

# Service Manual

Canon BW

**Encrypted Printing Software-A3**

**Canon**



## Application

This manual has been issued by Canon Inc. for qualified persons to learn technical theory, installation, maintenance, and repair of products. This manual covers all localities where the products are sold. For this reason, there may be information in this manual that does not apply to your locality.

## Corrections

This manual may contain technical inaccuracies or typographical errors due to improvements or changes in products. When changes occur in applicable products or in the contents of this manual, Canon will release technical information as the need arises. In the event of major changes in the contents of this manual over a long or short period, Canon will issue a new edition of this manual.

The following paragraph does not apply to any countries where such provisions are inconsistent with local law.

## Trademarks

The product names and company names used in this manual are the registered trademarks of the individual companies.

## Copyright

This manual is copyrighted with all rights reserved. Under the copyright laws, this manual may not be copied, reproduced or translated into another language, in whole or in part, without the written consent of Canon Inc.

***COPYRIGHT © 2001 CANON INC.***

*Printed in Japan*

## Caution










Use of this manual should be strictly supervised to avoid disclosure of confidential information.

---

# Symbols Used



---

This documentation uses the following symbols to indicate special information:

Symbol	Description
	Indicates an item of a non-specific nature, possibly classified as Note, Caution, or Warning.
	Indicates an item requiring care to avoid electric shocks.
	Indicates an item requiring care to avoid combustion (fire).
	Indicates an item prohibiting disassembly to avoid electric shocks or problems.
	Indicates an item requiring disconnection of the power plug from the electric outlet.
 Memo	Indicates an item intended to provide notes assisting the understanding of the topic in question.
 REF.	Indicates an item of reference assisting the understanding of the topic in question.
	Provides a description of a service mode.
	Provides a description of the nature of an error indication.

The following rules apply throughout this Service Manual:

1. Each chapter contains sections explaining the purpose of specific functions and the relationship between electrical and mechanical systems with reference to the timing of operation.

In the diagrams,  represents the path of mechanical drive; where a signal name accompanies the symbol, the arrow  indicates the direction of the electric signal.

The expression "turn on the power" means flipping on the power switch, closing the front door, and closing the delivery unit door, which results in supplying the machine with power.

2. In the digital circuits, '1' is used to indicate that the voltage level of a given signal is "High", while '0' is used to indicate "Low". (The voltage value, however, differs from circuit to circuit.) In addition, the asterisk (\*) as in "DRMD\*" indicates that the DRMD signal goes on when '0'.

In practically all cases, the internal mechanisms of a microprocessor cannot be checked in the field. Therefore, the operations of the microprocessors used in the machines are not discussed: they are explained in terms of from sensors to the input of the DC controller PCB and from the output of the DC controller PCB to the loads.

The descriptions in this Service Manual are subject to change without notice for product improvement or other purposes, and major changes will be communicated in the form of Service Information bulletins.

All service persons are expected to have a good understanding of the contents of this Service Manual and all relevant Service Information bulletins and be able to identify and isolate faults in the machine."



---

---

# Contents

## Chapter 1 Specifications

1.1 Specifications .....	1- 1
1.1.1 Encrypted Printing - Requirements .....	1- 1
1.1.2 Encryption add-in .....	1- 1
1.1.3 Specifications and restrictions .....	1- 2

## Chapter 2 Functions

2.1 Basic Function .....	2- 1
2.1.1 Explanation of Encryption security terms .....	2- 1
2.2 New Function .....	2- 1
2.2.1 Encrypted printing process .....	2- 1
2.2.2 Features of encrypted secure printing .....	2- 2

## Chapter 3 Installation

3.1 Points to Note About Installation .....	3- 1
3.1.1 Points to Note for Installation .....	3- 1
3.2 Checking components .....	3- 1
3.2.1 Checking Items in the Package .....	3- 1
3.3 Installation procedure .....	3- 1
3.3.1 Installation procedure .....	3- 1
3.3.2 Obtaining and Registering the License Key .....	3- 2
3.3.3 Environment conditions for password-protected encrypted secure printing .....	3- 3

## Chapter 4 Maintenance

4.1 Reference matter in market service .....	4- 1
4.1.1 Checking encrypted print jobs .....	4- 1
4.1.2 Add-in information .....	4- 1
4.2 Troubleshooting .....	4- 1
4.2.1 Add-in - Global settings apply to multiple printers .....	4- 1
4.2.2 Add-in - Point and Print cannot be deleted .....	4- 1
4.2.3 Add-in - Poor terminal service operation .....	4- 2
4.2.4 Add-in - Enter Password and Edit Job Information dialog boxes displayed twice .....	4- 2
4.2.5 Add-in - Can't use NetSpot Job Monitor .....	4- 2
4.3 Related Service Mode .....	4- 2
4.3.1 Invalidating the License for Transfer to a Different Device (Level 2) .....	4- 2





---

## Chapter 1 Specifications

---



# Contents

1.1 Specifications .....	1-1
1.1.1 Encrypted Printing - Requirements .....	1-1
1.1.2 Encryption add-in .....	1-1
1.1.3 Specifications and restrictions .....	1-2



## 1.1 Specifications

### 1.1.1 Encrypted Printing - Requirements

The prerequisite requirements for encrypted printing on the iR6570/5570 are described below. Additional requirements for specific models are given in the table below.

1. UFR II Printer Kit-G3 or Multi-PDL Printer Kit-G1
2. HDD functioning normally
3. Encrypted module(Hardware or Software)

T-1-1

Encrypted Printing Software-A3				
iR Model	iR2270/2870/3570/4570	iR6570/5570	iR105/9070/8570/8500/8070/7200	iR7105/7095/7086
Security Expansion Board	USB Application Interface Board-D1	USB Application Interface Board-D1	USB Application Interface Board-D1	Security Expansion Board-F1
PCI Expansion Bus	Standard equipment	Expansion Bus-C1	Standard equipment	Expansion Bus-D1
Necessary memory capacity for Encrypted Printing	512MB	512MB	512MB	1GB
Usable printer function	UFR II Printer Kit-E3	UFR II Printer Kit-G3	UFR II Printer	UFR II Printer

T-1-2

iR C Model	iR C3170/C2570	iR C6870/5870
Security Expansion Board	Security Expansion Board-E1	Security Expansion Board-E1
Necessary memory capacity for Encrypted Printing	768MB	768MB
Usable printer function	Color UFR II Printer Kit-D1	Color UFR II Printer Kit-L1

The Security Expansion Board is not required in order to use the Secure Print feature. However it does improve the iR print processing speed when printing from Windows 2000.

#### Enabling the encrypted secure print feature

The encrypted secure print feature is implemented in the copier firmware, but is disabled by default. It must be enabled using a license key.

#### Compatible OS

For password-protected encrypted secure printing:

- Microsoft Windows XP Professional/Home Edition
- Microsoft Windows 2000 Server/Professional Service Pack 4
- Microsoft Windows Server 2003 (32 bit)

### 1.1.2 Encryption add-in

The encrypted secure print add-in is an option of the encrypted secure print feature which works in conjunction with compatible Canon printer drivers.

T-1-3

Microsoft Windows 2000 Professional/Server	
System	PC/AT CPU: Intel Pentium/133MHz or better processor RAM: (Professional)128MB or greater./(Server)256MB or greater HDD: (Professional) 655MB or greater of free disk space./(Server) 1GB or greater of free disk space
Software	Microsoft Windows 2000 compatible applications
Format	NTFS support only
Service Pack	SP4
Microsoft Windows XP Home Edition/Professional	
System	PC/AT CPU: Intel Pentium/Celeron series 300MHz or better processor RAM: 128MB or greater HDD: 1.5GB or greater of free disk space
Software	Microsoft Windows XPcompatible applications
Format	NTFS support only
Service Pack	
Microsoft Windows Server 2003 (32bit)	
System	PC/AT CPU: Intel Pentium/Celeron series 550MHz or better processor RAM: 128MB or greater HDD: 2GB or greater of free disk space
Software	Microsoft Windows Server 2003compatible applications
Format	NTFS support only

**Add-in for Client PC Pritner Driver support list**

T-1-4

iR or iR C Model Name	UFR II	UFR II	PCL5e/5c	PCL5e/5c	PS	PS
Type	US	UK	US	UK	US	UK
iR C6870N	Support	Support	Support	Support	Support	Support
iR C5870N	Support	Support	Support	Support	Support	Support
iR C3170	Support	Support	Support	Support	Support	Support
iR C2570	Non Support	Support	Non Support	Support	Non Support	Support
iR 2270/2870	Support	Support	Support	Support	Support	Support
iR 3570/4570	Support	Support	Support	Support	Support	Support
iR 85Plus	Support	Support	Support	Support	Support	Support
iR 8070	Support	Support	Support	Support	Support	Support
iR 105i	Support	Support	Support	Support	Support	Support
iR 9070	Support	Support	Support	Support	Support	Support
iR 5570/6570	Support	Support	Support	Support	Support	Support
iR 7086-7105	Support	Support	Support	Support	Support	Support

**Impact on previous secure print and save print functions**

When this Add-in is installed on the printer driver and a checkbox: Use Encrypted Secured Print is marked, existing [Secure Print], [Save] (in BOX), and [FormFile] save become disabled.

Do not specify these functions.

If they are set, a printing job is canceled displaying following error messages.

- Cannot print when Secured Print is set as the Output Method because Encrypted Secured Print is activated.
- Cannot print when Store is set as the Output Method because Encrypted Secured Print is activated.
- Cannot create a form file because Encrypted Secured Print is activated.

**1.1.3 Specifications and restrictions****Handling encrypted secure print jobs**

Password authentication is required only for printed output.

Encrypted secure print jobs can be stopped, restarted, deleted and promoted from the print job status window in the same way as for ordinary print jobs.

**Auto delete for encrypted secure print jobs**

The machine can be set to delete automatically encrypted secure print jobs that have been on hold for a pre-set length of time, which can be set to 1, 2, 3, 6, 12 or 24 hours.

**Restrictions for encrypted secure print jobs**

The following restrictions apply to encrypted secure print jobs.

- a) Encrypted secure print jobs are deleted immediately after printing and cannot be reprinted.
- b) In the event of an interruption in power to the controller while an encrypted secure print job is waiting to print, the job will be deleted.
- c) When an encrypted secure print job is selected in front of the device, none of the job information (including paper input and output options, number of copies and finishing options) can be modified.
- d) Where the PDL data for an Encrypted secure print job is too large to fit on the PDL spooler (HDD), the resulting memory overload generates an error and the job is cancelled. Normally, the maximum number of encrypted secure print jobs that can be stored without printing is the same as the maximum number of secure jobs (for plain text).

**Deletion from remote UI**

Deletion from a remote UI is not supported on this machine, due to the potential for unauthorized access to passwords and key information over the network. Encrypted secure print jobs cannot be browsed from a remote UI for the same reason.

---

## Chapter 2 Functions

---





# Contents

2.1 Basic Function .....	2-1
2.1.1 Explanation of Encryption security terms .....	2-1
2.2 New Function .....	2-1
2.2.1 Encrypted printing process .....	2-1
2.2.2 Features of encrypted secure printing .....	2-2



---

## 2.1 Basic Function

---

### 2.1.1 Explanation of Encryption security terms

#### Encrypted Secured Print Add-in:

This is a software module Canon newly provides. It is installed on host machine, analyzes CPCA job generated by driver, and generates encrypted job.

#### Security Token:

This is a mechanism or a device to conduct identification. It is a generic name for IC card or fingerprint authentication device, etc.

#### AES: (Advanced Encryption Standard)

This is an encryption technology that the National Institute of Standards and Technology (NIST) conducts selecting operation. Compared to DES, the encryption strength and speed have been improved.

This is used in encrypted secure print for Windows XP and Windows Server 2003.

#### 3DES: (3 Data Encryption Standard)

This is an encryption method developed by IBM. The U.S. Department of Commerce has adopted this algorithm.

In 3DES, an encryption process is done three times.

This is used in encrypted secure print for Windows2000.

#### RSA:

This is an algorithm for open key, developed by Ronald Rivest, Adi Shamir, and Leonard Adleman. It is considered as de facto standard on the Internet. They disclaimed the patent in 2000.

#### PBE: (Password Based Encryption)

This is a key generating method based on the input password.

It is relatively weak in terms of the strength as there is a limitation in the number of lines for human to memorize the password.

#### Password:

Common key generated by password encrypts PDL encryption key in encrypted secure print.

Password is used to generate common key in Password version encrypted secure print.

#### POP before SMTP:

This is a method to log in POP server prior to SMTP transmission.

It is an authentication method to continue SMTP transmission only when the client IP address used in SMTP transmission is confirmed to be identical to the IP address POP server has authenticated within the specified time. Mail server authenticates user ID in POP server, informs the authenticated client IP address to SMTP server, and then sends mail in SMTP server. It takes a certain period of time to complete this processing. In consideration of the processing time, 300mSEC idling time is given between POP authentication and SMTP transmission. When POP before SMTP transmission occurs during POP reception, the transmission (POP authentication) has to wait until the POP reception is completed, and POP authentication and SMTP transmission are executed after completing POP reception. An error occurred during POP server connection is treated as transmission error.

#### SMTP AUTH:

This is a method to receive mails only from registered users by conducting user authentication in connecting to SMTP. It is standardized as RFC2554 in March 1999. Using ESMTP protocols, which are expansion of SMTP, and authentication mechanism of SASL (Simple Authentication and Security Layer) stipulated in RFC2222, it conducts user authentication by taking a Server Challenge and responding user ID and password.

#### RFC

RFC stands for Request For Comments.

This is officially issued by IETF (Internet Engineering Task Force).

Standard specifications, such as protocols used on the Internet, are described in it.

RFC documents have a series of control numbers.

RFC documents are de facto standard though IETF is not an international standardization organization.

#### APOP

APOP stands for Authenticated Post Office Protocol.

This protocol encrypts password used at receiving mail in POP3. It generates disposable password every time, and that can prevent password data from being abused by third parties. It becomes available only when both mail server and mail software of client are compatible with APOP. This does not encrypt the body of e-mail.

#### SHA-1

Secure Hash Algorithm 1 is a hash function used to authentication or digital signature. It can detect whether the original is not tampered at some midpoint in communication by comparing the hash values of both ends of the communication path. It is applied to IPsec which encrypts IP packet to send.

---

## 2.2 New Function

---

### 2.2.1 Encrypted printing process

#### Secure printing

Executable via printer driver only.

A document (print data) equipped with numeric password protection is sent to iR from a computer.

A document sent to iR with a numeric password is called a secure print document. A secure print document can be printed without divulging the contents of the document to a person who does not know the numeric password. In order to print a secure print document, the user must enter the numeric password in iR after sending the document data from the computer.

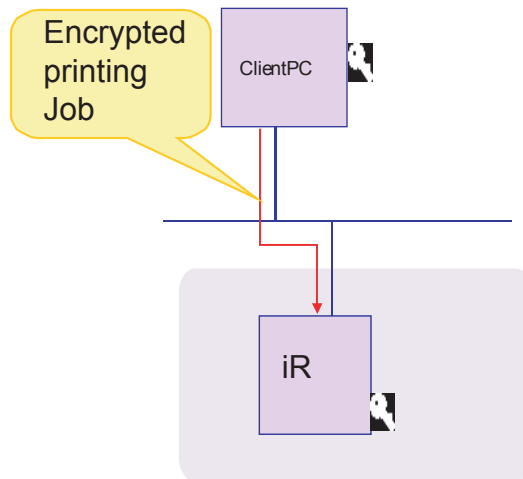
#### Encrypted secure printing

The encryption add-in is added to the printer driver and the selected in the Encrypted-P tab in the printer driver properties.

At the iR end, an iR256 MB expansion RAM is installed to make the 512 MB model, and the license key is entered in the secure print encryption expansion kit to enable encryption.

At the iR C end, an iR256 MB expansion RAM is installed to make the 768 MB model, and the license key is entered in the secure print encryption expansion kit to enable encryption.

Print data can be encrypted prior to transmission from the computer to iR. The user at the iR end enters the password in order to decrypt the encrypted secure document for printing.



F-2-1

The encrypted printing add-in must be installed on all client printer drivers in order to utilize the encrypted printing feature. The add-in can be installed in the following printer drivers.

- \_ Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 or later (Hereafter, PCL5e/5c)
- \_ Canon UFR II Printer Driver for Microsoft Windows Version 1.20 or later (Hereafter, UFR II)
- \_ Canon PS-Roman Printer Driver for Microsoft Windows Version Ver.2.60 or later (Hereafter, PS3)

## 2.2.2 Features of encrypted secure printing

### Features of encrypted secure printing

Secure printing requires the user name and password for printing. Encrypted secure printing provides additional security by encrypting print data sent over the network.

### Compatible PDLs

The encrypted secure printing function is compatible with UFR II, PCL and PS-Roman(PDL formats using CPCA packets).

### Compatible interfaces and protocols

Encryption is performed at the CPCA level and is not interface or protocol dependent. Saving the print driver as a file does not damage the encrypted function.

### Equipment configuration

The required configuration for encrypted secure printing is described below.

#### -HDD

The HDD is used to store jobs in pending status. An HDD must be installed on machines where it is available as an optional extra.

#### -Encryption module

The encryption module is used to decrypt encrypted keys and PDLs.

A software implementation uses an encryption library, while a hardware implementation uses encryption hardware.

---

## Chapter 3 Installation

---



# Contents

3.1 Points to Note About Installation .....	3-1
3.1.1 Points to Note for Installation .....	3-1
3.2 Checking components .....	3-1
3.2.1 Checking Items in the Package .....	3-1
3.3 Installation procedure .....	3-1
3.3.1 Installation procedure .....	3-1
3.3.2 Obtaining and Registering the License Key .....	3-2
3.3.3 Environment conditions for password-protected encrypted secure printing .....	3-3





## 3.1 Points to Note About Installation

### 3.1.1 Points to Note for Installation

This information applies to the following black-and-white machines.

-iR2270/2870/3570/4570  
 -iR6570/5570  
 -iR105/9070/8570/8500/8070/7200

The PCI bus expansion kit is not required on the iR C color machine. The security expansion board, if used, should be an E1 security expansion board.

At least 768 MB of memory is required in order use the security expansion board in conjunction with secure printing.

#### Note

1. Check that the package has not been opened and that the security seal is still intact. If the package is open and/or the security seal is broken, check that this was done by the user.
2. During installation, check that the following options are available. Installation instructions are packaged together with each option.

The following information describes the options required for different forms of password-protected encrypted secure printing.

**-iR2270/2870/3570/4570**  
 -iR 256MB Expansion RAM  
 -USB Application Interface Board-D1

**-iR6570/5570**  
 -iR 256MB Expansion RAM  
 -Expansion Bus-C1  
 -USB Application Interface Board-D1

**-iR105/9070/8570/8500/8070/7200**  
 -iR 256MB Expansion RAM  
 -USB Application Interface Board-D1

#### **iR C3170/C2570/C6870/C5870**

-Security Expansion Board-E1

At least 768 MB of memory is required in order use the security expansion board in conjunction with secure printing.

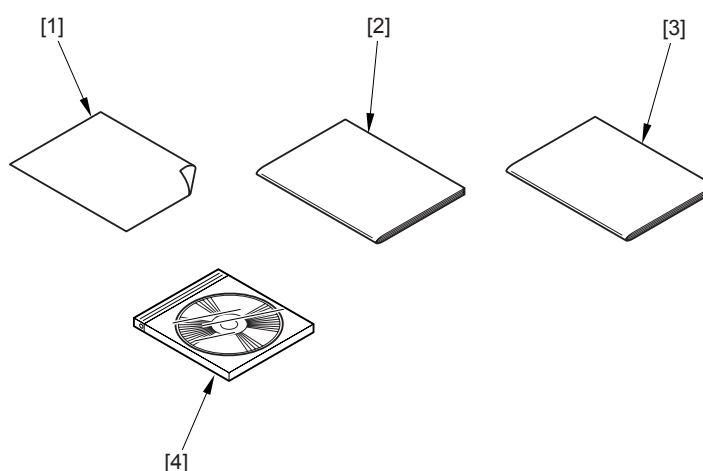
#### PC:

\_\_ Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 or later (Hereafter, PCL5e/5c)  
 \_\_ Canon UFR II Printer Driver for Microsoft Windows Version 1.20 or later (Hereafter, UFR II)  
 \_\_ Canon PS-Roman Printer Driver for Microsoft Windows Version Ver.2.60 or later (Hereafter, PS3)  
 \_\_ Encrypted Secured Print Driver Add-in for Client PC

A minimum of 512 MB of free memory is required. If this is not available, install the optional extra iR 256 MB expansion RAM B1 (NB: not available overseas).

## 3.2 Checking components

### 3.2.1 Checking Items in the Package



F-3-1

[1]	LA Certificate	1 pc
[2]	Licence Registration Booklet	1 pc
[3]	Encrypted Printing Software User Guide	1 pc
[4]	Encrypted Secured Print Driver Add-in CD-ROM	1 pc

## 3.3 Installation procedure

### 3.3.1 Installation procedure

When the secure printing encryption expansion kit A3 is installed, encrypted print jobs can be sent from a computer to the iR, decrypted using the password-protected encrypted secure printing feature, and finally printed.

After completing the steps outlined in 3.1.1 Preparing for Installation, proceed as follows.

### 1. Obtaining and registering the license key

Check that the secure printing encryption expansion kit A3 is functioning normally, in accordance with the password-protected encrypted secure printing environment conditions.

### 3.3.2 Obtaining and Registering the License Key

When ready, obtain the license key from the License Management System (LMS), and install it. As a rule, the user must obtain the license on his or her own. Detailed instructions are given in the User's Guide, and the following is an outline of the procedure:

---

#### MEMO:

#### What is the License Management System?

Commonly referred to as the LMS, it is a new license server scheme set up by Canon Inc. to offer a means of enabling software options installed on an iR engine. The options are centrally controlled by means of licenses with the aim of preventing unauthorized copying. Unlike those conventional methods that rely on PCs or dongles, options are enabled using "license keys." Although different guidelines may be implemented in different countries or sales areas, the user is assumed to perform the acquisition and installation work. An option comes with a license access number certificate. The option becomes enabled when its license key is installed to the iR engine, obtained using the license access number that is unique to the option. The LMS (Web server) is the source of license keys.

When the user feeds the license access number indicated on the license access number certificate and the serial number of the iR device, the LMS will generate a license key that consists of 24 numerals representing the option in question. The license key will contain the device serial number information so that it cannot be used on a different device. This information will be stored in the device's memory and, therefore, the option will remain enabled even when a component is replaced for repairs.

---

#### Obtaining and Installing a License Key

1) Access the LMS using the following URL, and go through the instructions on the display to obtain a license key:

<http://www.canon.com/LMS/license/>



To obtain a license key, you will need the 16-digit number indicated on the license access number certificate and the serial number of the device to which you want to install the license (e.g., ABC01234). You can find out the serial number of an iR device by pressing its Counter key. (The number will appear next to 'Serial No.')

2) Record the 16-digit license key number indicated by the Web browser in the number field of the license access number certificate.

---

#### MEMO:

The 16-digit license key number can be printed out last with LMS.



Be sure that the user does not make a mistake when recording the number. Advise the user to keep the license access number certificate in a safe place.

3) Type in the license key number by making the following selections in user mode: system control settings>license control. Press [Start] to enable the option. An error message will appear if the validation fails. Go through the indicated instructions:

"The license key number may be wrong. Check the number."

>>Be sure that the key in use is one issued for the device in question.

>>Be sure that the key number has been correctly entered.

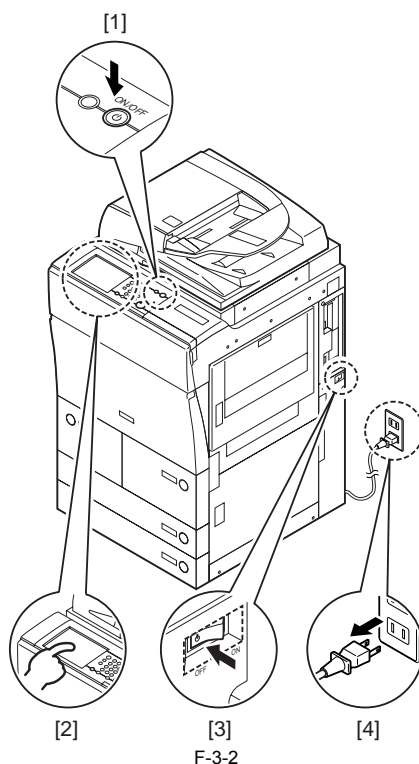
>>Be sure that the key is appropriate.

"The option has already been enabled."

>>Check to see if the option has already been enabled.

4) Hold down the control panel power switch for 3 sec or more. Perform the instructions on the screen to go through the shut-down sequence, allowing you to turn off the main power switch. When ready, turn off the main power switch.

<iR6570/5570 Series>



- 5) Wait for 10 sec; then, turn the main power switch back on.
- 6) See that the registered license has become valid. (The validation takes place when the device is turned back on.)
- 7) When the device started up normally, make the appropriate service mode settings to suit the needs of the user.

### 3.3.3 Environment conditions for password-protected encrypted secure printing

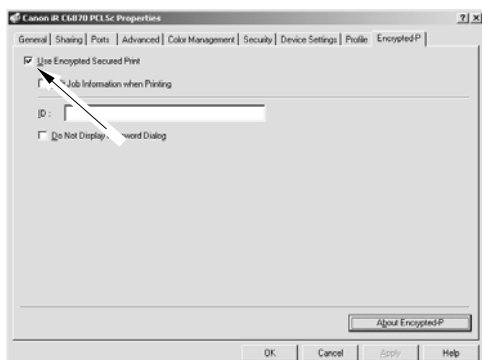
Once installation is complete, check operation as follows.

#### iR:

- It is connected to the user's network.
- The Encrypted Printing Software has been installed, and the appropriate license has been registered.
- The iR engine is capable of receiving and printing UFR II or PCL5e/5c or PS printer driver data from a PC.

#### PC:

- It is connected to the user's network, and appropriate network settings have been made.
  - An UFR II or PCL5e/5c, PS printer driver has been installed, and appropriate printer settings have been made.
  - The Encrypted Secured Print Driver Add-in for Client PC has been installed.
  - The appropriate encryption settings have been made as part of printer settings.
- start>settings>printer (For 'Printer Properties', see that 'Use Encrypted Secured Print' is checked (selected) on the Encrypted-P tab.)



F-3-3

Client PC

T-3-1

Login to the client PC as an administrator and create the printer driver
Install Encrypted Secured Printer Driver Add-in for Client PC
In the printer driver properties window, click on the Encrypted-P tab. Then, It is confirmed that [Use Encrypted Secured Print] is checked.
Print

iR settings

T-3-2

Using the control panel counter keys (123 keys), check that the iR license has been registered correctly. Press the Check Device Configuration button on the counter key window. Encrypted secure printing should be displayed in the list.
Check that encrypted print data can be received normally.
Enter the authorization password on the iR control panel and print.

---

## Chapter 4 Maintenance

---



# Contents

4.1 Reference matter in market service .....	4-1
4.1.1 Checking encrypted print jobs.....	4-1
4.1.2 Add-in information.....	4-1
4.2 Troubleshooting.....	4-1
4.2.1 Add-in - Global settings apply to multiple printers .....	4-1
4.2.2 Add-in - Point and Print cannot be deleted .....	4-1
4.2.3 Add-in - Poor terminal service operation .....	4-2
4.2.4 Add-in - Enter Password and Edit Job Information dialog boxes displayed twice .....	4-2
4.2.5 Add-in - Can't use NetSpot Job Monitor .....	4-2
4.3 Related Service Mode .....	4-2
4.3.1 Invalidating the License for Transfer to a Different Device (Level 2).....	4-2





## 4.1 Reference matter in market service

### 4.1.1 Checking encrypted print jobs

The following minimum configuration is required to check the operation of password-protected encrypted secure printing.

#### Computer

- Encryption Secure Print Driver Add-In for Client PC
- PC running Windows 2000/XP/Server 2003
- Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 or later (Hereafter, PCL5e/5c)
- Canon PS-Roman Printer Driver for Microsoft Windows Version Ver.2.60 or later (Hereafter, PS3)
- Canon UFR II Printer Driver for Microsoft Windows Version 1.20 or later (Hereafter, UFR II)

#### iR

Secure printing encryption function expansion enabled

#### Connection

- One-to-one connection from computer to iR using Ethernet cross cable.
- Ethernet addressed registered in computer and iR.
- Ping test successful.
- Establish port connection in properties window of printer driver on computer.
- Test print successful.

#### Operation

- Printer driver properties > [Encrypted-P]Tab. Check [Use Encrypted Secured Print] checkbox.
- Perform a test print via the control panel system status --> print --> secure print at the iR. If the printing instruction from the computer is successful, encrypted secure printing is operating normally.

#### Note:

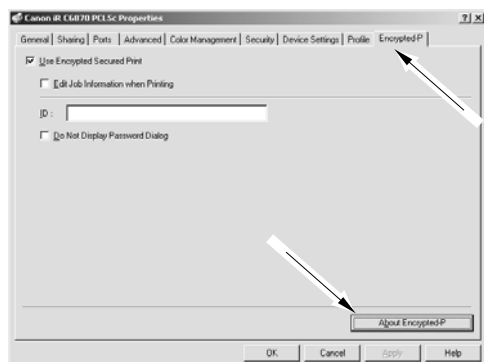
For secure printing without encryption, PDL data is processed upon arrival at the iR before being stored in the HDD. For encrypted secure printing, the PDL data is stored as is without further modification. Thus, printing time for encrypted secure printing at the iR takes longer on account of the additional PDL processing time. A high level of security is provided, since the contents of the HDD cannot be accessed by third parties.

### 4.1.2 Add-in information

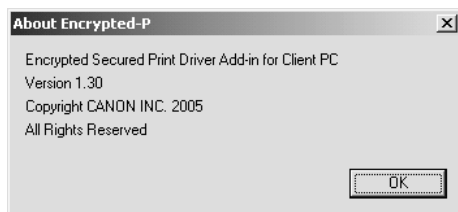
Information about installed add-ins can be viewed by selecting "About Encrypted-P" in the printer driver.

#### Procedure

1. Click on "About Encrypted-P" on the Encrypted-P tab sheet page in the Printer Properties to display the version number of the Encrypted Secured Printer Driver Add-in for Client PC.



F-4-1



F-4-2

## 4.2 Troubleshooting

### 4.2.1 Add-in - Global settings apply to multiple printers

#### Condition

Where multiple printers exist, selecting ID and Don't Show Password Input Dialog Box in the Encrypted-P tab of any one printer will change the settings in the Encrypted-P tabs of all printers.

#### Cause

Where the add-in is installed in the printer driver, it must be started. ID and password settings cannot be modified for individual printers. This is part of the basic specifications of this security add-in, and is designed to prevent the add-in functionality from being bypassed and rendered inoperable.

#### Response

Basic specifications of the add-in.

### 4.2.2 Add-in - Point and Print cannot be deleted

#### Condition

For client PCs running Windows XP Home/Professional Edition or Windows Server 2003 where the add-in has been installed using Point & Print, deleting the add-in or driver from the PC where the original driver was installed using the add-in uninstaller does not result in removal of the target add-in or printer driver from the client PC.

#### Cause

This is caused by problems in the Point & Print operating environment in connection with OS specifications (and associated bugs) related to file handling and updating printer drivers on the server. If files associated with printer drivers and add-ins installed on the server are deleted, printer drivers on the client side will not be updated automatically.

**Response**

The following procedure is required when synchronizing the printer driver versions installed with Point & Print between client and server PCs.

1. Delete the printer driver, add-in or both on the server PC.
2. Run the uninstaller on the client PC as for the server PC.

**4.2.3 Add-in - Poor terminal service operation**

**Condition**

Where terminal services are used with password-protected Encrypted Secure Printing version, proper password transmission between the server and clients cannot be guaranteed.

**Cause**

Server-client communication in terminal services is implemented as a Windows function and cannot be administered using the add-in.

**Response**

The response must be taken at the user end, since printing via terminal services is outside the scope of the operation guarantee for the add-in.

**4.2.4 Add-in - Enter Password and Edit Job Information dialog boxes displayed twice**

**Condition**

In an application such as Word, clicking Cancel in the Enter Password or Edit Job Information dialog box causes the dialog box to be displayed again.

**Cause**

In an application such as Word, clicking Cancel in the Enter Password or Edit Job Information dialog box causes the dialog box to be displayed again.

**Response**

Basic specifications of the add-in.

**4.2.5 Add-in - Can't use NetSpot Job Monitor**

NetSpot Job Monitor (NSJM) is not compatible with this add-in. When the add-in is installed and Encrypted Secure Printing is selected, NSJM will not operate properly.

---

**4.3 Related Service Mode**

---

**4.3.1 Invalidating the License for Transfer to a Different Device (Level 2)**

**Service Mode Item Used to Invalidate a License for Transfer to a Different Device (Level 2)**

**Possible Situation**

A license may be used on a different device through transfer, as when replacing the device at the end of a lease agreement. To do so, the user must first invalidate the existing license by performing a set of steps referred to as "invalidation of a license" using service mode. At times, both source and target of transfer may be the same device, and a license therefore may also be invalidated only temporarily. It is important to note that the user must contact the Sales Company to make a license good regardless of whether it has been invalidated intentionally or inadvertently.

**Invalidation Procedure**

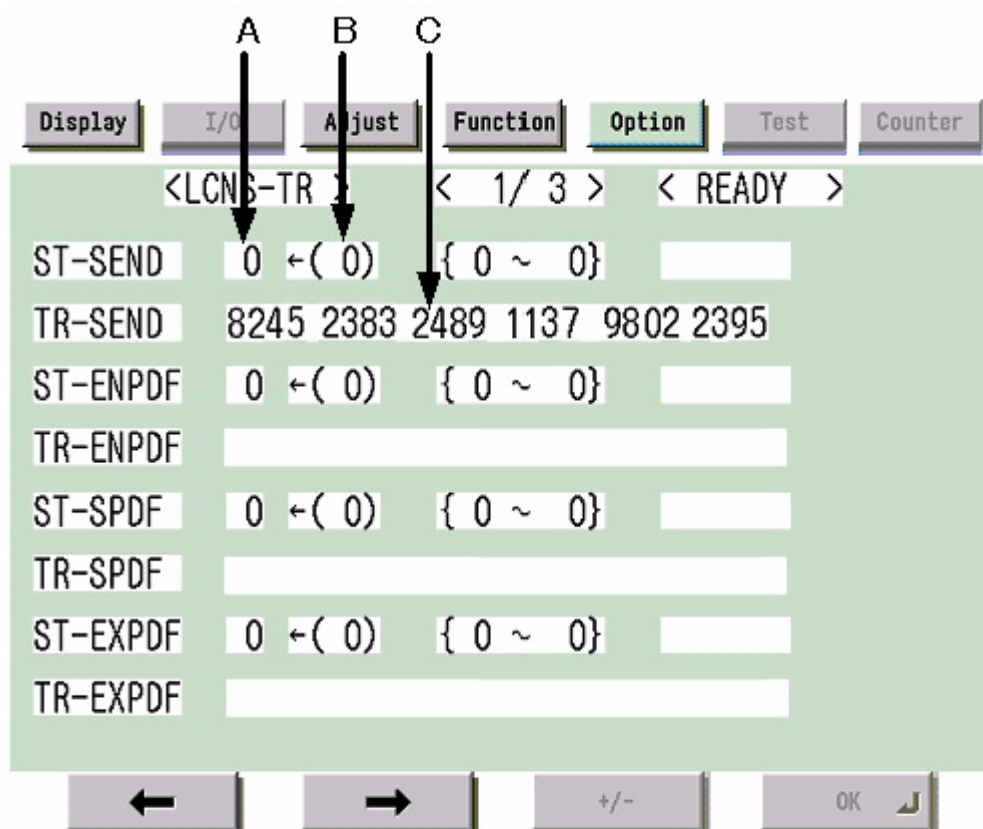
Invalidation consists in invalidating the license in service mode and generating an invalidation certificate that proves the completion of invalidation. Invalidation may take place for individual optional functions, and a specific function becomes no longer available as soon as an invalidation certificate is issued. The user contacts the Sales Company and provides the following: the invalidation certificate, the device serial number of the source of transfer, the device serial number of the target of transfer, reason of transfer. In response, the Sales Company may issue a license key for new installation on a different device. The user must take note of the new license key in writing, and keep it as a record after registering it to the target device.

**Installation Procedure**

1. Start service mode, and activate Level 2 so that the following is true:

COPIER>OPTION>LCNS-TR

The following screen appears, showing the current status of various options:



F-4-3

**Screen Design:**

**SET-xxxx:** indicates the license status. If installed, the option is identified as '1' under A.

To invalidate an option for transfer, select it, and type in '0' under B; then, click [OK] so that the option will be invalidated and an invalidation certificate will be issued.

**TR-xxxx:** indicates any invalidation certificates that have been generated under C.

**xxxx may be any of the following:**

**SEND:** SEND function

**ENPDF:** encryption PDF

**SPDF:** searchable PDF

**EXPDF:** PDF function expansion (encryption PDF + searchable PDF)

**LIPS:** LIPS function

**PDFDR:** PDF Direct print function

**SCR:** encryption secured printing

**HDCLR:** HDD encryption + full deletion (Security Kit)

**BRDIM:** BarDIMM

**VNC:** Remote Operators Software

**WEB:** Web Access

**HRPDF:PDF** High Compression

**Memo:**

Not all foregoing options are available in all countries and regions.

2. If an option has already been installed, '1' will be indicated under A. If you want to invalidate it, select it, and type in '0' so that the indication under B will change to '0'.
3. Thereafter, when [OK] is pressed, the indication under A will change to '0' and, at the same time, an invalidation certificate will be indicated in the form of a number. Take note of it in writing together with the serial number of the target device.
4. When the target device is ready, check its serial number.
5. Contact the Sales Company, and provide the following: invalidation certificate for transfer, serial number of the source device, serial number of the target device. The Sales Company, in response, may issue a new license key that may be registered on the target device.
6. Register the new license key to the target device, and check to make sure that the function has been enabled.



Nov 14 2005

**Canon**