January 1, 2016
White Paper

The Printer Working Group

IPP Job Password Repertoire

Status: Final

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

Title: *IPP Job Password Repertoire*

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

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

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

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

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

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

About the IEEE-ISTO

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

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

http://www.ieee-isto.org

About the IEEE-ISTO PWG

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

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

For additional information regarding the Printer Working Group visit:

http://www.pwg.org

Contact information:

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

About the Internet Printing Protocol Work Group

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

For additional information regarding IPP visit:

http://www.pwg.org/ipp/

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

Table of Contents

List of Tables

1. Introduction

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

2. Terminology

2.1 Conformance Terminology

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

2.2 Terms Used in This Document

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

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

2.3 Protocol Role Terminology

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

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

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

2.4 Printing Terminology

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

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

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

2.5 Acronyms and Organizations

IANA: Internet Assigned Numbers Authority, http://www.iana.org/

IETF: Internet Engineering Task Force, http://www.ietf.org/

ISO: International Organization for Standardization, http://www.iso.org/

PWG: Printer Working Group, http://www.pwg.org/

3. Rationale for IPP Job Password Repertoire

Existing specifications define the following:

1. Internet Printing Protocol (IPP): Job and Printer Extensions – Set 2 (JPS2) [PWG5100.11] defines the "job-password" attribute for a Client to associate a password with the job. The Printer holds the Job in 'pending-held' state until a user provides that password. The "job-password-supported" attribute conveys the maximum length of the password.

2. Internet Printing Protocol (IPP): Job and Printer Extensions – Set 2 (JPS2) [PWG5100.11] defines the "job-password-encryption" attribute to specify the hashing algorithm used to obfuscate the value sent in the corresponding "job-password" attribute. The "job-password-encryption-supported" Printer Description attribute conveys the hashing algorithms supported by the Printer.

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

1. Proposes the definition of additional Printer Description attributes to convey restrictions on the length and range of acceptable characters supported by the "job-password" Job Template attribute, so that these additional constraints may be conveyed without breaking backward compatibility.

2. Recommends deprecation of some of the hashing algorithms, clarifies the definitions of existing ambiguous keywords, and propose the definition of new values.

3.1 Use Cases

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

3.1.1 Secure Print with Limited Control Panel

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

3.2 Exceptions

No exceptions identified as of this writing.

3.3 Out of Scope

The following are considered out of scope for this document:

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

3.4 Design Requirements

The design requirements for this document are:

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

The design recommendations for this document are:

1. Outlining best-practice user experience

4. Printer Description Attributes

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

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

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

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

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

The keywords are named according to a 'REGISTRY_ENCODING_RANGE' naming structure convention. Table 1 lists the standard keywords. Vendor repertoire keywords, prefixed with "vendor_" to indicate a vendor-specific registry, may also be used. Vendor repertoire keywords SHOULD be registered with the PWG to achieve interoperability. As an example, a vendor may choose to register the 'vendor_us-ascii_lowercase' keyword to specify a repertoire limited to using only lowercase characters from the US ASCII encoding.

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

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

Keyword	*Description*
'iana_us-ascii_digits'	Value must consist of only ASCII digits (0x30-0x39)
'iana_us-ascii_letters'	Value must consist of only US ASCII letters (0x41-0x5A, 0x61-0x7A)
'iana_us-ascii_complex'	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)
'iana_us-ascii_any'	Value must consist of US ASCII printable characters (0x20-0x7e)
'iana_utf-8_digits'	Value must consist of only UTF-8 numerical digits
'iana_utf-8_letters'	Value must consist of UTF-8 letters
'iana_utf-8_any'	Value must consist of UTF-8 printable characters

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

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

5. Updates to Existing Attributes

5.1 job-password-encryption-supported

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

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

6. Internationalization Considerations

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

7. Security Considerations

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

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

1. Validate the HTTP Host request header in order to protect against DNS rebinding attacks,

2. Provide confidentiality of data in transit using TLS encryption [RFC5246] of Client and Proxy connections,

3. Authenticate Clients and Proxies using X.509 certificate validation, HTTP authentication methods, and/or other mechanisms, and

4. Provide confidentiality of Document and Job data at rest.

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

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

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

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

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

8. References

8.1 Informative References

[ISO10646] "Information technology -- Universal Coded Character Set (UCS)", ISO/IEC 10646:2011

[NIST-FIPS-180-4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", August 2015, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[PWG5100.11] T. Hastings, D. Fullman, "IPP: Job and Printer Operations - Set 2", PWG 5100.11-2010, October 2010, http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-20101030- 5100.11.pdf

[PWG5101.2] E. Bradshaw, I. McDonald, "RepertoireSupported Element", PWG 5101.2-2004, http://ftp.pwg.org/pub/pwg/candidates/cs-crrepsup10-20040201-5101.2.pdf

[RFC3629] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629, November 2003, http://www.ietf.org/rfc/rfc3629.txt

[RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange" RFC 5198, March 2008, http://www.ietf.org/rfc/rfc5198.txt

[SP800-131] E. Barker, A. Roginsky, NIST Special Publication (SP) 800-131A (Draft), "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", July 2015

[UNICODE] Unicode Consortium, "Unicode Standard", Version 8.0.0, June 2015, http://www.unicode.org/versions/Unicode8.0.0/ asdfsaf

[UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, September 2014, http://www.unicode.org/reports/tr39/tr39-9.html

[UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2013, http://www.unicode.org/faq/security.html

9. Authors' Addresses

Primary authors:

Smith Kennedy
HP Inc.
11311 Chinden Blvd.
Boise ID 83714
smith.kennedy@hp.com

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

Michael Sweet - Apple Inc.
Ira McDonald - High North
William Wagner - TIC
Daniel Manchala - Xerox