



Secure Printing with ISPP in the Intermate100 and Intermate101

**Supplement to the
Print Server Administration Manual 7th Edition**

9 December 2002

NOTICES

Disclaimers

Intermate A/S makes no warranty of any kind with regard to the contents or use of this document, and specifically disclaims any express or implied warranties on merchant ability or fitness for any particular purpose.

Intermate A/S shall not be liable for errors contained herein or for incidental or consequential damages in connection with the performance or use of this product.

Information in this document is liable to change without notice and does not represent a commitment on the part of Intermate A/S.

Trademarks

Intermate is a registered trademark of Intermate A/S.

VPS/Secure is a registered trademark of LRS - Levi, Ray & Shoup, Inc.

Any other trademarks appearing in this document are the property of their respective owners.

Copyrights

© Copyright Intermate A/S 2002. All rights reserved. No part of this document may be copied or reproduced in any way, except where noted, without the written consent of Intermate A/S.

Intermate A/S
Kongevejen 194 A
3460 Birkerød
Denmark

www.intermate.com

TABLE OF CONTENTS

1. Introduction to the document	4
2. Secure Printing with ISPP	5
2.1 Basic principles.....	5
2.2 Current system requirements and limitations	5
2.3 Network Destination Option (NDO) and Secure Printing	6
3. Setting Key and Key Size	6
4. Raw socket ports	8
4.1 Using the dedicated ISPP raw socket port	8
4.2 Making normal raw socket ports secure	8
5. Secure IPDS printing	10
A. Exploiting NDO with secure printing	11

1. Introduction to the document

Products covered

This document applies to the following Intermate multi-protocol print servers:

- Intermate100 (based on the G22 software)
- Intermate101 (based on the G32 software)

Scope and purpose of the document

This document updates and brings together the following material:

- Entirely new material on configuration of keys and key size on the [ISPP] page in the Configurations > Basic group.
- Extracts from the chapter on configuring raw socket services from the "Intermate100 and Intermate101 Print Server Administration Manual" (7th edition, 25 June 2002, gg-00-07) .
- An extract of material on IPDS settings from the "Printing Environment Guide for IBM Mainframe Hosts" (3rd Edition, 25 June 2002, PEG-Main-03).

At present, the document is a supplement to the manuals mentioned above. The material will be worked into future editions of these manuals.

2. Secure Printing with ISPP

2.1. Basic principles

This print server uses the Interimate Secure Print Protocol for secure printing. The **ISPP** is designed for providing print language independent and protocol independent encrypted (secure) printing from a host through a TCP/IP based print server (such as the Interimate101).

The print server functions as **decryption hardware**. It receives print jobs encrypted at the host, decrypts the data, and sends the jobs to the target printer.

Output is controlled—as always in this print server—via logical printers and/or via direct targeting (if you have the Network Destination Option, NDO).

User-configurable settings include encryption/decryption key and length plus configuration of the ports which can be secured.

2.2. Current system requirements and limitations

License key from Interimate

You must have a licence key for ISPP on the Interimate print server.

Only IBM Mainframe Hosts running VPS/Secure™

At this time, the implementation of ISPP in this print server only covers printing from IBM Mainframe Hosts. The host in question (OS/390 mainframe) must be running VPS/Secure™ from LRS (Levi, Ray & Shoup, Inc.). Product information can be found at http://www.lrs.com/EOM/OP_VPS_Secure.htm.

About encryption/decryption key and key size

VPS/Secure™ enables the user to specify the encryption/decryption key and key length. This can either be done at the host or through the decryption hardware (this print server) by using its native menus. The use of native menus is described in “[Setting Key and Key Size](#)” [page 6].

About the secure ports in this implementation

The ISPP implementation is currently limited to the Raw Socket protocol for standard print (e.g. PCL) and the PPD/PPR protocol with IPDS print in mind. Up to 6 secure ports can be configured:

- a dedicated secure raw socket port [page 8]
- 4 standard raw socket ports page [page 8], and
- the IPDS TCP port [page 10].

2.3. Network Destination Option (NDO) and Secure Printing

The print server's NDO functions are the same whether or not you use secure printing. We have found, however, that some users find it helpful to see examples which are specifically tailored to secure printing; these examples are found in the appendix to this document, "[Exploiting NDO with secure printing](#)" [page 11].

3. Setting Key and Key Size

When you leave all settings at their default and the host encryption software is properly configured, the host will initialize contact using an installation key and then deliver a fully functional user key (AES Key Size 16) to the print server.

If you need to change these settings, use the [Secure Printing (ISPP)] page in the Configurations > Basic group, as shown in figure 1 [page 7].

Important The same key is used for all secure ports.

Figure 1 Key configuration

Parameter	Values and comments (* marks the default setting for a parameter)
AES Key Size	AES16*, AES24, AES32
AES Decryption Key [Encoded bytes max:32]	<p>This field is for manual entry of a key. Default is blank.*</p> <p>A typed-in key must be entered as a binary string following the conventions shown in the appendix on "String Syntax" in the "Print Server Administration Manual". You may, but do not have to, choose a different AES Key Size than the default AES16.</p> <p>If you want to prevent a host from sending a key which will replace the manually entered key, be sure to disable "Allow Host Change of Key".</p> <p>If you type in a key, consult your VPS/Secure™ documentation or your network administrator for information on how to enter this key on the host.</p>
Enable Installation Key	<p>Yes*, No.</p> <p>The "installation key" is the hard-coded AES16 key delivered as factory default on all of our print servers. It is only used to get things started (communication initialization and line initialization). It cannot be used for printing.</p> <p>Using this function is completely independent of the method you choose for delivery of fully functional keys (manual key entry (above) versus allowing the host to send a key to the print server (below)).</p>
Allow Host Change of Key	<p>Yes*, No.</p> <p>"Host change of key" means "host-requested change of the user key".</p> <p>If the host tries to send a key and you have disabled "Allow Host Change of Key", the print server will respond with an error code.</p> <p>Multiple hosts: If the print server will be receiving jobs from more than one host, disable "Allow Host Change of Key". Otherwise you risk getting jobs from one host blocked by another host if that host changes the key.</p>

4. Raw socket ports

4.1. Using the dedicated ISPP raw socket port

The [ISPP Port] page in the Configurations > Input Control group can be used to change the port number for this dedicated port from the default setting (9111), and/or to specify "Output to".

Make sure that the port number you use matches an appropriate printer definition and that you do not use this number in any of your normal Raw Socket definitions on the print server

Please consult the "Print Server Administration Manual" if you want some tips about choosing TCP Port numbers for each raw socket service—and/or if you need help in understanding how to use "Output to".

Remember to **Save & Cont.** and then **Reboot** to activate

Important At this time, only jobs from an IBM mainframe host running VPS/Secure™ can be processed.

4.2. Making normal raw socket ports secure

As a supplement to using the dedicated ISPP raw socket port, you can secure one or more of the normal Raw Socket services on the print server.

Important If you choose to enable Secure Print (ISPP) on a given port, please remember that this port will only accept encrypted jobs. In addition, at this time, only jobs from an IBM mainframe host running VPS/Secure™ can be processed.

The configuration page to use is [Raw Socket] in the Configurations > Input Control group.

Below, [2 \[page 9\]](#), is a screen shot showing the first two of the four possible raw socket services you can configure.

TCP Port 2 has been given port number 9101 and has been made secure using the radio button provided.

Figure 2 *Securing a normal raw socket service*

TCP Port 1

TCP Port 1 : [min=1024, max=65500]

Output to : ▼

Secure Print (ISPP) : Yes
 No

TCP Port 2

TCP Port 2 : [min=1024, max=65500]

Output to : ▼

Secure Print (ISPP) : Yes
 No

Please consult the "Print Server Administration Manual" if you want some tips about choosing TCP Port numbers for each raw socket service—and/or if you need help in understanding how to use "Output to".

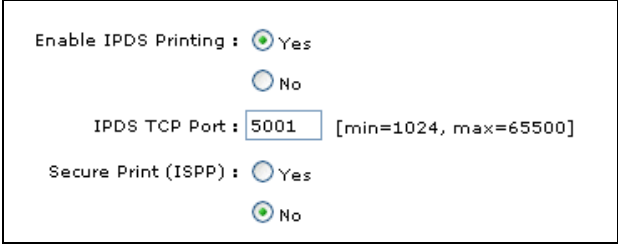
Remember to **Save & Cont.** and then **Reboot** to activate

5. Secure IPDS printing

Use the [IPDS] page in the Configurations > IPDS Option group.

Below, is a screen shot of the top of that page.

Figure 3 [IPDS] page, top - port definition



The screenshot shows a configuration interface with the following elements:

- Enable IPDS Printing :** A radio button group with Yes and No.
- IPDS TCP Port :** A text input field containing the value `5001`, followed by a range constraint `[min=1024, max=65500]`.
- Secure Print (ISPP) :** A radio button group with Yes and No.

Choose your IPDS TCP Port (default is 5001) and secure the port by changing the Secure Print (ISPP) setting from No to Yes. The port will not accept non-encrypted jobs.

Remember to **Save & Cont.** and then **Reboot** to activate

Important

At this time, only jobs from an IBM mainframe host running VPS/SecureTM can be processed.

Appendix A. Exploiting NDO with secure printing

If you want to be able to use more than one network destination to print decrypted print jobs to, choose one of the following two models.

- A** Differentiation by port and direct targetting.
- B** Differentiation by using logical printers and load balancing. Load balancing requires that all of the physical printers in a load balancing pool are identical.

The following examples assume that you want to use all of your network destinations as well as the local printer. The examples only show the configuration of Raw Socket ports; we return to the question of IPDS at the end of the examples.

A. Example of differentiation by port and direct targetting

Example 1 A solution could look like this:

[Raw Socket] page in Configurations > Input Control:

- TCP Port1, 9100, Secure Print Yes, Output to Local Printer
- TCP Port2, 9101, Secure Print Yes, Output to Network Destination 1
- TCP Port3, 9102, Secure Print Yes, Output to Network Destination 2
- TCP Port4, 9103, Secure Print Yes, Output to Network Destination 3

[ISPP Port] page in Configurations > Input Control:

- TCP Port 9111, Output to Network Destination 4

Note that this solution makes no raw socket ports available to receive unencrypted jobs.

B. Examples of differentiation with logical printers

Example 2 Define a pool as the target for a logical printer

- For the sake of example, let us say that you have done this with Logical Printer 6, and the pool includes all of the 5 physical printers known to the print server.

[ISPP Port] page in Configurations > Input Control:

- TCP Port 9111, Output to Logical Printer 6

This leaves all of your usual Raw Socket ports free to receive unencrypted jobs.

Example 3 More than one pool as targets.

If you are not able to put all of the physical printers in a single pool, spread them out over two pools. For example:

- Logical Printer 6 is defined with Local Printer (0 in the pool) plus Network Destinations 2 and 3
- Logical Printer 7 is defined with Network Destinations 1 and 4

[Raw Socket] page in Configurations > Input Control:

- TCP Port4, 9112, Secure Print Yes, Output to Logical Printer 6

[ISPP Port] page in Configurations > Input Control:

- TCP Port 9111, Output to Logical Printer 7

This takes up one of your usual Raw Socket ports leaving the other free to receive unencrypted jobs.

What about IPDS?

The configurations shown in the examples above do not affect IPDS. You can secure the IPDS TCP Port and select any target you want in "Output to" on the basic [IPDS] page in the "Configurations > IPDS Option" group.

If you use direct targetting, you can reach one of your physical printers. If you use logical printers and can define a load balancing pool, you can target all of the printers in the load balancing pool.

Important: Even though you choose Load Balancing, you are still limited to a single IPDS host session. Load Balancing can still be worthwhile, for example to handle several different jobs within the session or to send a job to the printer with the least load in the defined pool.

Need to know more about logical printers and/or NDO?

Please consult the Print Server Administration Manual.