



The Printer Working Group

January 1, 2016
White Paper

IPP Job Password Repertoire

Status: Draft

Abstract: This whitepaper defines new IPP attributes to allow a Printer supporting the "job-password" attribute to more specifically articulate the repertoire of allowable values it will accept.

This document is a White Paper. For a definition of a "White Paper", see: <http://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf>

This document is available electronically at:

<http://ftp.pwg.org/pub/pwg/ipp/whitepaper/wp-job-password-repertoire-20160101.pdf>

1 Copyright © 2015-2016 The Printer Working Group. All rights reserved.

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,
4 published and distributed, in whole or in part, without restriction of any kind, provided that
5 the above copyright notice, this paragraph and the title of the Document as referenced
6 below are included on all such copies and derivative works. However, this document itself
7 may not be modified in any way, such as by removing the copyright notice or references to
8 the IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO.

9 Title: *IPP Job Password Repertoire*

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
17 property or other rights that might be claimed to pertain to the implementation or use of the
18 technology described in this document or the extent to which any license under such rights
19 might or might not be available; neither does it represent that it has made any effort to
20 identify any 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
24 shall not be responsible for identifying patents for which a license may be required by a
25 document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the
26 legal validity or scope of those patents that are brought to its attention. Inquiries may be
27 submitted to the IEEE-ISTO by e-mail at: 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
33 that there are no other ways to produce, test, measure, purchase, market, or provide other
34 goods and services related to its scope.

35

36 **About the IEEE-ISTO**

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

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

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

44 **About the IEEE-ISTO PWG**

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

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

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 About the Internet Printing Protocol Work Group

69 The Internet Printing Protocol (IPP) working group has developed a modern, full-featured
70 network printing protocol, which is now the industry standard. IPP allows a print client to
71 query a printer for its supported capabilities, features, and parameters to allow the
72 selection of an appropriate printer for each print job. IPP also provides Job information
73 prior to, during, and at the end of Job processing.

74 For additional information regarding IPP visit:

75 <http://www.pwg.org/ipp/>

76 Implementers of this specification are encouraged to join the IPP mailing list in order to
77 participate in any discussions of the specification. Suggested additions, changes, or
78 clarification to this specification, should be sent to the IPP mailing list for consideration.
79

Table of Contents

80

81 1. Introduction 6

82 2. Terminology 6

83 2.1 Conformance Terminology 6

84 2.2 Terms Used in This Document 6

85 2.3 Protocol Role Terminology 6

86 2.4 Printing Terminology..... 7

87 2.5 Acronyms and Organizations 7

88 3. Rationale for IPP Job Password Repertoire..... 8

89 3.1 Use Cases..... 8

90 3.1.1 Secure Print with Limited Control Panel..... 8

91 3.2 Exceptions..... 8

92 3.3 Out of Scope 9

93 3.4 Design Requirements 9

94 4. Printer Description Attributes 9

95 4.1 job-password-minimum-length (integer(0:255))..... 9

96 4.2 job-password-repertoire-supported (1setOf (type2 keyword | name)) 9

97 4.3 job-password-repertoire-configured (type2 keyword | name) 10

98 5. Updates to Existing Attributes 10

99 5.1 job-password-encryption-supported 10

100 6. Internationalization Considerations 11

101 7. Security Considerations 11

102 8. References..... 12

103 9. Authors' Addresses 12

104 10. Change History 13

105 10.1 October 12, 2015..... 13

106 10.2 September 9, 2015..... 14

107 10.3 April 14, 2015 14

108 10.4 February 4, 2015 14

List of Figures

112 **No table of figures entries found.**

113 This is an automatic table of contents. To use it, apply heading styles (on the Home tab) to

114 the text that goes in your table of contents, and then update this table.

115

116 If you want to type your own entries, use a manual table of contents (in the same menu as

117 the automatic one).

118

List of Tables

119

120 Table 1: job-password-repertoire-supported keyword definitions..... 10

121

122

123 **1. Introduction**

124 The "Internet Printing Protocol (IPP): Job and Printer Extensions – Set 2 (JPS2)"
125 [PWG5100.11] already defines a collection of attributes to enable "Secure Print", by
126 defining the "job-password" and "job-password-encryption" Job Template attributes.
127 However, some Output Devices do not have a sophisticated control panel, but can still
128 accept passwords if the password provided by the User is limited to comply with a
129 particular pattern. The existing "job-password-supported" attribute contains a maximum
130 acceptable length for the "job-password" attribute. The "job-password-allowable-pattern"
131 attribute defined below provides a mechanism for a Printer to convey minimum and
132 maximum password length, as well as limitations on acceptable character ranges on a per-
133 character basis.

134 **2. Terminology**

135 **2.1 Conformance Terminology**

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

141 **2.2 Terms Used in This Document**

142 *Secure Print*: An IPP feature described in [PWG5100.11] to restrain Job processing until a
143 Job password has been provided to the Printer.

144 *Encrypted Document*: A Document submitted as part of a job that Job or Print Document
145 confidentiality while the Document is in the process of being rendered.

146 **2.3 Protocol Role Terminology**

147 This document defines the following protocol roles in order to specify unambiguous
148 conformance requirements:

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

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

154 **2.4 Printing Terminology**

155 Normative definitions and semantics of printing terms are imported from the Printer MIB v2
156 [RFC3805], Printer Finishings MIB [RFC3806], Internet Printing Protocol/1.1: Model and
157 Semantics [RFC2911], and IPP: Job Progress Attributes [RFC3381].

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

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

163 **2.5 Acronyms and Organizations**

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

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

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

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

168

169 3. Rationale for IPP Job Password Repertoire

170 Existing specifications define the following:

- 171 1. Internet Printing Protocol (IPP): Job and Printer Extensions – Set 2 (JPS2)
172 [PWG5100.11] defines the "job-password" attribute for a Client to associate a
173 password with the job. The Printer holds the Job in 'pending-held' state until a user
174 provides that password. The "job-password-supported" attribute conveys the
175 maximum length of the password.
- 176 2. Internet Printing Protocol (IPP): Job and Printer Extensions – Set 2 (JPS2)
177 [PWG5100.11] defines the "job-password-encryption" attribute to specify the
178 hashing algorithm used to obfuscate the value sent in the corresponding "job-
179 password" attribute. The "job-password-encryption-supported" Printer Description
180 attribute conveys the hashing algorithms supported by the Printer.

181 To enhance the fidelity of the user experience when accepting job passwords, this white
182 paper:

- 183 1. Proposes the definition of additional Printer Description attributes to convey
184 restrictions on the length and range of acceptable characters supported by the "job-
185 password" Job Template attribute, so that these additional constraints may be
186 conveyed without breaking backward compatibility.
- 187 2. Recommends deprecation of some of the hashing algorithms, clarifies the
188 definitions of existing ambiguous keywords, and propose the definition of new
189 values.

190 3.1 Use Cases

191 The following use cases are germane to the new IPP attributes and their semantics.

192 3.1.1 Secure Print with Limited Control Panel

193 Duncan has an end-of-year evaluation document that he needs to print but is worried that
194 someone else might see. He wants the Printer to hold the Job until he gets to the Printer to
195 release it. Duncan chooses a Printer supporting Secure Print, which has a limited set of
196 control panel buttons (Up, Down, OK, Back) and a user can only enter numerical
197 passwords between 4-8 digits long. The Printer provides these restrictions to the Client;
198 the Client provides the user with feedback on the limitations, and only accepts a password
199 that complies with these restrictions.

200 3.2 Exceptions

201 No exceptions identified as of this writing.

202 3.3 Out of Scope

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

- 204 1. Authentication infrastructure that may be used by the Printer, such as LDAP or
205 RADIUS
- 206 2. The method of inputting a job password or user credential into the Printer

207 3.4 Design Requirements

208 The design requirements for this document are:

- 209 1. Define attributes for constraining the acceptable value formats for "job-
210 password" that are backward compatible with [PWG5100.11].
- 211 2. Register all attributes and operations with IANA and the PWG

212 The design recommendations for this document are:

- 213 1. Outlining best-practice user experience

214 4. Printer Description Attributes

215 4.1 job-password-length-supported (rangeOfInteger(0:255))

216 The 4.1 "job-password-length-supported" Printer Description attribute is a range that
217 specifies the minimum and maximum supported length of the unencrypted password,
218 measured in characters rather than octets. The character set encoding is specified by the
219 "job-password-repertoire-configured" attribute (Section 4.3). The Printer is configured to
220 accept an empty password if the range's minimum value is 0 (zero).

221 This attribute complements the existing "job-password-supported" attribute [PWG5100.11],
222 which specifies the maximum password length supported before encryption, measured in
223 octets.

224 4.2 job-password-repertoire-supported (1setOf (type2 keyword))

225 The "job-password-repertoire-supported" attribute enumerates the job password
226 repertoires (allowable characters, character sets and encodings) the Printer can be
227 configured to use.

228 The keywords are named according to a 'REGISTRY_ENCODING_RANGE' naming
229 structure convention. Table 1 lists the standard keywords. Vendor repertoire keywords,
230 prefixed with "vendor_" to indicate a vendor-specific registry, may also be used. Vendor
231 repertoire keywords SHOULD be registered with the PWG to achieve interoperability. As
232 an example, a vendor may choose to register the 'vendor_us-ascii_lowercase' keyword to

233 specify a repertoire limited to using only lowercase characters from the US ASCII
234 encoding.

235 The "utf-8" encoding name indicates the use of Network Unicode [RFC5198].

236 **Table 1: job-password-repertoire-supported keyword definitions**

<i>Keyword</i>	<i>Description</i>
<i>'iana_us-ascii_digits'</i>	Value must consist of only ASCII digits (0x30-0x39)
<i>'iana_us-ascii_letters'</i>	Value must consist of only US ASCII letters (0x41-0x5A, 0x61-0x7A)
<i>'iana_us-ascii_complex'</i>	Value must consist of US ASCII letters and numbers, with at least one uppercase letter, one lowercase letter, and one digit (0x30-0x39, 0x41-0x5A, 0x61-0x7A)
<i>'iana_us-ascii_any'</i>	Value must consist of US ASCII printable characters (0x20-0x7e)
<i>'iana_utf-8_digits'</i>	Value must consist of only UTF-8 numerical digits
<i>'iana_utf-8_letters'</i>	Value must consist of UTF-8 letters
<i>'iana_utf-8_any'</i>	Value must consist of UTF-8 printable characters

237 **4.3 job-password-repertoire-configured (type2 keyword)**

238 The "job-password-repertoire-configured" attribute indicates the password repertoire
239 currently configured for this Printer. The value of this attribute **MUST** be one of the set of
240 values listed in the "job-password-repertoire-supported" attribute defined in §4.2. A
241 supporting Client can use this attribute's value to limit User input so that the value in "job-
242 password" will comply with the configured password repertoire.

243 **5. Updates to Existing Attributes**

244 **5.1 job-password-encryption-supported**

245 "Internet Printing Protocol (IPP): Job and Printer Extensions – Set 2 (JPS2)"
246 [PWG5100.11] defines the "job-password-encryption-supported" attribute, and includes in
247 that definition a number of keywords. The 'sha' keyword indicated SHA-1.

248 This document proposes that the following values defined for "job-password-encryption-
249 supported" be deprecated: 'md2', 'md4', 'md5', 'sha'.

250 **6. Internationalization Considerations**

251 For interoperability and basic support for multiple languages, implementations use the
252 Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [RFC3629]
253 encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for Network
254 Interchange [RFC5198].

255 **7. Security Considerations**

256 The hash algorithms proposed to be deprecated in section 5.1 SHOULD NOT be used in
257 new Printers.

258 The IPP extensions defined in this document require the same security considerations as
259 defined in the IPP/1.1: Model and Semantics [RFC2911]. In addition, Infrastructure Printers
260 MUST:

- 261 1. Validate the HTTP Host request header in order to protect against DNS rebinding
262 attacks,
- 263 2. Provide confidentiality of data in transit using TLS encryption [RFC5246] of Client
264 and Proxy connections,
- 265 3. Authenticate Clients and Proxies using X.509 certificate validation, HTTP
266 authentication methods, and/or other mechanisms, and
- 267 4. Provide confidentiality of Document and Job data at rest.

268 Clients and Proxies MUST authenticate their connections to Infrastructure Printers, such
269 as by validating the Infrastructure Printer's X.509 certificate or using other in-band mutual
270 authentication protocols.

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

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

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

276 Unicode Security FAQ [UNISECFAQ] – common Unicode security issues

277 8. References

278 8.1 Informative References

- 279 [ISO10646] "Information technology -- Universal Coded Character Set (UCS)",
280 ISO/IEC 10646:2011
- 281 [NIST-FIPS-180-4] National Institute of Standards and Technology, "Secure Hash
282 Standard (SHS)", August 2015,
283 <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>
- 284 [PWG5100.11] T. Hastings, D. Fullman, "IPP: Job and Printer Operations - Set 2",
285 PWG 5100.11-2010, October 2010,
286 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-
287 20101030- 5100.11.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-20101030-5100.11.pdf)
- 288 [PWG5101.2] E. Bradshaw, I. McDonald, "RepertoireSupported Element", PWG
289 5101.2-2004, [http://ftp.pwg.org/pub/pwg/candidates/cs-crrepsup10-
290 20040201-5101.2.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-crrepsup10-20040201-5101.2.pdf)
- 291 [RFC3629] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC
292 3629, November 2003, <http://www.ietf.org/rfc/rfc3629.txt>
- 293 [RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange"
294 RFC 5198, March 2008, <http://www.ietf.org/rfc/rfc5198.txt>
- 295 [SP800-131] E. Barker, A. Roginsky, NIST Special Publication (SP) 800-131A
296 (Draft), "Transitions: Recommendation for Transitioning the Use of
297 Cryptographic Algorithms and Key Lengths", July 2015
- 298 [UNICODE] Unicode Consortium, "Unicode Standard", Version 8.0.0, June 2015,
299 [http://www.unicode.org/versions/Unicode8.0.0/ asdfsaf](http://www.unicode.org/versions/Unicode8.0.0/asdfsaf)
- 300 [UTS39] Unicode Consortium, "Unicode Security Mechanisms", UTS#39,
301 September 2014, <http://www.unicode.org/reports/tr39/tr39-9.html>
- 302 [UNISECFAQ] Unicode Consortium "Unicode Security FAQ", November 2013,
303 <http://www.unicode.org/faq/security.html>

304

305 9. Authors' Addresses

306 Primary authors:

307 Smith Kennedy

308 HP Inc.
309 11311 Chinden Blvd.
310 Boise ID 83714
311 smith.kennedy@hp.com

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

314 Michael Sweet - Apple Inc.
315 Ira McDonald - High North
316 William Wagner - TIC
317 Daniel Manchala - Xerox
318 Zaphod Beeblebrox - President of the Galaxy

319 **10. Change History**

320 **10.1 January 1, 2016**

321 Updated as per IPP WG conference call discussion on 2015-12-07:

- 322 • Accepted the change to replace "job-password-minimum-length" with "job-
323 password-length-supported"
- 324 • Removed "iana_utf-8_complex" from Table 1
- 325 • Added security considerations boilerplate and accompanying references by
326 borrowing from 5100.18 (INFRA).

327 **10.2 November 28, 2015**

328 Updated as per IPP WG conference call discussion on 2015-10-19:

- 329 • Changed list of hash algorithms to list the ones deprecated. New ones will just be
330 registered as per the standard IANA process, and won't be mentioned here.
- 331 • Some confusion over the way to evolve the "job-password-minimum-length"
332 attribute, caused by a mistaken understanding of the "job-password-supported"
333 attribute defined in JPS2
- 334 • Fixed keyword structure for "job-password-repertoire-supported" to align on
335 convention, and also mentioned Network Unicode

336 **10.3 October 12, 2015**

337 Updated as per IPP WG conference call discussion on 2015-09-21:

- 338 • Changed title
- 339 • Changed the keyword names for job-password-repertoire to comply with PWG
340 5101.2
- 341 • Added the "job-password-repertoire-configured" attribute
- 342 • Updated the references
- 343 • Refactored Table 2

344 **10.4 September 9, 2015**

345 Updated after a hiatus using notes from the April 2015 PWG F2F and other inputs.
346 Renamed the attributes several times, added keyword definitions for many UTF-8 format
347 types, and added a new section for extending the definition of the "job-password-
348 encryption" keyword range, and to clarify the definitions and deprecate many of the old
349 values.

350 **10.5 April 14, 2015**

351 Updated as per IPP WG discussion, in preparation for 2015 April F2F (Sunnyvale)
352 discussion in IPP WG and IDS WG.

353 **10.6 February 4, 2015**

354 Initial revision, presented at Feb. 2015 F2F