



The Printer Working Group

April 18, 2019  
IPP Registration

Deleted: January 31

## IPP Encrypted Jobs and Documents v1.0 (TRUSTNOONE)

Status: Interim

Abstract: This [specification](#) defines new encrypted IPP message formats [and operations](#) that provide IPP with end-to-end encryption of IPP Job attributes, Document attributes, and Document data.

Deleted: document

This document is a PWG Working Draft. For a definition of a "PWG Working Draft", see:

<https://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf>

This document is available electronically at:

<https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20190418.docx>

<https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20190418.pdf>

Deleted: <https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20190131.docx>

Field Code Changed

Field Code Changed

Deleted: <https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20190131.pdf>

1 Copyright © [2015-2019](#) The Printer Working Group. All rights reserved.

Deleted: 2018

2 [This document may be copied and furnished to others, and derivative works that comment](#)  
3 [on, or otherwise explain it or assist in its implementation may be prepared, copied, published](#)  
4 [and distributed, in whole or in part, without restriction of any kind, provided that the above](#)  
5 [copyright notice, this paragraph and the title of the Document as referenced below are](#)  
6 [included on all such copies and derivative works. However, this document itself may not be](#)  
7 [modified in any way, such as by removing the copyright notice or references to the IEEE-](#)  
8 [ISTO and the Printer Working Group, a program of the IEEE-ISTO.](#)

9 Title: *IPP Encrypted Jobs and Documents v1.0 (TRUSTNOONE)*

10 [The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES,](#)  
11 [WHETHER EXPRESS OR IMPLIED INCLUDING \(WITHOUT LIMITATION\) ANY IMPLIED](#)  
12 [WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.](#)

13 [The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make](#)  
14 [changes to the document without further notice. The document may be updated, replaced](#)  
15 [or made obsolete by other documents at any time.](#)

16 [The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property](#)  
17 [or other rights that might be claimed to pertain to the implementation or use of the technology](#)  
18 [described in this document or the extent to which any license under such rights might or](#)  
19 [might not be available; neither does it represent that it has made any effort to identify any](#)  
20 [such rights.](#)

21 [The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents,](#)  
22 [or patent applications, or other proprietary rights which may cover technology that may be](#)  
23 [required to implement the contents of this document. The IEEE-ISTO and its programs shall](#)  
24 [not be responsible for identifying patents for which a license may be required by a document](#)  
25 [and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the legal validity](#)  
26 [or scope of those patents that are brought to its attention. Inquiries may be submitted to the](#)  
27 [IEEE-ISTO by e-mail at: \[ieee-isto@ieee.org\]\(mailto:ieee-isto@ieee.org\).](#)

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

32 [Use of this document is wholly voluntary. The existence of this document does not imply that](#)  
33 [there are no other ways to produce, test, measure, purchase, market, or provide other goods](#)  
34 [and services related to its scope.](#)

35

37 **About the IEEE-ISTO**

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

43 For additional information regarding the IEEE-ISTO and its industry programs visit:

44 <http://www.ieee-isto.org>

45 **About the IEEE-ISTO PWG**

46 The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and  
47 Technology Organization (ISTO) with member organizations including printer  
48 manufacturers, print server developers, operating system providers, network operating  
49 system providers, network connectivity vendors, and print management application  
50 developers. The PWG is chartered to make printers and the applications and operating  
51 systems supporting them work together better. All references to the PWG in this document  
52 implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.”

53 To meet this objective, the PWG documents the results of their work as open standards that  
54 define print related protocols, interfaces, procedures, and conventions. A PWG standard is  
55 a stable, well understood, and technically competent specification that is widely used with  
56 multiple independent and interoperable implementations. Printer manufacturers and  
57 vendors of printer related software benefit from the interoperability provided by voluntary  
58 conformance to these standards.

59 For additional information regarding the Printer Working Group visit:

60 <http://www.pwg.org>

61 **Contact information:**

62 [The Printer Working Group](#)  
63 [c/o The IEEE Industry Standards and Technology Organization](#)  
64 [445 Hoes Lane](#)  
65 [Piscataway, NJ 08854](#)  
66 [USA](#)

67  
68

**Deleted:** The material contained herein is not a license, either expressed or implied, to any IPR owned or controlled by any of the authors or developers of this material or the Printer Working Group. The material contained herein is provided on an “AS IS” basis and to the maximum extent permitted by applicable law, this material is provided AS IS AND WITH ALL FAULTS, and the authors and developers of this material and the Printer Working Group and its members hereby disclaim all warranties and conditions, either expressed, implied or statutory, including, but not limited to, any (if any) implied warranties that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.¶

## Table of Contents

86		
87	1. Introduction .....	6
88	2. Terminology .....	6
89	2.1 Conformance Terminology .....	6
90	2.2 Printing Terminology .....	6
91	2.3 Protocol Role Terminology .....	7
92	2.4 Other Terminology .....	7
93	2.5 Acronyms and Organizations .....	9
94	3. Requirements .....	10
95	3.1 Rationale .....	10
96	3.2 Use Cases .....	10
97	3.2.1 Printing Encrypted Document Locally on Printer .....	10
98	3.2.2 Pull Print Encrypted Document from Print Service to Local Printer .....	10
99	3.2.3 Query Job Receipt After Printing .....	11
100	3.3 Exceptions .....	11
101	3.3.1 Unauthorized Access to Document Data .....	11
102	3.3.2 Signed Document Modified .....	11
103	3.4 Out of Scope .....	11
104	3.5 Design Requirements .....	11
105	4. Model .....	13
106	4.1 Printer Behavior .....	13
107	4.2 Proxy Behavior .....	14
108	4.3 Client Behavior .....	14
109	5. Document Formats .....	14
110	5.1 application/ipp+pgp-encrypted .....	14
111	6. Operations .....	15
112	6.1 Acknowledge-Encrypted-Job-Attributes .....	15
113	6.1.1 Acknowledge-Encrypted-Job-Attributes Request .....	15
114	6.1.2 Acknowledge-Encrypted-Job-Attributes Response .....	16
115	6.2 Fetch-Encrypted-Job-Attributes .....	16
116	6.2.1 Fetch-Encrypted-Job-Attributes Request .....	16
117	6.2.2 Fetch-Encrypted-Job-Attributes Response .....	17
118	6.3 Get-Encrypted-Job-Attributes .....	18
119	6.3.1 Get-Encrypted-Job-Attributes Request .....	18
120	6.3.2 Get-Encrypted-Job-Attributes Response .....	18
121	7. Attributes .....	19
122	7.1 Operation Attributes .....	19
123	7.1.1 encrypted-job-request-format (mimeMediaType) .....	19
124	7.1.2 encrypted-job-request-id (integer(1:MAX)) .....	19
125	7.1.3 requesting-user-pgp-public-key (1setOf text(MAX)) .....	19
126	7.2 Printer Description Attributes .....	20
127	7.2.1 pgp-document-format-supported (1setOf mimeType) .....	20
128	7.2.2 printer-pgp-public-key (1setOf text(MAX)) .....	20
129	7.2.3 printer-pgp-repertoire-configured (type2 keyword) .....	20
130	7.2.4 printer-pgp-repertoire-supported (1setOf type2 keyword) .....	20
131	8. Additional Semantics for Existing Operations .....	20

132 8.1 Print-Job and Send-Document: Encrypted IPP Message Data ..... 20  
133 9. Additional Values for Existing Attributes ..... 21  
134 9.1 printer-state-reasons (1setOf type2 keyword) ..... 21  
135 10. Conformance Requirements ..... 21  
136 10.1 Printer Conformance Requirements ..... 21  
137 10.2 Infrastructure Printer Conformance Requirements ..... 21  
138 10.3 Client Conformance Requirements ..... 21  
139 10.4 Proxy Conformance Requirements ..... 22  
140 11. Internationalization Considerations ..... 22  
141 12. Security Considerations ..... 23  
142 12.1 PGP Cipher Suite Considerations ..... 23  
143 12.2 Unicode Considerations ..... 23  
144 13. IANA Considerations ..... 23  
145 13.1 Attribute Registrations ..... 23  
146 13.2 Type2 keyword Registrations ..... 24  
147 13.3 Type2 enum Registrations ..... 24  
148 13.4 Operation Registrations ..... 24  
149 13.5 MIME Media Type Registration ..... 25  
150 14. References ..... 26  
151 14.1 Normative References ..... 26  
152 14.2 Informative References ..... 27  
153 15. Authors' Addresses ..... 28  
154 16. Appendix A: File Formats Considered ..... 28  
155 16.1 OpenPGP ..... 28  
156 16.2 S/MIME ..... 29  
157 16.3 ZIP Archive ..... 29  
158 17. Change History ..... 30  
159 17.1 April 18, 2019 ..... 30  
160 17.2 January 31, 2019 ..... 30  
161 17.3 March 28, 2018 ..... 31  
162 17.4 February 19, 2018 ..... 31  
163 17.5 February 5, 2018 ..... 31  
164 17.6 February 4, 2015 ..... 32  
165  
166

## 167 1. Introduction

168 This [specification](#) defines new encrypted IPP message formats that provide IPP with end-  
169 to-end encryption of IPP Job attributes, Document attributes, and Document data. The  
170 encrypted formats use public key cryptography with an optional password to effectively  
171 protect the IPP message/Document data payload from intermediaries and when the data is  
172 at rest in the destination Output Device.

173 The new message formats reuse the existing OpenPGP [RFC4880] message format to  
174 protect the combination of IPP message and document data normally sent in the clear as  
175 part of a Job Creation Request.

## 176 2. Terminology

### 177 2.1 Conformance Terminology

178 Capitalized terms, such as MUST, MUST NOT, RECOMMENDED, REQUIRED, SHOULD,  
179 SHOULD NOT, MAY, and OPTIONAL, have special meaning relating to conformance as  
180 defined in Key words for use in RFCs to Indicate Requirement Levels [RFC2119]. The term  
181 CONDITIONALLY REQUIRED is additionally defined for a conformance requirement that  
182 applies to a particular capability or feature.

### 183 2.2 Printing Terminology

184 Normative definitions and semantics of printing terms are imported from IETF Printer MIB  
185 v2 [RFC3805], IETF Finisher MIB [RFC3806], and IETF Internet Printing Protocol/1.1  
186 [STD92].

187 *Document*: An object created and managed by a Printer that contains the description,  
188 processing, and status information. A Document object may have attached data and is  
189 bound to a single Job.

190 *Job*: An object created and managed by a Printer that contains description, processing, and  
191 status information. The Job also contains zero or more Document objects.

192 *Logical Device*: a print server, software service, or gateway that processes jobs and either  
193 forwards or stores the processed job or uses one or more Physical Devices to render output.

194 *Output Device*: a single Logical or Physical Device

195 *Physical Device*: a hardware implementation of an endpoint device, e.g., a marking engine, a  
196 fax modem, etc.

Deleted: IPP Registration

## 198 **2.3 Protocol Role Terminology**

199 This document also defines the following protocol roles in order to specify unambiguous  
200 conformance requirements:

201 *Client*: Initiator of outgoing connections and sender of outgoing operation requests  
202 (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] User Agent).

203 *Printer*: Listener for incoming connections and receiver of incoming operation requests  
204 (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] Server) that represents one or more  
205 Physical Devices or a Logical Device.

## 206 **2.4 Other Terminology**

207 *Certificate*: A type that binds an entity's name to a Public Key with a Digital Signature  
208 [RFC5751].

209 Digital Signature: A cryptographic hash of data (a Certificate, a Document, a message, etc.)  
210 that has been associated with an entity that can be verified mathematically, for example by  
211 using Public-Key Encryption.

212 [Encrypted Job: A Job whose Document data, Job Receipt, and Job Ticket are encrypted  
213 using a public key so that only the recipient of the information can access it.](#)

214 [Job Receipt: The Job Status attributes that provide a summary of the work performed by the  
215 Printer such as the owner, state, dates and times, actual values used for Job Template  
216 attributes, and work counters.](#)

217 [Job Ticket: The operation and Job Template attributes supplied in a Job Creation request.](#)

218 *One-Time Pad*: A symmetric encryption key that is randomly generated and is used to  
219 encrypt or decrypt a single message.

220 *OpenPGP*: Security software using PGP 5.x [RFC4880]

221 *Private Key*: The recipient's key value in Public-Key Encryption.

222 *Public Key*: The sender's key value in Public-Key Encryption.

223 *Public-Key Encryption*: An encryption technique that uses a paired (asymmetric) key  
224 algorithm for secure data communication. Messages are encrypted with one key value and  
225 decrypted using the other key value, so the security of the technique depends on verifying  
226 that the first key originated from the intended recipient. This is typically done by comparing  
227 a cryptographic hash (Digital Signature) of the recipient's Certificate against a hash that was  
228 encrypted using the second key.

229 *Symmetric-Key Encryption*: An encryption technique that uses a single (symmetric) key  
230 algorithm for secure data communication. Messages are encrypted and decrypted with the  
231 same secret key value, so the security of the technique depends on the confidentiality of the  
232 key. This is typically done by using One-Time Pads.  
233



234 **2.5 Acronyms and Organizations**

235 *IANA*: Internet Assigned Numbers Authority, <http://www.iana.org/>

236 *IETF*: Internet Engineering Task Force, <http://www.ietf.org/>

237 *ISO*: International Organization for Standardization, <http://www.iso.org/>

238 *PWG*: Printer Working Group, <http://www.pwg.org/>

239

### 240 3. Requirements

#### 241 3.1 Rationale

242 Existing specifications define the following:

- 243 1. The Internet Printing Protocol/1.1 [\[STD92\]](#) defines the "document-format"  
244 attribute.
- 245 2. "Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps'  
246 URI Scheme" **Error! Reference source not found.** defines the IPP over  
247 HTTPS transport binding which provides session transport encryption.

Deleted: : Model and Semantics [RFC8011]...

248 This [specification](#) defines a new IPP convention for encrypting Jobs and Documents by:

Deleted: IPP Registration

- 249 1. Defining a set of standard encrypted IPP message formats that securely convey  
250 Job and Document information;
- 251 2. Defining new IPP Printer Description attributes that convey information about the  
252 encryption capabilities of the Printer;
- 253 3. [Defining amended IPP Job and Document operation semantics for encrypted  
254 IPP messages; and](#)
- 255 4. [Defining new operations for transferring Encrypted Job Receipts.](#)

Deleted: and

Deleted: .

#### 256 3.2 Use Cases

##### 257 3.2.1 Printing Encrypted Document Locally on Printer

258 Garrett is visiting a client and needs to print a sensitive document but wants to be sure that  
259 a print job with the document is not readable if it is recovered from the printer or print server,  
260 and that he can detect whether it has been changed.

261 Garrett chooses a printer supporting end-to-end encryption, makes his job choices, enters a  
262 passcode for the print job, and taps "Print" to submit his choices. The client software  
263 validates the public key of the receiving printer, encrypts the print job request using the public  
264 key and passcode, and sends it to the printer. Garrett then goes to the printer and enters his  
265 passcode, allowing the printer to decrypt the print job using his passcode and the  
266 corresponding private key.

##### 267 3.2.2 Pull Print Encrypted Document from Print Service to Local Printer

268 Helen is on the train, viewing a document on her tablet and wants to print a copy when she  
269 gets to work. Helen taps the control to print the document, and a print dialog UI is presented  
270 on the tablet's screen. Her tablet is configured with a printer that is a personal account on a  
271 cloud print service. She selects that to be the target printer, chooses "Encrypt Job" in the  
272 printing options presented, and specifies a credential to be used for encryption. She then  
273 taps "Print", and the document is encrypted and sent to her cloud print service account.

279 Later, when Helen arrives at the office, she goes to a printer that she identifies as one that  
280 can pull jobs from her cloud print service. Helen chooses the document or the job containing  
281 the document and taps “Print”. The printer asks for the credential to decrypt the document  
282 and Helen provides that to the printer. The printer decrypts and prints the document, and  
283 Helen collects it from the output bin.

### 284 3.2.3 Query Job Receipt After Printing

285 Jane wishes to query the job receipts of a printer in order to do accounting of encrypted print  
286 jobs for the day. She uses her client software to send a query for the job receipt of each  
287 encrypted job, providing her public key and authentication credentials to the printer. The  
288 printer then validates her credentials and returns an encrypted job receipt using her public  
289 key. Her client software then decrypts the job receipt using her private key and retrieves the  
290 needed accounting information from the decrypted receipt.

## 291 3.3 Exceptions

### 292 3.3.1 Unauthorized Access to Document Data

293 Herbert is a disenchanted IT administrator who wishes to examine everyone's print jobs and  
294 sends each print job's document content to a repository for later examination. Herbert is  
295 unable to read the encrypted documents because he does not have the private key or  
296 passcode associated with the print job.

### 297 3.3.2 Signed Document Modified

298 Garrett prints another document and the document is changed by some entity at some stage  
299 in the print system between the client and the printer. The printer notifies Garrett that the  
300 document has been changed. Garrett chooses to abandon the output since it can no longer  
301 be trusted.

## 302 3.4 Out of Scope

303 The following are considered out of scope for this document:

- 304 1. Authentication infrastructure that may be used by the Printer, such as LDAP or  
305 RADIUS, and
- 306 2. Definition of the method for loading public and private keys on a Printer.

## 307 3.5 Design Requirements

308 The design requirements for this [specification](#) are:

- 309 1. Define IPP attributes and values to describe the supported encryption methods  
310 and public keys,
- 311 2. Define amended semantics for all affected IPP operations,

Deleted: registration

- 313 3. Register all new IPP attributes, attribute keywords, attribute enum values,  
314 operations, and other IPP specific values in the IANA IPP registry,
- 315 4. Define security requirements necessary to support encrypted Jobs and  
316 Documents,
- 317 5. Define MIME media types for providing encrypted IPP Job Template and  
318 Document Template attributes along with Document data, and
- 319 6. Register all new MIME media types in the IANA MIME Media Type registry.

320 The design recommendations for this [specification](#) are:

- 321 1. Define best-practices for user experience.
- 322

Deleted: registration

## 324 4. Model

325 This document defines a new encrypted printing model where the Printer provides attributes  
326 to the Client containing a Certificate to use for encryption [of messages from the Client to the](#)  
327 [Printer](#). Clients then use the [Printer](#) Certificate (and optionally a User-supplied [Certificate](#)  
328 [and/or](#) passphrase) to produce an encrypted IPP message containing the operation, Job  
329 Template, and [/or](#) Document Template attributes along with the associated Document data.  
330 The encrypted message is sent in a Print-Job or Send-Document request as the request's  
331 Document data. Because the encrypted IPP message uses Public-Key Encryption, it can  
332 only be decrypted by the entity that possesses the Private Key corresponding to the [Printer's](#)  
333 Certificate and (if used) the User passphrase.

Deleted: provided

334 Because this model encapsulates the encrypted data as a Document, it does not offer  
335 support for encrypted Print Jobs that use the Print-URI or Send-URI operations. However,  
336 such Jobs can still use traditional access control mechanisms (authentication, passwords,  
337 etc.) to protect access to sensitive Document data.

338 Clients can request an [Encrypted Job Receipt](#) using a supplied [User Certificate](#), subject to  
339 the Printer's access control policies. [The contents of the Encrypted Job Receipt are only](#)  
340 [guaranteed to be stable once the Job reaches a terminating state, just as for regular Job](#)  
341 [Receipts](#).

Deleted: Once a Job reaches a terminating state, ...

Deleted: encrypted

### 342 4.1 Printer Behavior

343 When enabled, the Printer MUST provide a Certificate for each of the supported encrypted  
344 message formats along with the supported and configured End User password repertoire in  
345 the Printer Description attributes defined in section 7.2. If decryption and processing is  
346 performed by the Printer, it MUST also provide a list of document formats that are supported  
347 inside encrypted IPP messages.

348 When a Print-Job or Send-Document request is received, the Printer validates any attributes  
349 that are provided in the unencrypted portion of the IPP message and defers additional  
350 validation and processing until the Job moves to the 'processing' state and the Document  
351 data can be decrypted. Document data MUST remain encrypted when the Job is not in the  
352 'processing' or 'processing-stopped' states.

353 [As part of the Print-Job and Send-Document request, Clients include the End User's Public](#)  
354 [Key in the encrypted portion of the request. Printers use this Public Key to authenticate the](#)  
355 [Client in subsequent Get-Encrypted-Job-Attributes requests](#).

356 When the Printer is acting as an Infrastructure Printer [PWG5100.18] and the Certificate and  
357 repertoire information is supplied by the Proxy, the Printer does no additional validation or  
358 processing of the Document data and MUST pass the Document data to the Proxy without  
359 decryption or alteration.

364 Printers can require encrypted Print Jobs by listing only the encrypted IPP message formats  
365 in the "document-format-supported" Printer Description attribute.

## 366 4.2 Proxy Behavior

367 A Proxy [PWG5100.18] for a Printer that conforms to this [specification](#), provides the  
368 Infrastructure Printer with the Certificates, repertoire, and document format values using the  
369 Update-Output-Device-Attributes operation. If the Proxy has access to the corresponding  
370 Private Keys, it MUST NOT provide them to the Infrastructure Printer.

Deleted: registration

371 Proxies can require encrypted Print Jobs by reporting only the encrypted IPP message  
372 formats in the "document-format-supported" Printer Description attribute supplied in the  
373 Update-Output-Device-Attributes request.

374 If supported by the Infrastructure Printer, Proxies receive notifications when a Client has  
375 requested an [Encrypted](#) Job Receipt. When such an event occurs, the Proxy fetches the  
376 [Encrypted](#) Job request, generates the [Encrypted](#) Job Receipt, and acknowledges the  
377 request with the attached [Encrypted](#) Job Receipt.

Deleted: encrypted

Deleted: encrypted

Deleted: encrypted

Deleted: encrypted

## 378 4.3 Client Behavior

379 When an End User initiates a print action, the Client software will query the Printer's  
380 capabilities and status using the Get-Printer-Attributes request. If the response contains the  
381 attributes listed in section 7.2, the Client software can either automatically encrypt the Job  
382 Creation Request or offer the End User the option to do so. [When encrypting the request  
383 message, the Client generates a single session key which is encrypted only using the  
384 Printer's Public Key. The End User's Public Key is provided as an operation attribute in the  
385 encrypted request message, allowing the Printer to authenticate the Client in a subsequent  
386 Get-Encrypted-Job-Attributes request.](#)

Deleted: ,

387 As part of the encryption process, Clients SHOULD allow End Users to provide a passphrase  
388 conforming to the Printer's configured password repertoire.

## 389 5. Document Formats

### 390 5.1 application/ipp+pgp-encrypted

391 This MIME media type consists of an IPP message ("application/ipp") followed by Document  
392 data that is stored inside an OpenPGP message [RFC4880]. The symmetric key for the  
393 message is encrypted using the Public Key from the "printer-pgp-public-key (1setOf  
394 text(MAX))" Printer Description attribute (section 7.2.2) and any passphrase supplied by the  
395 End User as described in section 3.7.2.2 of [RFC4880].

402 **6. Operations**

403 **6.1 Acknowledge-Encrypted-Job-Attributes**

404 This operation is sent by a Proxy to acknowledge the receipt of an [Encrypted](#) Job attributes  
405 request from a Client that was retrieved using a Fetch-Encrypted-Job-Attributes request.  
406 Infrastructure Printers that support [Encrypted](#) Jobs MUST support this operation.

Deleted: encrypted

Deleted: encrypted

407 **6.1.1 Acknowledge-Encrypted-Job-Attributes Request**

408 The following groups of attributes are part of an Acknowledge-Encrypted-Job-Attributes  
409 request:

410 Group 1: Operation Attributes

411 "attributes-charset" (charset) and  
412 "attributes-natural-language" (naturalLanguage):

413 The Client MUST supply and the Printer MUST support both of these  
414 attributes.

415 Target:

416 The "printer-uri" (uri) operation attribute which is the target Printer for the  
417 operation.

418 "output-device-uuid" (uri):

419 The Proxy MUST supply and the Infrastructure Printer MUST support this  
420 attribute which provides the identity of the Output Device for the request.

421 "encrypted-job-request-id" (integer(1:MAX)):

422 The Proxy MUST supply and the Infrastructure Printer MUST support this  
423 attribute that specifies which [Encrypted](#) Job request is being acknowledged.

Deleted: encrypted

424 "encrypted-job-request-format" (mimeMediaType):

425 The Proxy MUST supply and the Infrastructure Printer MUST support this  
426 attribute that specifies the [Encrypted](#) Job Receipt format.

Deleted: encrypted

427 Group 2: Encrypted Job Receipt Message

428 The [Encrypted](#) Job Receipt message.

Deleted: encrypted

434 **6.1.2 Acknowledge-Encrypted-Job-Attributes Response**

435 The following groups of attributes are part of an Acknowledge-Encrypted-Job-Attributes  
436 response:

437 Group 1: Operation Attributes

438 "attributes-charset" (charset) and  
439 "attributes-natural-language" (naturalLanguage):

440 The Printer MUST return both of these attributes.

441 "status-message" (text(255)) and/or  
442 "detailed-status-message" (text(MAX)):

443 The Printer MAY return one or both of these attributes.

444 Group 2: Unsupported Attributes

445 See [RFC8011] for details on returning Unsupported Attributes.

446 Group 3: Printer Attributes

447 "printer-state-reasons" (1setOf type2 keyword):

448 The state of the Infrastructure Printer after processing the request. Clients  
449 can look for the presence of the 'encrypted-job-request' keyword to know  
450 whether to send another Fetch-Encrypted-Job-Attributes request.

451 **6.2 Fetch-Encrypted-Job-Attributes**

452 This operation allows a Proxy to fetch a request for [Encrypted](#) Job attributes from the Client.  
453 The Infrastructure Printer

Deleted: encrypted

454 **6.2.1 Fetch-Encrypted-Job-Attributes Request**

455 The following groups of attributes are part of a Fetch-Encrypted-Job-Attributes request:

456 Group 1: Operation Attributes

457 "attributes-charset" (charset) and  
458 "attributes-natural-language" (naturalLanguage):

459 The Client MUST supply and the Printer MUST support both of these  
460 attributes.

461 Target:



463           The "printer-uri" (uri) operation attribute which is the target Printer for the  
464           operation.

465           "output-device-uuid" (uri):

466           The Proxy MUST supply and the Infrastructure Printer MUST support this  
467           attribute which provides the identity of the Output Device for the request.

### 468 **6.2.2 Fetch-Encrypted-Job-Attributes Response**

469   The following groups of attributes are part of a Fetch-Encrypted-Job-Attributes response:

470   Group 1: Operation Attributes

471           "attributes-charset" (charset) and  
472           "attributes-natural-language" (naturalLanguage):

473           The Printer MUST return both of these attributes.

474           "status-message" (text(255)) and/or  
475           "detailed-status-message" (text(MAX)):

476           The Printer MAY return one or both of these attributes.

477           "job-id" (integer(1:MAX)):

478           The Job identifier for the Printer.

479           "encrypted-job-request-id" (integer(1:MAX)):

480           A unique identifier for the [Encrypted](#) Job request is being fetched.

**Deleted:** encrypted

481           "requested-attributes" (1setOf keyword):

482           The requested attributes sent by the Client to the Infrastructure Printer that  
483           specify which attributes the Client would like returned.

484           "requesting-user-name" (name(MAX)) and "requesting-user-uri" (uri):

485           The name and URI of the User requesting the attributes.

486           "requesting-user-pgp-public-key" (1setOf text(MAX)):

487           The PGP public key supplied by the Client to be used for encrypting the Job  
488           attributes.

489   Group 2: Unsupported Attributes

490           See [RFC8011] for details on returning Unsupported Attributes.

### 492 6.3 Get-Encrypted-Job-Attributes

493 This attribute allows a Client to query [Encrypted](#) Job attributes from a Printer. Once  
494 authorized, the attributes are encrypted using the [Public Key](#) supplied by the Client and  
495 returned as data following the IPP response.

Deleted: encrypted

Deleted: public

Deleted: key

496 [If the supplied Public Key does not match the one supplied in the corresponding Print-Job  
497 or Send-Document request \(section 8.1\) or a Public Key that has been registered with the  
498 Printer through some means outside of IPP \(e.g., for Administrators or Operators\), the  
499 Printer MUST reject the request with the 'client-error-forbidden' status code.](#)

#### 500 6.3.1 Get-Encrypted-Job-Attributes Request

501 The following groups of attributes are part of a Get-Encrypted-Job-Attributes request:

502 Group 1: Operation Attributes

503 "attributes-charset" (charset) and  
504 "attributes-natural-language" (naturalLanguage):

505 The Client MUST supply and the Printer MUST support both of these  
506 attributes.

507 Target:

508 The "printer-uri" (uri) and "job-id" (integer(1:MAX)) operation attributes which  
509 are the target Job for the operation.

510 "requested-attributes" (1setOf keyword):

511 The Client MAY supply and the Printer MUST support this attribute which  
512 specifies the attributes the Client would like returned.

513 "requesting-user-name" (name(MAX)) and "requesting-user-uri" (uri):

514 The name and URI of the User requesting the attributes.

515 "requesting-user-pgp-public-key" (1setOf text(MAX)):

516 The PGP public key supplied by the Client to be used for encrypting the Job  
517 attributes.

#### 518 6.3.2 Get-Encrypted-Job-Attributes Response

519 The following groups of attributes are part of an Get-Encrypted-Job-Attributes response:

520 Group 1: Operation Attributes

524 "attributes-charset" (charset) and  
525 "attributes-natural-language" (naturalLanguage):  
526 The Printer MUST return both of these attributes.

527 "status-message" (text(255)) and/or  
528 "detailed-status-message" (text(MAX)):  
529 The Printer MAY return one or both of these attributes.

530 "encrypted-job-request-format" (mimeMediaType):

531 The Printer MUST return this attribute that specifies the [Encrypted Job](#)  
532 Receipt format.

Deleted: encrypted

533 Group 2: Unsupported Attributes

534 See [RFC8011] for details on returning Unsupported Attributes.

535 Group 3: Encrypted Job Receipt Message

536 The [Encrypted Job](#) Receipt message.

Deleted: encrypted

## 537 7. Attributes

### 538 7.1 Operation Attributes

#### 539 7.1.1 encrypted-job-request-format (mimeMediaType)

540 This attribute specifies the MIME media type for the [Encrypted Job](#) attributes message.

Deleted: encrypted

#### 541 7.1.2 encrypted-job-request-id (integer(1:MAX))

542 This attribute specifies a unique request identifier for the Acknowledge-Encrypted-Job-  
543 Attributes and Fetch-Encrypted-Job-Attributes operations.

#### 544 7.1.3 requesting-user-pgp-public-key (1setOf text(MAX))

545 This attribute specifies the PGP public key to use when encrypting the IPP Job Receipt using  
546 PGP. [The values are concatenated to form the Base64-encoded PGP public key block.](#)

## 550 7.2 Printer Description Attributes

### 551 7.2.1 pgp-document-format-supported (1setOf mimeType)

552 The "pgp-document-format-supported" Printer Description attribute specifies the set of  
553 Document formats that can be embedded in Document data of type "application/ipp+pgp-  
554 encrypted".

Deleted: -

### 555 7.2.2 printer-pgp-public-key (1setOf text(MAX))

556 This attribute specifies the PGP public key to use when encrypting IPP requests using PGP.  
557 [The values are concatenated to form the Base64-encoded PGP public key block.](#)

### 558 7.2.3 printer-pgp-repertoire-configured (type2 keyword)

559 This attribute specifies the password repertoire currently configured in the Printer. The value  
560 of this attribute MUST be one of the set of values specified by the Printer's "printer-pgp-  
561 repertoire-supported" attribute. A supporting Client can use this attribute's value to limit End  
562 User input when encrypting the symmetric key for PGP.

### 563 7.2.4 printer-pgp-repertoire-supported (1setOf type2 keyword)

564 This attribute specifies the repertoires the Printer can be configured to use if the Printer  
565 supports an additional passphrase at the Printer console. Any keyword registered for use  
566 with "job-password-repertoire-supported" can be listed.

## 567 8. Additional Semantics for Existing Operations

### 568 8.1 Print-Job and Send-Document: Encrypted IPP Message Data

569 This [specification](#) adds additional semantics when a Client submits Document data in the  
570 format 'application/ipp+pgp-encrypted'. When supplied, the Printer that decrypts the data for  
571 processing MUST:

Deleted: registration

- 572 1. Merge any attributes in the encrypted message with the attributes provided in  
573 the unencrypted portion of the original request,
- 574 2. Validate the combined request attributes as required for a standard request, and
- 575 3. Abort or continue processing the Job using the merged attributes.

576 When merging attributes, the values of encrypted attributes take precedence since a Client  
577 MAY send obfuscated values in the unencrypted portion of the request, e.g., "requesting-  
578 user-name" and "job-name".

579 [Clients MUST include the "requesting-user-pgp-public-key" \(section 7.1.3\) operation](#)  
580 [attribute in the encrypted Document data.](#)

## 583 9. Additional Values for Existing Attributes

### 584 9.1 printer-state-reasons (1setOf type2 keyword)

585 This [specification](#), adds the 'encrypted-job-attributes-requested' keyword, which is present  
586 when one or more Get-Encrypted-Job-Attributes requests are pending on an Infrastructure  
587 Printer.

Deleted: registration

## 588 10. Conformance Requirements

### 589 10.1 Printer Conformance Requirements

590 In order for a Printer to claim conformance to this document, a Printer MUST support:

- 591 1. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
- 592 2. The Get-Encrypted-Job-Attributes operation as defined in section 6;
- 593 3. The attributes and values defined in section 7.2;
- 594 4. The additional semantics defined in section 8;
- 595 5. The internationalization considerations defined in section 11; and
- 596 6. The security considerations defined in section 12.

### 597 10.2 Infrastructure Printer Conformance Requirements

598 In order for an Infrastructure Printer to claim conformance to this document, an Infrastructure  
599 Printer MUST support:

- 600 1. The restrictions on processing of encrypted data as defined in section 4.1;
- 601 2. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
- 602 3. The Acknowledge-Encrypted-Job-Attributes, Fetch-Encrypted-Job-Attributes,  
603 and Get-Encrypted-Job-Attributes operations as defined in section 6;
- 604 4. The attributes and values defined in section 7.2;
- 605 5. The additional semantics defined in section 8;
- 606 6. The additional values defined in section 9;
- 607 7. The internationalization considerations defined in section 11; and
- 608 8. The security considerations defined in section 12.

### 609 10.3 Client Conformance Requirements

610 In order for a Client to claim conformance to this document, a Client MUST support:

- 611 1. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
- 612 2. The Get-Encrypted-Job-Attributes operation as defined in section 6;
- 613 3. The attributes and values defined in section 7.2;
- 614 4. The internationalization considerations defined in section 11; and

616 5. The security considerations defined in section 12.

#### 617 **10.4 Proxy Conformance Requirements**

618 In order for a Proxy to claim conformance to this document, a Proxy MUST support:

- 619 1. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
- 620 2. The Acknowledge-Encrypted-Job-Attributes and Fetch-Encrypted-Job-Attributes
- 621 operations as defined in section 6;
- 622 3. The attributes and values defined in section 7.2;
- 623 4. The additional semantics defined in section 8;
- 624 5. The additional values defined in section 9;
- 625 6. The internationalization considerations defined in section 11; and
- 626 7. The security considerations defined in section 12.

#### 627 **11. Internationalization Considerations**

628 For interoperability and basic support for multiple languages, conforming implementations

629 MUST support:

- 630 • The Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [STD63]
- 631 encoding of Unicode [UNICODE] [ISO10646]; and
- 632 • The Unicode Format for Network Interchange [RFC5198] which requires transmission
- 633 of well-formed UTF-8 strings and recommends transmission of normalized UTF-8
- 634 strings in Normalization Form C (NFC) [UAX15].

635 Unicode NFC is defined as the result of performing Canonical Decomposition (into base

636 characters and combining marks) followed by Canonical Composition (into canonical

637 composed characters wherever Unicode has assigned them).

638 WARNING – Performing normalization on UTF-8 strings received from Clients and

639 subsequently storing the results (e.g., in Job objects) could cause false negatives in Client

640 searches and failed access (e.g., to Printers with percent-encoded UTF-8 URIs now

641 'hidden').

642 Implementations of this specification SHOULD conform to the following standards on

643 processing of human-readable Unicode text strings, see:

- 644 • Unicode Bidirectional Algorithm [UAX9] – left-to-right, right-to-left, and vertical
- 645 • Unicode Line Breaking Algorithm [UAX14] – character classes and wrapping
- 646 • Unicode Normalization Forms [UAX15] – especially NFC for [RFC5198]
- 647 • Unicode Text Segmentation [UAX29] – grapheme clusters, words, sentences

- 648 • Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization

- 649 • Unicode Collation Algorithm [UTS10] – sorting

- 650 • Unicode Locale Data Markup Language [UTS35] – locale databases

651 Implementations of this specification are advised to also review the following informational  
652 documents on processing of human-readable Unicode text strings:

- 653 • Unicode Character Encoding Model [UTR17] – multi-layer character model

- 654 • Unicode Character Property Model [UTR23] – character properties

- 655 • Unicode Conformance Model [UTR33] – Unicode conformance basis

**Deleted:** <#>Unicode in XML and other Markup Languages [UTR20] – XML usage

## 656 12. Security Considerations

657 [The following sub-sections define security considerations in addition to those defined in the](#)  
658 [Internet Printing Protocol/1.1 \[STD92\]](#).

**Deleted:** The IPP extensions defined in this document require the same

**Deleted:** security considerations

**Deleted:** as

**Deleted:** : Model and Semantics

**Deleted:** RFC8011

### 659 12.1 PGP Cipher Suite Considerations

660 [Clients and Printers MUST use modern cipher suites with Authenticated Encryption with](#)  
661 [Associated Data \(AEAD\)](#).

### 662 12.2 Unicode Considerations

**Deleted:** .

663 Implementations of this specification SHOULD conform to the following standard on  
664 processing of human-readable Unicode text strings:

- 665 • Unicode Security Mechanisms [UTS39] – detecting and avoiding security attacks

666 Implementations of this specification are advised to also review the following informational  
667 document on processing of human-readable Unicode text strings:

- 668 • Unicode Security FAQ [UNISECFAQ] – common Unicode security issues

## 669 13. IANA Considerations

### 670 13.1 Attribute Registrations

671 The attributes defined in this document will be published by IANA according to the  
672 procedures in [the Internet Printing Protocol/1.1 \[STD92\]](#) in the following file:

**Deleted:** IPP/1.1 Model and Semantics [RFC2911] section...

673 <https://www.iana.org/assignments/ipp-registrations>

**Deleted:** 6.2

686 The registry entries will contain the following information:

Printer Description attributes:	Reference
-----	-----
pgp-document-format-supported (1setOf mimeType)	[TRUSTNOONE]
printer-pgp-public-key (1setOf text(MAX))	[TRUSTNOONE]
printer-pgp-repertoire-configured (type2 keyword)	[TRUSTNOONE]
printer-pgp-repertoire-supported (1setOf type2 keyword)	[TRUSTNOONE]

### 694 13.2 Type2 keyword Registrations

695 The attributes defined in this document will be published by IANA according to the  
696 procedures in [the Internet Printing Protocol/1.1 \[STD92\]](#) in the following file:

697 <https://www.iana.org/assignments/ipp-registrations>

698 The registry entries will contain the following information:

Attributes (attribute syntax)	Reference
Keyword Attribute Value	-----
-----	-----
printer-pgp-repertoire-configured (type2 keyword)	[TRUSTNOONE]
< all printer-pgp-repertoire-supported values >	[TRUSTNOONE]
printer-pgp-repertoire-supported (1setOf type2 keyword)	[TRUSTNOONE]
< all job-password-repertoire-supported values >	[TRUSTNOONE]
printer-state-reasons (1setOf type2 keyword)	[RFC8011]
encrypted-job-attributes-requested	[TRUSTNOONE]

### 708 13.3 Type2 enum Registrations

709 The enum values defined in this specification will be published by IANA according to the  
710 procedures in [the Internet Printing Protocol/1.1 \[STD92\]](#) in the following file:

711 <http://www.iana.org/assignments/ipp-registrations>

712 The registry entries will contain the following information:

Attributes (attribute syntax)		Reference
Enum Value	Enum Symbolic Name	-----
-----	-----	-----
operations-supported (1setOf type2 enum)		[RFC8011]
0x0068	Acknowledge-Encrypted-Job-Attributes	[TRUSTNOONE]
0x0069	Fetch-Encrypted-Job-Attributes	[TRUSTNOONE]
0x006A	Get-Encrypted-Job-Attributes	[TRUSTNOONE]

### 720 13.4 Operation Registrations

721 The operations defined in this specification will be published by IANA according to the  
722 procedures in [the Internet Printing Protocol/1.1 \[STD92\]](#) in the following file:

Deleted: Attribute

Deleted: Value

Deleted: I

Deleted: PP/1.1 Model and Semantics [RFC2911] section 6.1...



728 <http://www.iana.org/assignments/ipp-registrations>

729 [The registry entries will contain the following information:](#)

730	<u>Operation Name</u>	<u>Reference</u>
731	-----	-----
732	<a href="#">Acknowledge-Encrypted-Job-Attributes</a>	<a href="#">[TRUSTNOONE]</a>
733	<a href="#">Fetch-Encrypted-Job-Attributes</a>	<a href="#">[TRUSTNOONE]</a>
734	<a href="#">Get-Encrypted-Job-Attributes</a>	<a href="#">[TRUSTNOONE]</a>
735	<a href="#">Print-Job(extension)</a>	<a href="#">[TRUSTNOONE]</a>
736	<a href="#">Send-Document(extension)</a>	<a href="#">[TRUSTNOONE]</a>

### 737 [13.5 MIME Media Type Registration](#)

738 [The MIME media type defined in this white paper will be published by IANA according to the](#)  
 739 [procedures in the Media Type Specifications and Registration Procedures \[BCP13\] in the](#)  
 740 [following file:](#)

741 <https://www.iana.org/assignments/media-types>

742 [The registry will contain the following information:](#)

743 [Type name: application](#)  
 744  
 745 [Subtype name: ipp+pgp-encrypted](#)  
 746  
 747 [Required parameters: N/A](#)  
 748  
 749 [Optional parameters: N/A](#)  
 750  
 751 [Encoding considerations: Binary](#)  
 752  
 753 [Security considerations: Same as application/pgp-encrypted](#)  
 754  
 755 [Interoperability considerations: Same as for application/pgp-encrypted and](#)  
 756 [application/ipp](#)  
 757  
 758 [Published specification: \[this specification\]](#)  
 759  
 760 [Applications that use this media type: IPP](#)  
 761  
 762 [Fragment identifier considerations: N/A](#)  
 763  
 764 [Additional information:](#)  
 765  
 766 [Deprecated alias names for this type: N/A](#)  
 767 [Magic number\(s\): N/A](#)  
 768 [File extension\(s\): N/A](#)  
 769 [Macintosh file type code\(s\): N/A](#)  
 770  
 771 [Person & email address to contact for further information: Michael Sweet,](#)  
 772 [msweet@apple.com](mailto:msweet@apple.com)  
 773

774 [Intended usage: COMMON](#)

775

776 [Restrictions on usage: N/A](#)

777

778 [Author/Change controller: The Printer Working Group, c/o The IEEE Industry](#)

779 [Standards and Technology Organization, 445 Hoes Lane, Piscataway, NJ](#)

780 [08854, USA](#)

781

782 [Provisional registration? \(standards tree only\): No](#)

## 783 14. References

### 784 14.1 Normative References

785 [\[BCP13\]](#) [N. Freed, J. Klensin, T. Hansen, "Media Type Specifications and](#)

786 [Registration Procedures", RFC 6838/BCP 13, January 2013,](#)

787 <https://tools.ietf.org/html/bcp14>

788 [BCP14] S. Bradner, "Key words for use in RFCs to Indicate Requirement

789 Levels", RFC 2119/BCP 14, March 1997,

790 <https://tools.ietf.org/html/bcp14>

791 [ISO10646] "Information technology -- Universal Coded Character Set (UCS)",

792 ISO/IEC 10646:2011

793 [\[PWG5100.12\]](#) [M. Sweet, I. McDonald, "IPP Version 2.0, 2.1, and 2.2", PWG](#)

794 [5100.12-2015, October 2015,](#)

795 [https://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-](https://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.pdf)

796 [5100.12.pdf](https://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.pdf)

797 [\[PWG5100.18\]](#) [M. Sweet, I. McDonald, "IPP Shared Infrastructure Extensions](#)

798 [\(INFRA\)", PWG 5100.18-2015, June 2015,](#)

799 [https://ftp.pwg.org/pub/pwg/candidates/cs-ippinfra10-20150619-](https://ftp.pwg.org/pub/pwg/candidates/cs-ippinfra10-20150619-5100.18.pdf)

800 [5100.18.pdf](https://ftp.pwg.org/pub/pwg/candidates/cs-ippinfra10-20150619-5100.18.pdf)

801 [RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer, "OpenPGP

802 Message Format", RFC 4880, November 2007,

803 <https://tools.ietf.org/html/rfc4880>

804 [RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange",

805 RFC 5198, March 2008, <https://tools.ietf.org/html/rfc5198>

806 [RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1):

807 Message Syntax and Routing", RFC 7230, June 2014,

808 <https://tools.ietf.org/html/rfc7230>

809 [STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC

810 3629/STD 63, November 2003, <https://tools.ietf.org/html/std63>

**Deleted:** Status Code Registrations  
 The attributes defined in this document will be published by IANA according to the procedures in IPP/1.1 Model and Semantics [RFC2911] section 6.6 in the following file:  
<https://www.iana.org/assignments/ipp-registrations>  
 The registry entries will contain the following information:  
 Value Status Code  
 Name Reference  
 -----  
 0x0400:0x04FF - Client Error:  
 0x04XX - client-error-name - [REFERENCE]  
 0x0500:0x05FF - Server Error:  
 0x05XX - server-error-name - [REFERENCE]

**Field Code Changed**  
 Deleted: <https://tools.ietf.org/html/rfc2119>

**Deleted:** [PWG5100.12] - R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP/2.0 Second Edition", PWG 5100.12-2011, February 2011, <https://ftp.pwg.org/pub/pwg/candidates/cs-ipp20-20110214-5100.12.pdf>

**Field Code Changed**  
 Deleted: <https://tools.ietf.org/html/rfc3629>

- 840 [STD66] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier  
841 (URI): Generic Syntax", RFC 3986/STD 66, January 2005,  
842 <https://tools.ietf.org/html/std66>
- 843 [STD92] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1", STD 92,  
844 January 2017, <https://tools.ietf.org/html/std92>
- 845 [UAX9] Unicode Consortium, "Unicode Bidirectional Algorithm", UAX#9,  
846 <https://www.unicode.org/reports/tr9>
- 847 [UAX14] Unicode Consortium, "Unicode Line Breaking Algorithm", UAX#14,  
848 <https://www.unicode.org/reports/tr14>
- 849 [UAX15] Unicode Consortium, "Normalization Forms", UAX#15,  
850 <https://www.unicode.org/reports/tr15>
- 851 [UAX29] Unicode Consortium, "Unicode Text Segmentation", UAX#29,  
852 <https://www.unicode.org/reports/tr29>
- 853 [UAX31] Unicode Consortium, "Unicode Identifier and Pattern Syntax",  
854 UAX#31, <https://www.unicode.org/reports/tr31>
- 855 [UNICODE] Unicode Consortium, "Unicode Standard", Version 11.0.0, June 2018,  
856 <https://www.unicode.org/versions/Unicode11.0.0/>
- 857 [UTS10] Unicode Consortium, "Unicode Collation Algorithm", UTS#10,  
858 <https://www.unicode.org/reports/tr10>
- 859 [UTS35] Unicode Consortium, "Unicode Locale Data Markup Language",  
860 UTS#35, <https://www.unicode.org/reports/tr35>
- 861 [UTS39] Unicode Consortium, "Unicode Security Mechanisms", UTS#39,  
862 <https://www.unicode.org/reports/tr39>

## 863 14.2 Informative References

- 864 [EFAIL] D. Poddebniak, C. Dresen, J. Müller, F. Ising, S. Schinzel, S.  
865 Friedberger, J. Somorovsky, J. Schwenk, "Efail: Breaking S/MIME and  
866 OpenPGP Email Encryption using Exfiltration Channels", August  
867 2018,  
868 [https://www.usenix.org/conference/usenixsecurity18/presentation/pod  
869 debniak](https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak)
- 870 [UTR17] Unicode Consortium "Unicode Character Encoding Model", UTR#17,  
871 <http://www.unicode.org/reports/tr17>

Field Code Changed

Deleted: <https://tools.ietf.org/html/rfc3986...>

874 [UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23,  
875 <https://www.unicode.org/reports/tr23>

**Deleted:** [UTR20] Unicode Consortium “Unicode in XML and other Markup Languages”, UTR#20, <https://www.unicode.org/reports/tr20>

876 [UTR33] Unicode Consortium “Unicode Conformance Model”, UTR#33,  
877 <https://www.unicode.org/reports/tr33>

878 [UNISECFAQ] Unicode Consortium “Unicode Security FAQ”,  
879 <https://www.unicode.org/faq/security.html>

## 880 15. Authors' Addresses

881 Primary authors:

882 Smith Kennedy  
883 HP Inc.  
884 11311 Chinden Blvd. MS 506  
885 Boise, ID 83714  
886 smith.kennedy@hp.com  
887

888 Michael Sweet  
889 Apple Inc.  
890 One Apple Park Way  
891 M/S 111-HOMC  
892 Cupertino, CA 95014  
893 USA  
894 msweet@apple.com  
895

896 The authors would also like to thank the following individuals for their contributions to this  
897 standard:

898 Ira McDonald - High North, Inc.

## 899 16. Appendix A: File Formats Considered

900 The following file formats were considered in the development of this [specification](#). Some  
901 were selected while others were left out.

**Deleted:** IPP Registration

### 902 16.1 OpenPGP

903 The OpenPGP file format, defined in [RFC4880], has been used for signing and encrypting  
904 email message bodies as well as arbitrary file content. PGP depends on a "web of trust"  
905 trust model to establish trust but may also derive trust from more centralized trust models.

911 Certain older cipher suites utilizing the CFB mode of operation are vulnerable to attack  
912 [EFAIL]. This [specification requires](#) the use of modern cipher suites using Authenticated  
913 Encryption with Associated Data (AEAD).

**Deleted:** registration

**Deleted:** specifies

## 914 **16.2 S/MIME**

915 The S/MIME file format, defined in [RFC5751](#), is primarily used for signing and encrypting  
916 email message body content. Its cryptography is based on existing public key infrastructure  
917 (PKI) and depends on certificates issued by known certificate authorities (CAs) for  
918 establishing trust.

919 Unfortunately, S/MIME is vulnerable to several known CBC attacks [EFAIL] and (unlike  
920 OpenPGP) there are no available mitigations [at the time this specification was written](#).

## 921 **16.3 ZIP Archive**

922 The ZIP archive file format has encryption features, but the password-based encryption is  
923 weak, and implementations that support public key cryptography suffer from interoperability  
924 problems.  
925

928 **17. Change History**

929 **[17.1 April 18, 2019](#)**

- 930 • [Updated to use specification template \(now standards-track\).](#)
- 931 • [Changed Registration to Specification throughout](#)
- 932 • [Changed encrypted Job to Encrypted Job throughout](#)
- 933 • [Section 2.4: Added Encrypted Job, Job Receipt, and Job Ticket terms.](#)
- 934 • [Section 6.3: Only the originator and admins/operators can access the encrypted job](#)
- 935 [attributes](#)
- 936 • [Section 7.1.3: Base64 key block, application/ipp+pgp-encrypted mime type](#)
- 937 • [Section 7.2.2: Base64 key block](#)
- 938 • [Section 8.1: Added the requesting-user-pgp-public-key operation attribute to the](#)
- 939 [attributes that are included in the encrypted IPP message passed in Print-Job and](#)
- 940 [Send-Document requests.](#)
- 941 • [Section 11, 14.2: Drop XML Unicode TR](#)
- 942 • [Section 12: Added considerations for the PGP cipher suite used \(AEAD\)](#)
- 943 • [Section 13: Updated IANA stuff](#)
- 944 • [Section 14: Updated references](#)

945 **17.2 January 31, 2019**

- 946 • Dropped S/MIME due to EFAIL vulnerabilities
- 947 • Added reference to EFAIL presentation and paper
- 948 • Added use case for retrieving an encrypted job receipt
- 949 • Added Acknowledge-Encrypted-Job-Attributes, Fetch-Encrypted-Job-Attributes, and
- 950 Get-Encrypted-Job-Attributes operations
- 951 • Added 'encrypted-job-attributes-requested' printer state reason keyword.
- 952 • Updated all references as needed.

953 **17.3 March 28, 2018**

- 954 • Updated to current IPP Registration template.
- 955 • Abstract: Simplified
- 956 • Section 1: Rewrote
- 957 • Section 2: Added/updated terminology
- 958 • Section 3: Updated use cases, exceptions, out-of-scope, and requirements
- 959 • Section 4: Model, talk about how it all works together
- 960 • Section 5: Rewrite as application/ipp+pgp-encrypted and application/ipp+pkcs7-  
961 encrypted
- 962 • Section 6: Added S/MIME attributes, normalized to current template style
- 963 • Section 7: Added amended semantics for Print-Job and Send-Document
- 964 • Section 8: Expanded to spell out separate requirements for Printers, Infrastructure  
965 Printers, Clients, and Proxies
- 966 • Section 9: Added security considerations.
- 967 • Section 10: Updated with all of the current attributes and amended
- 968 • Updated all references.

969 **17.4 February 19, 2018**

970 Moved back to using Microsoft Word format. Incorporates product of feedback from February  
971 2018 PWG virtual F2F meeting and content from a slide set presented at that meeting by  
972 Mike Sweet ([https://ftp.pwg.org/pub/pwg/ipp/slides/ipp-document-encryption-february-](https://ftp.pwg.org/pub/pwg/ipp/slides/ipp-document-encryption-february-18.pdf)  
973 [18.pdf](https://ftp.pwg.org/pub/pwg/ipp/slides/ipp-document-encryption-february-18.pdf)).

974 **17.5 February 5, 2018**

975 Resurrected and updated with more current scheme, where the encryption attributes are  
976 now conveyed using new IPP attributes rather than embedded within the document format  
977 itself. Also rewrote the use cases and requirements to rekindle discussion about scope and  
978 possible solutions.

979 **17.6 February 4, 2015**

980 Initial revision, presented at PWG February 2015 F2F.