August 1, 2017
White Paper

The Printer Working Group

IPP Get-User-Printer-Attributes Operation (*USEROP*)

Status: Initial

Abstract: This document proposes a new Get-User-Printer-Attributes IPP operation that allows an IPP Client to retrieve the Printer's settings that are available to the Client's current User.

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:

https://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-userop-20170801.odt
~~https://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-userop-20170524.odt~~
https://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-userop-20170801.pdf
~~https://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-userop-20170524.pdf~~

Title: *IPP Get-User-Printer-Attributes Operation (USEROP)*

Table of Contents

List of Figures

List of Tables

1 Introduction

This document proposes a new Get-User-Printer-Attributes IPP operation that allows an IPP Client to retrieve the Printer's settings that are available to the Client's current User. It is semantically identical to the existing Get-Printer-Attributes IPP operation [RFC8011], with the key difference that the Printer will always respond with an authentication challenge. Once the Client has authenticated using the User's credentials, the Printer will respond with the settings for that user.

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 Rationale for IPP Get-User-Printer-Attributes Operation

While there are many solutions, both standard and non-standard, for creating print policies that provide a way to specify allowed or disallowed features according to individual users, systems, applications and so forth, there is no established method that is in-band of IPP. Having a print policy method using IPP would better support systems such as IPP Everywhere [PWG5100.14] in print infrastructures provided by public print providers, enterprises or educational environments such as university settings.

Technical justification for pursuing the creation of a new IPP operation rather than reusing or overloading existing operations such as Get-Printer-Attributes is discussed in section 4.

3.1 Use Cases

The need for solutions to these use cases emerged during the process of writing the IPP Implementor's Guide v2 [PWG5100.19].

3.1.1 Print Policy For Some Users Limits Print Capabilities

Sue wants to print her report on her department's workgroup printer. She wants to print it in color to make the color graphs look best. However, she has abused her printing privileges, so her department head has instructed the network administrator to restrict her user account's ability to print in color.

Sue opens the document on her laptop, chooses to print, and selects the department's workgroup printer. The Printer authenticates the laptop using Sue's credentials, and then provides the laptop with the print choices available for Sue's account, which does not include color printing. Sue decides whether to print it in black-and-white anyway or to print from one of the campus print centers, where she can pay to print in color.

Bob is an associate professor in the same department as Sue. His account has no limitations for color printing. He opens a document on his tablet, taps to print, and selects the department's workgroup printer. His tablet presents print options including the option of printing in color. Bob chooses to print in color, and prints his document, which prints in color as he expects.

Figure 3.1 illustrates this use case with a sequence diagram.

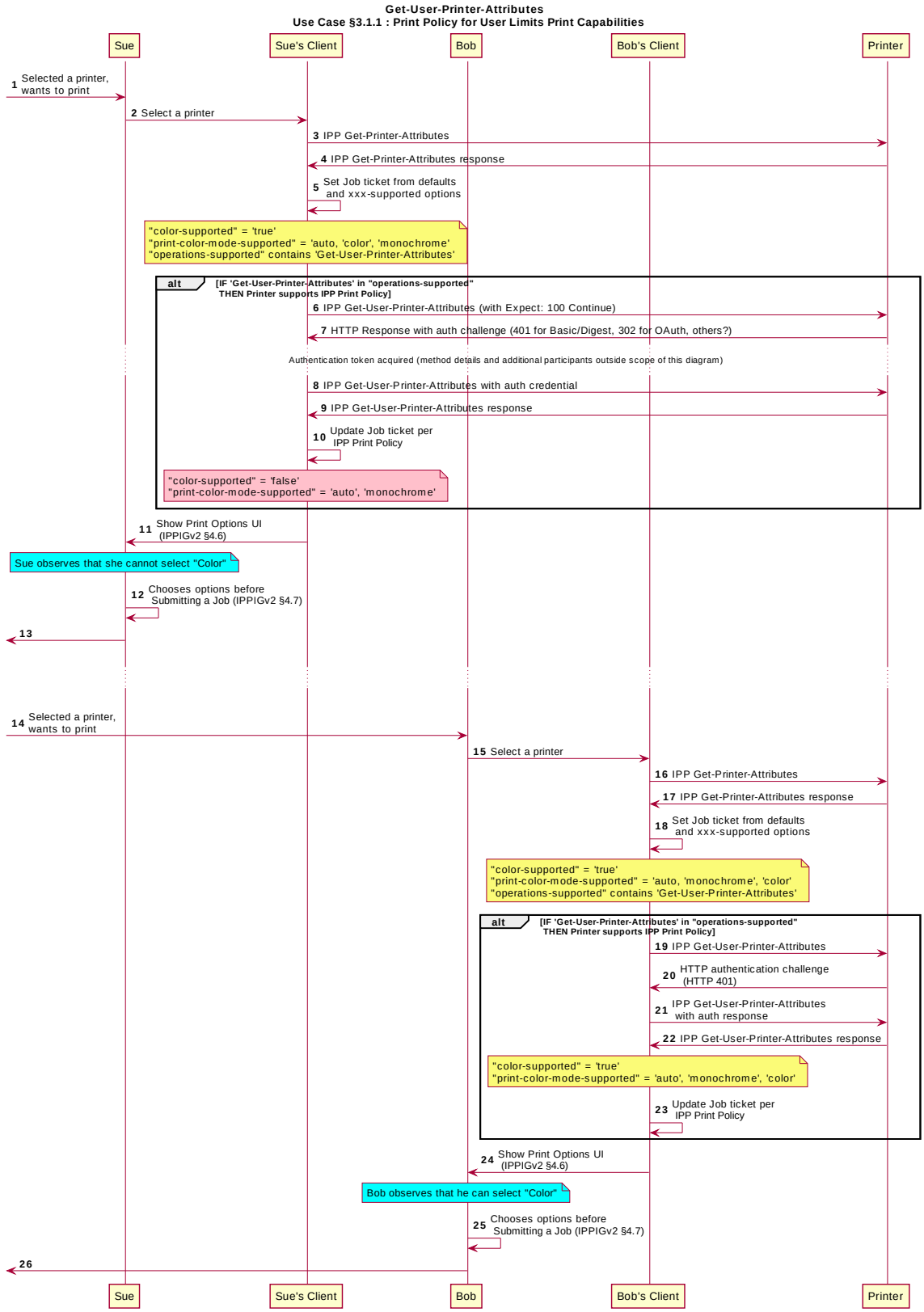

Figure 3.1 : Use Case 3.1.1 Sequence Diagram

3.1.2 User Not Listed in Print Policy Denied Ability to Print in Color

In this use case, a user who is not named in the print policy system is denied the ability to print using existing conventional IPP print protocol use. The Client may implement support for IPP Print Policy but authentication may fail, or the Client may have not implemented support for IPP Print Policy.

Duncan is at the office and needs to print a 5 page report that contains color diagrams before his next meeting. His office user account has been granted permission by his office network administrator to print in color. Duncan opens the document on his tablet, taps to print, and selects the desired Printer. The tablet fetches the Printer's default capabilities, and then authenticates using Duncan's user account to retrieve the print options available to him as per his account's print policy, including the option to print in color or monochrome. He prints the document using the color option, retrieves the hardcopy from the printer, and then goes on to his meeting.

Ed is visiting Duncan's office and needs to print a 3 page document. Ed is not listed as a user in the print policy. Ed opens the document on his laptop, clicks to print, and selects the Printer recommended by Duncan. The laptop does not support print policies or does but has no valid credentials. The Printer provides Ed's laptop with the default print capabilities. When the Job is submitted to the Printer, the Printer rejects the Job or identifies the setting that were adjusted, since unknown users don't have the right to print in color on this printer.

Figure 3.2 illustrates this use case with a sequence diagram.

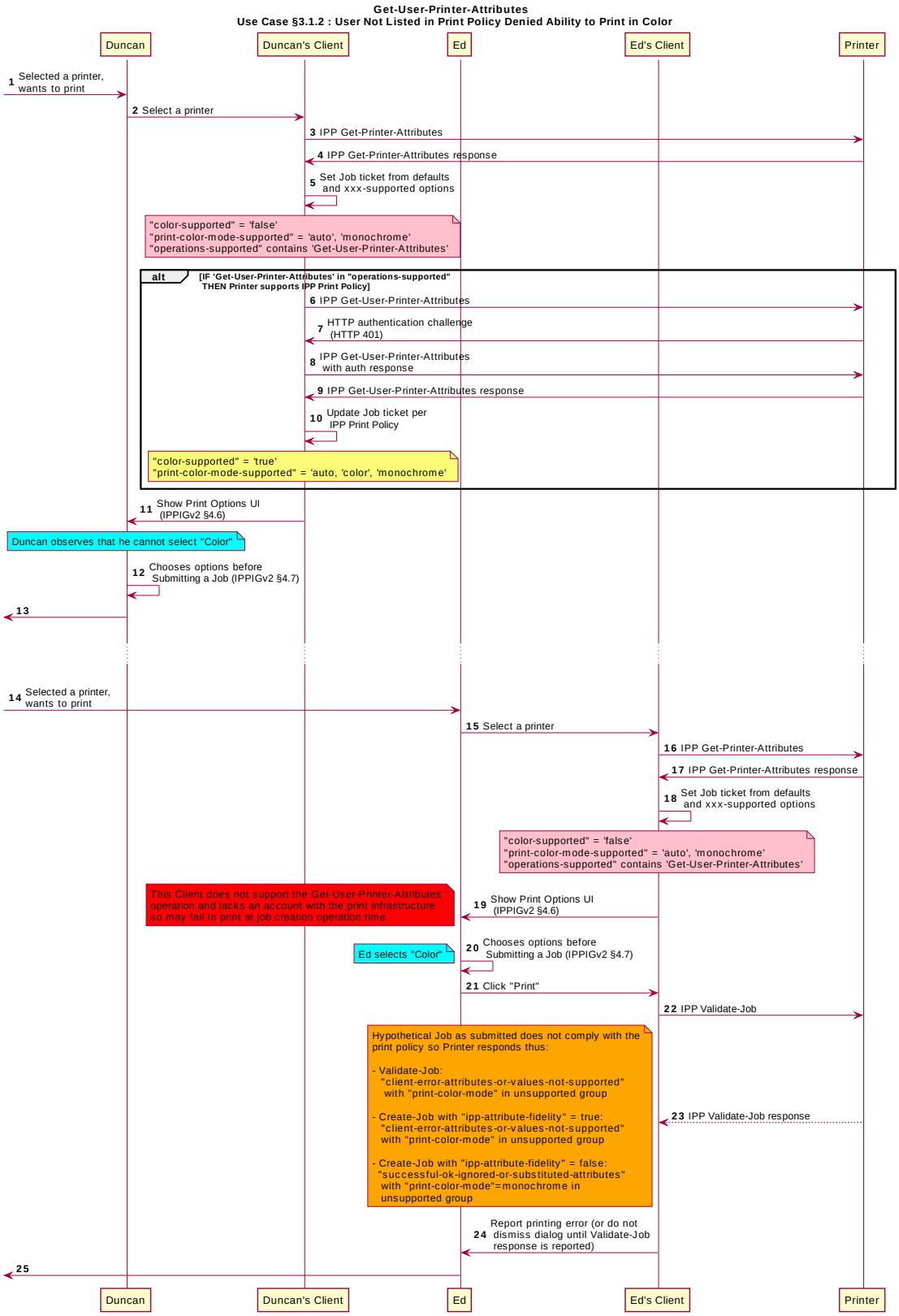

Figure 3.2 : Use Case 3.1.2 Sequence Diagram

3.2 Exceptions

There are no exceptions to the use cases in section 3.1.

3.3 Out of Scope

The following are considered out of scope for this document:

1. Definition of actual print policies.
2. Definition of how print policy management systems structure and/or organize the sets of users and their policies.
3. Definition of non-IPP protocols that can provide similar functionality.

3.4 Design Requirements

The design requirements for this document are:

1. Identify an appropriate set of IPP operations that allows a supporting Client to acquire from the target Printer the set of print features available for a particular User.
2. Identify an appropriate Printer behavior and expected Client behavior for a non-supporting Client (i.e. one that is unaware of this new system) can still be a legitimate actor in the print policy system.
3. Identify an appropriate set of IPP operations and attributes that allows a Printer to refer a Client to a trusted IPP Print Policy Service, such that the Client can assert that the options it provides with a submitted job do comply with a policy originating from that trusted policy server.
4. Maintain backward compatibility with existing versions of IPP (IPP/1.1, IPP/2.x).
5. Register all attributes and operations with IANA.

The design recommendations for this document are:

1. Recommend suitable authentication methods and guidelines for the use of those methods that could inform the creation of a high quality Client user experience.

4 Technical Solutions/Approaches

Although the existing Get-Printer-Attributes operation [RFC8011] conveys the needed information and could be used for this task, few~~no~~ legacy Clients expect the Printer to respond to a Get-Printer-Attributes operation with an HTTP authentication challenge. To preserve backward compatib~~A new operation with the appropriate semantics was decided to be the most efficient way to add this fac~~ility with legacy Clients, a new~~to the IPP ecosystem. Adding additional operation attributes to the Get-Printer-Attributes~~ operation is defined here, with semantics similar to Get-Printer-Attributes.~~to cause the Printer to respond with an authentication challenge could be done, but would require updating the core IPP specifications, which is procedurally not desirable. If the Printer were to filter its~~

~~response or respond with an authentication challenge if "requesting-user-name" were included in the operation request, that would be a change to existing behavior precedent.~~

5 IPP Operations

5.1 Get-User-Printer-Attributes Operation

This REQUIRED operation allows a Client to request the values of the attributes of a Printer. This operation is semantically similar to the Get-Printer- Attributes operation [RFC8011] except that the returned attributes and values MAY be different depending on the most authenticated user, and the Client MUST be prepared to respond to an HTTP authentication challenge. The Client detects whether the Printer supports this operation by examining the "operations-supported" attribute [RFC8011].

~~This REQUIRED operation allows a Client to request the values of the attributes of a Printer. The semantics of this operation are identical to the semantics for the Get-Printer-Attributes operation, with the difference that the Client MUST be prepared to respond to an HTTP authentication challenge. The Client detects whether the Printer supports this operation by examining the "operations-supported" attribute [RFC8011].~~

If the Client initiates the Get-User-Printer-Attributes operation over a non-TLS connection, the Client MUST be prepared to receive an HTTP 426 response to upgrade the connection to TLS [RFC2817]. The Printer MUST only send Get-User-Printer-Attributes responses over TLS connections.

5.1.1 Get-User-Printer-Attributes Request

The following groups of attributes are supplied as part of the Get-User-Printer-Attributes request:

Group 1: Operation Attributes

Natural Language and Character Set:

The "attributes-charset" and "attributes-natural-language" attributes as described in [RFC8011] Section 4.1.4.1.

Target:

The "printer-uri" (uri) operation attribute, which is the target for this operation as described in [RFC8011] Section 4.1.5.

Requesting User Name:

The "requesting-user-name" (name(MAX)) attribute SHOULD be supplied by the Client as described in [RFC8011] Section 9.3. In addition, the "requesting-user-uri" (uri) [PWG5100.13]and "requesting-user-vcard" (1setOf

text(MAX)) [PWG5100.SYSTEM] attribute SHOULD be supplied by the Client as described in their respective PWG specifications. These attributes SHOULD be sent even when HTTP authentication is used, since the “most authenticated user” principle applies here as with all IPP operations, as per [RFC8011] Section 9.3.

"requested-attributes" (1setOf keyword):

The "requested-attributes" (1setOf keyword) attribute SHOULD be supplied by the Client as described in [RFC8011] Section 4.2.5.1.

"document-format" (mimeMediaType):

The "document-format" (mimeMediaType) attribute SHOULD be supplied by the Client as described in [RFC8011] Section 4.2.5.1.

5.1.2 Get-User-Printer-Attributes Response

The Printer returns the following sets of attributes as part of the Get-User-Printer-Attributes response:

Group 1: Operation Attributes

Natural Language and Character Set:

The "attributes-charset" and "attributes-natural-language" attributes as described in [RFC8011] Section 4.1.4.1.

Status Message:

In addition to the REQUIRED status-code returned in every response, the response MAY include a "status-message" (text(255)) and/or a "detailed-status-message" (text(MAX)) operation attribute as described in [RFC8011] Appendix B and Section 4.1.6.

Group 2: Unsupported Attributes

See [RFC8011] Section 4.1.7 for details on returning unsupported attributes.

Group 3: Printer Attributes

This is the set of requested attributes and their current values. See [RFC8011] Section 4.2.5.2 for details.

6 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

~~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].~~

Security Considerations

The security considerations for the Get-User-Printer-Attributes operation build upon those defined for IPP/1.1 [RFC8011] and IPP/2.0 [PWG5100.12] for the Validate-Job, Create-Job and Print-Job operations. In addition to those security considerations, a Printer MUST NOT send a Get-User-Printer-Attributes response over a non-TLS connection.

6.1 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

~~The security considerations for the Get-User-Printer-Attributes operation are identical to those listed for IPP/1.1 [RFC8011] and IPP/2.0 [PWG5100.12].~~

References

6.2 Normative References

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

[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

~~[PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP/2.0 Second Edition", PWG 5100.12-2011, February 2011, http://ftp.pwg.org/pub/pwg/candidates/cs-ipp20-20110214-5100.12.pdf~~

[PWG5100.14] M. Sweet, I. McDonald, A. Mitchell, J. Hutchings, "IPP Everywhere", 5100.14-2013, January 2013, http://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-5100.14.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

[PWG5100.SYSTEM] I. McDonald, “IPP System Service v1.0”, PWG 5100.SYSTEM, TBD, http://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippsystem10-20170719.pdf

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

[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

[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

6.3 Informative References

[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

~~[UNICODE] The Unicode Consortium, “The Unicode Standard, Version 6.2.0”, ISBN 978-1-936213-07-8, September 2012, http://www.unicode.org/versions/Unicode6.2.0/~~

Authors' Addresses

Primary authors:

Smith Kennedy
11311 Chinden Blvd. MS 506
Boise, ID 83714
smith.kennedy@hp.com

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

Mike Sweet – Apple Inc.
Ira McDonald – High North Inc.

7 Change History

7.1 August 1, 2017

Updated as per feedback from July 20, 2017 IPP WG meeting minutes and feedback:

- Added sub-sections for the Get-User-Printer-Attributes request and response, leveraging text from RFC 8011 and 5100.SYSTEM
- Updated Internationalization section to use Unicode 10 and added a bunch of references.
- Updated references to add System, and full standard of IPP/2.0 (5100.12)
- Other editorial fixes

7.2 May 24, 2017

Updated as per feedback from May 2017 F2F review.

- Removed previous use cases 3.1.2-3.1.5; renamed 3.1.6 to be new 3.1.2, with updated sequence diagram that includes Validate-Job / Create-Job response.
- Removed section 6 – no new IPP attributes need to be defined as of this draft.

7.3 April 18, 2017

- Updated and clarified the description in section 4 “Technical Solutions/Approaches” to explain with more detail why it is not practical to use the venerable Get-Printer-Attributes operation for the task of conveying print policies.

7.4 April 4, 2017

- Updated with new and elaborated use cases and accompanying sequence diagrams to better articulate the breadth of the problem space.

7.5 February 1, 2017

- Editorial changes.

7.6 January 30, 2017

- Initial draft.

