



Secure Socket Layer (SSL)

Last Updated: 11th March 2007

Author: James Evans (BIE P&S Product Planning)

Machines included:

HL-4040CN	✓
HL-4050CDN	✓
HL-4070CDW	✓
DCP-9040CN	✓
DCP-9045CDN	✓
MFC-9440CN	✓
MFC-9840CDW	✓

Contents

- 1) Basic overview
- 2) Brief history
- 3) Benefit of using SSL
- 4) How to Use
- 5) Technical Overview

1: Basic Overview

Secure Socket Layer (SSL) is an effective method of protecting data which is sent over a local or wide area network and is now available on Brothers range of colour laser network machines. It works by encrypting data sent over a network, i.e. a print job, so anyone trying to capture it will not be able to read it as all the data will be encrypted.

It can be configured on both wired and wireless networks and will work with other forms of security such as WPA keys and firewalls.

2: Brief History of SSL

SSL was originally created to secure web traffic information, in particular data sent between web browsers and servers. For example, when you use Internet Banking and you see https:// and the little padlock in bottom right hand corner of the web browser, you are using SSL. It then grew to work with other applications such as telnet, printers and FTP software in order to become a universal solution for online security. Its original design intentions are still being used today by many online retailers and banks to secure sensitive data, such as credit card numbers, customer records etc.

SSL uses extremely high levels of encryption and is trusted by banks all over the world since it is unlikely that it will be broken. According to VeriSign™, a leading online SSL Certificate Authority (CA)¹, it would take a hacker 'well over a lifetime' to hack through a standard SSL encrypted document.

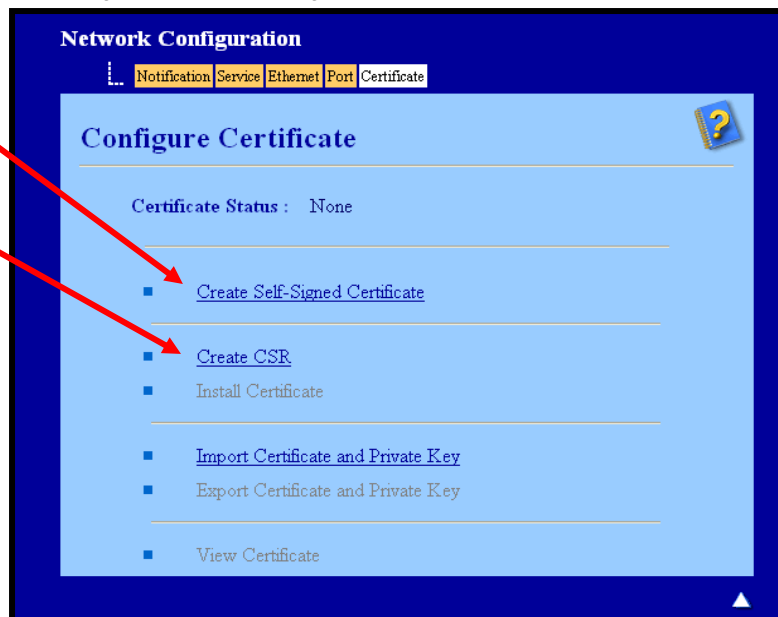
3: Benefit of using SSL

The sole benefit to using SSL on Brother's colour laser network machines is to provide secure printing over an IP network by restricting unauthorised users from being able to read data sent to the printer. Its key selling point is that it can be used print confidential data securely. For example, a HR department for a large company may be printing wage slips on a regular basis. Without encryption, the data contained on these wage slips can be read by other network users. However, with SSL, anyone trying to capture the data will only see a confusing page of code and not the actual wage slip.

4: How to use (standard Install)

Printing over a secured network requires a digital certificate to be installed on both the printer and device which is sending data to the printer, e.g. a computer. In order to configure the certificate, the user needs to log onto the printer remotely through a web browser using its IP address and click on 'network configuration' then 'configure certificate'. From here, the user has two options:

1. To create and install a self signed certificate
2. To use a certificate from a Certificate Authority¹ (CA)



¹ CA is an external body who attests to the credentials on a digital certificate.

4.1. Creating a self signed certificate

After clicking on 'Create Self-Signed Certificate', you will need to enter a hostname name or IP address, followed by an expiry date (this is usually filled in) and click on 'Submit'. The machine will then write this information into a certificate.

The screenshot shows the 'Network Configuration' interface with the 'Certificate' tab selected. The 'Create Self-Signed Certificate' dialog box is open, displaying the following information:

- Common Name:** BRN8A87EC (Input FQDN or IP address, Host name)
- Valid Date:** 14 / 02 / 2012 23:59:59 UTC (DD / MM / YYYY)

Buttons for 'Cancel' and 'Submit' are visible. A red arrow points from the 'Submit' button to a second dialog box titled 'Writing Data to the machine'.

After a few moments, you will be asked how secure you want the SSL connection to be by disabling certain functions.

Brother recommends disabling the Telnet, FTP, TFTP protocols and the network management with older versions of BRAdmin (2.8 or less) for secure communication. If you enable them, user authentication is not secure.

The dialog box contains the following text:

By using the configuration that you specified, this printer is enabled in secure communication mode. Changing the configuration of the following functions is recommended for secure communication. Please confirm the items you want to change, and click the 'OK' button. Check the box on the left of the function you would like to disable and click the "OK" button. (See Network User's Guide.)

- Disable Telnet
- Disable FTP
- Disable TFTP
- Disable network management with older versions of BRAdmin

An 'OK' button is located at the bottom of the dialog.

4.2. Creating a Certificate Signing Request (CSR)

A CSR is a request sent to a CA in order to authenticate the credentials contained within the certificate.

After clicking on 'Create CSR' you will need to input your company details then click 'next'. Your company details are required so that a CA can confirm your identity and attest to the outside world.

Network Configuration

Notification Service Ethernet Port Certificate

Create CSR

Common Name (Required)
(Input FQDN or IP address, Host name)

Organization

Organization Unit

City/Locality

State/Province

Country/Region (Ex. 'US' for USA)

Cancel Submit

Network Configuration

Create Self-Signed Certificate

Writing Data to the machine

After a few moments, you will be presented with the certificate, which can be saved into a small file or copied and pasted directly into an online CSR form offered by a Certificate Authority. Examples of Certificate Authorities include VeriSign™ and Thawte™. Brother recommends you follow your CA policy regarding the method to send a CSR to your CA.

Network Configuration

CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBsTCCARoCAQAwcTESMBAGAlUEAxMjQ1J0OEE4NOVDMSUwIwYDVQQKExxCcm90
aGVyIEIudGVybmFOaW9uYWwgRXVyb3B1MRIwEAYDVQQHEw1BdWRlbnNoYXcxEzAR
BgNVBAGTK1hhbnNoZXN0ZXIxCzAJBgNVBAYTAkdCMIGfMAAGCSqGSIb3DQEBAQUA
A4GNADCBiQKBggQDeP4G1/qwcg6y1vV1gRkpPBec3cdUm6nbWW//31QvVWavIxSOM
6TmF+GWIUudGtS11frYrd/oncw3PpHQ/EA9rLBcmCfxIar7PLN3sdpTb4BkUSg9j
cgj9CwJctG/qdrcHQjvgBH/OqViS3GjNCayswOQeBDRHI95UBVp2H2G86QIDAQAB
oAAwDQYJKoZIhvcNAQEFBQADgYEA03ULxhc4S2682s69PC8sAg/7LMnkfTm2QnGx
13S/jKBW4+GYTgWOFYBDQsST4Z35hExgmJte6mTV1ZK2+9YM5a3fm+QIMQ6K7jG1
R21LW1Z+cXMqMRn6XiD/UpNd1aBEGELuokslocKZJoJ3GcP14WE4CD/kbYUqJ9ge
PYvMS7Y=
-----END CERTIFICATE REQUEST-----
```

Return Save

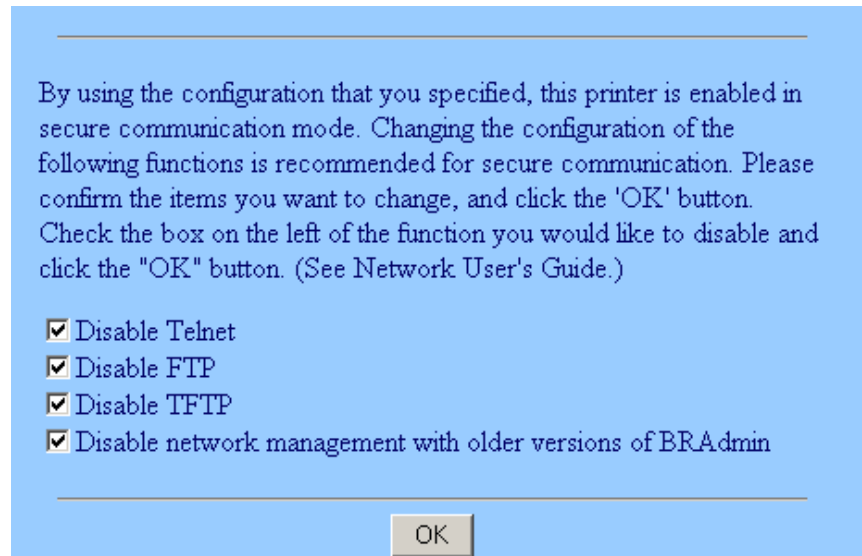
When you receive the certificate from a CA, follow the steps below to install it into the print server (Only a certificate issued with this printer's CSR can be installed).

Click Install Certificate on the configure certificate page.



Specify the file of the certificate that has been issued by a CA then click Submit. Now the certificate has been created successfully, check the box on the left of each function you want to disable and then click OK.

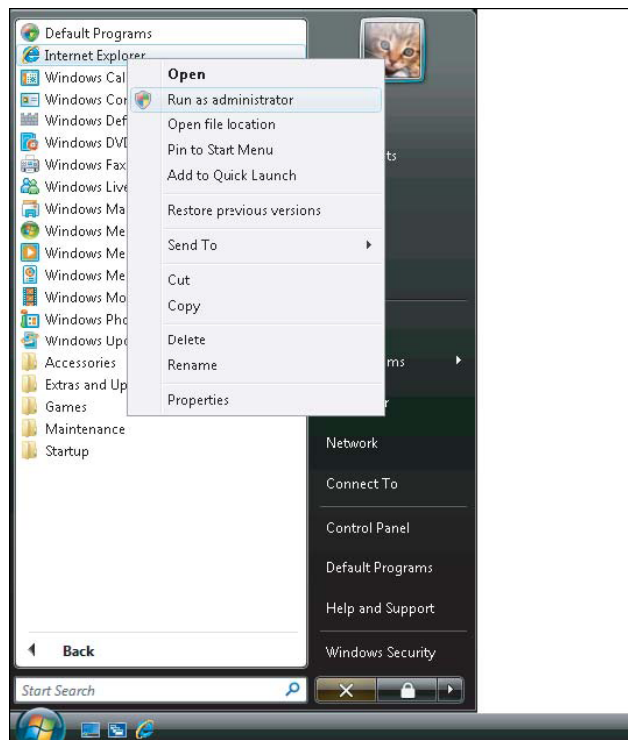
Brother recommends disabling the Telnet, FTP, TFTP protocols and the network management with older versions of BRAdmin (2.8 or less) for secure communication. If you enable them, user authentication is not secure.



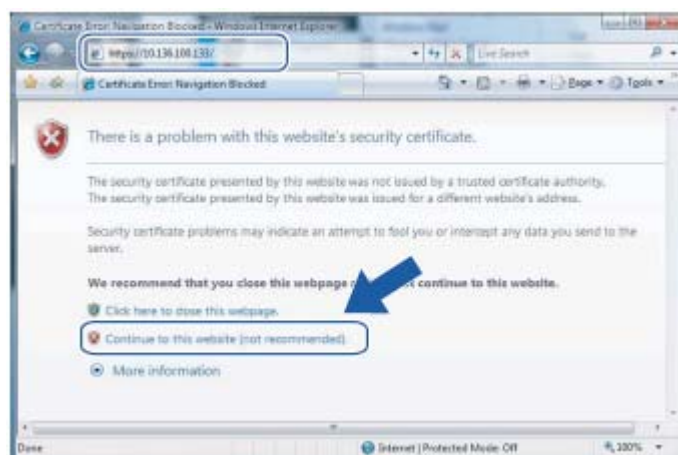
Restart the printer to activate the configuration.

4.3 Installing the certificate onto Windows Vista™

Firstly, log on your computer with Administrator rights. Click 'Start' and 'All Programs'. Then, right click 'Internet Explorer', and then click 'Run as administrator'.



Click on 'Continue to this website'

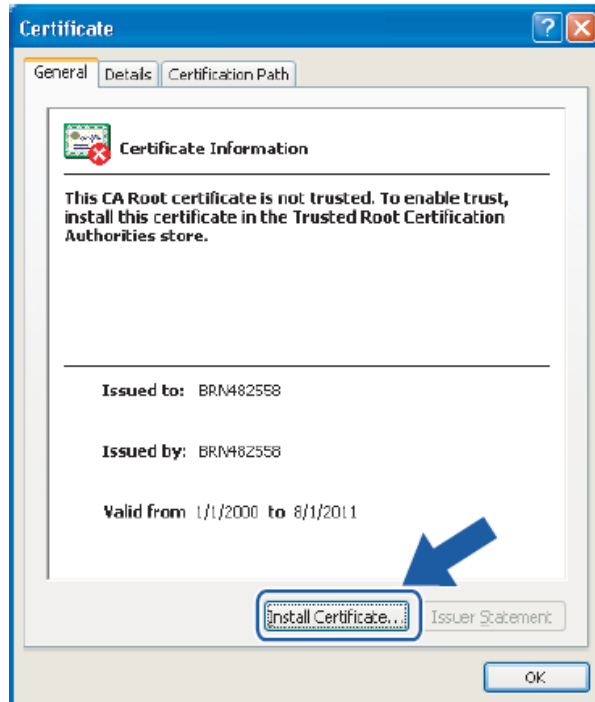


Click 'Certificate Error' then click 'View certificates'. For the rest of installation, please go to section 4.4.



4.4 Installing the certificate onto Windows® XP.

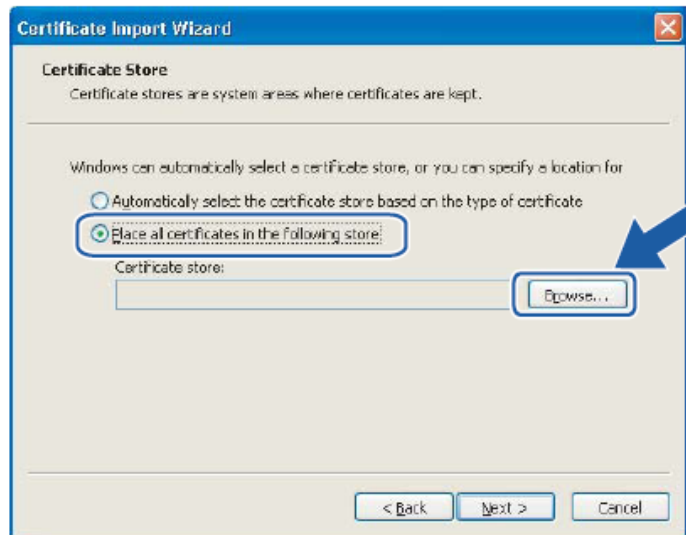
Launch Internet Explorer and type "https://printer's IP address/" into your browser to access your printer. After this, click 'view certificate' then 'install certificate'.



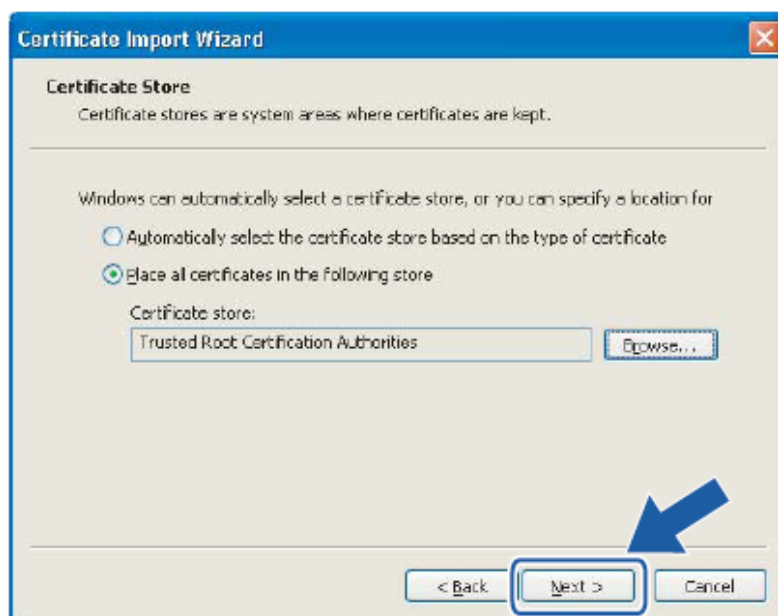
You will be then be presented with the 'Certificate Import Wizard'. Press 'next' to enter.



You will now need to specify a location to install the certificate. Brother recommends you select 'Place all certificates in the following store' and clicking 'browse'



Then, choose 'Trusted Root Certificate Authorities' and click 'OK' followed by 'next'



On the next screen, simply click 'finish'. You will then be asked to install the certificate, which can be done by clicking 'Yes'.

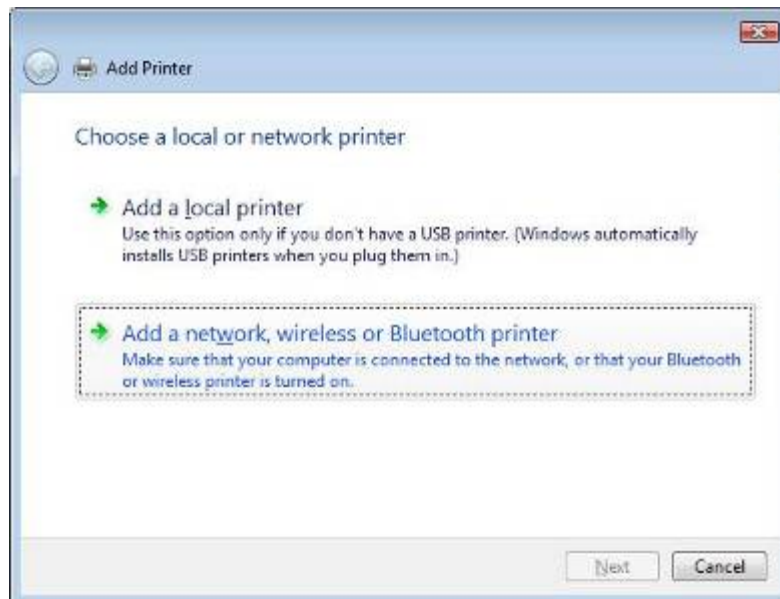
Each computer wanting to print securely must do the same. However, once it has been installed, these steps will not need to be repeated unless the certificate changes.

Secure printing will only occur when configured with the Internet Printing Protocol² (IPP) and not over a standard network installation. To configure IPP, please refer to the network user guide,

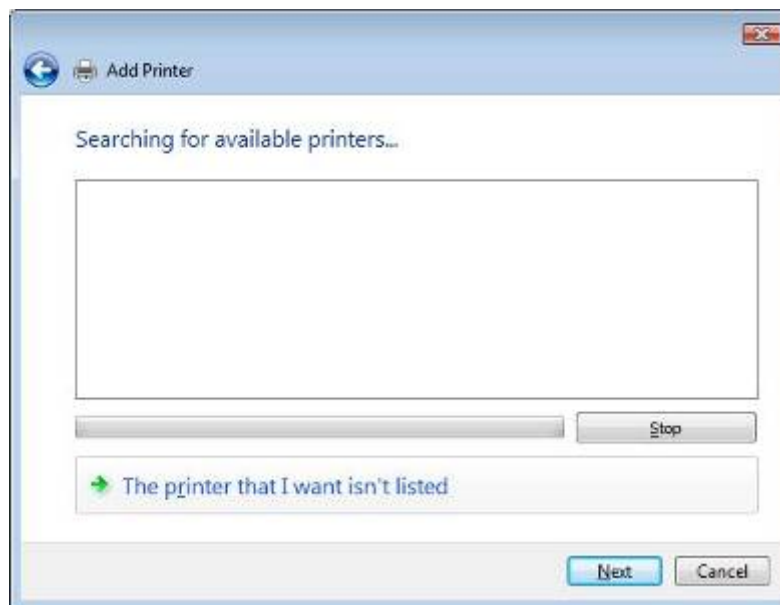
² IPP is a standard printing protocol used for managing and administering print jobs. It can be used both locally and globally so anyone in the world can print to the same printer

4.5 Configuring IPP onto Windows Vista™

Enter the 'Add printer Wizard' and click 'Add a network, wireless or Bluetooth printer'.



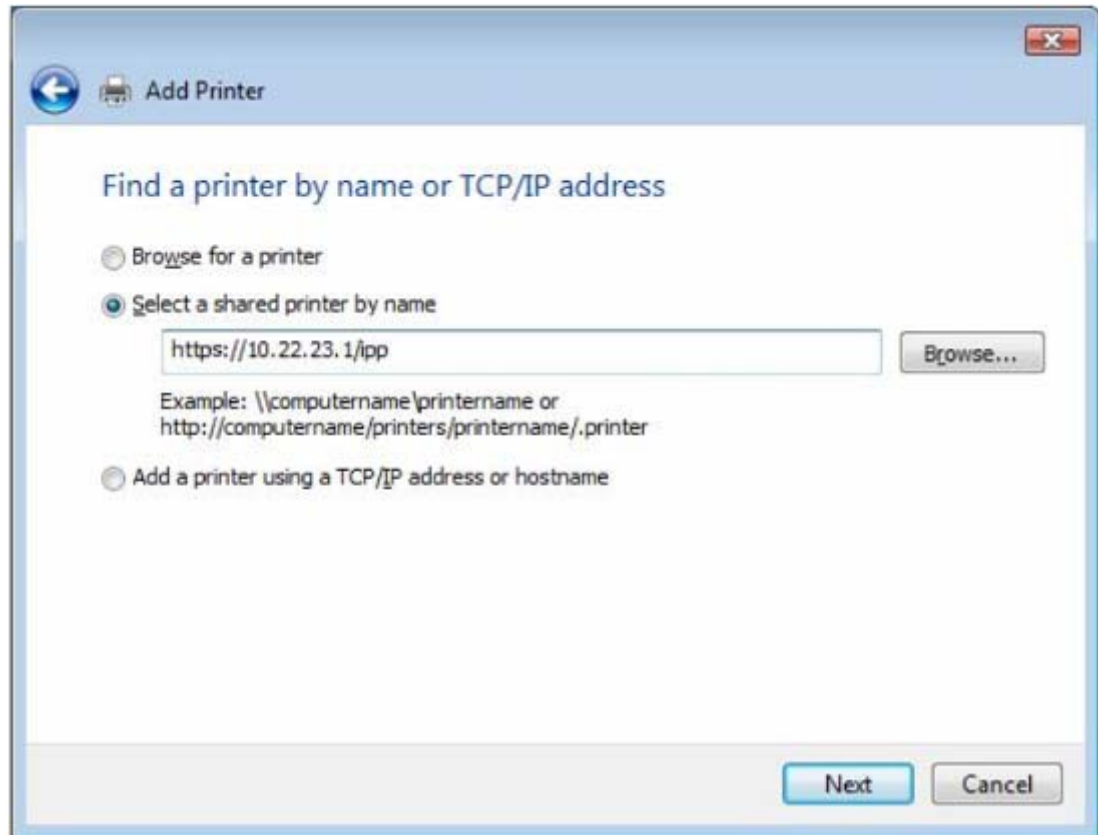
Click, 'The printer that I want isn't listed'



Select 'Select a shared printer by name' and then enter the following in the URL field:
https://printer's IP address/ipp (where "printer's IP address" is the printer's IP address or the node name).

Please note:

It is important that you use 'https://' and not 'http://' otherwise printing over IPP will not be secure.

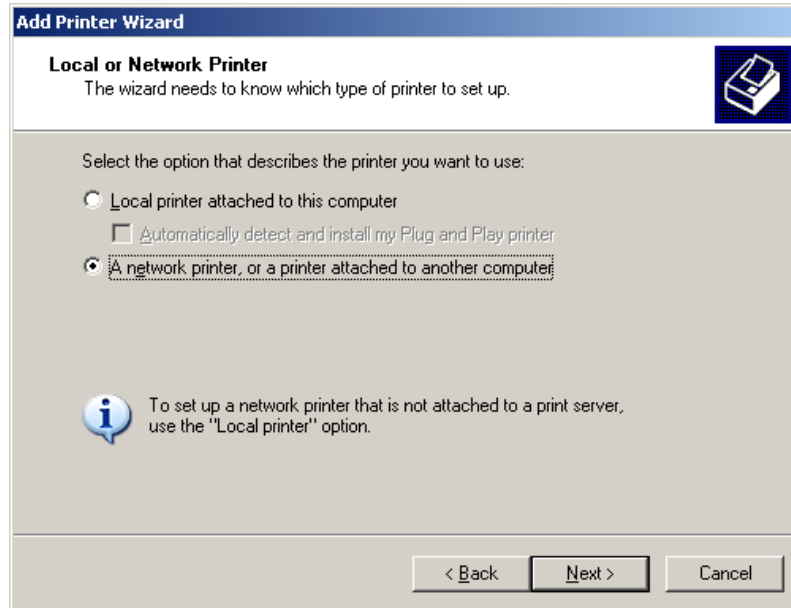


The wizard will search for the printer over the network and will either find the drivers or ask you to select a manufacturer from a list or on a disk. If the driver is on a disk, simply select browse and select where the driver is located.

The printer driver will install and ask you if you want to make the printer default and if you want to print a test page. After this, the printer is installed and ready for secure printing.

4.6 Configuring IPP onto Windows® XP

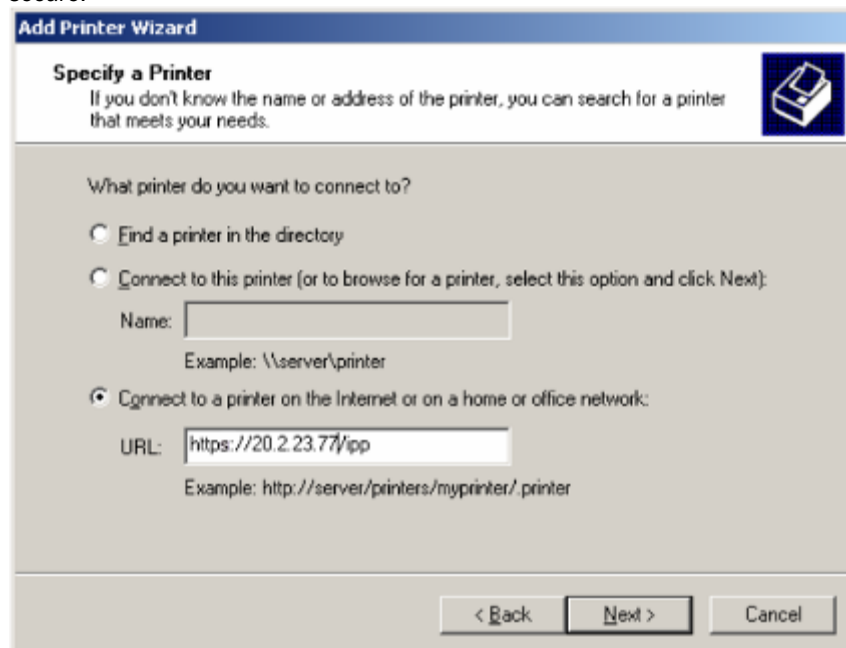
Enter the 'Add Printer Wizard' and select 'A network printer, or a printer attached to another computer'.



Enter the 'Add printer Wizard' and select 'A network printer, or a printer attached to another computer'. Select Connect to a printer on the Internet or on a home or office network and then enter the following in the URL field: `https://printer's IP address/ipp`. After, click next.

Please note:

It is important that you write `https://` and not `http://` otherwise printing over IPP will not be secure.



The wizard will search for the printer over the network and will either find the drivers or ask you to select a manufacturer from a list or on a disk. If the driver is on a disk, simply select browse and select where the driver is located.

The printer driver will install and ask you if you want to make the printer default and if you want to print a test page. After this, the printer is installed and ready for secure printing.

For more detailed instruction for how to use, please refer to the user guide.

5: Technical Overview

Secure Socket Layer (SSL) is a method for protecting data on transport layer sent over a local or wide area network by using the Internet Printing Protocol (IPP), to prevent unauthorised users being able to read them.

It achieves this by using authentication protocols in the form of digital keys, of which there is 2:

1. A public key – known by everyone who is printing.
2. A private key – known only by the printer used to decrypt packets and make them readable again by the printer.

The public key uses either 1024bit encryption and is contained inside a digital certificate, which must be installed onto the client PC. These certificates can either be self signed or approved by a Certificate Authority (CA).

First, there are three different keys, Private, Public and Shared.

The Private key, know only to the printer, is associated with the Public key but not contained within the clients (senders) digital certificate. When the user first established the connection, the printer will send the Public key with the certificate. The client PC trusts that the Public key is from the printer with the certificate. The client generates the Shared key, and encodes it with the Public key, then sends to the printer. The printer encodes the Shared key with the Private key. Now the printer and client shared the Shared key safely, and established the safe connection for print data transferring.

The print data is encoded and decoded with the Shared key.

SSL will not stop unauthorised users from accessing packets, however, it will make them unreadable without the private key, which is not disclosed to anyone apart from the printer.

It can be configured on both wired and wireless networks and will work with other forms of security such as WPA keys and firewalls, given the appropriate configuration.