

1 **IEEE-ISTO**  
2 **Printer Working Group**  
3 **IPP Fax Project**  
4 **Standard for IPPFAX/1.0 Protocol**

5  
6 **Working Draft**  
7 **Maturity: Initial**  
8  
9



10  
11 **Version 1.0**  
12 **May 24, 2004**  
13  
14

15  
16 **Abstract:** This document specifies the IPPFAX/1.0 protocol. The IPPFAX requirements [ifx-req] are derived from the requirements for  
17 Internet Fax [RFC2542].  
18 In summary, IPPFAX is used to provide a synchronous, reliable exchange of image Documents between clients and servers. The  
19 primary use envisaged of this protocol is to provide a synchronous image transmission service for the Internet. Contrast this with the  
20 Internet FAX protocol specified in [RFC2305] and [RFC2532] that uses the SMTP mail protocol as a transport.  
21 The IPPFAX/1.0 protocol is a specialization of the IPP/1.1 [RFC2911], [RFC2910] protocol supporting a subset of the IPP operations  
22 with increased conformance requirements in some cases, some restrictions in other cases, and some additional REQUIRED  
23 attributes. The IPPFAX Protocol uses the 'ippfax' URL scheme (instead of the 'ipp' URL scheme) in all its operations. Most of the  
24 new attributes defined in this document MAY be supported by IPP Printers as OPTIONAL extensions to IPP as well  
25 An IPPFAX Printer object is called a Receiver. A Receiver MUST support at least the PDF/IS as specified in [PWG5102.3-2004] which  
26 is defined for the 'application/pdf' document format MIME type. A Print System MAY be configured to support both the IPPFAX and  
27 IPP protocols concurrently, but each protocol requires separate Printer objects with distinct URLs.  
28

29 This document is available electronically at: [wd-afx10-20040524.pdf](http://wd-afx10-20040524.pdf), .doc  
30 A version showing the changes from the previous version is available at: [wd-afx10-20040524-rev.pdf](http://wd-afx10-20040524-rev.pdf)  
31 The latest version of this specification is available at: [ftp://pwg.org/pub/pwg/QUALDOCS/wd-afx10-latest.pdf](http://ftp://pwg.org/pub/pwg/QUALDOCS/wd-afx10-latest.pdf), .doc

32 **Copyright (C) 2004, IEEE ISTO. All rights reserved.**

33 This document may be copied and furnished to others, and derivative works that comment on, or otherwise explain it  
34 or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without  
35 restriction of any kind, provided that the above copyright notice, this paragraph and the title of the Document as  
36 referenced below are included on all such copies and derivative works. However, this document itself may not be  
37 modified in any way, such as by removing the copyright notice or references to the IEEE-ISTO and the Printer  
38 Working Group, a program of the IEEE-ISTO.

39 Title: The IPPFAX/1.0 Protocol

40 The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES, WHETHER EXPRESS  
41 OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR  
42 FITNESS FOR A PARTICULAR PURPOSE.

43 The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make changes to the document  
44 without further notice. The document may be updated, replaced or made obsolete by other documents at any time.

45 The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might  
46 be claimed to pertain to the implementation or use of the technology described in this document or the extent to  
47 which any license under such rights might or might not be available; neither does it represent that it has made any  
48 effort to identify any such rights.

49 The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or  
50 other proprietary rights which may cover technology that may be required to implement the contents of this  
51 document. The IEEE-ISTO and its programs shall not be responsible for identifying patents for which a license may  
52 be required by a document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the legal  
53 validity or scope of those patents that are brought to its attention. Inquiries may be submitted to the IEEE-ISTO by e-  
54 mail at:

55 [ieee-isto@ieee.org](mailto:ieee-isto@ieee.org).

56 The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its designees) is, and shall at  
57 all times, be the sole entity that may authorize the use of certification marks, trademarks, or other special  
58 designations to indicate compliance with these materials.

59 Use of this document is wholly voluntary. The existence of this document does not imply that there are no other  
60 ways to produce, test, measure, purchase, market, or provide other goods and services related to its scope.

**61 About the IEEE-ISTO**

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

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

67

**68 About the IEEE-ISTO PWG**

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

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

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

**82 Contact information:**

83 IFX Web Page: <http://www.pwg.org/qualdocs>

84 IFX Mailing List: [ifx@pwg.org](mailto:ifx@pwg.org)

85 To subscribe to the ipp mailing list, send the following email:

86 1) send it to [majordomo@pwg.org](mailto:majordomo@pwg.org)

87 2) leave the subject line blank

88 3) put the following two lines in the message body:

89 subscribe ifx

90 end

91

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

94

95	<b>Contents</b>	
96	1 Introduction .....	7
97	1.1 Typical exchange.....	8
98	2 Terminology .....	8
99	2.1 Conformance Terminology .....	8
100	2.2 Other Terminology .....	9
101	3 IPPFAX Model.....	10
102	3.1 Printer Object Relationships.....	10
103	3.2 A Printer object with multiple URLs.....	10
104	4 Common IPPFAX Operation Attribute Semantics.....	11
105	4.1 printer-uri (uri) operation attribute .....	11
106	4.2 version-number parameter .....	11
107	4.3 ippfax-version (type2 keyword) operation attribute.....	12
108	5 IPPFAX Printer Description Attributes.....	12
109	5.1 printer-uri-supported (1setOf uri).....	13
110	5.2 ipp-versions-supported (1setOf type2 keyword).....	13
111	5.3 ippfax-versions-supported (1setOf type2 keyword).....	14
112	5.4 operations-supported (1setOf type2 enum) .....	14
113	5.5 document-format-supported (1setOf mimeType) .....	15
114	5.6 document-format-version-supported (1setOf text(127)) .....	15
115	5.7 digital-signatures-supported (1setOf type2 keyword).....	15
116	5.8 pdl-override-supported (type2 keyword).....	15
117	6 IPPFax Job Description Attributes .....	15
118	6.1 sending-user-vcard (text(MAX)).....	16
119	6.2 receiving-user-vcard (text(MAX)).....	16
120	6.3 xxx-supplied attributes .....	17
121	7 IPPFAX Operations.....	17
122	7.1 Required Operations and Features .....	17
123	7.2 Get-Printer-Attributes.....	18
124	7.3 Print-Job .....	18
125	7.3.1 Operation Attributes .....	18
126	7.3.2 Job Template Attributes .....	21
127	7.3.3 Delivery Confirmation using the Print-Job response .....	23
128	7.3.4 Originator identifier image.....	23
129	7.4 Cancel-Job operation.....	23

130	7.5 Get-Job-Attributes .....	23
131	7.6 Get-Jobs.....	23
132	8 Security considerations.....	23
133	8.1 Internet Threat Model.....	24
134	8.1.1 Passive Attacks.....	24
135	8.1.2 Active Attacks .....	25
136	8.2 Enterprise Threat Model.....	26
137	8.3 Mobile Threat Model.....	26
138	8.4 HTTP Threat Model .....	26
139	8.5 TLS Security Services .....	27
140	8.5.1 Data Integrity and Authentication .....	28
141	8.5.2 Data Privacy .....	28
142	8.6 IPPFAX Printer Security Attributes .....	28
143	8.6.1 uri-authentication-supported (1setOf type2 keyword) .....	28
144	8.6.2 uri-security-supported (1setOf type2 keyword) .....	29
145	9 Attribute Syntaxes .....	29
146	10 Status codes .....	29
147	11 Conformance Requirements .....	29
148	11.1 Operation Conformance Requirements .....	30
149	12 IPPFAX URL Scheme.....	32
150	12.1 IPPFAX URL Scheme Applicability and Intended Usage.....	32
151	12.2 IPPFAX URL Scheme Associated IPPFAX Port.....	33
152	12.3 IPPFAX URL Scheme Associated MIME Type .....	33
153	12.4 IPPFAX URL Scheme Character Encoding.....	33
154	12.5 IPPFAX URL Scheme Syntax in ABNF .....	33
155	12.6 IPPFAX URL Examples.....	34
156	12.7 IPPFAX URL Comparisons .....	35
157	13 IANA Considerations .....	35
158	14 References .....	35
159	14.1 Normative .....	35
160	14.2 Informative .....	36
161	15 Authors' addresses.....	39
162	16 Appendix B: vCard Example.....	41

163 17 Revision History (to be removed when standard is approved) ..... 41

164

165

**Table of Tables**

166 Table 1 - Printer Description attributes conformance requirements ..... 13

167 Table 2 - Summary of Job Description attributes..... 16

168 Table 3 - Print-Job operation attributes..... 19

169 Table 4 - IPPFAX Defaults for unsupported Job-Template Attributes..... 21

170 Table 5 - Authentication Requirements..... 29

171 Table 6 - Digest Authentication Conformance Requirements ..... 29

172 Table 7 - Security (Integrity and Privacy) Requirements..... 29

173 Table 8 - Transport Layer Security (TLS) Conformance Requirements..... 29

174 Table 9 - Conformance for IPPFax/1.0 Operations..... 31

175

176 **1 Introduction**

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

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

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

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

192 An IPPFAX Printer object is called a Receiver. A Receiver must support at least PDF/IS [PWG5102.3-  
193 2004] which is defined for the 'application/pdf' document format MIME type.

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

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

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

203

**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].¶

204 | **1.1 Typical exchange**

Deleted: (informative)  
Formatted: Bullets and Numbering

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

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

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

214 | 3. The Sender can determine other PDF versions supported by the Receiver and the Sender can  
215 discover “media-supported” and “media-ready”.

Deleted: MAY  
Deleted: MAY

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

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

Deleted: SHOULD

221 | **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

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

224 | **2 Terminology**

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

226 **2.1 Conformance Terminology**

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



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

234 **2.2 Other Terminology**

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

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

240 **IPPFAX Protocol** The protocol defined in this document.

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

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

246 **Print Service** The print functionality offered by a Printer object.

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

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

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

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

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

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

257 **Document** The electronic representation of a set of one or more pages that the Sender sends to the  
258 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 support ... [1]

- 259 **Sending User** The person interacting with the Sender.
- 260 **Receiving User** The intended human recipient of the Document being sent by the Sender to the Receiver.
- 261 **IPP Job** A job submitted by an IPP client to an IPP Printer object using the IPP Protocol.
- 262 **IPPFAX Job** A job submitted by a Sender to a Receiver using the IPPFAX Protocol.
- 263 **PDF/is** The file format defined by [PWG5102.3-2004].
- 264 The terminology defined in [RFC2911], such as **attribute**, **operation**, **request**, **response**, **operation**  
265 **attribute**, **Printer Description attribute**, **Job Description attribute**, **integrity**, and **privacy** is also used  
266 in this document with the same capitalization conventions and semantics.

## 267 **3 IPPFAX Model**

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

### 269 **3.1 Printer Object Relationships**

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

### 275 **3.2 A Printer object with multiple URLs**

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

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

284

## 285 **4 Common IPPFAX Operation Attribute Semantics**

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

### 290 **4.1 printer-uri (uri) operation attribute**

291 This operation attribute specifies the transfer path to the Receiver for the operation. As in IPP/1.1, the  
292 client MUST supply the “printer-uri” operation attribute in every IPPFAX request (see [RFC2911] section  
293 3.1.5). For IPPFAX, the attribute value MUST be a URL using the ‘ippfax’ scheme (see section 12)  
294 specifying the Receiver’s network location.

295 The following is an example value of the target “printer-uri” operation attribute and “printer-uri-supported”  
296 Printer Description attribute:

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

298 As in IPP/1.1 [RFC2911] for each operation, the Receiver NEED NOT validate that the “printer-uri”  
299 operation attribute is present and that the value supplied by the Sender matches one of the Receiver’s  
300 “printer-uri-supported” Printer Description attribute (see section 5.1). For URI matching rules see section  
301 12.7. If the Receiver does validate the “printer-uri” operation attribute and the URI value supplied does not  
302 match any value of the Receiver’s “printer-uri-supported” Printer Description attribute, the Receiver  
303 MUST reject the request, return the ‘client-error-attributes-or-values-not-supported’ status code, and return  
304 the attribute and value in the Unsupported Attributes Group.

### 305 **4.2 version-number parameter**

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

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

311

### 312 **4.3 ippfax-version (type2 keyword) operation attribute**

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

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

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

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

## 326 **5 IPPFAX Printer Description Attributes**

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

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

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

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

335

**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 mimeType) *	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

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

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

#### 340 **5.1 printer-uri-supported (1setOf uri)**

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

#### 345 **5.2 ipp-versions-supported (1setOf type2 keyword)**

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

353 Standard keyword values are (from [RFC2911]):

354 ‘1.1’: The IPPFAX operations meets encoding conformance requirements of IPP version 1/1 as specified  
355 in [RFC2911] and [RFC2910].  
356

**357 5.3 ippfax-versions-supported (1setOf type2 keyword)**

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

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

365 Standard keyword values are:

366 ‘1.0’: Meets the conformance requirements of IPPFAX 1/0 as specified in this document.

367

**368 5.4 operations-supported (1setOf type2 enum)**

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

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

376 A receiver MUST only support the following operations:

Formatted: Not Highlight

- 377 • get-printer-attributes
- 378 • print-job
- 379 • cancel-job
- 380 • get-jobs
- 381 • get-job-attributes

382 A receiver MUST NOT support any other operation.

383 **5.5 document-format-supported (1setOf mimeType)**

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

387 **5.6 document-format-version-supported (1setOf text(127))**

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

392 **5.7 digital-signatures-supported (1setOf type2 keyword)**

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

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

397 **5.8 pdl-override-supported (type2 keyword)**

398 This attribute (see [RFC 2911] section 4.4.28) identifies Receiver implementation support for overriding  
399 document data instructions with IPPFax job attributes. A Receiver MUST support this printer subscription  
400 attribute with the value 'attempted'. . A Receiver MUST attempt to override at least the media attribute.  
401

402 **6 IPPFax Job Description Attributes**

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

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 (mimeType)**	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



427 **6.3 xxx-supplied attributes**

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

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

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

Deleted:

437 **7 IPPFAX Operations**

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

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

Formatted: Bullets and Numbering

444 **7.1 Required Operations and Features**

445 All IPPFax Senders and Receivers MUST support the following operations:

- 446
- 447 1. Get-Printer-Attributes - If the document-format-version is not PDF/is or the media is not  
 448 iso\_a4 210x297mm or na\_letter 8.5x11in, then the Sender MUST verify that the Receiver can  
 449 support the alternate attributes. Rational: Using Get-Printer-Attributes would avoid rejection of  
 450 the job which is important if the document data is very large.
  - 451 2. Print-Job - Sender MUST submit the IPPFAX job with a single document (Create-Job, Send-  
 452 document and Send-URI and Print-URI MUST NOT be supported by Senders or Receivers).
  - 453 3. Get-Job-Attributes - The Sender MUST support and MUST use this operation to check for  
 454 successful job completion unless the Sending User wishes otherwise. Job-History MUST be

Formatted: Bullets and Numbering

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

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

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

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

463 All IPPFax Receivers MUST support receiving PFD/is version 1.0 as defined in [PWG5102.3-  
464 2004].

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

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

← - - - Formatted: Bullets and Numbering

467 **7.2 Get-Printer-Attributes**

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

Deleted: r

Deleted:

Deleted: a

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

← - - - Formatted: Bullets and Numbering

472 **7.3 Print-Job**

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

← - - - Formatted: Bullets and Numbering

476 **7.3.1 Operation Attributes**

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

479 **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 <sup>1</sup>	MUST
document-name (name(MAX)) *	7.3.1.2	MAY	MUST
compression (type3 keyword) *		MAY	MUST
document-format (mimeMediaType) *	7.3.1.3	MUST <sup>2</sup>	MUST
document-format-version (type2 keyword) *	7.3.1.4	MUST <sup>3</sup>	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 <sup>3</sup>	MUST
receiving-user-vcard (text(MAX))	6.2	SHOULD <sup>3</sup>	MUST

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

482

Formatted: Bullets and Numbering

483 **7.3.1.1 ipp-attribute-fidelity**

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

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

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

<sup>3</sup> These attributes were not defined in [RFC2911].

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

Formatted: Bullets and Numbering

#### 491 **7.3.1.2 document-name (naturalLanguage)**

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

Formatted: Bullets and Numbering

#### 495 **7.3.1.3 document-format (mimeMediaType)**

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

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

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

Formatted: Bullets and Numbering

#### 506 **7.3.1.4 document-format-version (type2 keyword)**

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

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

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

515 See section 5.6.

516 **7.3.1.5 document-charset (charset)**

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

Formatted: Bullets and Numbering

520 **7.3.1.6 document-natural-language (naturalLanguage)**

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

Formatted: Bullets and Numbering

524 **7.3.1.7 document-digital-signature (type2 keyword)**

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

Formatted: Bullets and Numbering

528 **7.3.2 Job Template Attributes**

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

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

Formatted: Bullets and Numbering

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

537

538 **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

### 539 **7.3.2.1 media (type2 keyword | name(MAX))**

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

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

545 A Receiver MUST at least support the sizes ‘na\_letter\_8.5x11in’ and ‘iso\_a4\_210x297mm’ and MUST be  
 546 able to print on at least one of those two sizes. The Receiver MAY scale down at most 10% (PDF/is  
 547 directives may prohibit this scaling for quality reasons), overflow to another page, or truncate. If the  
 548 Receiver does truncate then it MUST notify the Receiving User. A Receiver MUST perform only  
 549 isomorphic scaling.

550  
 551 A Sender SHOULD use PDF Crop boxes when the Sender knows that the imageable region is less than the  
 552 media size. If the crop box is the union of the lesser size of iso\_a4\_210x297mm and na\_letter\_8.5x11in  
 553 minus 1/2 of an inch, then the Sender can be sure that the majority of Receivers can print the complete  
 554 image without loss of data. However, this does not eliminate that the possibility that data may be lost.

555

Formatted: Bullets and Numbering

### 556 **7.3.2.2 media-supported**

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

559 ‘na\_letter\_8.5x11in’

560 ‘iso\_a4\_210x297mm’

561 ‘choice\_iso\_a4\_210x297mm\_na\_letter\_8.5x11in’ - represents both ‘na\_letter\_8.5x11in’ and  
 562 ‘iso\_a4\_210x297mm’ and indicates that either is acceptable. See [PWG5100.7].

563 **7.3.3 Delivery Confirmation using the Print-Job response**

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

568 **7.3.4 Originator identifier image**

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

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

575 **7.4 Cancel-Job operation**

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

578 **7.5 Get-Job-Attributes**

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

582 **7.6 Get-Jobs**

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

585 **8 Security considerations**

586 This section describes the security threats against IPPFAX/1.0 Senders and Receivers. This section also  
587 addresses the security-related attributes of Printer objects (i.e., protocol endpoints of Receivers). This  
588 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]

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

591  
 592 Warning: If an implementation of a secure IPPFAX Receiver is enabled on a single network host system  
 593 simultaneously with another traditional print protocol (e.g., IPP/1.1 [RFC2911]), new security threats  
 594 appear. Administrators and users are warned that this configuration facilitates denial-of-service attacks and  
 595 and local file system attacks against the network host system (and thus against the IPPFAX service).  
 596 Beware.  
 597

## 598 **8.1 Internet Threat Model**

599  
 600 This section is adapted from section 3 of IETF Guidelines for Writing RFC Text on Security  
 601 Considerations [RFC3552].

602  
 603 In the Internet threat model, we assume that the end systems engaging in a protocol exchange have not  
 604 themselves been compromised. Protecting against an attack when either of the end systems has itself been  
 605 compromised is extraordinarily difficult.

606  
 607 By contrast, we assume that the attacker has nearly complete control of the communications channel over  
 608 which the end systems communicate. This means that the attacker can read any PDU (Protocol Data Unit)  
 609 on the network and undetectably remove, change, or inject forged packets onto the wire. This includes  
 610 being able to generate packets that appear to be from a trusted machine. Thus, even if the end-system with  
 611 which you wish to communicate is itself secure, the Internet environment provides no assurance that  
 612 packets which claim to be from that system in fact are.

613  
 614 The meaning of a PDU changes at different protocol layers. At the IP layer [RFC791], it's an IP packet. At  
 615 the TCP layer [RFC793], it's a TCP segment. At the IPP/1.1 [RFC2911] application layer, it's a single IPP  
 616 operation request or response.  
 617

### 618 **8.1.1 Passive Attacks**

619 In a passive attack, the attacker reads packets off the network but does not write them. On most common  
 620 LAN configurations, including Ethernet, 802.3, and FDDI, any machine on the wire can read all traffic  
 621 destined for any other machine on the same LAN. Note that switching hubs make this sort of sniffing  
 622 substantially more difficult, since traffic destined for a machine only goes to the network segment that  
 623 machine is located on.  
 624

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



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

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

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

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

### 643 **8.1.2 Active Attacks**

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

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

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

656 (1) Message Replay Attacks

658 (2) Message Insertion Attacks

660 (3) Message Deletion Attacks

662 (4) Message Modification Attacks

663

**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

664 (5) Man-In-The-Middle Attacks

665  
666

## 667 8.2 Enterprise Threat Model

668

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

673

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

676

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

679

680

## 681 8.3 Mobile Threat Model

682

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

685

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

688

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

690

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

694

695

## 696 8.4 HTTP Threat Model

697

698 Senders and Receivers are vulnerable to the following HTTP threats described in section 15 "Security  
699 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

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 2, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

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

- 700
- 701 (1) Personal Information Attacks - HTTP/1.1 clients and servers in
- 702 Sender and Receiver implementations MUST protect sensitive personal
- 703 information, such as name, email address, etc. (see section 15.1 of
- 704 [RFC2616]).
- 705
- 706 (2) Filename and Pathname Attacks - HTTP/1.1 servers in Receiver
- 707 implementations MUST NOT expose "nearby" resources that were NOT
- 708 explicitly configured for network access by administrators (see
- 709 section 15.2 of [RFC2616]).
- 710
- 711 (3) DNS Spoofing Attacks - HTTP/1.1 clients and servers in Sender and
- 712 Receiver implementations SHOULD NOT cache DNS name resolution results
- 713 beyond their time-to-live value (see section 15.3 of [RFC2616]).
- 714
- 715 (4) HTTP Location Header Spoofing Attacks - HTTP/1.1 servers in
- 716 Receiver implementations MUST verify the validity of Location and
- 717 Content-Location header data when supporting multiple trust domains
- 718 (see section 15.4 of [RFC2616]).
- 719
- 720 (5) HTTP Content-Disposition Headers Attacks - HTTP/1.1 servers in
- 721 Receiver implementations MUST defend against Content-Disposition
- 722 header attacks (see section 15.5 of [RFC2616]).
- 723
- 724 (6) Retention of Authentication Credentials Attacks - HTTP/1.1 clients
- 725 in Sender implementations SHOULD NOT retain cached user
- 726 authentication credentials beyond an administratively configured
- 727 idle client time (see section 15.6 of [RFC2616]).
- 728
- 729 (7) HTTP Proxy Attacks - HTTP/1.1 servers in Receiver implementations
- 730 SHOULD take active measures to defend against distributed
- 731 denial-of-service attacks (see section 15.7 of [RFC2616]).
- 732
- 733

734 **8.5 TLS Security Services**

735

**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

736

**8.5.1 Data Integrity and Authentication**

737

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.

742

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.

748

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.

751

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

753

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].

756

757

758

**8.5.2 Data Privacy**

759

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

760

761

762

763

764

**8.6 IPPFAX Printer Security Attributes**

765

766

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

767

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).

768

769

770

**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

771 Senders MUST support the values 'none' and 'digest' and SHOULD support the value 'certificate'.  
 772 Receivers MUST support the values 'none', 'digest', and 'certificate'. Senders and Receivers MUST NOT  
 773 support the values 'basic' (due to cleartext passwords) or 'requesting-user-name' (due to no password).  
 774

Formatted: Font: (Default) Arial, 12 pt

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

775 **8.6.2 uri-security-supported (1setOf type2 keyword)**

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

Formatted: Normal

776  
777 This attribute (see [RFC2911] section 4.4.3) identifies the security mechanisms (for data integrity and data  
 778 privacy) used for each URI listed in the "printer-uri-supported" attribute (see section 5.1).

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.¶

779  
780 Senders MUST support the value 'ssl3' and/or 'tls'. Receivers MUST support the value 'tls' and SHOULD  
 781 support the value 'ssl3' (for best interworking). Senders and Receivers MUST NOT support the values  
 782 'none' or 'ssl2' (to avoid compromised data integrity).  
 783  
 784

**<#>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. ¶

789 **9 Attribute Syntaxes**

790 No new attribute syntaxes are defined in this document.

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.¶

791 **10 Status codes**

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

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. ¶

794 **11 Conformance Requirements**

795 **Need to be re-worked.**

The distribution of private keys to Senders or Receivers is outside the scope of this document, but if it is done (... [4])

796 The Sender MUST:

Deleted: ¶

- 797 • Support PDF/is, see section 1

- 798 • Support the only the operations listed in Section 1.1

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

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

801 The Receiver MUST:

802 Document Originator MUST:

803

#### 804 **11.1 Operation Conformance Requirements**

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

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

- 835 5. The Sender MUST validate that the target Printer is IPPFAX-capable using the Get-Printer-  
836 Attributes operation and validate that the Receiver supports the job using the Validate-Job operation  
837 as specified in section **Error! Reference source not found.**
- 838 6. The Sender MUST supply and the Receiver MUST support the operation/Job Description attributes  
839 for Identify Exchange as described in section **Error! Reference source not found.**
- 840 7. The Sender MUST support submitting and the Receiver MUST accept IPPFAX Jobs as defined in  
841 section **Error! Reference source not found.**
- 842 8. The Sender MUST place the Sender’s identity in the document according to section **Error!**  
843 **Reference source not found.**
- 844 9. The Sender and Receiver MUST support the operations as indicated in section 7.
- 845 10. The Sender and Receiver MUST support the security mechanisms indicated in section 8, including  
846 TLS.

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

## 849 12 IPPFAX URL Scheme

850 Use pwg-ippfax rather than ippfax

851 Need to be re-worked to be consistent RFC 3510

852 Need to register a port with IANA for IPPFax.

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

### 855 12.1 IPPFAX URL Scheme Applicability and Intended Usage

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

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



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

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

## 864 **12.2 IPPFAX URL Scheme Associated IPPFAX Port**

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

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

## 868 **12.3 IPPFAX URL Scheme Associated MIME Type**

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

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

## 873 **12.4 IPPFAX URL Scheme Character Encoding**

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

## 880 **12.5 IPPFAX URL Scheme Syntax in ABNF**

881 The IPP protocol places a limit of 1023 octets (NOT characters) on the length of a URI (see section 4.1.5  
882 'uri' in [RFC2911]). An IPPFAX Receiver MUST return 'client-error-request-value-too-long' (see section  
883 13.1.4.10 in [RFC2911]) when a URI received in a request is too long.

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

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

891 The IPPFAX URL scheme syntax in ABNF is as follows:

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

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

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

899 If the ‘abs\_path’ is not present in the URL, it MUST be given as “/” when used as a Request-URI for a  
 900 resource (see section 5.1.2 of [RFC2616]). If a proxy receives a host name which is not a fully qualified  
 901 domain name, it MAY add its domain to the host name it received. If a proxy receives a fully qualified  
 902 domain name, the proxy MUST NOT change the host name.

## 903 12.6 IPPFAX URL Examples

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

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

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

910 The following literal IPv4 addresses:

```
911   192.9.5.5           ; IPv4 address in IPv4 style
912   186.7.8.9          ; IPv4 address in IPv4 style
```

914 are represented in the following example IPPFAX URLs:

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

917

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

919           ::192.9.5.5                   ; IPv4 address in IPv6 style  
 920           ::FFFF:129.144.52.38       ; IPv4 address in IPv6 style  
 921           2010:836B:4179::836B:4179   ; IPv6 address per RFC 2373

922

923 are represented in the following example IPPFAX URLs:

924           ippfax://[::192.9.5.5]/listener  
 925           ippfax://[::FFFF:129.144.52.38]/listener  
 926           ippfax://[2010:836B:4179::836B:4179]/listeners/tom

927

## 928 12.7 IPPFAX URL Comparisons

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

- 931           • A port that is empty or not given MUST be treated as equivalent to the port as defined in section  
 932           12.2 for that IPPFAX URL;

## 933 13 IANA Considerations

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

936 Operation Attributes:

937 ippfax-version (type2 keyword)                   IEEE-ISTO 510n.y 4.3

938

939 Operation/Job Description attributes:

940 sending-user-vcard (text (MAX))                   IEEE-ISTO 510n.y 6.1

941 receiving-user-vcard (text (MAX))                IEEE-ISTO 510n.y 6.2

942

943 Printer Description Attributes:

944 ippfax-versions-supported (1setOf type2 keyword) IEEE-ISTO 510n.y 5.3

## 945 14 References

### 946 14.1 Normative

947 [IANA-MT]

948 IANA Registry of Media Types: <ftp://ftp.iana.org/iana/assignments/media-types/>.

- 949 [IANA-PORTREG]  
950 IANA Port Numbers Registry. <ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers>.
- 951 [PWG5102.3-2004]  
952 Seeler, R., "PDF Image-Streamable (PDF/is)", Work in Progress,  
953 <ftp://pwg.org/pub/pwg/QUALDOCS/pwg-ifx-pdfis-latest.pdf>.  
954
- 955 [jobx]  
956 Hastings, T. and P. Zehler, "IPP Job Extensions", May 19, 2000,  
957 [ftp://ftp.pwg.org/pub/pwg/ipp/new\\_JOBX/wd-ippjobx10-20030518.pdf](ftp://ftp.pwg.org/pub/pwg/ipp/new_JOBX/wd-ippjobx10-20030518.pdf), work in progress.
- 958
- 959 **14.2 Informative**
- 960
- 961 [ifx-req]  
962 Moore, P., "IPP Fax transport requirements", October 16, 2000,  
963 <ftp://ftp.pwg.org/pub/pwg/QUALDOCS/requirements/ifx-transport-requirements-01.pdf>.
- 964
- 965
- 966 [RFC2542]  
967 Masinter, "Terminology and Goals for Internet Fax", RFC2542.
- 968 [RFC3380]  
969 Kugler, C, Hastings, T., Lewis, H., "Internet Printing Protocol (IPP): Job and Printer Administrative  
970 Operations", <draft-ietf-RFC3380-03.txt>, July 17, 2001.
- 971 [RFC 3382]  
972 deBry, R., , Hastings, T., Herriot, R., "Internet Printing Protocol (IPP): collection attribute  
973 syntax", RFC 3382, September, 2002 .
- 974 [ipp-get-method]  
975 Herriot, Kugler, and Lewis, "The 'ippget' Delivery Method for Event Notifications" , <draft-ietf-  
976 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.

- 1008 [RFC2119]  
1009 Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", RFC2119.
- 1010 [RFC2246]  
1011 Dierks, Allen "The TLS Protocol Version 1.0", RFC 2246.
- 1012 [RFC2305]  
1013 Toyoda, Ohno, Murai, Wing "A Simple Mode of Facsimile Using Internet Mail", RFC2305.
- 1014 [RFC2373]  
1015 R. Hinden, S. Deering. IP Version 6 Addressing Architecture, RFC 2373, July 1998.
- 1016 [RFC2396]  
1017 Berners-Lee, T. et al. Uniform Resource Identifiers (URI): Generic Syntax, RFC 2396, August  
1018 1998.
- 1019 [RFC2409]  
1020 Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
- 1021 [RFC2425]  
1022 T. Howes, M. Smith, F. Dawson, "A MIME Content-Type for Directory Information", RFC 2425,  
1023 September 1998.
- 1024 [RFC2426]  
1025 Dawson, Howes, "vCard MIME Directory Profile", RFC 2426, September 1998 [version v3.0].
- 1026 [RFC2532]  
1027 Masinter, Wing, "Extended Facsimile Using Internet Mail", RFC2532.
- 1028 [RFC2616]  
1029 R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext  
1030 Transfer Protocol - HTTP/1.1", RFC 2616, June 1999.
- 1031 [RFC2617]  
1032 J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP  
1033 Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.
- 1034 [RFC2732]  
1035 R. Hinden, B. Carpenter, L. Masinter. Format for Literal IPv6 Addresses in URL's, RFC 2732,  
1036 December 1999.
- 1037 [RFC2818]  
1038 E. Rescorla, "HTTP Over TLS", May 2000.

- 1039 [RFC2910]  
 1040 Herriot, Butler, Moore, Turner, Wenn, "Internet Printing Protocol/1.1: Encoding and Transport",  
 1041 RFC2910, September 2000.
- 1042 [RFC2911]  
 1043 deBry, Hastings, Herriot, Isaacson, Powell, "Internet Printing Protocol/1.1: Model and Semantics",  
 1044 RFC2911, September 2000.
- 1045 [RFC3196]  
 1046 Hastings, T., Manros, C., Zehler, P., Kugler, C., and H. Holst, "Internet Printing Protocol/1.1:  
 1047 Implementer's Guide", RFC 3196, November, 2001.
- 1048 [X509]  
 1049 CCITT. Recommendation X.509: "The Directory - Authentication Framework", 1988.

1050 **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: <a href="mailto:hastings@cp10.es.xerox.com">hastings@cp10.es.xerox.com</a>	Ira McDonald High North Inc 221 Ridge Ave Grand Marais, MI 49839  Phone: +1 906-494-2434 Email: <a href="mailto:imcdonald@sharplabs.com">imcdonald@sharplabs.com</a>
	Gail (Songer) Giansiracusa Peerless Systems Corp 2381 Rosecrans Ave El Segundo, CA 90245  Phone: +1 650-358 8875 Email: <a href="mailto:gsonger@peerless.com">gsonger@peerless.com</a>
	Rick Seeler Adobe Systems Incorporated 321 Park Ave. <span style="float: right;">San Jose, CA 95110</span>  Phone: +1 408- 536-4393 Email: <a href="mailto:rseeler@adobe.com">rseeler@adobe.com</a>

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

1051  
1052 Contact Information:  
1053  
1054 IPPFAX Web Page: <http://www.pwg.org/qualdocs/>  
1055 IPPFAX Mailing List: [ifx@pwg.org](mailto:ifx@pwg.org)  
1056  
1057 To subscribe to the IPPFAX mailing list, send the following email:  
1058 1) send it to [majordomo@pwg.org](mailto:majordomo@pwg.org)  
1059 2) leave the subject line blank  
1060 3) put the following two lines in the message body:  
1061 subscribe ifx  
1062 end  
1063

1064 Implementers of this specification document are encouraged to join the IPPFAX Mailing List in order  
1065 to participate in any discussions of clarification issues and review of registration proposals for  
1066 additional attributes and values. In order to reduce spam the mailing list rejects mail from non-  
1067 subscribers, so you must subscribe to the mailing list in order to send a question or comment to the  
1068 mailing list.  
1069

1070 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 - Océ
Harry Lewis - IBM	Ron Bergman - Hitachi Koki
Howard Sidorski - Neteon	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	

1071

1072

1. Appendix A:

1073

**16 Appendix B: vCard Example**

1074

**Update the example**

1075

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

1076

BEGIN:VCARD

1077

VERSION:3.0

1078

N:Moore;Paul

1079

FN:Paul Moore

1080

ORG:Netreon

1081

TEL;CELL;VOICE:1+206-251-7008

1082

ADR;WORK;;;10900 NE 8th St;Bellvue;WA;98004;United States of America

1083

EMAIL;PREF;INTERNET:pmoore@netreon.com

1084

REV:19991207T215341Z

1085

END:VCARD

1086

1087

1088

**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, Neteon	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	

1089

1090

**Allow Cancel-job for Administrators.**

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.

### 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.

Font: (Default) Times New Roman, 12 pt

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.

## 8.1 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 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 it 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].

## 8.2 Data Privacy (encryption)

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

## 8.3 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).

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 <b>MUST</b> be able to configure the Printer to not support the 'none' value (by means outside the scope of this document)
requesting-user-name	<b>MUST NOT</b>	<b>MUST NOT</b>
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	<b>MUST</b> support and <b>MUST</b> use, including the MD5 and MD5-session algorithms and Message Integrity, unless using 'certificate' or 'negotiate'	<b>MUST</b> support and MAY use, including the MD5 and MD5-session algorithms and Message Integrity
certificate	<b>SHOULD</b> support and MAY use when not using any of the above	<b>MUST</b> support and MAY use. For this value, the Receiver <b>MUST</b> 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.

### **8.5 Using 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).

### **8.6 Access control**

#### **Needs re-writing**

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.

## **8.7 Reduced feature set**

### **Needs re-writing**

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.