March 11, 2018
Whitepaper

The Printer Working Group

IPP Job Save Password (SAVEPASSWORD)

Status: Interim

Abstract: This white paper defines a new “job-save-accesses” operation attribute that specifies persistent access credentials that will persist with the Job even when saved, and that the Printer will require be provided when initially printing or re-printing that Job.

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

~~Abstract: This document is a whitepaper that proposes the creation of a new “save-password” Job Template attribute that provides the Job with a persistent password that will need to be provided when initially printing or re-printing that Job.~~

~~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/tb-savepassword-20180311.odt
~~http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-savepassword-20180205.odt~~
http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-savepassword-20180311.pdf
~~http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-savepassword-20180205.pdf~~

Copyright © 2017-2018 The Printer Working Group. All rights reserved.

Title: IPP Job Save Password *(SAVEPASSWORD)*

Table of Contents

List of Figures

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, to support scenarios involving a password protected saved job, new attributes need to be defined 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.

2.2 Other Terms Used in This Document

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

2.3 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 Save Password

3.1 Use Cases

3.1.1 Protecting a Saved Document with a Persistent Password

Wilma has written a 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

Harvey, an employee from another department, walks up to Wilma's departmental MFD. The .

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 Operation Attributes

4.1 job-save-accesses (collection | no-value)

The OPTIONAL "job-save-accesses" operation attribute allows the Client to provide authentication information for a referenced saved Job.

The collection value contains zero of more member attributes which provide the authentication information required for the Job to be reprinted. A Client MAY also provide the no- value out-of-band value to specify that no authentication information is necessary.

Printers specify which member attributes are supported using the "job-save-accesses-supported" Printer attribute (section XXX).

4.1.1 access-oauth-token (1setOf octetString(MAX))

The OPTIONAL "access-oauth-token" member attribute provides a Base64-encoded OAuth Access Token as defined in The OAuth 2.0 Authorization Framework [RFC6749]. When the size of the access token exceeds 1023 octets (the maximum size of an octetString value), the Client separates the token into multiple octetString values and sends the result as an ordered set to the Printer. The Printer reassembles each octetString to produce the complete access token value to be used to access the Document URI.

Printers that support this attribute MUST list 'access-oauth-token' in the "job-save-accesses-supported" Printer Description attribute.

4.1.2 access-oauth-uri (uri)

The OPTIONAL “access-oauth-uri” member attribute is the authorization server that issued the “access-oauth-token” member attribute. See Authorization Server [RFC6749] section 1.1.

4.1.3 access-password (text(MAX))

The OPTIONAL "access-password" member attribute provides a password string, typically for HTTP Basic or Digest authentication [RFC2617]. Clients MUST provide the password using the UTF-8 encoding [STD63] in Unicode Normalization Form C as required for Network Unicode [RFC5198]. Printers MUST convert the password, as needed, to whatever encoding is required to access the Document URI.

Printers that support this attribute MUST list 'access-password' in the "job-save-accesses-supported" Printer Description attribute.

4.1.4 access-pin (text(MAX))

The OPTIONAL "access-pin" member attribute provides a Personal Identification Number string. Clients MUST restrict the characters to the US ASCII digits '0' (code 48) through '9' (code 57) and Printers MUST reject values containing characters other than the digits '0' through '9'.

Printers that support this attribute MUST list 'access-pin' in the "job-save-accesses-supported" Printer Description attribute.

4.1.5 access-user-name (text(MAX))

The OPTIONAL "access-user-name" member attribute provides a user name string, typically for HTTP Basic or Digest authentication [RFC2617]. Clients MUST provide the user name using the UTF-8 encoding [STD63] in Unicode Normalization Form C as required for Network Unicode [RFC5198]. Printers MUST convert the user name, as needed, to whatever encoding is required by the Document URI.

Printers that support this attribute MUST list 'access-user-name' in the "job-save-accesses-supported" Printer Description attribute.

4.1.6 access-x509-certificate (1setOf octetString(MAX))

The OPTIONAL "access-x509-certificate" member attribute provides a PEM-encoded X.509 certificate identifying the User or Client that is making the request. When the size of the certificate exceeds 1023 octets (the maximum size of an octetString value), the Client separates the certificate into multiple octetString values and sends the result as an ordered set to the Printer. The Printer reassembles each octetString to produce the complete X.509 certificate to be used to access the Document URI.

Printers that support this attribute MUST list 'access-x509-certificate' in the "job-save-accesses-supported" Printer Description attribute and MUST provide an implementation-defined method for loading the corresponding private key that is used for authenticating the holder of the X.509 certificate.

5 Printer Description Attributes

5.1 job-save-accesses-configured (1setOf (type2 keyword))

The “job-save-accesses-configured” Printer Description attribute specifies the member attributes currently configured for use with “job-save-accesses”. This attribute's set of values MUST be a subset of the set of values specified by the Printer's “job-save-accesses-supported” attribute. This attribute MUST be supported if the “job-save-accesses-supported” Printer Description attribute is supported.

5.2 job-save-accesses-supported (1setOf (type2 keyword))

The “job-save-accesses-supported” Printer Description attribute specifies the supported member attributes of the “job-save-accesses” operation attribute. This attribute MUST be supported if the “job-save-accesses” operation attribute is supported.

5.3 ~~save-password-supported (rangeOfInteger(0:255))~~

6 ~~The “save-password” Printer Description attribute specifies whether the Printer supports the persistent Job password specified by the “save-password” Job Template attribute, and if so, what range of lengths the Printer's password policy requires for the unencrypted value of “save-password”. If the Client allows the User to provide it with an unencrypted password value shorter than the lower bounds of “save-password-supported”, the behavior is undefined but the Job may never print.~~

6.1 ~~save-password-encryption-supported (1setOf (type2 keyword))~~

7 ~~The “save-password-encryption-supported” Printer Description attribute specifies the encryption formats supported by the Printer for encrypting “save-password”. Any of the keywords registered for the “job-password-encryption” attribute may be listed in the “save-password-encryption-supported” attribute, except for the keyword 'none' and all the keywords that are deprecated by the PWG in the IANA IPP Registry [IANA-IPP] as of this writing: 'sha', 'md2', 'md4', 'md5'. The 'sha3-256' encryption hashing algorithm MUST be supported if this attribute is supported, to ensure interoperability between implementations. This attribute MUST be supported if the “save-password” member attribute of “job-save-disposition” is supported.~~

7.1 ~~save-password-repertoire-configured (1setOf (type2 keyword))~~

8 ~~The “save-password-repertoire-configured” Printer Description attribute specifies the set of repertoires the Printer is configured to accept for a Job's “save-password-repertoire” attribute. The values specified by “save-password-repertoire-configured” MUST be present in the set of keyword values specified by “save-password-repertoire-supported”.~~

8.1 ~~save-password-repertoire-supported (1setOf (type2 keyword))~~

9 ~~The "save-password-repertoire-supported" Printer Description attribute specifies the range of repertoires the Printer supports that may be configured for listing in the Printer's "save-password-repertoire-configured" attribute. All keywords specified in the "save-password-repertoire-supported" must be registered in the IANA IPP Registry [IANA-IPP] for the "job-password-repertoire" attribute [IPPREPERTOIRE]. The 'iana_utf-8_any' keyword MUST be supported if this attribute is supported. This attribute MUST be supported if the "save-password-repertoire" member attribute of "job-save-disposition" is supported.~~

10 ~~Additional Values and Semantics for Existing Attributes~~

10.1 ~~job-save-disposition Member Attributes~~

11 ~~This specification defines several new "job-save-disposition" member attributes to support the specification of a Job Save Password.~~

11.1.1 ~~save-password (octetString(1024))~~

12 ~~The "save-password" member attribute specifies a password for the Job, which is semantically analogous to the "job-password" Operation attribute [PWG5100.11]. The Printer MUST NOT process the Job unless a User provides a password value that matches the value stored in "save-password" to authorize the Printer to allow its release. This member attribute MUST be present if the "save-password-encryption" member attribute is present.~~

13 ~~The maximum length of this attribute is greater than the length of "save-password-supported" because this attribute needs to accommodate encrypted passwords which have longer fixed lengths.~~

13.1.1 ~~save-password-encryption (type2 keyword)~~

14 ~~The "save-password-encryption" Job Template attribute specifies the hashing algorithm the Client employed to obfuscate the password value specified in the "save-password" Job Template attribute. This member attribute MUST be present if the "save-password" member attribute is present. The value held by "save-password-encryption" MUST be one of the values in the "save-password-encryption-supported" Printer Description attribute.~~

14.1.1 ~~save-password-repertoire (type2 keyword)~~

15 ~~The "save-password-repertoire" Job Template attribute specifies the repertoire selected for the "save-password" attribute. This member attribute MUST be present if the "save-password" member attribute is present. The value held by "save-password-repertoire" MUST be one of the values in the "save-password-repertoire-supported" Printer Description attribute.~~

15.1 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) [RFC3629] 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

16 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. Additionally, the operation attributes defined in this IPP Registration MUST NOT be sent over a non-encrypted connection~~, plus additional security considerations below~~.

16.1 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

17 IANA Considerations

17.1 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-save-accesses (collection | no-value)	[SAVEPASSWORD]
access-oauth-token (1setOf octetString(MAX))	[SAVEPASSWORD]
access-oauth-uri (uri)	[SAVEPASSWORD]
access-password (text(MAX))	[SAVEPASSWORD]
access-pin (text(MAX))	[SAVEPASSWORD]
access-user-name(text(MAX))	[SAVEPASSWORD]
access-x509-certificate (1setOf octetString(MAX))	[SAVEPASSWORD]

Printer Description attributes:	Reference
job-save-accesses-configured (1setOf (type2 keyword))	[SAVEPASSWORD]
job-save-accesses-supported (1setOf (type2 keyword))	[SAVEPASSWORD]

18 References

18.1 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

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

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

[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

18.2 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

19 Authors' Addresses

Primary authors (using Address style):

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

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

~~Turanga Leela - Planet Express~~
~~Zapp Brannigan - Democratic Order of Planets~~
~~Wowbanger The Infinitely Prolonged – Independent Consultant~~
Ira McDonald – High North Inc.
Mike Sweet – Apple Inc.

20 Change History

20.1 March 11~~February 5~~, 2018

Updated as per feedback from February 2018 PWG F2F ~~Dec. 14, 2017 IPP WG teleconference~~ 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

20.2 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.
-
- December 5, 2017

Initial revision.

