The Printer Working Group

April 24, 2018
IPP Registration

IPP Job Reprint Password (REPRINTPWD)

Status: Interim

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

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

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

This document is available electronically at:

https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippreprintpwd-20180424.odt
https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippreprintpwd-20180424.pdf

Title: IPP Job Reprint Password *(REPRINTPWD)*

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:

https://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

Table of Contents

114 # List of Figures

115 # List of Tables

1. Introduction

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

2. Terminology

2.1. Protocol Roles 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.

1.1 Other Terms Used in This Document

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

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

1.2 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. Requirements for IPP Job Reprint Password

3.1. Use Cases

3.1.1. Protecting a Saved Document with a Persistent Password

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

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

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

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

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

3.2. Exceptions

3.2.1. Unauthorized Re-printing Disallowed From Printer Control Panel

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

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

3.3. Out of Scope

The following are considered out of scope for this document:

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

3.4. Design Requirements

The design requirements for this document are:

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

The design recommendations for this document are:

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

4. New Operation Attributes For Existing Operations

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

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

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

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

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

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

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

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

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

5. Printer Description Attributes

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

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

If the "job-reprint-password" Operation attribute is supported, then this attribute MUST be supported.

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

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

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

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

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

6. Additional Semantics For Existing Operations

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

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

7. Internationalization Considerations

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

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

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

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

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

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

8. Security Considerations

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

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

8.1. Human-readable Strings

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

9. IANA Considerations

9.1. Attribute Registrations

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

http://www.iana.org/assignments/ipp-registrations

The registry entries will contain the following information:


```
   Operation attributes:                              Reference
   ---------------------------------                  ---------------
   job-reprint-password (octetString(255) | no-value)
                                                       [REPRINTPWD]
   job-reprint-password-encryption
       type2 keyword | name(MAX))                      [REPRINTPWD]

   Printer Description attributes:                    Reference
   ---------------------------------                  ---------------
   job-reprint-password-supported
       (rangeOfInteger(0:255))                         [REPRINTPWD]
   job-reprint-password-encryption-supported
       (1setOf (type3 keyword | name(MAX)))            [REPRINTPWD]
   job-reprint-password-repertoire-supported
       (1setOf (type2 keyword))                        [REPRINTPWD]
```

10. References

10.1. Normative References

[IPPREPERTOIRE] S. Kennedy, “IPP Job Password Repertoire”, January 2016, https://ftp.pwg.org/pub/pwg/ipp/whitepaper/wp-job-password-repertoire-20160101.pdf

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

[PWG5100.5] D. Carney, T. Hastings, P. Zehler. “Internet Printing Protocol (IPP): Document Object”, PWG 5100.5-2003, October 2003, http://ftp.pwg.org/pub/pwg/candidates/cs-ippdocobject10-20031031-5100.5.pdf

[PWG5100.11] T. Hastings, D. Fullman, "IPP: Job and Printer Extensions – Set 2 (JPS2)", PWG 5100.11-2010, October 2010, https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-20101030-5100.11.pdf

[PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP Version 2.0, 2.1, and 2.2", PWG 5100.12-2015, October 2015, http://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.pdf

[PWG5100.13] M. Sweet, I. McDonald, P. Zehler, "IPP: Job and Printer Extensions - Set 3 (JPS3)", PWG 5100.13-2012, July 2012, http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf

[PWG5100.19] S. Kennedy, "IPP Implementor's Guide v2.0", PWG 5100.19-2015, August 2015, http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-20150821-5100.19.pdf

[RFC2817] R. Khare, S. Lawrence, “Upgrading to TLS Within HTTP/1.1”, RFC 2817, May 2000, https://www.ietf.org/rfc/rfc2817.txt

[RFC3510] R. Herriot, I. McDonald, “Internet Printing Protocol/1.1: IPP URL Scheme”, RFC 3510, April 2003, https://tools.ietf.org/html/rfc3510

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

[RFC6749] D. Hardt, “The OAuth 2.0 Authorization Framework”, RFC 6749, October 2012, http://www.ietf.org/rfc/rfc6749

[RFC7616] R. Shekh-Yusef, Ed., D. Ahrens, S. Bremer, “HTTP Digest Access Authentication”, RFC 7616, September 2015, https://www.ietf.org/rfc/rfc7616.txt

[RFC7617] J. Reschke, “The 'Basic' HTTP Authentication Scheme”, RFC 7617, September 2015, https://www.ietf.org/rfc/rfc7617.txt

[RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, June 2014, http://www.ietf.org/rfc/rfc7230.txt

[RFC7472] I. McDonald, M. Sweet, “Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps' URI Scheme”, RFC 7472, March 2015, https://tools.ietf.org/html/rfc7472

[RFC8010] M. Sweet, I. McDonald, “Internet Printing Protocol/1.1: Encoding and Transport”, RFC 8010, January 2017, https://www.ietf.org/rfc/rfc8010.txt

[RFC8011] M. Sweet, I. McDonald, “Internet Printing Protocol/1.1: Model and Semantics”, RFC 8011, January 2017, https://www.ietf.org/rfc/rfc8011.txt

[STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629/STD 63, November 2003, http://www.ietf.org/rfc/rfc3629.txt

[UAX9] Unicode Consortium, “Unicode Bidirectional Algorithm”, UAX#9, May 2016, http://www.unicode.org/reports/tr9

[UAX14] Unicode Consortium, “Unicode Line Breaking Algorithm”, UAX#14, June 2016, http://www.unicode.org/reports/tr14

[UAX15] Unicode Consortium, “Normalization Forms”, UAX#15, February 2016, http://www.unicode.org/reports/tr15

[UAX29] Unicode Consortium, “Unicode Text Segmentation”, UAX#29, June 2016, http://www.unicode.org/reports/tr29

[UAX31] Unicode Consortium, “Unicode Identifier and Pattern Syntax”, UAX#31, May 2016, http://www.unicode.org/reports/tr31

[UNICODE] The Unicode Consortium, “Unicode® 10.0.0”, June 2017, http://unicode.org/versions/Unicode10.0.0/

[UTS10] Unicode Consortium, “Unicode Collation Algorithm”, UTS#10, May 2016, http://www.unicode.org/reports/tr10

[UTS35] Unicode Consortium, “Unicode Locale Data Markup Language”, UTS#35, October 2016, http://www.unicode.org/reports/tr35

[UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, June 2016, http://www.unicode.org/reports/tr39

10.2. Informative References

[IANA-IPP] IANA Internet Printing Protocol (IPP) Registrations, http://www.iana.org/assignments/ipp-registrations

[UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November2016, http://www.unicode.org/faq/security.html

[UTR17] Unicode Consortium “Unicode Character Encoding Model”, UTR#17, November 2008, http://www.unicode.org/reports/tr17

[UTR20] Unicode Consortium “Unicode in XML and other Markup Languages”, UTR#20, January 2013, http://www.unicode.org/reports/tr20

[UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23, May 2015, http://www.unicode.org/reports/tr23

[UTR33] Unicode Consortium “Unicode Conformance Model”, UTR#33, November 2008, http://www.unicode.org/reports/tr33

11. 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:

Ira McDonald – High North Inc.

Mike Sweet – Apple Inc.

12. Change History

12.1. April 24, 2018

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

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

12.2. April 4, 2018

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

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

1.3 March 13, 2018

Updated as per feedback from IPP WG reflector:

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

1.4 March 11, 2018

Updated as per feedback from February 2018 PWG F2F review:

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

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

- Propose this be moved to IPP Registration candidate status

1.5 February 5, 2018

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

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

1.6 December 5, 2017

Initial revision.

