Advanced Function Presentation Consortium

Recommended Method to Encrypt IPDS Communications

AFPC-0019-01

AFPConsortium™
Advanced Function Presentation

AFPC-0019-01
First Edition (December 2025)

This is the first edition, and is produced by the AFP Consortium (AFPC). This edition remains current until a new edition is published.

Internet

Visit our home page, where this publication and others are available:
`www.afpconsortium.org`

Chapter 1. Recommendation

Background

When using the Intelligent Printer Data Stream (IPDS) in an Advanced Function Presentation (AFP) environment, a bidirectional communication occurs between the IPDS generator (generally an AFP server or host) and the IPDS receiver (generally a printer or transform). The architecture that defines the protocol for this communication does not contain functionality to encrypt the bytes passing over the network.

In today’s environment, there is a need to enable IPDS generators and IPDS receivers to communicate in a secure way. However, if a generator implements one secure method while a receiver implements a different secure method, they will not be able to communicate in a secure way. Therefore, the AFP Consortium is making the recommendation below.

This document is an official recommendation from the AFP Consortium. All existing and newly-developed IPDS implementations should follow this recommendation to ensure interoperability.

Recommended Method to Encrypt IPDS Communication

All IPDS implementations that wish to provide secure IPDS communications are recommended to use the Transport Layer Security (TLS) protocol to encrypt both directions of the bidirectional IPDS communication.

TLS is a widely-used, well-known, and highly-trusted method for securing network communications. As such, there are open-source implementations available, and most or all operating systems and networking subsystems will include built-in support for its use, making the addition of TLS support to IPDS implementations relatively straightforward.

It is important to realize that the use of TLS does not change the data content of the packets making up the IPDS communication in any way—that is, neither the protocol that defines how the TCP/IP IPDS communication is accomplished, nor the IPDS architecture itself, is changing due to this recommendation.

Note that this is a recommendation, and thus does not require all IPDS implementations to implement support for TLS. Nor does it prohibit implementations from implementing support for other methods of securing the IPDS communication. However, the intent of this recommendation is that two IPDS implementations that wish to communicate with one another in a secure fashion will have at least one method, TLS, in common.

Implementations are recommended to use TLS version 1.3, or a later version if there is one available.

Note: Full encryption of all IPDS data flowing over the network could potentially cause many performance problems on printers, especially high-speed printers. The extra overhead of encrypting the IPDS data on the host, then decrypting the data on the printer, is generally considered to be relatively small when using TLS, but will by definition slow IPDS data transmission speed. Since IPDS printers print at the same time as they are receiving the print data, the slower transmission speed could cause printers to be unable to print at rated speed.

The recommendation in this document is stating that *if* a secure IPDS communication is needed, the recommended way to do that is by using TLS. However, in general, it would also be recommended to only use such TLS encryption when it is truly needed.

Port Number

So as not to disrupt current IPDS implementations, encrypted IPDS using TLS should use a different port number than unencrypted IPDS.

The recommended default port number to use for encrypted IPDS communication is 8801. If all implementations use this as their default port number for TLS IPDS communication, interoperability will be available without required user intervention in specifying a port number.

However, as with unencrypted IPDS communication that has traditionally often used port 5001, implementations should allow the user to change the port number from 8801 to some other port number of the user's choosing.

For implementations that can run in a "dual-simplex mode", where one controller is controlling two separate simplex printers, the recommended default port numbers to use are 8802 for one such simplex printer, and 8803 for the other.

Chapter 2. About the AFP Consortium

The AFP Consortium is an international group bringing together voices from across the printing and presentation industry to keep the AFP architecture up to date and continually improving. AFP Consortium members, often market competitors, work together to ensure this stable, efficient, flexible architecture continues to thrive, even as the world of printing and presentation changes.

The Advanced Function Presentation (AFP) architectures began as the strategic, general purpose document and information presentation architecture for the IBM Corporation. The first specifications and products go back to 1984. Although all of the components of the architecture have grown over the years, the major concepts of object-driven structures, print integrity, resource management, and support for high print speeds were built in from the start.

In the early twenty-first century, IBM saw the need to enable applications to create color output that is independent from the device used for printing and to preserve color consistency, quality, and fidelity of the printed material. This need resulted in the formation, in October 2004, of the AFP Color Consortium (AFPCC). The goal was to extend the object architectures with support for full-color devices including support for comprehensive color management. The idea of doing this via a consortium consisting of the primary AFP architecture users was to build synergism with partners from across the relevant industries, such as hardware manufacturers that produce printers as well as software vendors of composition, work flow, viewer, and transform tools. Quickly more than 30 members came together in regular meetings and work group sessions to create the AFP Color Management Object Content Architecture (CMOCA). A major milestone was reached by the AFP Color Consortium with the initial official release of the CMOCA specification in May 2006.

Since the cooperation between the members of the AFP Color Consortium turned out to be very effective and valuable, it was decided to broaden the scope of the consortium efforts and IBM soon announced its plans to open up the complete scope of the AFP architecture to the consortium. In June 2007, IBM's role as founding member of the consortium was transferred to the InfoPrint Solutions Company, an IBM/Ricoh joint venture; currently Ricoh holds the founding member position. In February 2009, the consortium was incorporated under a new set of bylaws with tiered membership and shared governance resulting in the creation of a formal open standards body called the AFP Consortium (AFPC). Ownership of and responsibility for the AFP architectures was transferred at that time to the AFP Consortium.

Advanced Function Presentation Consortium

Recommended Method to Encrypt IPDS Communications

AFPC-0019-01