IEEE-ISTO

Printer Working Group

IPP Fax Project

Standard for IPPFAX/1.0 Protocol

Working Draft

Maturity: Initial

Version 1.0
May 24, 2004

Abstract: This document specifies the IPPFAX/1.0 protocol. The IPPFAX requirements [ifx-req] are derived from the requirements for Internet Fax [RFC2542].
In summary, IPPFAX is used to provide a synchronous, reliable exchange of image Documents between clients and servers. The primary use envisaged of this protocol is to provide a synchronous image transmission service for the Internet. Contrast this with the Internet FAX protocol specified in [RFC2305] and [RFC2532] that uses the SMTP mail protocol as a transport.
The IPPFAX/1.0 protocol is a specialization of the IPP/1.1 [RFC2911], [RFC2910] protocol supporting a subset of the IPP operations with increased conformance requirements in some cases, some restrictions in other cases, and some additional REQUIRED attributes. The IPPFAX Protocol uses the 'ippfax' URL scheme (instead of the 'ipp' URL scheme) in all its operations. Most of the new attributes defined in this document MAY be supported by IPP Printers as OPTIONAL extensions to IPP as well
An IPPFAX Printer object is called a Receiver. A Receiver MUST support at least the PDF/is as specified in [PWG5102.3-2004] which is defined for the 'application/pdf' document format MIME type . A Print System MAY be configured to support both the IPPFAX and IPP protocols concurrently, but each protocol requires separate Printer objects with distinct URLs.

This document is available electronically at: wd-ifx10-20040524.pdf, .doc

A version showing the changes from the previous version is available at: wd-ifx10-20040524-rev.pdf

The latest version of this specification is available at: ftp://pwg.org/pub/pwg/QUALDOCS/wd-ifx10-latest.pdf, .doc

About the IEEE-ISTO

The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and flexible operational forum and support services. The IEEE-ISTO provides a forum not only to develop standards, but also to facilitate activities that support the implementation and acceptance of standards in the marketplace. The organization is affiliated with the IEEE (http://www.ieee.org/) and the IEEE Standards Association (http://standards.ieee.org/).

For additional information regarding the IEEE-ISTO and its industry programs visit http://www.ieee-isto.org.

About the IEEE-ISTO PWG

The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and Technology Organization (ISTO) with member organizations including printer manufacturers, print server developers, operating system providers, network operating systems providers, network connectivity vendors, and print management application developers. The group is chartered to make printers and the applications and operating systems supporting them work together better. All references to the PWG in this document implicitly mean "The Printer Working Group, a Program of the IEEE ISTO." In order to meet this objective, the PWG will document the results of their work as open standards that define print related protocols, interfaces, procedures and conventions. Printer manufacturers and vendors of printer related software will benefit from the interoperability provided by voluntary conformance to these standards.

In general, a PWG standard is a specification that is stable, well understood, and is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, and enjoys significant public support.

For additional information regarding the Printer Working Group visit: http://www.pwg.org

Contact information:

IFX Web Page: http://www.pwg.org/qualdocs
IFX Mailing List: ifx@pwg.org

To subscribe to the ipp mailing list, send the following email:
1) send it to majordomo@pwg.org
2) leave the subject line blank
3) put the following two lines in the message body:
subscribe ifx
end

Implementers of this specification are encouraged to join the IFX Mailing List in order to participate in any discussions of clarifications or review of registration proposals for additional names.

95 # Contents

Table of Tables

1 Introduction

This document specifies the IPPFAX/1.0 protocol. The IPPFAX requirements [ifx-req] are derived from the requirements for Internet Fax [RFC2542].

In summary IPPFAX is used to provide a synchronous, reliable exchange of image documents between clients and servers. The primary use envisaged of this protocol is to provide a synchronous image transmission service for the Internet. Contrast this with the Internet FAX protocol specified in [RFC2305] and [RFC2532] that uses the SMTP mail protocol as a transport.

IPPFAX is primarily intended as a method of supporting a synchronous, secure, high quality document distribution protocol over the Internet. It therefore discusses paper, pages, scanning and printing, etc. There is, however, no requirement that the input documents come from actual paper nor is there a requirement that the output of the process be printed paper. The only conformance requirements are those associated with the exchange of data over the network.

The IPPFAX/1.0 protocol is a specialization of the IPP/1.1 [RFC2911], [RFC2910] protocol supporting a subset of the IPP operations with increased conformance requirements in some cases, some restrictions in other cases, and some additional REQUIRED attributes. The IPPFAX Protocol uses the 'ippfax' URL scheme (instead of the 'ipp' URL scheme) for all operations.

An IPPFAX Printer object is called a Receiver. A Receiver must support at least PDF/is [PWG5102.3-2004] which is defined for the 'application/pdf' document format MIME type.

An IPPFAX client is called a Sender. The user of the Sender is called the Sending User. The Sending User either (1a) loads the Document into the Sender or (1b) causes the Sender to generate the Document data by means outside the scope of this standard, (2) indicates the Receiver's network location, and (3) starts the exchange.

The target market for an IPPFAX receiver is a midrange imaging device that can support the minimum memory requirements that are required by the data format PDF/is, but the image format is structured in such a way that the Receiver is not required to include a disk or other permanent storage.

IPPFax Senders and Receivers must support the operations, Get-Printer-Attributes, Print-Job, Get-Job-Attributes, and should support for authorized administrators Get-Jobs and Cancel-Job. See Section 7

Deleted: MUST

Deleted: A Print System MAY be configured to support both the IPPFAX and IPP protocols concurrently for a single output device (or multiple output devices), but each protocol requires separate Printer objects with distinct URLs. Note - It is assumed that the reader is familiar with IPP/1.1 [RFC2911], [RFC2910]

Deleted: ,

Deleted: [RFC3196], and [ipp-iig-bis].

Deleted: <#>Required Operations and features (normative)¶
All IPPFax Senders and Receivers MUST support the following operations:¶
¶
<#>Get-Printer-Attributes - If the document-format-version is not PDF/is or the media is not iso_a4_210x297mm or na_letter_8.5x11in, then the Sender MUST verify that the Receiver can support the alternate attributes. Rational: Using Get-Printer-Attributes would avoid rejection of the job which is important if the document data is very large. ¶
<#>Print-Job - Sender MUST submit the IPPFAX job with a single document (Create-Job, Send-document and Send-URI and Print-URI MUST NOT be supported by Senders or Receivers).¶
<#>Get-Job-Attributes - The Sender MUST support and MUST use this operation to check for successful job completion unless the Sending User wishes otherwise. Job-History MUST be retained by the Receiver for at least 5 minutes after job completion. See 4.3.7.2 of RFC2911 for printer object Job-History discussion.¶
<#>Get-Jobs – Receivers MUST support this operation but only for authenticated Administrators or Operators.¶
<#>Job-Cancel – Receivers MUST support this operation but only for authenticated Administrators or Operators.¶
All IPPFax Senders and Receivers MUST NOT support any other IPP operations including job operations and administrative operation.¶
All IPPFax Receivers MUST support receiving PFD/is version 1.0 as defined in [PWG5102.3-2004].¶
All IPPFax Senders MUST support generating and transmitting PFD/is version 1.0 as defined in [PWG5102.3-2004].¶

1.1 Typical exchange

Deleted: (informative)
Formatted: Bullets and Numbering

This section lists a typical exchange of information between a Sender and a Receiver using the four operations listed in section 0.

1. The Sending User determines the network location of the Receiver (value of the "printer-uri" operation attribute) – see section 4.1. This document does not specify how the Sending User does this. Possible methods include directory lookup, search engines, business cards, network discovery protocols such as SLP, etc. See Appendix E Generic Directory Schema of IPP/1.1 [RFC 2911].

2. The Sending User either (1) loads the Document into the Sender or (2) causes the Sender to generate the Document data by means outside the scope of this document, indicates the Receiver's network location and starts the exchange.

3. The Sender can determine other PDF versions supported by the Receiver and the Sender can discover "media-supported" and "media-ready".

Deleted: MAY
Deleted: MAY

4. The Sender converts the document, if necessary, into PDF/is or another PDF subset depending on the Receiver's capabilities. The PDF/is data format is described in detail in the "PDF Image-Streamable (PDF/is)" specification [PWG5102.3-2004].

5. The Sender submits the document in a Print-Job request to the Receiver. The Sender can include the sending user vCard[RFC2426, RFC2425] and receiving user vCard in the Print-Job operations.

Deleted: SHOULD

6. The Receiver returns a Print-Job response to the Sender, who in turns informs the Sending-User.

Deleted:
Deleted: .
Deleted: The Sender
Deleted: MUST
Formatted: Highlight
Formatted: Highlight
Deleted: MUST
Formatted: Highlight

7. The Sender can use Get-Job-Attributes to check for successful job completion unless the Sending User requests otherwise.

2 Terminology

This section defines the following additional terms that are used throughout this standard.

2.1 Conformance Terminology

Capitalized terms, such as **MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, MAY, NEED NOT,** and **OPTIONAL**, have special meaning relating to conformance to this specification. These terms are defined in [RFC2911] section 13.1 on conformance terminology, most of which is taken from RFC 2119 [RFC2119]. In order to help the reader compare and contrast the IPP and IPPFAX protocols, this document uses lower case "must", "may" etc., to reproduce IPP Protocol conformance requirements

for IPP clients and IPP Printer objects as stated in other documents. If such reproduction in this document contradicts an IPP document, it is a mistake, and that IPP document prevails.

2.2 Other Terminology

This standard defines a logical model of an IPPFAX interchange. The following terms are introduced and capitalized in order to indicate their specific meaning:

IPP Protocol The protocol defined in [RFC2911] and [RFC2910] and any IPP Protocol Extension document (see section 14). For the IPP/1.1 Protocol each operation request must use the 'ipp' URL scheme.

IPPFAX Protocol The protocol defined in this document.

Printer object (or Printer) A hardware or software entity that accepts protocol operation requests and returns protocol responses as defined in IPP1.1 (see [RFC2911]).

> Note: For brevity, this document uses the term "Receiver" instead of "IPPFAX Printer object". This document uses the term "Printer object" (and "Printer") when the statement is intended to apply to a Printer object that can support the IPP Protocol or the IPPFAX protocol (but not both).

Print Service The print functionality offered by a Printer object.

IPP Printer object A Printer object that supports the IPP Protocol and offers the IPP Print Service (by definition).

Receiver The Printer object that accepts IPPFAX protocol operations and receives the Document sent by the Sender. A Receiver offers the IPPFAX Print Service (by definition).

Print System All of the Printer objects on a single managed host network node.

client A hardware and/or software entity that initiates protocol operation requests and accepts responses. However, this document uses the term "Sender", instead of "IPPFAX client".

IPP client A client that uses the IPP Protocol to interact with an IPP Printer object.

Sender A client that uses the IPPFAX Protocol to query a Receiver and transmit a Document to that Receiver.

Document The electronic representation of a set of one or more pages that the Sender sends to the Receiver.

Deleted: or a future revision

Deleted: and any future extension document. For the IPPFAX Protocol each operation request MUST use the 'ippfax' URL scheme (see section 4.1 and 12).

Deleted: Unless a specific version number is appended to "IPPFAX", such as "IPPFAX/1.0", the term IPPFAX applies to all versions.

Formatted: Highlight

Deleted: . A Printer object MAY be: (1) an IPP Printer object or (2) an IPPFAX Printer object, DEPENDING ON IMPLEMENTATION (see section **Error! Reference source not found.**), but MUST NOT be both (since they support some different operations and attributes and are really two different kinds of Print Services).

Formatted: Highlight

Deleted: A Printer object MAY support multiple URLs with different security, authentication, and/or access control (see [RFC2911] sections 4.4.1, 4.4.2, 4.4.3, and 8). However, each URL for a Printer object MUST support the same operations and attributes with the same values, except as restricted depending on the security, authentication, and/or access control implied by the URL. In other words, each URL for a given Printer object is offering the same Print Service.

Formatted: Highlight

Deleted: MAY

Deleted:

Deleted: Several different Printer objects MAY offer the same Print Service. A Print Service MUST support only one printer object

Deleted: . A Print System MAY support IPP and IPPFAX protocols concurrently (see section **Error! Reference source not found.**) for a single output device (or multiple output devices), but each protocol requires separate Printer objects with distinct URLs.

Deleted: A client MAY be: (1) an IPP client, (2) an IPPFAX client, or (3) both.

Deleted: This document uses the term "client" when the statement is intended to apply to a client that MAY suppor... [1]

Sending User The person interacting with the Sender.

Receiving User The intended human recipient of the Document being sent by the Sender to the Receiver.

IPP Job A job submitted by an IPP client to an IPP Printer object using the IPP Protocol.

IPPFAX Job A job submitted by a Sender to a Receiver using the IPPFAX Protocol.

PDF/is The file format defined by [PWG5102.3-2004].

The terminology defined in [RFC2911], such as **attribute**, **operation**, **request**, **response**, **operation attribute**, **Printer Description attribute**, **Job Description attribute, integrity,** and **privacy** is also used in this document with the same capitalization conventions and semantics.

3 IPPFAX Model

This sub-section defines the IPPFAX Model and its relationship to the IPP Protocol and Model.

3.1 Printer Object Relationships

A Print System MAY support one or more Printer objects on a single network host. RFC 2911 [RFC2911] defines the relationship between Printer objects and output devices to be many to many (see [RFC2911] section 2.1). So one Printer object can represent one or more output devices and an output device can be represented by one or more Printer objects. The same relationships hold for the IPPFAX Protocol so that the relationship between Receivers and output devices is many to many.

3.2 A Printer object with multiple URLs

For a Printer object that has multiple URLs, the multiple URLs MUST only be aliases for the Printer object, not connections to different Print Services. In other words, the semantics of operations and attributes accessed by the different URLs for a given Printer object MUST differ only in the security, authentication, and/or access control depending on the URL used.

The three parallel “printer-uri-supported” (1setOf uri), “uri-authentication-supported” (1setOf type2 keyword), and “uri-security-supported” (1setOf type2 keyword) Printer Description attributes (see [RFC2911] sections 4.4.1, 4.4.2, and 4.4.3, respectively) MUST contain the URLs, authentication, and security, respectively, supported by the Printer object.

4 Common IPPFAX Operation Attribute Semantics

This section describes the IPPFAX/1.0 operation attribute semantics that are common to all operations. IPPFAX/1.0 does not define any new operations. Instead, IPPFAX/1.0 semantics are provided using existing IPP operations in [RFC2911], with increased conformance requirements as specified in this document.

4.1 printer-uri (uri) operation attribute

This operation attribute specifies the transfer path to the Receiver for the operation. As in IPP/1.1, the client MUST supply the "printer-uri" operation attribute in every IPPFAX request (see [RFC2911] section 3.1.5). For IPPFAX, the attribute value MUST be a URL using the 'ippfax' scheme (see section 12) specifying the Receiver's network location.

The following is an example value of the target "printer-uri" operation attribute and "printer-uri-supported" Printer Description attribute:

ippfax://www.acme.com/ippfax-printers/printer5

As in IPP/1.1 [RFC2911] for each operation, the Receiver NEED NOT validate that the "printer-uri" operation attribute is present and that the value supplied by the Sender matches one of the Receiver's "printer-uri-supported" Printer Description attribute (see section 5.1). For URI matching rules see section 12.7. If the Receiver does validate the "printer-uri" operation attribute and the URI value supplied does not match any value of the Receiver's "printer-uri-supported" Printer Description attribute, the Receiver MUST reject the request, return the 'client-error-attributes-or-values-not-supported' status code, and return the attribute and value in the Unsupported Attributes Group.

4.2 version-number parameter

This IPP/1.1 operation parameter ([RFC2911] section 3.1.8) specifies the major and minor version number of the IPP Protocol being used *as part of the IPPFAX Protocol*. As in IPP/1.1, the Sender MUST supply this parameter in every request and the Receiver MUST return this parameter in every response.

For IPPFAX version 1.0 as specified in this document, the Sender MUST supply the IPP version number parameter with a value of '1.1' or a higher minor version number.

4.3 ippfax-version (type2 keyword) operation attribute

The value of this operation attribute indicates the version of the IPPFAX Protocol and encoding that the Sender is requesting and the Receiver is returning. The Sender MUST supply this operation attribute in every request and the Receiver MUST return this operation attribute in every response. This operation attribute MUST be placed in the Operation Attributes Group *immediately* after the operation attributes whose order is specified in IPP/1.1 [RFC2911]. The semantics of the "ippfax-version" operation attribute are the same for the IPPFAX Protocol as the "version-number" parameter for IPP 1.1(see [RFC2911] section 3.1.8).

For IPPFAX version 1.0 as specified in this document, the Sender MUST supply the IPPFax version operation attribute with the keyword value of '1.0'.

The Receiver MUST list the IPPFAX versions supported in the "ippfax-versions-supported" (1setOf type2 keyword) Printer Description attribute (see section 5.3).

The Sender MUST send and the Receiver MUST check both the IPP (see section 4.2) and IPPFAX version numbers supplied by the Sender in each request, not just the IPPFAX version number.

5 IPPFAX Printer Description Attributes

This section defines the IPPFAX Printer Description attributes and the IPP Printer Description attributes whose semantics are augmented for IPPFAX.

Table 1 lists all the IPPFAX conformance requirements for IPP and IPPFAX Printer Description attributes whose semantics are defined in this document.

All Printer Description attributes not listed in Table 1 have the same conformance requirements as defined in IPP/1.1 [RFC2911] or other IETF or PWG standards track IPP documents.

See section 7.3.2 for the Receiver conformance requirements for the "xxx-supported", "xxx-default", and "xxx-ready" Job Template Printer attributes.

Table 1 - Printer Description attributes conformance requirements

Attribute Name (attribute syntax)	IPP Fax Receiver support	Section
printer-uri-supported (1setOf uri) *	MUST	5.1
ipp-versions-supported (1setOf type2 keyword) *	MUST	5.2
ippfax-versions-supported (1setOf type2 keyword)	MUST	5.3
operations-supported (1setOf type2 enum) *	MUST	5.4
document-format-supported (1setOf mimeMediaType) *	MUST	5.5
document-format-version-supported (1setOf text(127)) **	MUST	5.6
digital-signature-supported (1setOf type2 keyword) **	MUST	5.7
pdl-override-supported (type2 keyword) *	MUST	5.8

* These IPP/1.1 attributes are defined in [RFC2911], but have enhanced semantics defined in this document.

** These IPP attributes are defined in [PWG 5100.7], but have enhanced or constrained semantics defined in this document.

5.1 printer-uri-supported (1setOf uri)

This attribute (see [RFC2911] section 4.4.1) contains the set of target URIs that the Receiver supports, i.e., the URI values that a client can supply as values of the "printer-uri" target operation attribute in requests. A Receiver MUST support this Printer Description attribute. This attrbribute MUST only contain URIs using the 'ippfax' scheme.

5.2 ipp-versions-supported (1setOf type2 keyword)

This attribute (see [RFC2911] section 4.4.1.4) identifies the version or versions of the IPP encoding that this Receiver supports as part of the IPPFAX Protocol (rather than indicating that the Receiver supports the IPP Protocol), including major and minor versions, i.e., the version numbers for which this Receiver meets the conformance requirements. The Receiver MUST support this Printer Description attribute. The Receiver MUST compare the "version-number" parameter (see section 4.2), with the values of this attribute in order to determine whether the Printer supports the IPP version requested by the Sender *as part of the IPPFAX Protocol*.

Standard keyword values are (from [RFC2911]):

'1.1': The IPPFAX operations meets encoding conformance requirements of IPP version 1/1 as specified in [RFC2911] and [RFC2910].

5.3 ippfax-versions-supported (1setOf type2 keyword)

This attribute identifies the version or versions of the IPPFAX Protocol that this Receiver supports, including major and minor versions, i.e., the version numbers for which this Receiver meets the conformance requirements. The support of this attribute indicates that this Printer object is a Receiver as opposed to a regular IPP Printer object

The Receiver MUST compare the "ippfax-version" operation attribute (see section 4.3) supplied by the Sender in each request, with the values of this attribute in order to determine whether the Receiver supports the IPPFAX version requested by the Sender.

Standard keyword values are:

'1.0': Meets the conformance requirements of IPPFAX 1/0 as specified in this document.

5.4 operations-supported (1setOf type2 enum)

This attribute (see [RFC 2911] section 4.4.15) identifies the set of supported operations for this Receiver and contained Job objects. A Receiver MUST support this Printer Description attribute.

The values of this attribute MAY depend on the URL supplied in the "printer-uri" operation attribute and/or MAY depend on the authority of the authenticated requesting user. For example, a Receiver that supports administrative operations MUST NOT support administrative operations for use by end users, but such a Receiver MAY return the administrative operation enums to end users. See section 9 for conformance requirements for these operations.

Formatted: Not Highlight

A receiver MUST only support the following operations:

- get-printer-attributes
- print-job
- cancel-job
- get-jobs
- get-job-attributes

A receiver MUST NOT support any other operation.

5.5 document-format-supported (1setOf mimeMediaType)

This attribute (see [RFC 2911] section 4.4.22) identifies which document formats the Receiver supports. The Receiver MUST support this Printer Description attribute. Both the Sender and Receiver MUST only support ‘application/pdf’.

5.6 document-format-version-supported (1setOf text(127))

This attribute (see [PWG 5100.7] section 7.8) identifies which PDF subsets the Receiver supports. A Receiver MUST support this attribute and a Sender MAY support this attribute. Both the Sender and Receiver MUST support the ‘PDF/is-1.0’ subset of PDF. The Receiver MAY support other subsets of PDF and if it does then the Receiver MUST only list subsets that it fully supports.

5.7 digital-signatures-supported (1setOf type2 keyword)

This attribute (see [PWG 5100.7] section 7.4) identifies which digital signature technologies are supported by the Receiver. A Receiver MUST support this Printer Description attribute.

If the Receiver cannot validate the digital signature or if the digital signature fails to verify, then the Receiver MUST notify the Receiving User using an implementation specific method.

5.8 pdl-override-supported (type2 keyword)

This attribute (see [RFC 2911] section 4.4.28) identifies Receiver implementation support for overriding document data instructions with IPPFax job attributes. A Receiver MUST support this printer subscription attribute with the value ‘attempted’. . A Receiver MUST attempt to override at least the media attribute.

6 IPPFax Job Description Attributes

This section defines the IPPFAX Printer Description attributes and the IPP Printer Description attributes whose semantics are augmented for IPPFAX or are new to IPPFax. .

405 **Table 2 - Summary of Job Description attributes**

Attribute	Sender supplies *	Receiver supports
sending-user-vcard (text(MAX))	MAY	MUST
receiving-user-vcard (text(MAX))	SHOULD	MUST
compression-supplied (type3 keyword) **	MUST NOT	MUST
document-charset-supplied (charset) **	MUST NOT	MUST
document-digital-signature-supplied (type2 keyword)**	MUST NOT	MUST
document-format-details-supplied (1setOf collection) **	MUST NOT	MUST NOT
document-format-supplied (mimeMediaType)**	MUST NOT	MUST
document-format-version-supplied (text(127)) **	MUST NOT	MUST
document-message-supplied (text(MAX))**	MUST NOT	MUST NOT
document-name-supplied (name (MAX)) **	MUST NOT	MUST
document-natural-language-supplied (naturalLanguage)**	MUST NOT	MUST

406 *Sender supplies as an operation attribute in a Print-Job operation.
407 ** These IPP attributes are defined in [PWG 5100.7]
408

409 ### 6.1 sending-user-vcard (text(MAX))

410 This Job Description attribute identifies the Sending User in MIME vCard v3.0 [RFC2426, RFC2425]
411 format (See Appendix B for a sample vCard). The Receiver MUST support this job description attribute
412 according to the vCard v3.0 specification and MUST populate it with the value of the corresponding Print-
413 Job operation attribute. The Receiver MUST support MAX (1023) octets of text. However, the Receiver
414 MAY ignore any image, logo, and sound parts of the vCard, in which case it MUST still accept the Print-
415 Job request and return the 'successful-ok-ignored-or-substituted-attributes' status code (see [RFC2911]
416 section 13.1.2.2). The Receiver MAY choose to use this information on a job start and end sheet (banner
417 page) for the job.

Formatted: Not Highlight

418 ### 6.2 receiving-user-vcard (text(MAX))

419 This Job Description attribute identifies the intended Receiving User in MIME vCard v3.0 [RFC2426,
420 RFC2425] format (See Appendix B for a sample vCard). The Receiver MUST support this Job
421 Description operation attribute and MUST populate it with the value of the corresponding Print-Job
422 operation attribute. The Receiver MUST support MAX (1023) octets of text. However, the Receiver
423 MAY ignore any image, logo, and sound parts of the vCard, in which case it MUST still accept the Print-
424 Job request and return the 'successful-ok-ignored-or-substituted-attributes' status code (see [RFC2911]
425 section 13.1.2.2).The Receiver MAY choose to use this information on a job start and end sheet (banner
426 page) for the job.

Formatted: Not Highlight

6.3 xxx-supplied attributes

An IPPFax Receiver implementation MUST supported compression-supplied, document-charset-supplied, document-digital-signature-supplied, document-format-supplied, document-format-version-supplied, document-name-supplied, and document-natural-language-supplied Job-Description attributes as defined in [PWG 5100.7]

An IPPFax Receiver MUST NOT implement document-format-details-supplied and document-message-supplied Job-Description attributes.

SHOULD WE INCLUDE Job-Progress attributes job-impressions-completed, job-media-sheets-completed, job-k-octets-processed from RFC 2911? (support job status in replacement of Notifications) Nothing from RFC3381 applies

Deleted:

7 IPPFAX Operations

An IPPFax Receiver implementation MUST support the Get-Printer Attributes, Print Job, Get-Job Attributes, Get-Jobs and Cancel-Job as defined in this section. An IPPFax Receiver MUST NOT support any other IPP operations.

An IPPFax Receiver MUST NOT support any optional job-template attributes features of IPP unless explicitly stated in this document. An IPPFax Receiver MAY support any optional operation attributes in the Print-Job operation and MAY support Job-Description attributes in Job Objects.

Formatted: Bullets and Numbering

7.1 Required Operations and Features

All IPPFax Senders and Receivers MUST support the following operations:

1. Get-Printer-Attributes - If the document-format-version is not PDF/is or the media is not iso_a4_210x297mm or na_letter_8.5x11in, then the Sender MUST verify that the Receiver can support the alternate attributes. Rational: Using Get-Printer-Attributes would avoid rejection of the job which is important if the document data is very large.

Formatted: Bullets and Numbering

2. Print-Job - Sender MUST submit the IPPFAX job with a single document (Create-Job, Send-document and Send-URI and Print-URI MUST NOT be supported by Senders or Receivers).

3. Get-Job-Attributes - The Sender MUST support and MUST use this operation to check for successful job completion unless the Sending User wishes otherwise. Job-History MUST be

retained by the Receiver for at least 5 minutes after job completion. See 4.3.7.2 of RFC2911 for printer object Job-History discussion.

4. Get-Jobs – Receivers MUST support this operation but only for authenticated Administrators or Operators.

5. Job-Cancel – Receivers MUST support this operation but only for authenticated Administrators or Operators.

All IPPFax Senders and Receivers MUST NOT support any other IPP operations including job operations and administrative operation.

All IPPFax Receivers MUST support receiving PFD/is version 1.0 as defined in [PWG5102.3-2004].

All IPPFax Senders MUST support generating and transmitting PFD/is version 1.0 as defined in [PWG5102.3-2004].

Formatted: Indent: Left: 0.25", Right: 0.3"

Formatted: Bullets and Numbering

7.2 Get-Printer-Attributes

The Sender and Receiver MUST support the discovery of Receiver capabilities using the Get-Printer-Attributes operation.

Deleted: r

Deleted:

Deleted: a

See Section 5 IPPFAX Printer Description Attributes for required Printer Description Attributes for IPPFax Receivers.

Formatted: Bullets and Numbering

7.3 Print-Job

The Sender and Receiver MUST support creating IPPFAX Jobs using the Print-Job operation. The Sender and Receiver MUST NOT support print by reference, i.e., MUST NOT support any other print operation, i.e. Create-Job, Send-Document, Print-URI and Send-URI operations.

Formatted: Bullets and Numbering

7.3.1 Operation Attributes

Table 3 lists the operation attributes for Print-Job operations for Senders, and Receivers. The Receiver MUST NOT support operations attributes defined in other IPP extension documents.

Table 3 - Print-Job operation attributes

Operation attribute	Section	Sender supplies	Receiver Supports
attributes-charset (charset)		MUST	MUST
attributes-natural-language (naturalLanguage)		MUST	MUST
printer-uri (uri)	4.1	MUST	MUST
requesting-user-name (name(MAX))		SHOULD	MUST
job-name (name(MAX))		MAY	MUST
ipp-attribute-fidelity (boolean)	7.3.1.1	MUST with 'true' value[1]	MUST
document-name (name(MAX)) *	7.3.1.2	MAY	MUST
compression (type3 keyword) *		MAY	MUST
document-format (mimeMediaType) *	7.3.1.3	MUST[2]	MUST
document-format-version (type2 keyword) *	7.3.1.4	MUST[3]	MUST
document-charset (charset) *	7.3.1.5	MAY	MUST
document-natural-language (naturalLanguage) *	7.3.1.6	MAY	MUST
document-digital-signature (type2 keyword)	7.3.1.7	MAY	MUST
job-k-octets (integer(0:MAX))		MAY	MAY
job-impressions (integer(0:MAX))		MAY	MAY
job-media-sheets (integer(0:MAX))		MAY	MAY
sending-user-vcard (1setOf text(MAX))	6.1	SHOULD[3]	MUST
receiving-user-vcard (text(MAX))	6.2	SHOULD[3]	MUST

* These IPPFax attributes MUST be copied to their corresponding xxx-supplied Job-Description attributes by the Receiver.

Formatted: Bullets and Numbering

7.3.1.1 ipp-attribute-fidelity

This operation attribute (see [RFC2911] section 3.2.1.1) indicates whether or not the client requires the Printer to support all Job Template attributes and values supplied. The Sender MUST supply this operation attribute in the Print-Job operations and the value MUST be 'true'. A Receiver MUST validate and support this operation attribute.

[1] [RFC2911] does not require the client to supply the "ipp-attribute-fidelity" and allows the client to supply either the 'true' or 'false' value.

[2] The [RFC2911] does not require the IPP client to supply the "document-format" operation attribute.

[3] These attributes were not defined in [RFC2911].

If the Sender does not supply this attribute or supplies the 'false' value, the Receiver MUST reject the operation, MUST return the 'client-error-bad-request' status code, and SHOULD return the 'ipp-attribute-fidelity' attribute name keyword in the Unsupported Attributes Group.

Formatted: Bullets and Numbering

7.3.1.2 document-name (naturalLanguage)

A Sender MAY supply this operation attribute. A Receiver MUST support this operation attribute. The Receiver MUST copy the value of this attribute to the corresponding document-name-supplied Job Description attribute. (See section 5.2.8 of [PWG5100.7])

Formatted: Bullets and Numbering

7.3.1.3 document-format (mimeMediaType)

This operation attribute (see [RFC2911] section 3.2.1.1) identifies the MIME Media Type of the document that the Sender is sending. The Sender MUST supply this operation attribute in the Print-Job operation with a value of "application/PDF". A Receiver MUST validate that the value of attribute is "application/pdf". The Receiver MUST copy the value of this attribute to the corresponding document-format-supplied Job Description attribute. (See section 5.2.5 of [PWG5100.7])

If the Sender does not supply this attribute, the Receiver MUST reject the operation, MUST return the 'client-error-bad-request' status code, and SHOULD return the 'document-format' attribute name keyword in the Unsupported Attributes Group

Because only one document-format MAY be supported, attribute coloring is not relevant for IPPFax. If the Sender desires to send a different format, then it should use a different transmission protocol than IPPFax.

Formatted: Bullets and Numbering

7.3.1.4 document-format-version (type2 keyword)

This operation attribute is defined in section 3.2.5.7 in [PWG5100.7].

This operation attribute identifies the type2 keyword of the subset of PDF. The Sender MUST supply this operation attribute in the Print-Job operation to specify a subset of PDF. A Receiver MUST support and validate this operation attribute. If the supplied document-format-version is not in the Receivers document-format-version-supported list then the Receiver MUST reject the job with a status code "client-error-document-fomat-not-supported". The Receiver MUST copy the value of this attribute to the corresponding document-format-version-supplied Job Description attribute. (See section 5.2.6 of [PWG5100.7])

IPPFax Senders and Receivers MUST support PDF/is-1.0.

See section 5.6.

7.3.1.5 document-charset (charset)

A Sender MAY supply this operation attribute. A Receiver MUST support this operation attribute. The Receiver MUST copy the value of this attribute to the corresponding document-charset-supplied Job Description attribute. (See section 5.2.2 of [PWG5100.7])

7.3.1.6 document-natural-language (naturalLanguage)

A Sender MAY supply this operation attribute. A Receiver MUST support this operation attribute. The Receiver MUST copy the value of this attribute to the corresponding document-natural-language-supplied Job Description attribute. (See section 5.2.9 of [PWG5100.7])

7.3.1.7 document-digital-signature (type2 keyword)

A Sender MAY supply this operation attribute. A Receiver MUST support this operation attribute. The Receiver MUST copy the value of this attribute to the corresponding document-digital-signature-supplied Job Description attribute. (See section 5.2.3 of [PWG5100.7])

7.3.2 Job Template Attributes

As in [RFC2911], the term "Job Template attribute" is actually up to four attributes: the "xxx" Job attribute, and the "xxx-default", "xxx-supported", and possibly the "xxx-ready" Printer attributes.

As in [RFC2911], if a Receiver supports the "xxx" Job Template attribute, then it MUST support the corresponding "xxx-default" (if defined) and "xxx-supported" Printer attributes as well, and MAY support the "xxx-ready" attribute (if defined).

Senders MUST supply and Receivers MUST support the Job-Template attribute except "media"[RFC2911] job-template attribute section 7.3.2.1. Senders MUST NOT supply and Receivers MUST NOT support any other Job-Template attributes.

Table 4 - IPPFAX Defaults for unsupported Job-Template Attributes

Job Template attribute	IPPFax default behavior
copies (integer(1:MAX))	1 copy
finishings (1setOf type2 enum)	Administrator configuration
job-hold-until (type3 keyword | name(MAX))	'no-hold'
job-priority (integer(1:100)	Administrator configuration
job-sheets (type3 keyword | name(MAX))	Administrator configuration

Job Template attribute	IPPFax default behavior
multiple-document-handling (type2 keyword)	No multiple document jobs
number-up (integer(1:MAX))	1
orientation-requested (type2 enum)	Administrator configuration
page-ranges (1setOf rangeOfInteger(1:MAX))	1:MAX
print-quality (type2 enum)	Administrator's choice
printer-resolution (resolution)	Administrator configuration
sides (type2 keyword)	Administrator configuration

Formatted: Bullets and Numbering

7.3.2.1 media (type2 keyword | name(MAX))

This Job Template attribute (see [RFC2911] section 4.2.11) identifies the medium to be used for all sheets of the job. The Sender MUST supply and the Receiver MUST support the "media" Job Template attribute in Print-Job requests. The Receiver MUST support the "media-default", and "media-supported" Printer attributes and SHOULD support the "media-ready" Printer attribute.

The Sender MUST supply Media Size Self Describing names defined in [PWG5101.1].

A Receiver MUST at least support the sizes 'na_letter_8.5x11in' and 'iso_a4_210x297mm' and MUST be able to print on at least one of those two sizes. The Receiver MAY scale down at most 10% (PDF/is directives may prohibit this scaling for quality reasons), overflow to another page, or truncate. If the Receiver does truncate then it MUST notify the Receiving User. A Receiver MUST perform only isomorphic scaling.

A Sender SHOULD use PDF Crop boxes when the Sender knows that the imageable region is less than the media size. If the crop box is the union of the lesser size of iso_a4_210x297mm and na_letter_8.5x11in minus 1/2 of an inch, then the Sender can be sure that the majority of Receivers can print the complete image without loss of data. However, this does not eliminate that the possibility that data may be lost.

Formatted: Bullets and Numbering

7.3.2.2 media-supported

The following standard keywords MUST be supported. Any other paper sizes supported MUST use the self-describing names as defined in ([PWG5101.1]):

'na_letter_8.5x11in'
'iso_a4_210x297mm'
'choice_iso_a4_210x297mm_na_letter_8.5x11in' - represents both 'na_letter_8.5x11in' and 'iso_a4_210x297mm' and indicates that either is acceptable. See [PWG5100.7].

7.3.3 Delivery Confirmation using the Print-Job response

The Sender knows when the Receiver has successfully received the entire Job when the Receiver returns the 'successful-ok' status code in the Print-Job Response. The Sender MUST then inform the Sending User by means outside the scope of this standard that the Job has successfully been transmitted, unless the Sending User requests otherwise.

7.3.4 Originator identifier image

Consistent with ITU-T T.30 facsimile, the Document Originator (generating application or Sender) MUST include an originator identifier image as required by PDF/is, [PWG5102.3-2004] section 7.1.

The Document Originator MUST include in the originator identifier image a human readable name of the person, organization or host system that generated this document and MAY include additional data such as Sending User vCard, Receiving User vCard, etc.

7.4 Cancel-Job operation

The Sender MAY support and the Receiver MUST support the Cancel-Job operation but only for authenticated Operators/Administrators.

7.5 Get-Job-Attributes

The Sender and Receiver MUST support the query of Job-Attributes using the Get-Job-Attributes operation.

7.6 Get-Jobs

The Sender MAY support and the Receiver MUST support the Get-Jobs operation but only for authenticated Operators/Administrators.

8 Security considerations

This section describes the security threats against IPPFAX/1.0 Senders and Receivers. This section also addresses the security-related attributes of Printer objects (i.e., protocol endpoints of Receivers). This section specifies the security conformance requirements and recommendations for IPPFAX/1.0 Sender and

Formatted: Bullets and Numbering
Deleted: j
Deleted: Document
Deleted: document
Deleted: received
Formatted: Bullets and Numbering
Deleted: or Sender
Formatted: ref-id
Deleted: place
Deleted: in one of the following
Deleted: places
Deleted: , DEPENDING ON IMPLEMENTATION
Deleted: :
Deleted: <#>On a cover page automatically generated by the Sender that is pre-pended before the first page of user data in the PDF document.¶
<#>Merged with the first page of the document.¶
<#>At the top of every page of the sent Document. ¶
Deleted: Sender
Deleted:
Deleted: (
Deleted:
Deleted: Receiver identity
Deleted:)
Deleted: Reference PDF/is method.¶
Formatted: Bullets and Numbering
Deleted: Only Operators/Administrators can cancel IPPFax jobs.¶
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Deleted: Separate into two sections! Get-Jobs is Operator/Admin only operation¶
The public nature of IPPFAX interactions make it inappropriate for a client to be able to query a Receiver for certain information about jobs that it did not send.¶
The Receiver SHOULD restrict th ... [2]
Formatted ... [3]

Receiver implementations, largely by reference to applicable underlying protocol specifications, for example, IPP/1.1 [RFC2911], HTTP/1.1 [RFC2616], and TLS/1.0 [RFC2246].

Warning: If an implementation of a secure IPPFAX Receiver is enabled on a single network host system simultaneously with another traditional print protocol (e.g., IPP/1.1 [RFC2911]), new security threats appear. Administrators and users are warned that this configuration facilitates denial-of-service attacks and and local file system attacks against the network host system (and thus against the IPPFAX service). Beware.

8.1 Internet Threat Model

This section is adapted from section 3 of IETF Guidelines for Writing RFC Text on Security Considerations [RFC3552].

In the Internet threat model, we assume that the end systems engaging in a protocol exchange have not themselves been compromised. Protecting against an attack when either of the end systems has itself been compromised is extraordinarily difficult.

By contrast, we assume that the attacker has nearly complete control of the communications channel over which the end systems communicate. This means that the attacker can read any PDU (Protocol Data Unit) on the network and undetectably remove, change, or inject forged packets onto the wire. This includes being able to generate packets that appear to be from a trusted machine. Thus, even if the end-system with which you wish to communicate is itself secure, the Internet environment provides no assurance that packets which claim to be from that system in fact are.

The meaning of a PDU changes at different protocol layers. At the IP layer [RFC791], it's an IP packet. At the TCP layer [RFC793], it's a TCP segment. At the IPP/1.1 [RFC2911] application layer, it's a single IPP operation request or response.

8.1.1 Passive Attacks

In a passive attack, the attacker reads packets off the network but does not write them. On most common LAN configurations, including Ethernet, 802.3, and FDDI, any machine on the wire can read all traffic destined for any other machine on the same LAN. Note that switching hubs make this sort of sniffing substantially more difficult, since traffic destined for a machine only goes to the network segment that machine is located on.

Formatted: Font: (Default) Arial, 12 pt

Formatted: Heading 2, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Arial, 12 pt

Formatted: Heading 3, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt

Wireless communications channels deserve special consideration, especially with the recent and growing popularity of wireless-based LANs, such as those using 802.11. Since the data is simply broadcast on well known radio frequencies, an attacker simply needs to be able to receive those transmissions. Such channels are especially vulnerable to passive attacks. Although many such channels include cryptographic protection, it is often of very poor quality.

Senders and Receivers MUST support TLS/1.0 and MUST always use at least TLS/1.0 data integrity services for protection against the following passive attacks described in [RFC3552]:

(1) Confidentiality Violations - Senders and Receivers MUST support and MAY use TLS/1.0 data privacy services for protection against exposure of private business data.

(2) Password Sniffing - Senders and Receivers MUST NOT transfer any cleartext passwords over unencrypted channels (TLS/1.0 data privacy services or HTTP/1.1 Digest Authentication over TLS/1.0 data integrity services MAY be used instead).

8.1.2 Active Attacks

Formatted: Font: (Default) Arial, 12 pt

Formatted: Heading 3, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt

In an active attack, the attacker writes packets to the network and may read responses from the network. Active attacks that involve sending forged packets but not receiving any responses are called "blind attacks".

When IP [RFC791] is used without IPsec [RFC2401], there is no authentication for the packet source address. Active attacks that involve forging an IP packet with a false source address are called "spoofing attacks".

Senders and Receivers MUST support TLS/1.0 and MUST always use at least TLS/1.0 data integrity services for protection against the following active attacks described in [RFC3552]:

(1) Message Replay Attacks

(2) Message Insertion Attacks

(3) Message Deletion Attacks

(4) Message Modification Attacks

(5) Man-In-The-Middle Attacks

8.2 Enterprise Threat Model

In the enterprise threat model, we can no longer assume that the end systems engaging in a protocol exchange have not themselves been compromised. Physical security of workstations and network printers in an enterprise network is often the weakest point of security defenses. And IPPFAX jobs typically produce hardcopy, which an inside attacker can simply steal.

Network security problems are actually worse inside an enterprise network. Firewalls and border routers no longer provide any useful protection.

Users and administrators who deploy IPPFAX products in enterprise networks MUST enforce the use of TLS/1.0 and SHOULD consider the use of strong Client and Server Authentication during TLS/1.0 startup.

8.3 Mobile Threat Model

In the mobile threat model, we can no longer defend against attackers based on network topology. Mobile clients may access home, business, or commercial IPPFAX products via:

(1) Public Wireless - Cellular ISPs, IEEE 802.11 wireless Ethernet "hot spots" in airports, etc.

(2) Local Wireless - Bluetooth/IRDA-enabled laptops and printers, etc.

Users and administrators who deploy IPPFAX products in mobile networks MUST enforce the use of TLS/1.0 and SHOULD consider the use of strong Client and Server Authentication during TLS/1.0 startup. IPsec [RFC2401] also offers significant security advantages in mobile networks.

8.4 HTTP Threat Model

Senders and Receivers are vulnerable to the following HTTP threats described in section 15 "Security Considerations" of HTTP/1.1 [RFC2616]:

Formatted: Font: (Default) Arial, 12 pt

Formatted: Heading 2, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt

(1) Personal Information Attacks - HTTP/1.1 clients and servers in Sender and Receiver implementations MUST protect sensitive personal information, such as name, email address, etc. (see section 15.1 of [RFC2616]).

(2) Filename and Pathname Attacks - HTTP/1.1 servers in Receiver implementations MUST NOT expose "nearby" resources that were NOT explicitly configured for network access by administrators (see section 15.2 of [RFC2616]).

(3) DNS Spoofing Attacks - HTTP/1.1 clients and servers in Sender and Receiver implmentations SHOULD NOT cache DNS name resolution results beyond their time-to-live value (see section 15.3 of [RFC2616]).

(4) HTTP Location Header Spoofing Attacks - HTTP/1.1 servers in Receiver implementations MUST verify the validity of Location and Content-Location header data when supporting multiple trust domains (see section 15.4 of [RFC2616]).

(5) HTTP Content-Disposition Headers Attacks - HTTP/1.1 servers in Receiver implementations MUST defend against Content-Disposition header attacks (see section 15.5 of [RFC2616]).

(6) Retention of Authentication Credentials Attacks - HTTP/1.1 clients in Sender implementations SHOULD NOT retain cached user authentication credentials beyond an administratively configured idle client time (see section 15.6 of [RFC2616]).

(7) HTTP Proxy Attacks - HTTP/1.1 servers in Receiver implementations SHOULD take active measures to defend against distributed denial-of-service attacks (see section 15.7 of [RFC2616]).

8.5 TLS Security Services

Formatted: Font: (Default) Arial, 12 pt

Formatted: Heading 2, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt

8.5.1 Data Integrity and Authentication

Senders and Receivers MUST immediately perform TLS/1.0 startup [RFC2246] on all new transport layer connections, _prior_ to establishing HTTP/1.1 session layer connections. Senders and Receivers MUST successfully establish TLS/1.0 data integrity services or else MUST abort the TLS connection.

A Receiver MUST have a TLS certificate. A Sender MUST authenticate the Sender using TLS Server Authentication. Therefore, a Sender MUST have the public keys of the top-level public key Certificate Authorities (as current browsers do). If a Sender gets a public key from a Receiver that is doesn't recognize, then the Sender MUST inform the Sending User that data integrity has been lost and MUST abort the TLS connection.

A Sender MAY have a TLS certificate for TLS Client Authentication. A Receiver MAY reject TLS/1.0 connections from Senders that do not have a TLS certificate.

A Sender MAY use its own TLS certificate or it MAY use one associated with the Sending User.

The method of distribution of private keys to Senders or Receivers is outside the scope of this document, but if it is done over the network, it MUST be done over a secure channel. See Internet Key Exchange (IKE) [RFC2409].

8.5.2 Data Privacy

A Sender or a Receiver MAY negotiate TLS data privacy services (i.e., encryption) as defined in TLS/1.0 [RFC2246].

8.6 IPPFAX Printer Security Attributes

8.6.1 uri-authentication-supported (1setOf type2 keyword)

This attribute (see [RFC2911] section 4.4.2) identifies the Client Authentication mechanism associated with each URI listed in the "printer-uri-supported" attribute (see section 5.1).

Formatted: Font: (Default) Arial, 12 pt
Formatted: Heading 3, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Arial, 12 pt
Formatted: Heading 3, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Arial, 12 pt
Formatted: Heading 2, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Arial, 12 pt
Formatted: Heading 3, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Times New Roman, 12 pt

Senders MUST support the values 'none' and 'digest' and SHOULD support the value 'certificate'. Receivers MUST support the values 'none', 'digest', and 'certificate'. Senders and Receivers MUST NOT support the values 'basic' (due to cleartext passwords) or 'requesting-user-name' (due to no password).

8.6.2 uri-security-supported (1setOf type2 keyword)

This attribute (see [RFC2911] section 4.4.3) identifies the security mechanisms (for data integrity and data privacy) used for each URI listed in the "printer-uri-supported" attribute (see section 5.1).

Senders MUST support the value 'ssl3' and/or 'tls'. Receivers MUST support the value 'tls' and SHOULD support the value 'ssl3' (for best interworking). Senders and Receivers MUST NOT support the values 'none' or 'ssl2' (to avoid compromised data integrity).

9 Attribute Syntaxes

No new attribute syntaxes are defined in this document.

10 Status codes

No new Status codes are defined and semantics for existing status codes have not been modified in this document.

11 Conformance Requirements

Need to be re-worked.

The Sender MUST:

- Support PDF/is, see section 1
- Support the only the operations listed in Section 1.1

Formatted: Font: (Default) Arial, 12 pt

Formatted: Heading 3, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Normal

Deleted: IPPFAX presents an interesting challenge of balancing security and openness. Many of the envisaged uses of IPPFAX require confidentiality of the data – at the same time the Receiver typically has no prior knowledge of the Sender or the Sending User. This last point will normally rule out all user-based authentication and access control. This is the reason for the restrictions placed on querying and canceling IPPFAX Jobs.¶
<#>Data Integrity and authentication ¶
Any exchange between a Sender and a Receiver MUST be carried using the data integrity mechanism specified in IPP/1.1 namely TLS/1.0 [RFC2246] or later versions of TLS. ¶
A Receiver MUST have a TLS certificate and be authenticated by the sender.¶
A Sender MAY have a TLS certificate for client authentication. A Receiver MAY decide to reject requests that come from Senders that do not have a TLS certificate and return the 'client-error-not-authenticated' status code.¶
A Sender MAY use its own TLS certificate or it can use one associated with the Sending User.¶
A Receiver MUST have a TLS certificate, and the Send MUST have the public keys of the top level public key Certificate Authorities (as current browsers do). If a Sender gets a public key from a Receiver that is doesn't recognize, the Sender MUST resolve the unrecognized key or inform the Sending User that data integrity has been lost and MUST abort the job. ¶
The distribution of private keys to Senders or Receivers is outside the scope of this document, but if it is done ... [4]

Deleted: ¶

Formatted: Bulleted + Level: 1 + Aligned at: 0.75" + Tab after: 1" + Indent at: 1"

- Multiple URL's must conform to the rules in section 3.2
- Implement Operations defined in section 7 as required for Senders

The Receiver MUST:

Document Originator MUST:

11.1 Operation Conformance Requirements

Error! Reference source not found. lists the conformance requirements for Printer operations for (1) an IPP/1.1 Printer ('ipp' URL), (2) the non-privileged IPPFAX Sender, (3) an IPPFAX Receiver receiving a request from a non-privileged User, and (4) an IPPFAX Receiver receiving a request from an authenticated and authorized operator or administrator, if the Receiver supports operator/administrator authentication and authorization.

Error! Reference source not found. lists the conformance requirements for Job and Subscription operations for (1) an IPP/1.1 Printer ('ipp') URL, (2) the non-privileged IPPFAX Sender which MUST be on the same URL as the job was created (the target "printer-uri" MUST match the Job's "job-printer-uri" Job Description attribute), (3) an IPPFAX Receiver receiving a request from the Job or Subscription Object Owner, (4) from some other non-privileged user, and (5) if the operation is supported at all - from an authenticated and authorized operator or administrator.

816 **Table 5 - Conformance for IPPFax/1.0 Operations**

Operation Name	IPPFAX Sender support for a User	IPPFAX Receiver from a User	IPPFAX Receiver from an Operator	Reference
Print-Job	MUST	MUST	MUST	section
Get-Jobs	MUST NOT	MUST NOT	MUST	section 7.5
Get-Printer-Attributes	MUST	MUST	MUST	sections **Error! Reference source not found.**, 5
Cancel-Job				
Get-Job-Attributes				

817 Legend:
818

819 Legend:
820 **MAY*** - Get-Job-Attributes restricts certain. See section 7.5.
821 **Owner** refers to the owner of the Job or Subscription object.
822

823

824 This section summarizes the conformance requirements for Senders and Receivers that are defined
825 elsewhere in this document.

826 1. A Sender and Receiver MUST observe the attribute name space conventions specified in section
827 **Error! Reference source not found.**.

828 2. The Sender MUST supply and the Receiver MUST support (1) the "printer-uri" operation attribute
829 with the 'ippfax' scheme, (2) the "version-number" parameter with the IPP/1.1 '1.1' (or higher
830 minor version) value, and (3) the "ippfax-version" operation attribute with the IPPFAX/1.0 '1.0'
831 keyword value in all operations to get the IPPFAX semantics as described in section 4.

832 3. The Receiver MUST support the Get-Printer-Attributes operation as described in sections **Error!**
833 **Reference source not found.**.

834 4. The Receiver MUST support the Printer Description attributes as specified in section 5.

5. The Sender MUST validate that the target Printer is IPPFAX-capable using the Get-Printer-Attributes operation and validate that the Receiver supports the job using the Validate-Job operation as specified in section **Error! Reference source not found.**.

6. The Sender MUST supply and the Receiver MUST support the operation/Job Description attributes for Identify Exchange as described in section **Error! Reference source not found.**.

7. The Sender MUST support submitting and the Receiver MUST accept IPPFAX Jobs as defined in section **Error! Reference source not found.**.

8. The Sender MUST place the Sender's identity in the document according to section **Error! Reference source not found.**.

9. The Sender and Receiver MUST support the operations as indicated in section 7.

10. The Sender and Receiver MUST support the security mechanisms indicated in section 8, including TLS.

The [set-ops], enable-printer and disable-printer operations MUST only be preformed on a connection that has been authenticated by TLS and the user has the rights to perform them.

12 IPPFAX URL Scheme

Use pwg-ippfax rather than ippfax

Formatted: Highlight

Formatted: Normal

Need to be re-worked to be consistent RFC 3510

Need to register a port with IANA for IPPFax.

This section is intended for use in registering the 'ippfax' URL scheme with IANA and fully conforms to the requirements in [RFC2717].

12.1 IPPFAX URL Scheme Applicability and Intended Usage

This document defines the 'ippfax' URL (Uniform Resource Locator) scheme for specifying the location of an IPPFAX Receiver which implements the IPPFAX Protocol specified in this document.

The 'ippfax' URL scheme defined in this document is based on the ABNF for the basic hierarchical URL syntax in [RFC2396]; however relative URL forms, parameters, and/or query parts are NOT allowed in an IPPFAX URL. The 'ippfax' URL scheme is case-insensitive in the host name or host address part;

however the path part is case-sensitive, as in [RFC2396]. Codepoints outside [US-ASCII] MUST be hex escaped by the mechanism defined in [RFC2396].

The intended usage of the 'ippfax' URL scheme is COMMON.

12.2 IPPFAX URL Scheme Associated IPPFAX Port

All IPPFAX URLs which do NOT explicitly specify a port MUST be used over IANA-assigned well-known port xxx [TBA by IANA] for the IPPFAX Protocol.

See: IANA Port Numbers Registry [IANA-PORTREG].

12.3 IPPFAX URL Scheme Associated MIME Type

All IPPFAX protocol operations (requests and responses) MUST be conveyed in an 'application/ipp' MIME media type [RFC2910] as registered in [IANA-MT]. IPPFAX URLs MUST refer to IPPFAX Receivers which support this 'application/ipp' operation encoding.

See: IANA MIME Media Types Registry [IANA-MT].

12.4 IPPFAX URL Scheme Character Encoding

The IPPFAX URL scheme defined in this document is based on the ABNF for the HTTP URL scheme defined in HTTP/1.1 [RFC2616], which is derived from the URI Generic Syntax [RFC2396] and further updated by [RFC2732] and [RFC2373] (for IPv6 addresses in URLs). The IPPFAX URL scheme is case-insensitive in the 'scheme' and 'host' (host name or host address) part; however, the 'abs_path' part is case-sensitive, as in [RFC2396]. Code points outside [US-ASCII] MUST be hex escaped by the mechanism specified in [RFC2396].

12.5 IPPFAX URL Scheme Syntax in ABNF

The IPP protocol places a limit of 1023 octets (NOT characters) on the length of a URI (see section 4.1.5 'uri' in [RFC2911]). An IPPFAX Receiver MUST return 'client-error-request-value-too-long' (see section 13.1.4.10 in [RFC2911]) when a URI received in a request is too long.

Note: IPPFAX Receivers ought to be cautious about depending on URI lengths above 255 bytes, because some older client or proxy implementations might not properly support these lengths.

IPPFAX URLs MUST be represented in absolute form. Absolute URLs always begin with a scheme name followed by a colon. For definitive information on URL syntax and semantics, see "Uniform Resource Identifiers (URI): Generic Syntax and Semantics" [RFC2396]. This specification adopts the definitions of "port", "host", "abs_path", and "query" from [RFC2396], as updated by [RFC2732] and [RFC2373] (for IPv6 addresses in URLs).

The IPPFAX URL scheme syntax in ABNF is as follows:

```
ippfax_URL = "ippfax:" "//" host [ ":" port ] [ abs_path [ "?" query ]]
```

If the port is empty or not given, the IANA-assigned port as defined in section 12.2 is assumed. The semantics are that the identified resource (see section 5.1.2 of [RFC2616]) is located at the IPPFAX Notification Recipient listening for HTTP connections on that port of that host, and the Request-URI for the identified resource is 'abs_path'.

Note: The use of IP addresses in URLs SHOULD be avoided whenever possible (see [RFC1900]).

If the 'abs_path' is not present in the URL, it MUST be given as "/" when used as a Request-URI for a resource (see section 5.1.2 of [RFC2616]). If a proxy receives a host name which is not a fully qualified domain name, it MAY add its domain to the host name it received. If a proxy receives a fully qualified domain name, the proxy MUST NOT change the host name.

12.6 IPPFAX URL Examples

The following are examples of valid IPPFAX URLs for Notification Recipient objects (using DNS host names):

```
ippfax://abc.com
ippfax://abc.com/listener
```

Note: The use of IP addresses in URLs SHOULD be avoided whenever possible (see [RFC1900]).

The following literal IPv4 addresses:

```
192.9.5.5                    ; IPv4 address in IPv4 style
186.7.8.9                    ; IPv4 address in IPv4 style
```

are represented in the following example IPPFAX URLs:

```
ippfax://192.9.5.5/listener
ippfax://186.7.8.9/listeners/tom
```


The following literal IPv6 addresses (conformant to [RFC2373]):

```
::192.9.5.5                  ; IPv4 address in IPv6 style
::FFFF:129.144.52.38         ; IPv4 address in IPv6 style
2010:836B:4179::836B:4179    ; IPv6 address per RFC 2373
```

are represented in the following example IPPFAX URLs:

```
ippfax://[::192.9.5.5]/listener
ippfax://[::FFFF:129.144.52.38]/listener
ippfax://[2010:836B:4179::836B:4179]/listeners/tom
```

12.7 IPPFAX URL Comparisons

When comparing two IPPFAX URLs to decide if they match or not, the comparer MUST use the same rules as those defined for HTTP URI comparisons in [RFC2616], with the sole following exception:

- A port that is empty or not given MUST be treated as equivalent to the port as defined in section 12.2 for that IPPFAX URL;

13 IANA Considerations

IANA shall register the ippfax URL scheme as defined in section 12 according to the procedures of [RFC2717] and assign a well known port.

```
Operation Attributes:
ippfax-version (type2 keyword)            IEEE-ISTO 510n.y 4.3

Operation/Job Description attributes:
sending-user-vcard (text(MAX))                    IEEE-ISTO 510n.y 6.1
receiving-user-vcard (text(MAX))                  IEEE-ISTO 510n.y 6.2

Printer Description Attributes:
ippfax-versions-supported (1setOf type2 keyword) IEEE-ISTO 510n.y 5.3
```

14 References

14.1 Normative

[IANA-MT]
IANA Registry of Media Types: ftp://ftp.iana.orgisi.edu/in-notes/iana/assignments/media-types/.

[IANA-PORTREG]
IANA Port Numbers Registry. ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers.

[PWG5102.3-2004]
Seeler, R., "PDF Image-Streamable (PDF/is)", Work in Progress,
ftp://pwg.org/pub/pwg/QUALDOCS/pwg-ifx-pdfis-latest.pdf.

[jobx]
Hastings, T. and P. Zehler, "IPP Job Extensions", May 19, 2000,
ftp://ftp.pwg.org/pub/pwg/ipp/new_JOBX/wd-ippjobx10-20030518.pdf, work in progress.

14.2 Informative

[ifx-req]
Moore, P., "IPP Fax transport requirements", October 16, 2000,
ftp://ftp.pwg.org//pub/pwg/QUALDOCS/requirements/ifx-transport-requirements-01.pdf.

[RFC2542]
Masinter , "Terminology and Goals for Internet Fax", RFC2542.

[RFC3380]
Kugler, C, Hastings, T., Lewis, H., "Internet Printing Protocol (IPP): Job and Printer Administrative Operations", <draft-ietf-RFC3380-03.txt>, July 17, 2001.

[RFC 3382]
deBry, R., , Hastings, T., Herriot, R., "Internet Printing Protocol (IPP): collection attribute syntax",RFC 3382, September, 2002 .

[ipp-get-method]
Herriot, Kugler, and Lewis, "The 'ippget' Delivery Method for Event Notifications" , <draft-ietf-ipp-notify-get-06.txt>, November 19, 2001.

977 [ipp-iig-bis]
978 Hastings, T., Manros, C., Zehler, P., Kugler, C., and H. Holst, “Internet Printing Protocol/1.1:
979 Implementer’s Guide”, draft-ietf-ipp-implementers-guide-v11-04.txt, work in progress, intended to
980 obsolete RFC 3196 [RFC3196], October 8, 2001.

981 [RFC 3381]
982 Hastings, T., Bergman, R., Lewis, H., “Internet Printing Protocol (IPP): Job Progress Attributes”,
983 RFC 3381, September, 2002.

984 [ipp-ntfy]
985 Isaacson, S., Martin, J., deBry, R., Hastings, T., Shepherd, M., Bergman, R., “Internet Printing
986 Protocol/1.1: IPP Event Notification Specification”, <draft-ietf-ipp-not-spec-08.txt>, November 19,
987 2001.

988 [ipp-output-bin]
989 Hastings, T., and R. Bergman, “Internet Printing Protocol (IPP): output-bin attribute extension”,
990 IEEE-ISTO 5100.2-2001, February 7, 2001, ftp://ftp.pwg.org/pub/pwg/standards/pwg5100.2.pdf.

991 [ipp-prod-print]
992 Ocke, K., Hastings, T., “Internet Printing Protocol (IPP): Production Printing Attributes - Set1”,
993 IEEE-ISTO 5100.3-2001, February 12, 2001, ftp://ftp.pwg.org/pub/pwg/standards/pwg5100.3.pdf.

994 [ipp-set-ops]
995 Hastings, Herriot, Kugler, and Lewis, “Job and Printer Set Operations”, <draft-ietf-ipp-job-printer-
996 set-ops-05.txt>, August 28, 2001.

997 [ipp-uri-scheme]
998 Herriot, McDonald, “IPP URL Scheme”, <draft-ietf-ipp-url-scheme-03.txt>,April 3, 2001.

999 [pwg-media]
1000 Bergman, Hastings, “Media Standardized Names”, work in progress, when approved:
1001 ftp://ftp.pwg.org/pub/pwg/standards/pwg5101.1.pdf; current draft:
1002 ftp://ftp.pwg.org/pub/pwg/media-sizes/pwg-media-12.pdf, September 24, 2001.

1003 [RFC1900]
1004 B. Carpenter, Y. Rekhter. Renumbering Needs Work, RFC 1900, February 1996.

1005 [RFC2069]
1006 Franks, Hallam-Baker, Hostetler, Leach, Luotonen,, Sink, Stewart, “An Extension to HTTP: Digest
1007 Access Authentication”, RFC2069.

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", RFC2119.

[RFC2246]
Dierks, Allen "The TLS Protocol Version 1.0", RFC 2246.

[RFC2305]
Toyoda, Ohno, Murai, Wing "A Simple Mode of Facsimile Using Internet Mail", RFC2305.

[RFC2373]
R. Hinden, S. Deering. IP Version 6 Addressing Architecture, RFC 2373, July 1998.

[RFC2396]
Berners-Lee, T. et al. Uniform Resource Identifiers (URI): Generic Syntax, RFC 2396, August 1998.

[RFC2409]
Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2425]
T. Howes, M. Smith, F. Dawson, "A MIME Content-Type for Directory Information", RFC 2425, September 1998.

[RFC2426]
Dawson, Howes, "vCard MIME Directory Profile", RFC 2426, September 1998 [version v3.0].

[RFC2532]
Masinter, Wing, "Extended Facsimile Using Internet Mail", RFC2532.

[RFC2616]
R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol - HTTP/1.1", RFC 2616, June 1999.

[RFC2617]
J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC2732]
R. Hinden, B. Carpenter, L. Masinter. Format for Literal IPv6 Addresses in URL's, RFC 2732, December 1999.

[RFC2818]
E. Rescorla, "HTTP Over TLS", May 2000.

[RFC2910]
Herriot, Butler, Moore, Turner, Wenn, "Internet Printing Protocol/1.1: Encoding and Transport", RFC2910, September 2000.

[RFC2911]
deBry, Hastings, Herriot, Isaacson, Powell, "Internet Printing Protocol/1.1: Model and Semantics", RFC2911, September 2000.

[RFC3196]
Hastings, T., Manros, C., Zehler, P., Kugler, C., and H. Holst, "Internet Printing Protocol/1.1: Implementer's Guide", RFC 3196, November, 2001.

[X509]
CCITT. Recommendation X.509: "The Directory - Authentication Framework", 1988.

15 Authors' addresses

Thomas N. Hastings Xerox Corporation 701 Aviation Blvd. El Segundo, CA 90245 Phone: +1 310-333-6413 FAX: +1 310-333-5514 email: hastings@cp10.es.xerox.com	Ira McDonald High North Inc 221 Ridge Ave Grand Marais, MI 49839 Phone: +1 906-494-2434 Email: imcdonald@sharplabs.com
	Gail (Songer) Giansiracusa Peerless Systems Corp 2381 Rosecrans Ave El Segundo, CA 90245 Phone: +1 650-358 8875 Email: gsonger@peerless.com
	Rick Seeler Adobe Systems Incorporated 321 Park Ave. San Jose, CA 95110 Phone: +1 408- 536-4393 Email: rseeler@adobe.com

Dennis Carney IBM 6300 Diagonal Highway Boulder, CO 80301 Phone: +1 303-924-0565 Email: dcarney@us.ibm.com	

Contact Information:

IPPFAX Web Page: http://www.pwg.org/qualdocs/
IPPFAX Mailing List: ifx@pwg.org

To subscribe to the IPPFAX mailing list, send the following email:
1) send it to majordomo@pwg.org
2) leave the subject line blank
3) put the following two lines in the message body:
subscribe ifx
end

Implementers of this specification document are encouraged to join the IPPFAX Mailing List in order to participate in any discussions of clarification issues and review of registration proposals for additional attributes and values. In order to reduce spam the mailing list rejects mail from non-subscribers, so you must subscribe to the mailing list in order to send a question or comment to the mailing list.

Other Participants:

Aisushi Uchino - Epson	Marty Joel - Peerless
Bill Wagner - NetSilicon/DPI	Michael Wu - Heidelberg Digital
Carl-Uno Manros - Xerox	Mike Kuindersma - PrinterOn
Charles Kong - Panasonic	Norbert Schade - Oak Technology
Dan Calle - Digital Paper	Patrick Pidduck - PrinterOn
David Kellerman – Northlake	Peter Zehler – Xerox
Don Wright - Lexmark	Rich Heckelmann - Panasonic USA
Elliott Bradshaw – Oak Technologies	Richard Shockey - Newstar
Frank Martin - Brother	Rob Buckley - Xerox
Fumio Nagasaka – Epson	Robert Herriot - Xerox
Geoff Soord - Software 2000	Roelop Hamberg - Oce
Harry Lewis - IBM	Ron Bergman - Hitachi Koki
Howard Sidorski - Netreon	Satoshi Fujitani - Ricoh

Hugo Parra - Novell	Shigeru Udea - Canon
Jeff Christensen - Novell	Shinichi Tsuruyama - Epson
Jerry Thrasher - Lexmark	Stuart Rowley - Kyocera
John Thomas - Sharp Labs	Ted Tronson - Novell
Koichi “Hurry” Izuhara - Minolta	Toru Maeda - Canon
Lee Farrell - Canon Info Systems	Yiruo Yang – Epson
Lloyd McIntyre	Yuji Sasaki - JCI
Mark VanderWiele - IBM	Paul Moore -
John Pulera - Minolta	

1. Appendix A:

16 Appendix B: vCard Example

Update the example

The following ASCII text is a complete vCard v3.0 [RFC2426, RFC2425] example:

```
BEGIN:VCARD
VERSION:3.0
N:Moore;Paul
FN:Paul Moore
ORG:Netreon
TEL;CELL;VOICE:1+206-251-7008
ADR;WORK:;;10900 NE 8th St;Bellvue;WA;98004;United States of America
EMAIL;PREF;INTERNET:pmoore@netreon.com
REV:19991207T215341Z
END:VCARD
```

17 Revision History (to be removed when standard is approved)

Revision	Date	Author	Notes
1	1/16/01	Paul Moore, Netreon	Initial version
2	2/27/01	Paul Moore, Gail Songer, Netreon	Specify TLS as MUST Removed Cover page and combined device

			Added need for big text types
3	4/11/01	Gail Songer, Netreon	Move attribute definition to first reference
4	5/24/01	Tom Hastings	Editorially updated the document to follow the style of the IPP standard documents. Added 23 issues to be reviewed. Capitalized the special terms throughout without showing revisions in order to make the document with revisions more readable.
5	5/21/01	Tom Hastings, John Pulera, Ira McDonald	Updated from the 6/6/01 telecon agreements on most of the 23 issues. There are 20 issues remaining, mostly new.
6	7/27/01	Tom Hastings, Ira McDonald	Updated from the 6/29/01 telecon. There are 41 issues remaining, mostly new.
7	10/8/01	Tom Hastings, Ira McDonald	Updated with all the resolutions to the 41 ISSUES from the August 1, 2001 IPPFAX WG meeting in Toronto, and the subsequent telecons: August, 9, 14, and 17, 2001. There are 4 (new) issues remaining.
8	11/17/01	Tom Hastings	Updated with the agreements from the IPPFAX WG meeting, 10/24/01, Texas. See minutes. There are 5 issues remaining.
9	12/31/01	Tom Hastings	Updated with the agreements reached at the 12/14/01 telecon.
10	2/19/02	Tom Hastings	Updated with the agreements reached as the 2/5/02 IPPFAX WG meeting. There are no remaining issues.
11	9/20/02	Tom Hastings	Replaced all occurrences of UIF with PDFax and uif with PDFax.
12	10/16/02 10/24/02	Rick Seeler Gail Songer	Updated to reflect PDF/is as file format. Replace CONNEG with UPDF. Attributes for OPTIONAL PDF/is functionality.
13	11/22/02	Rick Seeler	Replaced ‘PDFax’ with ‘PDF/is’ or ‘pdfis’. Updated spec to match 0.3 PDF/is specification.
14	03/18/03	Gail Songer	Removed pdfis-profile-requested and pdfis-profile-supported and pdfis-profiles; all image formats are required Removed pdfis-cache-size-k-octets (now fixed value) Removed pdfis-banding-direction-supported Started to split references into two sections, “normative” and “informative” and update descriptions to references Other editorial changes

15	03/24/03	Gail Songer	Added digital-signatures-supported. Added pdf-format and pdf-format supported. Put “coloring” back to optional. Removed PDF data encryption (leave for a future version of PDF/is and IPPFax)
16		Gail Songer Dennis Carney	Remove all references to coloring Changed pdf-format to document-format-version Remove the requirement that [set-ops] supports document-format coloring (we only allow document-format==PDF) ALL admin operations require TLS to have authenticated the user and the user has admin rights Other editorial changes
17	05/21/03 05/28/03	Dennis Carney Tom Hastings	Editorial updates Added new ‘choice_iso_a4_210x297mm_na_letter_8.5x11in’ value for “media” and a reference to [jobx]. Fixed conformance for “media-ready”.
18	10/03 11/03	Gail Songer	Reviewed in light of the Requirements specification. Noted lots of places in which the document MUST be changed.
19	5/24/04	Gail (Songer) Giansiracusa	

Allow Cancel-job for Administrators.

Page 9: [1] Deleted **gsonger** **5/19/2004 1:24 PM**

This document uses the term "client" when the statement is intended to apply to a client that MAY support the IPP Protocol, the IPPFAX protocol, or both protocols.

Page 23: [2] Deleted **gsonger** **5/5/2004 1:42 PM**

Separate into two sections! Get-Jobs is Operator/Admin only operation

The public nature of IPPFAX interactions make it inappropriate for a client to be able to query a Receiver for certain information about jobs that it did not send.

The Receiver SHOULD restrict the job attributes that any Sender can request for any IPPFAX Job in a Get-Jobs or a Get-Job-Attributes operation to appropriate ones for a public service. For example, a Receiver MAY return only the following Job attributes:

job-id, job-uri
job-k-octets, job-k-octets-completed
job-media-sheets, job-media-sheets-completed,
time-at-creation, time-at-processing
job-state, job-state-reasons
number-of-intervening-jobs – NOT!!!!!

The exact choice of Job attributes that a client can query for IPPFAX Jobs, including not returning any, DEPENDS ON IMPLEMENTATION and the security policy in force and is outside the scope of this standard (as in IPP/1.1).

This attribute set allows a client to determine the load on a Receiver (and perhaps choose an alternative destination or warn the Sending User).

See the discussion in [RFC2911] section 8.4 for a description of how a Receiver MUST behave if it receives a request for an attribute outside this set.

An IPP administrator MAY read all attributes.

Page 23: [3] Formatted **gsonger** **5/24/2004 9:10 AM**

Font: (Default) Times New Roman, 12 pt

Page 29: [4] Deleted **gsonger** **5/24/2004 9:08 AM**

IPPFAX presents an interesting challenge of balancing security and openness. Many of the envisaged uses of IPPFAX require confidentiality of the data – at the same time the Receiver typically has no prior knowledge of the Sender or the Sending User. This last point will normally rule out all user-based authentication and access control. This is the reason for the restrictions placed on querying and canceling IPPFAX Jobs.

8.1Data Integrity and authentication

Any exchange between a Sender and a Receiver MUST be carried using the data integrity mechanism specified in IPP/1.1 namely TLS/1.0 [RFC2246] or later versions of TLS.

A Receiver MUST have a TLS certificate and be authenticated by the sender.

A Sender MAY have a TLS certificate for client authentication. A Receiver MAY decide to reject requests that come from Senders that do not have a TLS certificate and return the 'client-error-not-authenticated' status code.

A Sender MAY use its own TLS certificate or it can use one associated with the Sending User.

A Receiver MUST have a TLS certificate, and the Send MUST have the public keys of the top level public key Certificate Authorities (as current browsers do). If a Sender gets a public key from a Receiver that is doesn't recognize, the Sender MUST resolve the unrecognized key or inform the Sending User that data integrity has been lost and MUST abort the job.
The distribution of private keys to Senders or Receivers is outside the scope of this document, but if it is done over the network, it MUST be over a secure channel. See Internet Key Exchange (IKE) [RFC2409].

8.2Data Privacy (encryption)

A Sender MAY chose use data privacy (encryption) as defined in TLS/1.0 [RFC2246].

8.3uri-authentication-supported (1setOf type2 keyword)

This attribute (see [RFC2911] section 4.4.2) identifies the Client Authentication mechanism associated with each URI listed in the "printer-uri-supported" attribute (see section 5.1).
Table 5 - Authentication Requirements

"uri-authentication-supported" keyword	Sender support and usage	Receiver support and usage
none	MAY support and MAY use	MAY support and MAY use. If the 'none' value is supported by an implementation, then the administrator MUST be able to configure the Printer to not support the 'none' value (by means outside the scope of this document)
requesting-user-name	MUST NOT	MUST NOT
basic	MAY support and MAY use when the TLS channel is secured with Data Privacy using the cipher suites indicated below* or stronger	MAY support and MAY use when the TLS channel is secured with Data Privacy using the cipher suites indicated below* or stronger
digest	MUST support and MUST use, including the MD5 and MD5-sess algorithms and Message Integrity, unless using 'certificate' or 'negotiate'	MUST support and MAY use, including the MD5 and MD5-sess algorithms and Message Integrity
certificate	SHOULD support and MAY use when not using any of the above	MUST support and MAY use. For this value, the Receiver MUST validate the certificate for all client requests

* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA mandated by [RFC2246].
Table 6 compares the Digest Authentication requirements for IPP/1.1 clients, IPP/1.1 Printers, IPPFAX Senders, and IPPFAX Receivers.
Table 6 - Digest Authentication Conformance Requirements

Feature	IPP/1.1 Client	IPP/1.1 Printer	IPPFAX Sender	IPPFAX

				Receiver
MD5 and MD5-sess	must support must use	should support should use	MUST support MUST use	MUST support MUST use
The Message Integrity feature	must support may use	should support may use	MUST support MUST use	MUST support MUST use

8.4uri-security-supported (1setOf type2 keyword)

This attribute (see [RFC2911] section 4.4.3) identifies the security (Integrity and Privacy) mechanisms used for each URI listed in the "printer-uri-supported" attribute (see section 5.1).

Table 7 - Security (Integrity and Privacy) Requirements

uri-security-supported	Sender support and usage	Receiver support and usage
none	MUST NOT	MUST NOT
ssl2	MUST NOT	MUST NOT
ssl3	MUST NOT	MUST NOT
tls	TLS Data Integrity - MUST support and MUST use	MUST support and MUST use
	TLS Data Privacy - MUST support and MAY use. The Sender (device) MUST query the Sending User (human) before omitting Privacy (encryption).	MUST support and MAY use

Table 8 compares the TLS conformance requirements for IPP/1.1 clients, IPP/1.1 Printers, IPPFAX Senders, and IPPFAX Receivers.

Table 8 - Transport Layer Security (TLS) Conformance Requirements

TLS Feature	IPP/1.1 Client	IPP/1.1 Printer	IPPFAX Sender	IPPFAX Receiver
Server Authentication	must support should use	should support may use	MUST use	MUST support
Client Authentication*	may support may use	may support may use	SHOULD support	MUST support MAY use
Data Integrity	may support may use	should support should use	MUST use	MUST support
Data Privacy	may support may use	should support may use	MUST support MAY** use.	MUST support

* The 'certificate' keyword value for the "uri-authentication-supported" attribute [RFC2911].

** The Sender MUST query the Sending User before omitting the Data Privacy encryption.

Senders and Receivers MUST support the TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite as mandated by RFC 2246 [RFC2246]. All stronger cipher suites are OPTIONAL; weaker cipher suites MUST NOT be supported or used by Senders or Receivers.

A Receiver MAY support Basic Authentication (described in HTTP/1.1 [RFC2617]) for Client Authentication if the TLS channel is secured with Data Privacy. TLS with the above mandated cipher suite or stronger can provide such a secure channel.

8.5Using IPPFAX with TLS

The Sender MUST use only TLS for all IPPFAX operations on the IPPFAX URL. The client MUST start the transaction in TLS, rather than using HTTP upgrade requests. The following paragraph of [RFC2818] further explains:

> The agent acting as the HTTP client should also act as the TLS client. It should initiate a connection to the server on the appropriate port and then send the TLS ClientHello to begin the TLS handshake. When the TLS handshake has finished. The client may then initiate the first HTTP request. All HTTP data MUST be sent as TLS "application data". Normal HTTP behavior, including retained connections should be followed.

Contrast this IPPFAX requirement with the IPP requirement in section 8.2 of [RFC2910]. The following client actions compare IPP with IPPFAX from a client's point of view:

IPP/1.1 sequence:

1. Start TCP connection
2. Zero or more HTTP/IPP requests
3. HTTP/IPP request with Upgrade to TLS header
4. TLS handshake
5. Finish the HTTP/IPP request securely
6. Send more HTTP/IPP requests securely ...

IPPFAX sequence:

1. Start TCP connection
2. Send TLS ClientHello
3. Rest of TLS handshake
4. Send HTTP/IPPFAX requests securely ... (which usually will be a Get-Printer-Attributes, followed by the Print-Job operation).

8.6Access control

Needs re-writting

It is expected that the majority of IPPFAX Receivers will operate in a public mode when operating on the Internet, so that anonymous users can send documents without requiring client authentication (corresponding to the 'none' value for the "uri-authentication-supported" attribute - see section 8.3). However a Receiver MAY protect itself using any Client Authentication method specified in [RFC2911] (digest authentication [RFC2069] for example) to restrict access to any or all of its functionality.

However, the primary intent of IPPFAX is to create a controlled public access mode. It therefore does not really make much sense to combine IPPFAX and user authentication; they are achieving the same thing.

8.7Reduced feature set

Needs re-writting

An administrator or device implementer MAY choose to setup up a Print Service so that it only works as an IPPFAX Receiver (i.e., offers no ‘native’ IPP operations and does not accept IPP Jobs). In this mode it offers a restricted set of features and MAY be more safely connected to the Internet.

A Receiver that is operating in this mode MUST do so by rejecting any non-IPPFAX request and return a ‘client-error-attributes-or-values-not-supported’ error status code as indicated in section 4.1 for an unsupported value of the “printer-uri” operation attribute. For job operations attempted on IPPFAX Jobs, the Receiver MUST return the ‘client-error-not-authorized’ error status code, unless the Sender is authenticated as the system administrator and the Receiver supports such access.