



April 24, 2018
IPP Registration

The Printer Working Group

1 **IPP Job Reprint Password**
2 **(REPRINTPWD)**

3 *Status: Interim*

4 Abstract: This registration defines a new “job-reprint-password” operation attribute and
5 associated semantics to provide IPP with a mechanism to support password protection for
6 reprinting saved jobs.

7 This document is an IPP Registration. For a definition of an "IPP Registration Document",
8 see:

9 <https://ftp.pwg.org/pub/pwg/general/process/ipp-registry-policy.txt>

10 This document is available electronically at:

11 <https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippreprintpwd-20180424.odt>

12 <https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippreprintpwd-20180424.pdf>

13 Copyright © 2018 The Printer Working Group. All rights reserved.

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

21 Title: IPP Job Reprint Password (*REPRINTPWD*)

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

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

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

33 The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents,
34 or patent applications, or other proprietary rights which may cover technology that may be
35 required to implement the contents of this document. The IEEE-ISTO and its programs
36 shall not be responsible for identifying patents for which a license may be required by a
37 document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the
38 legal validity or scope of those patents that are brought to its attention. Inquiries may be
39 submitted to the IEEE-ISTO by e-mail at: ieee-isto@ieee.org.

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

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

47 **About the IEEE-ISTO**

48 The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and
49 flexible operational forum and support services. The IEEE-ISTO provides a forum not only
50 to develop standards, but also to facilitate activities that support the implementation and

51 acceptance of standards in the marketplace. The organization is affiliated with the IEEE
52 (<http://www.ieee.org/>) and the IEEE Standards Association (<http://standards.ieee.org/>).

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

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

55 **About the IEEE-ISTO PWG**

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

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

70 For additional information regarding the Printer Working Group visit:

71 <https://www.pwg.org>

72 Contact information:

73 The Printer Working Group
74 c/o The IEEE Industry Standards and Technology Organization
75 445 Hoes Lane
76 Piscataway, NJ 08854
77 USA

Table of Contents

78		
79	1.Introduction.....	6
80	2.Terminology.....	6
81	2.1.Protocol Roles Terminology.....	6
82	1.1 Other Terms Used in This Document.....	6
83	1.2 Acronyms and Organizations.....	6
84	3.Requirements for IPP Job Reprint Password.....	7
85	3.1.Use Cases.....	7
86	3.2.Exceptions.....	7
87	3.3.Out of Scope.....	8
88	3.4.Design Requirements.....	8
89	4.New Operation Attributes For Existing Operations.....	8
90	4.1.job-reprint-password (octetString(255) no-value).....	8
91	4.2.job-reprint-password-encryption (type2 keyword name(MAX)).....	9
92	5.Printer Description Attributes.....	9
93	5.1.job-reprint-password-supported (rangeOfInteger(0:255)).....	9
94	5.2.job-reprint-password-encryption-supported (1setOf (type3 keyword name(MAX))).....	9
95	5.3.job-reprint-password-repertoire-supported (1setOf (type2 keyword)).....	10
96	6.Additional Semantics For Existing Operations.....	10
97	6.1.Print-Job, Print-URI, Create-Job and job-reprint-accesses.....	10
98	7.Internationalization Considerations.....	10
99	8.Security Considerations.....	11
100	8.1.Human-readable Strings	11
101	9.IANA Considerations.....	11
102	9.1.Attribute Registrations.....	11
103	10.References.....	12
104	10.1.Normative References.....	12
105	10.2.Informative References.....	14
106	11.Authors' Addresses.....	14
107	12.Change History.....	15
108	12.1.April 24, 2018.....	15
109	12.2.April 4, 2018.....	15
110	1.3 March 13, 2018.....	15
111	1.4 March 11, 2018.....	15
112	1.5 February 5, 2018.....	16
113	1.6 December 5, 2017.....	16

114

List of Figures

115

List of Tables

116 **1. Introduction**

117 Users and network administrators are increasingly concerned about network and data
118 security, and this extends to printing. Most all Users are familiar with sending a Job to a
119 Printer and the Printer processing that Job fairly immediately, and some do so using a “job
120 password” that prevents the Job from being processed until the User provides that
121 password on the Printer's control panel to approve its release to processing. The IPP “job-
122 password” operation attribute [PWG5100.11] and related attributes provide support for this
123 workflow. Some Printers also support saving jobs for later printing or re-printing. In certain
124 cases there may be Users that wish to take advantage of both capabilities. Unfortunately
125 however, since “job-password” is an operation attribute, and that Job's processing is the
126 act of saving the Job, the “job-password” attribute does not persist beyond its being saved.
127 Therefore, in order for IPP to support scenarios involving a password protected saved job,
128 IPP must be extended with new attributes that convey a Job password that persists
129 beyond Job processing completion.

130 **2. Terminology**

131 **2.1. Protocol Roles Terminology**

132 This document defines the following protocol roles in order to specify unambiguous
133 conformance requirements:

134 *Client*: Initiator of outgoing IPP session requests and sender of outgoing IPP operation
135 requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] User Agent).

136 *Printer*: Listener for incoming IPP session requests and receiver of incoming IPP operation
137 requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] Server) that represents one
138 or more Physical Devices or a Logical Device.

139 **1.1 Other Terms Used in This Document**

140 *User*: A person or automata using a Client to communicate with a Printer.

141 *Saved Job*: A Saved Job is a Retained Job that the Printer retains indefinitely (until
142 removed by a Delete-Job or Purge-Jobs operation) so that a copy of it can be reprinted
143 any time using the Reprocess-Job or Resubmit-Job operations, rather than aging the job
144 out after an implementation-defined period. [PWG5100.11]

145 **1.2 Acronyms and Organizations**

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

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

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

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

150 **3. Requirements for IPP Job Reprint Password**

151 **3.1. Use Cases**

152 **3.1.1. Protecting a Saved Document with a Persistent Password**

153 Wilma has authored a departmental policy document that she intends to save on her
154 departmental MFD, to allow some of her peers to print copies as needed. But as the
155 document contains sensitive information, Wilma wishes to only allow those who know the
156 job's password to re-print copies. She is familiar with providing a password when
157 configuring a print job, and she is also familiar with configuring the job to be saved in the
158 printer. In the print dialog used to configure the print job on her computer, Wilma provides
159 a password, and also chooses to have the job saved. Wilma clicks "Print" and the
160 computer submits the job to the printer. The printer saves the job content and protects it
161 with the password provided.

162 **3.1.2. Re-printing a Saved Job Via Printer Control Panel**

163 Barney hears from Wilma that she has saved that document to the departmental MFD.
164 Wilma tells Barney the job's name, and Barney then goes to the MFD and looks up the job.
165 He taps on the control panel to have a copy printed, and is prompted to enter the job's
166 password. He enters that on the control panel, and the MFD prints a copy. Barney collects
167 it from the output bin and returns to his desk.

168 **3.1.3. Re-printing a Saved Job Using An IPP Client**

169 Barney sends an IM to Betty that Wilma has saved a job on the departmental MFD. Betty
170 opens her computer's print system and browses the saved jobs on the MFD. She selects
171 the job and clicks "Print" to have a copy made for her. A dialog is presented asking for the
172 job's password. Betty types in the job's password, and the MFD prints a copy. She collects
173 it from the MFD and returns to her office.

174 **3.2. Exceptions**

175 **3.2.1. Unauthorized Re-printing Disallowed From Printer Control Panel**

176 Harvey, an employee from another department, walks up to Wilma's departmental MFD.
177 He navigates the MFD's control panel user interface and sees Wilma's departmental policy
178 document listed on the control panel. He tries to get the MFD to produce a re-print. The
179 MFD challenges Harvey for the reprint password; Harvey doesn't know it. The MFD won't

180 re-print the document without receiving the reprint password, so Harvey walks away empty
181 handed.

182 **3.3. Out of Scope**

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

- 184 1. How the Document or Documents in a Job are stored by the Printer
- 185 2. Methods for encrypting the document itself.
- 186 3. Mechanisms for supporting per-user credentials / access control list for releasing
187 the stored job.

188 **3.4. Design Requirements**

189 The design requirements for this document are:

- 190 1. Use existing attributes or collections if possible.
- 191 2. Support at the least the fidelity supported currently by “job password” and “job-
192 password-encryption”
- 193 3. Register all attributes and operations with IANA

194 The design recommendations for this document are:

- 195 1. Reusing UI controls with similar enough purposes so that the user doesn't need to
196 be confused by e.g. needing to interact with different controls for different kinds of
197 passwords.

198 **4. New Operation Attributes For Existing Operations**

199 **4.1. job-reprint-password (octetString(255) | no-value)**

200 The REQUIRED "job-reprint-password" Operation attribute specifies the password the
201 Printer requires before permitting the saved Job to be reprinted. The Printer permanently
202 attaches the password to a saved Job [PWG5100.11]. A Client MAY provide a zero-length
203 value or the 'no-value' out-of-band value to specify that no authentication is required to
204 reprint the Job. The Printer MUST challenge the User for this password to authorize
205 reprinting that Saved Job if the value is a non-zero-length octetString.

206 The Printer MUST associate this operation attribute with the Job, and it MUST persist for
207 as long as the Job is retained and available for reprinting. The Printer MUST NOT allow
208 access to the Job's stored “job-reprint-password” attribute via IPP or any other protocol.

209 IPP operations that can and cannot include this operation attribute are listed in Section 6.1.
210 of this document. This attribute MUST NOT be included in any IPP operation responses.

211 A Client MUST NOT include the “job-reprint-password” Operation attribute in an Operation
212 sent over an insecure IPP connection. This Operation attribute MUST be present in the
213 Operation request if the “job-reprint-password-encryption” operation attribute is present.

214 **4.2. job-reprint-password-encryption (type2 keyword | name(MAX))**

215 The “job-reprint-password-encryption” Operation attribute specifies the hashing algorithm
216 used to obfuscate the password to produce the value specified by the “job-reprint-
217 password” operation attribute. This attribute is semantically similar to the “job-password-
218 encryption” operation attribute [PWG5100.11]. This attribute MUST NOT be included in
219 any IPP operation responses.

220 If the Client specifies a zero-length value or 'no-value' for “job-reprint-password” then the
221 value of this attribute MUST be 'none'.

222 This Operation attribute MUST be present in the Operation request if the “job-reprint-
223 password” operation attribute is present. The value of this attribute must be one of the
224 values listed in the Printer's “job-reprint-password-encryption-supported” Printer
225 Description attribute.

226 **5. Printer Description Attributes**

227 **5.1. job-reprint-password-supported (rangeOfInteger(0:255))**

228 The “job-reprint-password-supported” attribute specifies the minimum and maximum length
229 the Printer supports for the cleartext unencrypted password. A conforming Printer MUST
230 be able to accept 255 octets without truncation. However, a Printer MAY be implemented
231 as a gateway to another print system that cannot accept the full 255-octet range, in which
232 case the client MUST NOT allow an unencrypted password greater than the length
233 specified by this attribute.

234 If the “job-reprint-password” Operation attribute is supported, then this attribute MUST be
235 supported.

236 **5.2. job-reprint-password-encryption-supported (1setOf (type3 keyword |** 237 **name(MAX)))**

238 The “job-reprint-password-encryption-supported” Printer Description attribute specifies the
239 encryption methods the Printer supports for obfuscating the value of the “job-reprint-
240 password” Operation attribute. The set of allowable keywords for this attribute are the
241 same as those registered for the “job-password-encryption” attribute [PWG5100.11].
242 Deprecated keywords SHOULD NOT be listed.

243 If the Printer supports the "job-reprint-password" and "job-reprint-password-encryption"
244 Operation attributes, then this attribute MUST be supported.

245 **5.3. job-reprint-password-repertoire-supported (1setOf (type2 keyword))**

246 The "job-reprint-password-repertoire-supported" Printer Description attribute specifies the
247 password repertoire (set of allowable characters) supported by this Printer for the "job-
248 reprint-password" Operation attribute. A Client SHOULD use this attribute's value to limit
249 the range of allowable User input so that the value in "job-reprint-password" will be
250 supported by the Printer. If the value of the "job-reprint-password" Operation attribute is
251 encrypted, the Printer will be unable to reject the password at time of receipt, and the User
252 may never be able to successfully authenticate to reprint the Job.

253 **6. Additional Semantics For Existing Operations**

254 **6.1. Print-Job, Print-URI, Create-Job and job-reprint-accesses**

255 The "job-reprint-password" and "job-reprint-password-encryption" Operation attributes
256 MAY be included in Print-Job, Print-URI, and Create-Job operation requests [RFC8011] to
257 specify the persistent access credentials for a Job created by one of these operations.
258 Although the "job-reprint-password" and "job-reprint-password-encryption" attributes get
259 copied to the Job Object, the Printer MUST NOT include a Job's "job-reprint-password"
260 and "job-reprint-password-encryption" attributes as Job Description attributes in a Job
261 operation such as Get-Job-Attributes [RFC8011].

262 **7. Internationalization Considerations**

263 For interoperability and basic support for multiple languages, conforming implementations
264 MUST support the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8)
265 [STD63] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for
266 Network Interchange [RFC5198].

267 Implementations of this specification SHOULD conform to the following standards on
268 processing of human-readable Unicode text strings, see:

- 269 • Unicode Bidirectional Algorithm [UAX9] – left-to-right, right-to-left, and vertical
- 270 • Unicode Line Breaking Algorithm [UAX14] – character classes and wrapping
- 271 • Unicode Normalization Forms [UAX15] – especially NFC for [RFC5198]
- 272 • Unicode Text Segmentation [UAX29] – grapheme clusters, words, sentences
- 273 • Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization
- 274 • Unicode Collation Algorithm [UTS10] – sorting

- 275
- Unicode Locale Data Markup Language [UTS35] – locale databases

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

- 278
- Unicode Character Encoding Model [UTR17] – multi-layer character model
- 279
- Unicode in XML and other Markup Languages [UTR20] – XML usage
- 280
- Unicode Character Property Model [UTR23] – character properties
- 281
- Unicode Conformance Model [UTR33] – Unicode conformance basis

282 **8. Security Considerations**

283 The IPP extensions defined in this document require the same security considerations as
284 defined in the IPP/1.1: Model and Semantics [RFC8011], IPP: Job and Printer Extensions
285 – Set 2 (JPS2), and IPP Job Password Repertoire.

286 In addition to those requirements, the Printer MUST protect the values of “job-reprint-
287 accesses” at rest. Also, the Printer MUST reject any IPP operation sent over a non-
288 encrypted connection that includes the “job-reprint-accesses” attribute.

289 **8.1. Human-readable Strings**

290 Implementations of this specification SHOULD conform to the following standard on
291 processing of human-readable Unicode text strings, see:

- 292
- Unicode Security Mechanisms [UTS39] – detecting and avoiding security attacks

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

- 295
- Unicode Security FAQ [UNISECFAQ] – common Unicode security issues

296 **9. IANA Considerations**

297 **9.1. Attribute Registrations**

298 The attributes defined in this document will be published by IANA according to the
299 procedures in IPP Model and Semantics [RFC8011] section 6.2 in the following file:

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

301 The registry entries will contain the following information:

302	Operation attributes:	Reference
303	-----	-----
304	job-reprint-password (octetString(255) no-value)	
305		[REPRINTPWD]
306	job-reprint-password-encryption	
307	type2 keyword name(MAX)	[REPRINTPWD]
308	Printer Description attributes:	Reference
309	-----	-----
310	job-reprint-password-supported	
311	(rangeOfInteger(0:255))	[REPRINTPWD]
312	job-reprint-password-encryption-supported	
313	(1setOf (type3 keyword name(MAX)))	[REPRINTPWD]
314	job-reprint-password-repertoire-supported	
315	(1setOf (type2 keyword))	[REPRINTPWD]

316 10. References

317 10.1. Normative References

- 318 [IPPREPETOIRE] S. Kennedy, "IPP Job Password Repertoire", January 2016,
319 [https://ftp.pwg.org/pub/pwg/ipp/whitepaper/wp-job-password-](https://ftp.pwg.org/pub/pwg/ipp/whitepaper/wp-job-password-repertoire-20160101.pdf)
320 [repertoire-20160101.pdf](https://ftp.pwg.org/pub/pwg/ipp/whitepaper/wp-job-password-repertoire-20160101.pdf)
- 321 [ISO10646] "Information technology -- Universal Coded Character Set (UCS)",
322 ISO/IEC 10646:2011
- 323 [PWG5100.5] D. Carney, T. Hastings, P. Zehler. "Internet Printing Protocol (IPP):
324 Document Object", PWG 5100.5-2003, October 2003,
325 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippdocobject10-20031031-](http://ftp.pwg.org/pub/pwg/candidates/cs-ippdocobject10-20031031-5100.5.pdf)
326 [5100.5.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippdocobject10-20031031-5100.5.pdf)
- 327 [PWG5100.11] T. Hastings, D. Fullman, "IPP: Job and Printer Extensions – Set 2
328 (JPS2)", PWG 5100.11-2010, October 2010,
329 [https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-](https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-20101030-5100.11.pdf)
330 [20101030-5100.11.pdf](https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-20101030-5100.11.pdf)
- 331 [PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP Version 2.0, 2.1,
332 and 2.2", PWG 5100.12-2015, October 2015,
333 <http://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.pdf>
- 334 [PWG5100.13] M. Sweet, I. McDonald, P. Zehler, "IPP: Job and Printer Extensions -
335 Set 3 (JPS3)", PWG 5100.13-2012, July 2012,
336 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-](http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf)
337 [20120727-5100.13.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf)

- 338 [PWG5100.19] S. Kennedy, "IPP Implementor's Guide v2.0", PWG 5100.19-2015,
339 August 2015, [http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-
340 20150821-5100.19.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-20150821-5100.19.pdf)
- 341 [RFC2817] R. Khare, S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC
342 2817, May 2000, <https://www.ietf.org/rfc/rfc2817.txt>
- 343 [RFC3510] R. Herriot, I. McDonald, "Internet Printing Protocol/1.1: IPP URL
344 Scheme", RFC 3510, April 2003, <https://tools.ietf.org/html/rfc3510>
- 345 [RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange",
346 RFC 5198, March 2008, <https://www.ietf.org/rfc/rfc5198.txt>
- 347 [RFC6749] D. Hardt, "The OAuth 2.0 Authorization Framework", RFC 6749,
348 October 2012, <http://www.ietf.org/rfc/rfc6749>
- 349 [RFC7616] R. Shekh-Yusef, Ed., D. Ahrens, S. Bremer, "HTTP Digest Access
350 Authentication", RFC 7616, September 2015,
351 <https://www.ietf.org/rfc/rfc7616.txt>
- 352 [RFC7617] J. Reschke, "The 'Basic' HTTP Authentication Scheme", RFC 7617,
353 September 2015, <https://www.ietf.org/rfc/rfc7617.txt>
- 354 [RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1):
355 Message Syntax and Routing", RFC 7230, June 2014,
356 <http://www.ietf.org/rfc/rfc7230.txt>
- 357 [RFC7472] I. McDonald, M. Sweet, "Internet Printing Protocol (IPP) over HTTPS
358 Transport Binding and the 'ipps' URI Scheme", RFC 7472, March
359 2015, <https://tools.ietf.org/html/rfc7472>
- 360 [RFC8010] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1: Encoding and
361 Transport", RFC 8010, January 2017,
362 <https://www.ietf.org/rfc/rfc8010.txt>
- 363 [RFC8011] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1: Model and
364 Semantics", RFC 8011, January 2017,
365 <https://www.ietf.org/rfc/rfc8011.txt>
- 366 [STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC
367 3629/STD 63, November 2003, <http://www.ietf.org/rfc/rfc3629.txt>
- 368 [UAX9] Unicode Consortium, "Unicode Bidirectional Algorithm", UAX#9, May
369 2016, <http://www.unicode.org/reports/tr9>
- 370 [UAX14] Unicode Consortium, "Unicode Line Breaking Algorithm", UAX#14,
371 June 2016, <http://www.unicode.org/reports/tr14>
- 372 [UAX15] Unicode Consortium, "Normalization Forms", UAX#15, February 2016,
373 <http://www.unicode.org/reports/tr15>
- 374 [UAX29] Unicode Consortium, "Unicode Text Segmentation", UAX#29, June
375 2016, <http://www.unicode.org/reports/tr29>

- 376 [UAX31] Unicode Consortium, “Unicode Identifier and Pattern Syntax”,
377 UAX#31, May 2016, <http://www.unicode.org/reports/tr31>
- 378 [UNICODE] The Unicode Consortium, “Unicode® 10.0.0”, June 2017,
379 <http://unicode.org/versions/Unicode10.0.0/>
- 380 [UTS10] Unicode Consortium, “Unicode Collation Algorithm”, UTS#10, May
381 2016, <http://www.unicode.org/reports/tr10>
- 382 [UTS35] Unicode Consortium, “Unicode Locale Data Markup Language”,
383 UTS#35, October 2016, <http://www.unicode.org/reports/tr35>
- 384 [UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, June
385 2016, <http://www.unicode.org/reports/tr39>

386 10.2. Informative References

- 387 [IANA-IPP] IANA Internet Printing Protocol (IPP) Registrations,
388 <http://www.iana.org/assignments/ipp-registrations>
- 389 [UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2016,
390 <http://www.unicode.org/faq/security.html>
- 391 [UTR17] Unicode Consortium “Unicode Character Encoding Model”, UTR#17,
392 November 2008, <http://www.unicode.org/reports/tr17>
- 393 [UTR20] Unicode Consortium “Unicode in XML and other Markup Languages”,
394 UTR#20, January 2013, <http://www.unicode.org/reports/tr20>
- 395 [UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23,
396 May 2015, <http://www.unicode.org/reports/tr23>
- 397 [UTR33] Unicode Consortium “Unicode Conformance Model”, UTR#33,
398 November 2008, <http://www.unicode.org/reports/tr33>

399 11. Authors' Addresses

400 Primary authors:

401 Smith Kennedy
402 HP Inc.
403 11311 Chinden Blvd.
404 Boise ID 83714
405 smith.kennedy@hp.com

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

408 Ira McDonald – High North Inc.

409 Mike Sweet – Apple Inc.

410 **12. Change History**

411 **12.1. April 24, 2018**

412 Re-authored using the new PWG Working Draft template for Apache OpenOffice, moving
413 away from LibreOffice due to interoperability issues. Also, adopted changes recommended
414 in the April 12, 2018 IPP WG meeting:

- 415 • Returned to the “job-password” / “job-password-encryption” attribute set design
416 pattern from the “xxx-accesses” attribute set design pattern.

417 **12.2. April 4, 2018**

418 Updated as per feedback from IPP WG meeting on March 29, 2018

- 419 • Converted document to an IPP Registration document and made document
420 changes and file name changes to comply with that policy.
- 421 • Renamed “job-save-accesses” to “job-reprint-accesses”
- 422 • Removed “access-x509-certificate” but can add it back in later if its use becomes
423 more clearly defined

424 **1.3 March 13, 2018**

425 Updated as per feedback from IPP WG reflector:

- 426 • Fixed the abstract to make it less redundantly redundant.
- 427 • Fixed RFC references for HTTP Basic and Digest authentication
- 428 • Removed “job-save-accesses-configured” (but I still don't understand why some use
429 the “xxx” / “xxx-supported” model while others use “xxx” / “xxx-configured” / “xxx-
430 supported”...)
- 431 • Added new “Additional Semantics for Existing Operations” section
- 432 • Updated Security Considerations

433 **1.4 March 11, 2018**

434 Updated as per feedback from February 2018 PWG F2F review:

- 435 • Refactored the attributes used to leverage the attributes used in IPP Shared
436 Infrastructure Extensions and IPP Scan Service. This model is more appropriate

437 since job-save and its members become Job Description attributes, which are
438 required to be accessible via a Get-Job-Attributes operation. Access to the
439 credentials, even if hashed, would be unacceptable.

- 440 • Propose this be moved to IPP Registration candidate status

441 **1.5 February 5, 2018**

442 Updated as per feedback from Dec. 14, 2017 IPP WG teleconference review:

- 443 • Updated Use Cases, Out of Scope and Design Requirements sections
- 444 • Refactored to make the solution become member attributes of job-save, with
445 associated Printer Description attributes.

446 **1.6 December 5, 2017**

447 Initial revision.