**Information on IPPS connection establishment**

When an IPP printer is created, Windows will query the target printer to see if it has IPP or IPPS (or both) enabled. Based on the printer URL specified and on what protocol is enabled on the printer, the following table represents what protocol your Windows IPP/IPPS printer might employ.

Printer URL IPP and IPPS Enabled Protocol

ipp://printer1:631/ipp/print Port 631 IPP

ipps://printer1:631/ipp/print Port 631 IPPS:

ipps://printer1:443/ipp/print Port 443 IPPS

IPPS over port 631 on Windows uses implicit TLS – i.e. the client connects directly to port 631 and uses TLS almost from the start. The TLS handshake happens shortly after the TCP connection is established, without sending any data (except the TCP handshake) in an unencrypted state. In WireShark, this TLS handshake is manifested by the TLSv1.x ClientHello, packet, which sends to the printer the cipher suite and the TLS versions supported. The printer uses this information and selects the cipher suite and highest TLS version mutually supported to the client via the ServerHello message. Included in the ServerHello message is the digital certificate along with the identity of the issuing authority that (hopefully) the client Windows machine trusts. Once received, the client can now validate the certificate provided by the printer.

The next few messages consist of:

**Client Key Exchange**: The client sends a ClientKeyExchange message, which contains key material (e.g., a pre-master secret encrypted with the server’s public key) needed to establish the shared session key.

**ChangeCipherSpec**: The client sends a ChangeCipherSpec message indicating that subsequent messages will be encrypted.

**Finished**: The client sends a Finished message encrypted with the negotiated keys, proving that the handshake messages were received and processed correctly.

Printer **ChangeCipherSpec** and **Finished**: The printer (server) responds with its own ChangeCipherSpec and Finished messages. If all goes well, the connection is now encrypted between the client machine and the printer both ways.

It is important to know the IPP protocol itself doesn't mandate encryption - by default, traffic is unencrypted (IPP) unless IPPS is specified.