		
FDP_IFF.1		○		
FIA_ATD.1		○		
FIA_SOS.1			○	
FIA_UAU.2			○	
FIA_UAU.7			○	
FIA_UID.2	○			
FIA_USB.1		○		
FMT_MSA.3(1)		○		
FMT_MTD.1				○
FMT_SMF.1				○
FMT_SMR.1				○
FPT_RVM.1	○	○	○	○
FPT_SEP.1	○	○	○	○

The following table shows the correspondences between security functional requirements and security objectives for the IT environment.

Table 16: Correspondences between security objectives and security functional requirement for the IT environment

	OE. User ID information assignment
FMT_MSA.3(2)	O

As shown by the table, all security functional requirements for the IT environment have at least one corresponding security objective for the IT environment. Therefore, the need of all of the security functional requirements for the IT environment is satisfied.

8.2.2. Sufficiency of Security Functional Requirements

O. User identification before printing

This security objective requires the user be identified before the TOE transfers the print job(s) to the print output function of the printer.

According to FIA_UID.2, the TOE requires the user to identify him/herself before the print job(s) is(are) transferred to the print output function of the printer. Furthermore, according to FPT_RVM.1, these operations cannot be bypassed, and according to FPT_SEP.1, they are executed under a secure domain protected from interference and tampering by other subjects.

Therefore, this objective can be realized.

O. Print job control

This security objective requires that prints requested by a print owner be output only to the print owner.

According to FIA_ATD.1 and FIA_USB.1, the TOE associates the user ID information to a user process and maintains that association.

According to FDP_IFC.1 and FDP_IFF.1, the TOE transfers to the print output function of the printer only the print jobs for which “the job ID corresponding to an identified user ID information” matches “the job ID assigned to a print job”.

The job IDs assigned to print jobs have an initial value given by FMT_MSA.3(1). Furthermore, according to FPT_RVM.1, these operations cannot be bypassed, and according to FPT_SEP.1, they are executed under a secure domain protected from interference and tampering by other subjects.

Therefore, this objective can be realized.

O. Administrator authentication

This security objective requires the TOE to authenticate the administrator before permitting him/her access the printer setup information.

According to FIA_UAU.2, the TOE requires the administrator to successfully authenticate him/herself using the printer password and according to FIA_UAU.7, the authentication feedback be protected. Moreover, according to FIA_SOS.1, the printer password is always a 5 to 10 characters long combination of letters and numbers.

Furthermore, according to FPT_RVM.1, these operations cannot be bypassed, and according to FPT_SEP.1, they are executed under a secure domain protected from interference and tampering by other subjects.

Therefore, this objective can be realized.

O. Printer setup information

This security objective requires the access to printer setup information be restricted to administrators only.

According to FMT_MTD.1 and FMT_SMF.1, configuration of the authentication device settings, user ID information creation rule, authentication method settings, and change of printer password is limited to the administrator. In addition, according to FMT_SMR.1, the role of the administrator is maintained.

Furthermore, according to FPT_RVM.1, these operations cannot be bypassed, and according to FPT_SEP.1, they are executed under a secure domain protected from interference and tampering by other subjects.

Therefore, this objective can be realized.

OI. User ID information assignment

This security objective requires the print owner’s user ID information be added to print jobs.

According to FMT_MSA.3(2), the printer driver adds the print owner’s user ID information to print jobs.

Therefore, this objective can be realized.

8.2.3. Adequacy of Security Functional Requirements Dependencies

The table below shows the correspondences between security functional requirements and their dependencies.

Table 17: Security functional requirements dependencies

Functional requirement	Dependencies in CC	Dependencies in this ST	Non-satisfied dependencies	Rationale for non-satisfied dependencies
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	-	-

FDP_IFF.1	FDP_IFC.1
	FMT_MSA.3
		FDP_IFC.1
		FMT_MSA.3(1)
		FMT_MSA.3(2)		

FIA_ATD.1	-	-	-	-
FIA_SOS.1	-	-	-	-
FIA_UAU.2	FIA_UID.1		FIA_UID.1	(1)
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2		
FIA_UID.2	-	-	-	-
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	-	-
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1		FMT_MSA.1 FMT_SMR.1	(2)
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1		FMT_MSA.1 FMT_SMR.1	(3)
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1		
FMT_SMF.1	-	-	-	-
FMT_SMR.1	FIA_UID.1		FIA_UID.1	(1)
FPT_RVM.1	-	-	-	-
FPT_SEP.1	-	-	-	-

(1) Reason why it is not a problem even if FIA_UAU.2 and FMT_SMR.1 do not satisfy the dependency FIA_UID.1

FIA_UID.1 is a requirement applicable to user identification.

In this TOE, identification with FIA_UAU.2 and FMT_SMR.1 is necessary only for the administrator. According to the assumptions, an administrator is an individual that can be trusted. Therefore, it is enough if an administrator can be authenticated as such, with no need to identify each administrator one by one, even when there are multiple administrators.

Therefore, there is no need to satisfy FIA_UID.1 as identification is not necessary.

(2) Reason why it is not a problem even if FMT_MSA.3(1) does not satisfy the dependencies FMT_MSA.1 and FMT_SMR.1

FMT_MSA.1 is a requirement for authorizing the management of a security attribute to a user with a specific role.

The job ID which is a security attribute is initialized within the TOE with FMT_MSA.3(1); however, it cannot be changed afterwards.

Therefore, there is no need to satisfy FMT_MSA.1.

Furthermore, in accordance with the above, there is no need to satisfy FMT_SMR.1 either as it is a requirement related to the maintenance of the permitted role.

(3) Reason why it is not a problem even if FMT_MSA.3(2) does not satisfy the dependencies FMT_MSA.1 and FMT_SMR.1

FMT_MSA.1 is a requirement for authorizing the management of a security attribute to a user with a specific role.

Once the initial value of a user ID information which is a security attribute is given by the printer driver, it cannot be changed with FMT_MSA.3(2) afterwards.

Therefore, there is no need to satisfy FMT_MSA.1.

Furthermore, in accordance with the above, there is no need to satisfy FMT_SMR.1 either as it is a requirement related to the maintenance of the permitted role.

In this way, the dependencies of the security functional requirements are adequate.

8.2.4. Mutual Support Structure of Security Functional Requirements

The Table 18 below shows the mutual support structure of the security functional requirements.

Table 18: Mutual support structure of security functional requirements

Functional requirement	Bypass prevention	Tampering prevention	De-activation prevention	Defeat prevention
FDP_IFC.1	FPT_RVM.1	FPT_SEP.1	None	None
FDP_IFF.1	FPT_RVM.1	FPT_SEP.1	None	None
FIA_ATD.1	FPT_RVM.1	FPT_SEP.1	None	None
FIA_SOS.1	FPT_RVM.1	FPT_SEP.1	None	None
FIA_UAU.2	FPT_RVM.1	FPT_SEP.1	None	None
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	None	None
FIA_UID.2	FPT_RVM.1	FPT_SEP.1	None	None
FIA_USB.1	FPT_RVM.1	FPT_SEP.1	None	None
FMT_MSA.3(1)	FPT_RVM.1	FPT_SEP.1	None	None
FMT_MTD.1	FPT_RVM.1	FPT_SEP.1	None	None
FMT_SMF.1	FPT_RVM.1	FPT_SEP.1	None	None
FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	None	None
FPT_RVM.1	None	FPT_SEP.1	None	None
FPT_SEP.1	FPT_RVM.1	None	None	None

Bypass prevention

According to FPT_RVM.1, the following functional requirements that are implemented in SF. User identification function, SF. Print-job management function, SF. Settings management function, and SF. Printer settings function are always invoked during operation and cannot be bypassed.

FDP_IFC.1, FDP_IFF.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_MSA.3(1), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FPT_SEP.1

Tampering prevention

According to FPT_SEP.1, the memory space where the TSF is executed is not subject to interference from other illegal subjects.

De-activation prevention

This TOE does not include any function for de-activating the security functions. Therefore, there is no need to take any de-activation prevention measures.

Defeat prevention

This TOE does not need to be able to detect attacks aimed at disabling the security functions as they are never disabled. Therefore, there is no need to take any defeat prevention measures.

In this way, the mutual support structure for all of the TOE security functional requirements is adequate.

8.2.5. Consistency of Security Functional Requirements

The following describes the consistency of the security functional requirements selected in this ST.

Operation of Security Functional Requirements

In this ST, FMT_MSA.3 is repeatedly used. However, there is neither duplication nor conflict between FMT_MSA.3(1) and FMT_MSA.3(2) since their purpose and target are different.

Furthermore, the same security attribute (job ID, user ID information) is used as assignment or refinement of a functional requirement by multiple functional requirements (FIA_USB.1, DP_IFF.1, MT_MAS.3 and so on). However, there is neither duplication nor conflict among them as each of the functional requirements is for realizing a different function.

Expansion of Security Functional Requirements

The security function has not been expanded in this ST.

Dependencies of Security Functional Requirements

As described in 8.2.3, there is neither conflict nor inconsistency with regard to the dependencies of the security functional requirements.

Mutual Support among Security Functional Requirements

As described in 8.2.4, there is neither conflict nor inconsistency with regard to the mutual support among the security functional requirements.

In this way, there is no conflict among the security functional requirements selected in this ST, and they are internally consistent as well.

8.2.6. Adequacy of Minimum Strength of Function

This TOE 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. For 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, the minimum strength level of SOF-basic is adequate.

8.2.7. Adequacy of Evaluation Assurance Level

This TOE claims EAL2 as its evaluation assurance level.

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. Furthermore, the network is an environment protected from external networks such as the Internet which is accessed by an unspecified number of people. Since it is used in such an environment, vulnerability analysis for the TOE and testing of the functional specifications should also be evaluated.

Therefore, the evaluation assurance level of EAL2 is adequate.

8.2.8. Rationale for Security Assurance Requirements

This TOE claims EAL2 as its evaluation assurance level. As shown in Table 10, all assurance components in the EAL2 package, including dependencies, are selected in this TOE.

Therefore, the security assurance requirements selected in this TOE are adequate for satisfying EAL2.

8.3. TOE Summary Specification Rationale

This section describes the TOE summary specification rationale, and includes the needs and sufficiency of the TOE security functions, the adequacy of the assurance measures, and the rationale for the strength of function.

8.3.1. Needs of TOE Security Functions

Table 11 shows the correspondences between TOE security functions and TOE security functional requirements. As shown by the table, all TOE security functions have at least one corresponding TOE security functional requirement.

Therefore, the need of all of the TOE security functions is satisfied.

8.3.2. Sufficiency of TOE Security Functions

FDP_IFC.1, FDP_IFF.1

The SF. Print-job management function, performs the following flow control on the print job it holds upon receiving a user ID information from SF. User identification function in accordance with the print job control SFP.

- Creates a job ID list of print jobs with user ID information that matches the received user ID information from the print jobs that are held. (List is used on the assumption that there might be multiple print jobs)
- Transfers the print jobs corresponding to the job IDs in the created list to the print output function of the printer.
- When there are no print jobs with user ID information that matches the received user ID information, print job sending is put on hold.

Therefore, the requirements FDP_IFC.1 and FDP_IFF.1 are satisfied.

FIA_ATD.1

The SF. User identification function maintains the user ID information associated with the subject acting on behalf of the print owner.

Therefore, the requirement FIA_ATD.1 is satisfied.

FIA_SOS.1

The SF. Printer settings function, at printer password change, verifies that the password to be set is a 5 to 10 characters long combination of letters and numbers and rejects any password that does not satisfy these requirements.

Therefore, the requirement FIA_SOS.1 is satisfied.

FIA_UAU.2

The SF. Settings management function requires authentication by password before permitting access to the printer setup information.

Therefore, the requirement FIA_UAU.2 is satisfied.

FIA_UAU.7

The SF. Printer settings function displays characters such as "*" instead of the input characters when the administrator enters the requested printer password.

Therefore, the requirement FIA_UAU.7 is satisfied.

FIA_UID.2

The SF. User identification function requires the print owner be identified before the print job(s) is(are) transferred to the print output function of the printer.

Therefore, the requirement FIA_UID.2 is satisfied.

FIA_USB.1

The SF. User identification function associates the user ID information with the subject acting on behalf of the print owner.

Therefore, the requirement FIA_USB.1 is satisfied.

FMT_MSA.3(1)

The SF. Print-job management function automatically assigns a unique integer to a received print job.

Therefore, the requirement FIA_MSA.3(1) is satisfied.

FMT_MTD.1

The SF. Settings management function limits the configuration of the authentication device settings and authentication method settings, change of printer password, and change of user ID information creation rule to an authenticated administrator.

Therefore, the requirement FMT_MTD.1 is satisfied.

FMT_SMF.1

The SF. Settings management function provides a function to manage the printer password.

Therefore, the requirement FMT_SMF.1 is satisfied.

FMT_SMR.1

The SF. Settings management function maintains the role of the administrator and associates an authenticated subject with the role of administrator.

Therefore, the requirement FMT_SMR.1 is satisfied.

FPT_RVM.1

The SF. User identification function, SF. Print-job management function, SF. Settings management function, and SF. Printer settings function are implemented in a way that they cannot be bypassed.

Therefore, the requirement FMT_RVM.1 is satisfied.

FPT_SEP.1

To prevent interference from unauthorized subjects, SF. User identification function, SF. Print-job management function, SF. Settings management function, and SF. Printer settings function are executed in an independent memory space.

Therefore, the requirement FMT_SEP.1 is satisfied.

8.3.3. Strength of Function Rationale

Table 12 shows the security functions with probabilistic or permutational mechanism in this TOE and the corresponding claim of security strength. On the other hand, as indicated in 5.1.3, the minimum strength of function of this TOE is SOF-basic.

Therefore, they are consistent.

8.3.4. Adequacy of Assurance Measures

Table 13 shows the correspondences between assurance measures and security assurance requirements. As shown by the table, all of the assurance components required by EAL2 are satisfied.

Therefore, all assurance measures are satisfied.

8.4. PP Claims Rationale

This ST does not claim conformance to any PP.