



The Printer Working Group

December 5, 2017  
White Paper

1 **IPP Authentication Methods**  
2 **(IPPAUTH)**

3 | Status: ~~Interim~~**Initial**

4 Abstract: This document is a whitepaper that describes the interaction between IPP and  
5 various authentication mechanisms used by IPP's HTTP and HTTPS transports, and how  
6 they might affect the authentication user experience on systems running an IPP Client.

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

9 This document is available electronically at:

10 | <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20171205.odt>  
11 | <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20170802.odt>  
12 | <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20171205.pdf>  
13 | <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20170802.pdf>  
14 | [Copyright © 2017-2018 The Printer Working Group. All rights reserved.](#)

15 | ~~Copyright © 2017 The Printer Working Group. All rights reserved.~~

16 | Title: IPP Authentication Methods (*IPPAUTH*)

17 The material contained herein is not a license, either expressed or implied, to any IPR  
18 owned or controlled by any of the authors or developers of this material or the Printer  
19 Working Group. The material contained herein is provided on an “AS IS” basis and to the  
20 maximum extent permitted by applicable law, this material is provided AS IS AND WITH  
21 ALL FAULTS, and the authors and developers of this material and the Printer Working  
22 Group and its members hereby disclaim all warranties and conditions, either expressed,  
23 implied or statutory, including, but not limited to, any (if any) implied warranties that the use  
24 of the information herein will not infringe any rights or any implied warranties of  
25 merchantability or fitness for a particular purpose.

26 **Table of Contents**

27 1 Introduction.....4

28 2 Terminology.....4

29 2.1 Protocol Roles Terminology.....4

30 2.2 Other Terms Used in This Document.....4

31 2.3 Acronyms and Organizations.....4

32 3 Rationale for IPP Authentication Methods.....5

33 3.1 Client Authentication Methods.....5

34 3.1.1 The 'none' IPP Authentication Method.....6

35 3.1.2 The 'requesting-user-name' IPP Authentication Method.....7

36 3.1.3 The 'basic' IPP Authentication Method.....8

37 3.1.4 The 'digest' IPP Authentication Method.....9

38 3.1.5 The 'negotiate' IPP Authentication Method.....10

39 3.1.6 The 'oauth' IPP Authentication Method.....11

40 4 Implementation Recommendations.....13

41 4.1 Client Implementation Recommendations.....13

42 4.1.1 General Recommendations.....13

43 4.1.2 OAuth2 Recommendations.....13

44 4.2 Printer Implementation Recommendations.....13

45 5 Internationalization Considerations.....13

46 6 Security Considerations.....14

47 6.1 Human-readable Strings.....14

48 6.2 Client Security Considerations.....14

49 6.3 Printer Security Considerations.....15

50 7 References.....15

51 7.1 Normative References.....15

52 7.2 Informative References.....17

53 8 Authors' Addresses.....18

54 9 Change History.....19

55 9.1 December 5, 2017.....19

56 9.2 August 3, 2017.....19

57 **List of Figures**

Figure 3.1: Sequence diagram for the 'none' IPP Authentication Method.....6

Figure 3.2: Sequence diagram for the 'requesting-user-name' IPP Authentication Method.....7

Figure 3.3 : Sequence diagram for the 'basic' IPP Authentication Method.....8

Figure 3.4 : Sequence diagram for the 'digest' IPP Authentication Method.....9

Figure 3.5 : Sequence diagram for the 'negotiate' IPP Authentication Method.....10

Figure 3.6 : Sequence diagram for the 'oauth' IPP Authentication Method.....11

58 **List of Tables**

## 59 | Introduction

60 The Internet Printing Protocol (hereafter, IPP) uses HTTP as its underlying transport  
61 [RFC8010]. When an IPP Printer is configured to limit access to its services to only those  
62 Clients operated by an authorized User, IPP employs various different HTTP authentication  
63 methods. But since an IPP Client isn't usually a typical HTTP User Agent (e.g. it isn't a  
64 commonly used Web browser), some limits, constraints and conventions ought to be  
65 considered when implementing support for one of these different HTTP authentication  
66 methods.

## 67 | 1 Terminology

### 68 | 1.1 Protocol Roles Terminology

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

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

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

### 76 | 1.2 Other Terms Used in This Document

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

### 78 | 1.3 Acronyms and Organizations

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

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

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

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

## 83 **2 Rationale for IPP Authentication Methods**

84 This white paper describes how various HTTP based authentication systems integrate into  
85 IPP communications between a Client and a Printer. Although the authentication protocols  
86 themselves do not need to change to be integrated into IPP communications, the IPP  
87 Client is not a Web browser, so some considerations must be made by IPP Client  
88 implementors. The “uri-authentication-supported” attribute [RFC8011] Printer Description  
89 attribute indicates the authentication systems supported by the Printer.

### 90 **2.1 Client Authentication Methods**

91 The “uri-authentication-supported” attribute [RFC8011] indicates the authentication method  
92 used for a corresponding URI in “printer-uri-supported”. A Printer uses the identity to  
93 authorize access to capabilities such as operations, resources, and attributes. As in most  
94 other contexts, authentication is the process of establishing that an entity claiming to have  
95 a particular identity is who they say they are.

96 Each of the authentication method keywords currently registered for “uri-authentication-  
97 supported” is described below, with an accompanying sequence diagram for illustration  
98 purposes.

99 **2.1.1 The 'none' IPP Authentication Method**

100 The 'none' IPP Authentication Method [RFC8011] very simply indicates that the receiving  
 101 Printer is provided no method whatsoever to determine the identity of the User who is  
 102 operating the Client that is making IPP operation requests. The user name for the  
 103 operation is assumed to be 'anonymous'.

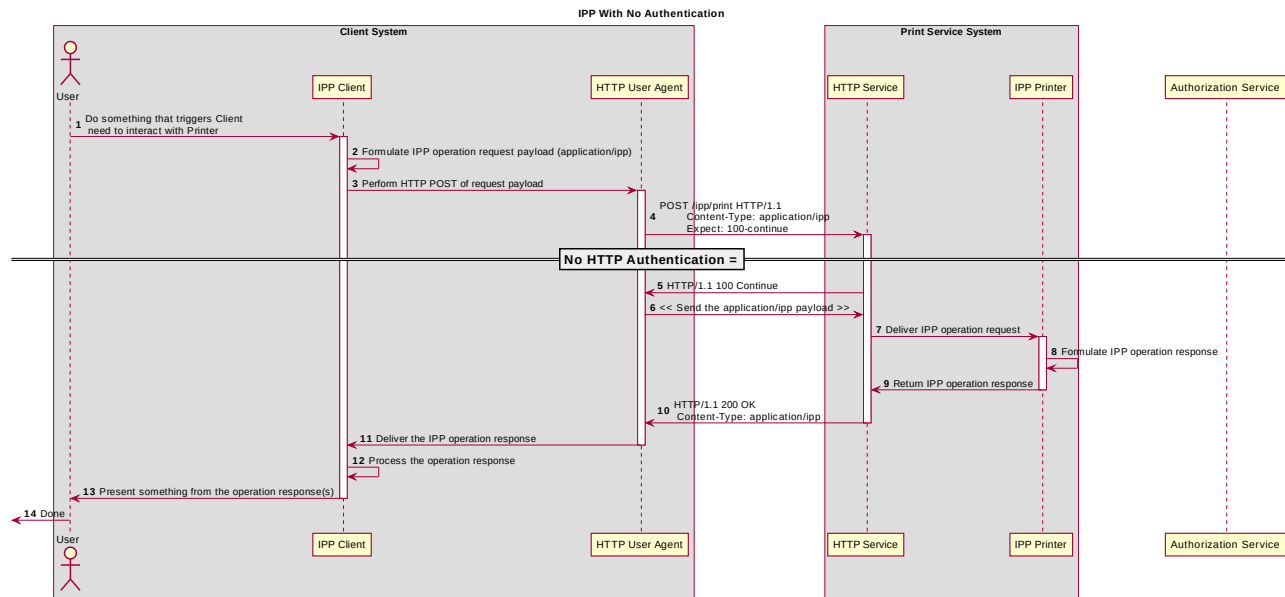


Figure 2.1: Sequence diagram for the 'none' IPP Authentication Method

104 This method is not recommended unless the Printer's operator has the objective of  
 105 providing an anonymous print service. In most cases, the Client SHOULD provide the  
 106 "requesting-user-name" operation attribute, as described in section 2.1.2.

107 **2.1.2 The 'requesting-user-name' IPP Authentication Method**

108 In the 'requesting-user-name' IPP Authentication Method [RFC8011], the Client MUST  
 109 provides the “requesting-user-name” operation attribute [RFC8011] in its IPP operation  
 110 request. The Printer uses this unauthenticated name as the identity of the actor operating  
 111 the Client.

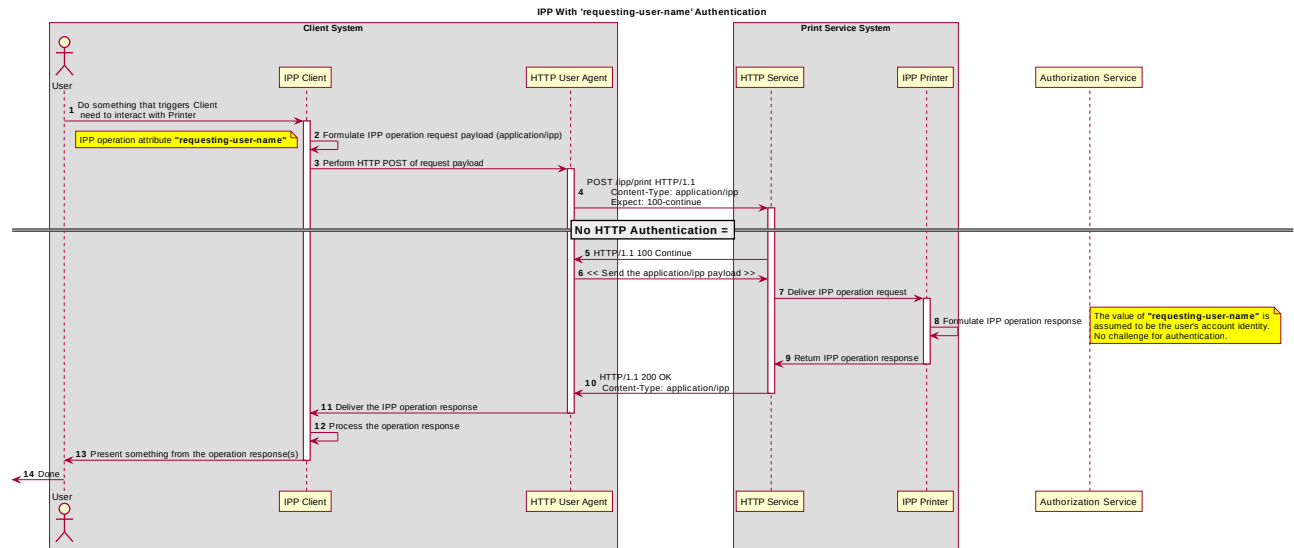


Figure 2.2: Sequence diagram for the 'requesting-user-name' IPP Authentication Method

112 This method is not recommended since there is no actual authentication performed as  
 113 there is no credential provided to prove the identity claimed in the “requesting-user-name”.

114 **2.1.3 The 'basic' IPP Authentication Method**

115 The 'basic' IPP Authentication Method uses HTTP “basic” authentication scheme  
 116 [RFC7617]. It is employed in IPP in much the same way that it is employed in conventional  
 117 HTTP workflows using a Web browser; when the IPP Client encounters an HTTP 401  
 118 Unauthorized response, it evaluates whether it supports the authentication method  
 119 identified by the value of the “WWW-Authenticate” header in the response. In this case, if  
 120 it supports 'basic', it will present UI asking the User to provide username and password  
 121 credentials that may be used to authenticate with the HTTP Server providing access to the  
 122 IPP Printer. If the HTTP Server successfully authenticates that set of credentials, then the  
 123 IPP operation request is passed on to the IPP Printer, which responds as usual.

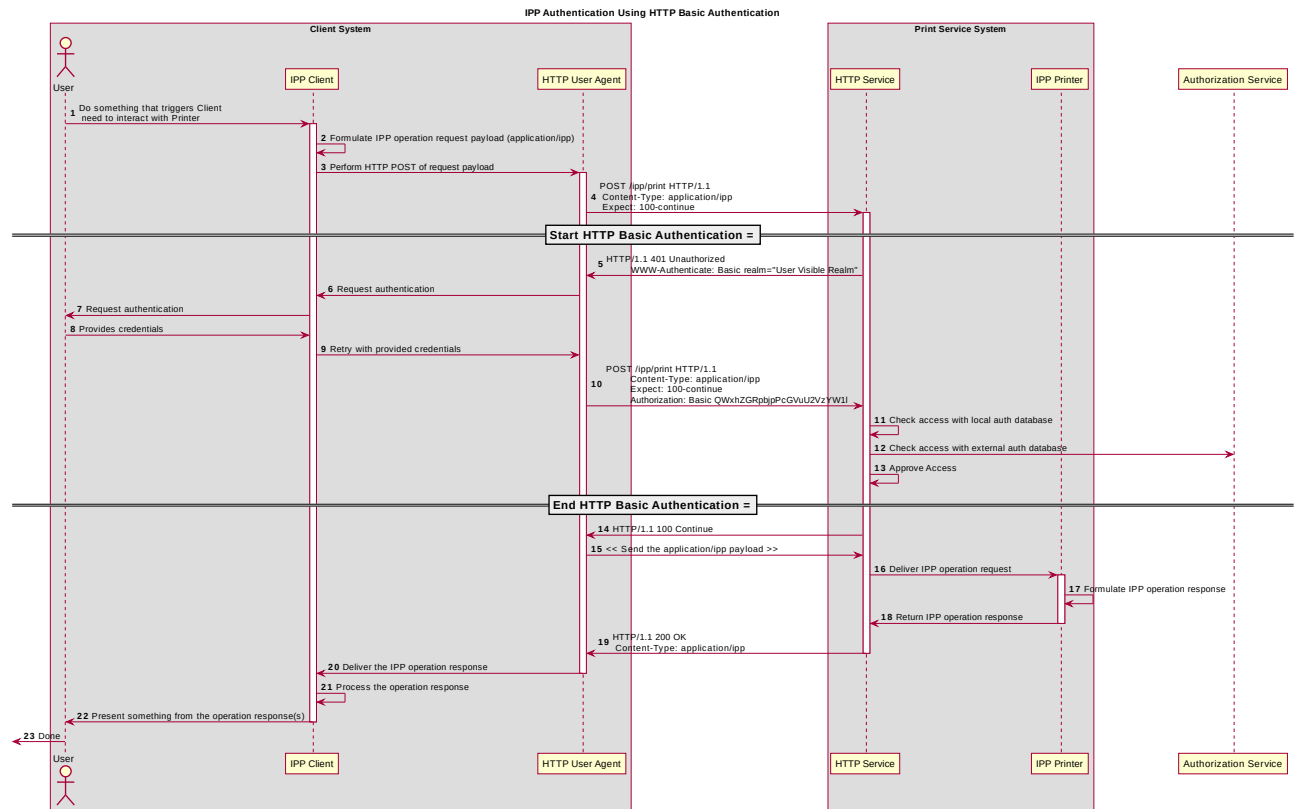


Figure 2.3 : Sequence diagram for the 'basic' IPP Authentication Method



124 **2.1.4 The 'digest' IPP Authentication Method**

125 The 'digest' IPP Authentication method uses the HTTP “digest” authentication scheme  
 126 [RFC7616]. It is employed in IPP in much the same way that it is employed in conventional  
 127 HTTP workflows using a Web browser; when the IPP Client encounters an HTTP 401  
 128 Unauthorized response, it evaluates whether it supports the authentication method  
 129 identified by the value of the “WWW-Authenticated” header in the response. In this case, if  
 130 it supports 'digest', it will present UI asking the User to provide username and password  
 131 credentials that may be used to authenticate with the HTTP Server providing access to the  
 132 IPP Printer. If the HTTP Server successfully authenticates that set of credentials, then the  
 133 IPP operation request is passed on to the IPP Printer, which responds as usual.

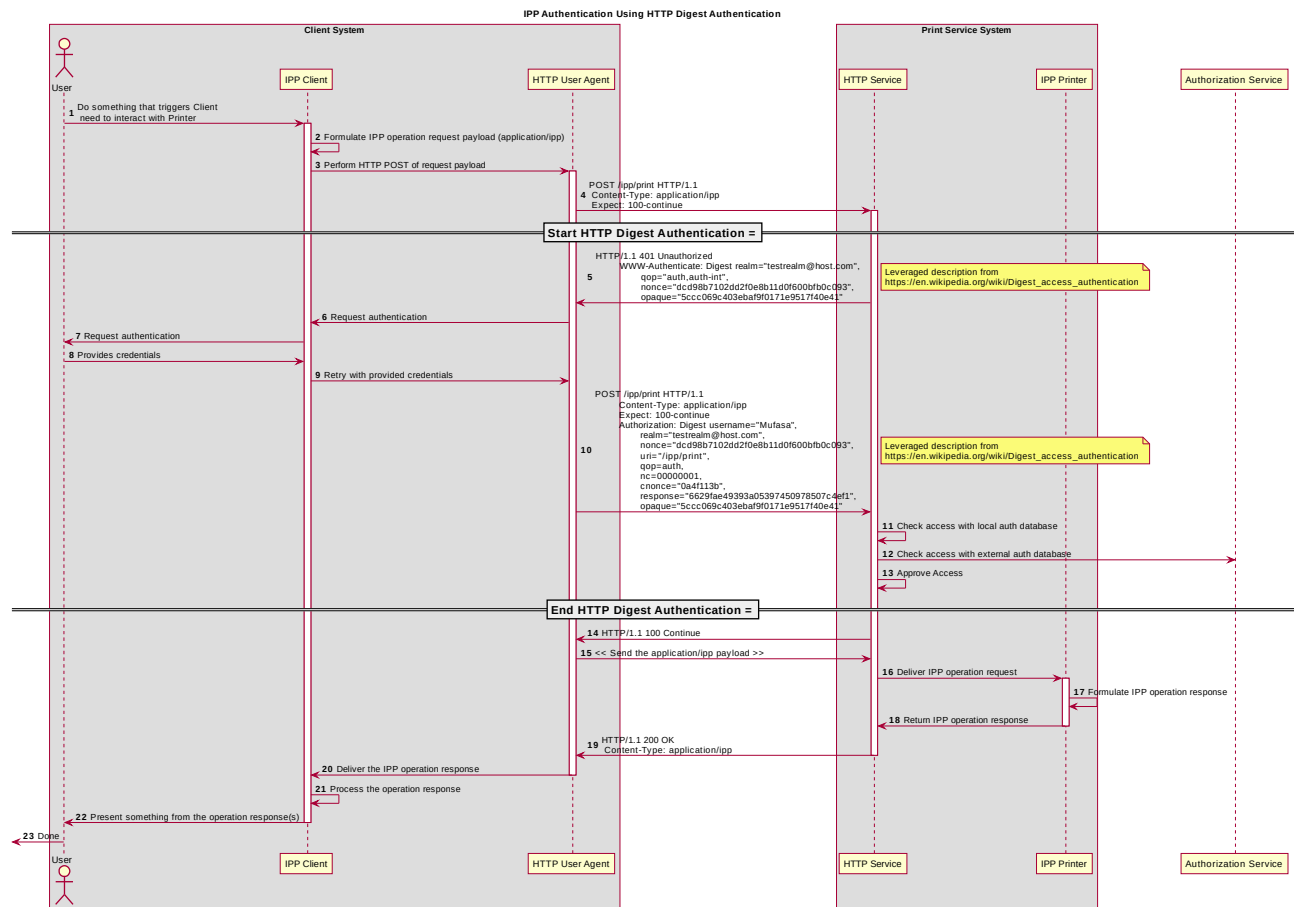


Figure 2.4 : Sequence diagram for the 'digest' IPP Authentication Method

134 **2.1.5 The 'negotiate' IPP Authentication Method**

135 The 'negotiate' IPP Authentication method uses the HTTP “negotiate” authentication  
 136 scheme [RFC4559].

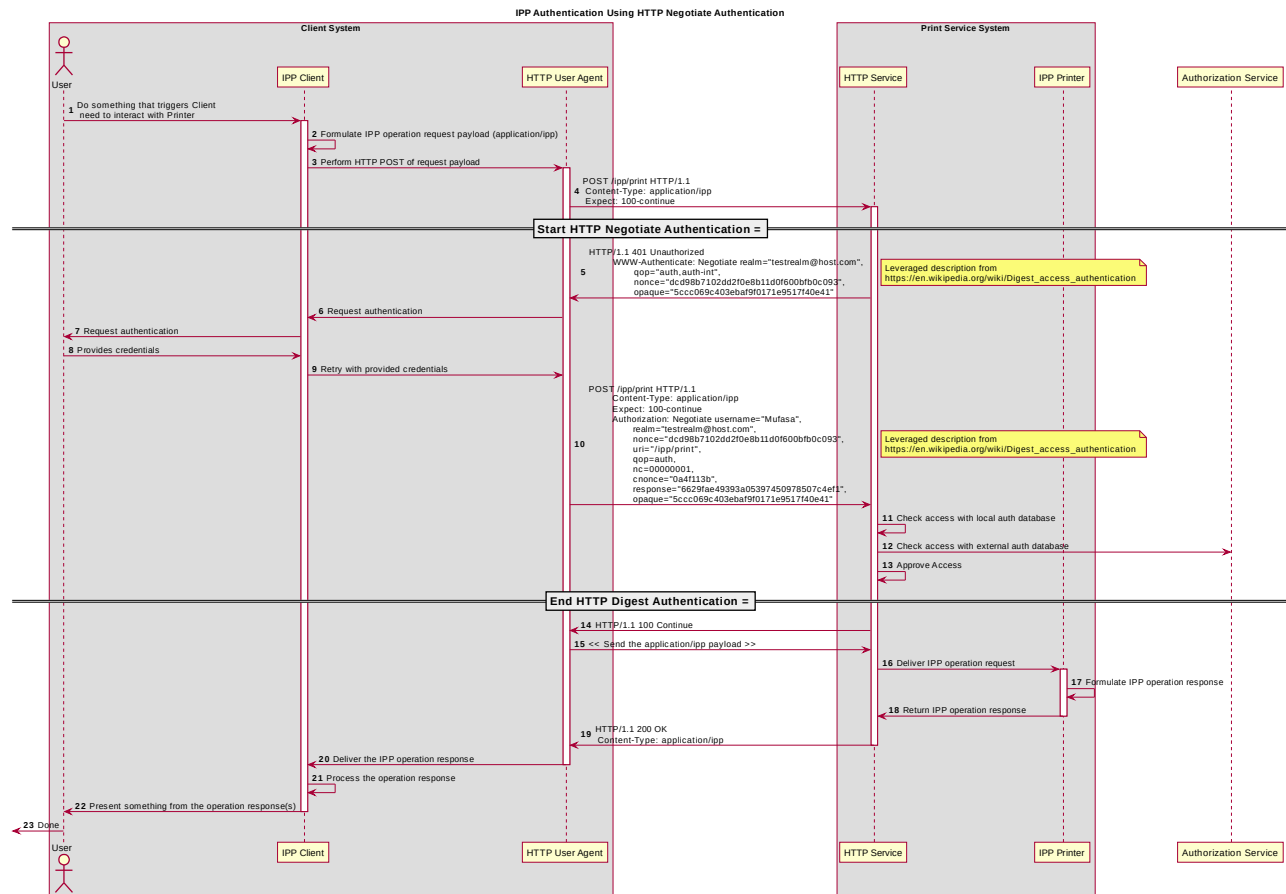


Figure 2.5 : Sequence diagram for the 'negotiate' IPP Authentication Method

137 **2.1.6 The 'oauth' IPP Authentication Method**

138 The 'oauth' IPP Authentication method uses the HTTP “oauth” authentication scheme  
139 [RFC5849].

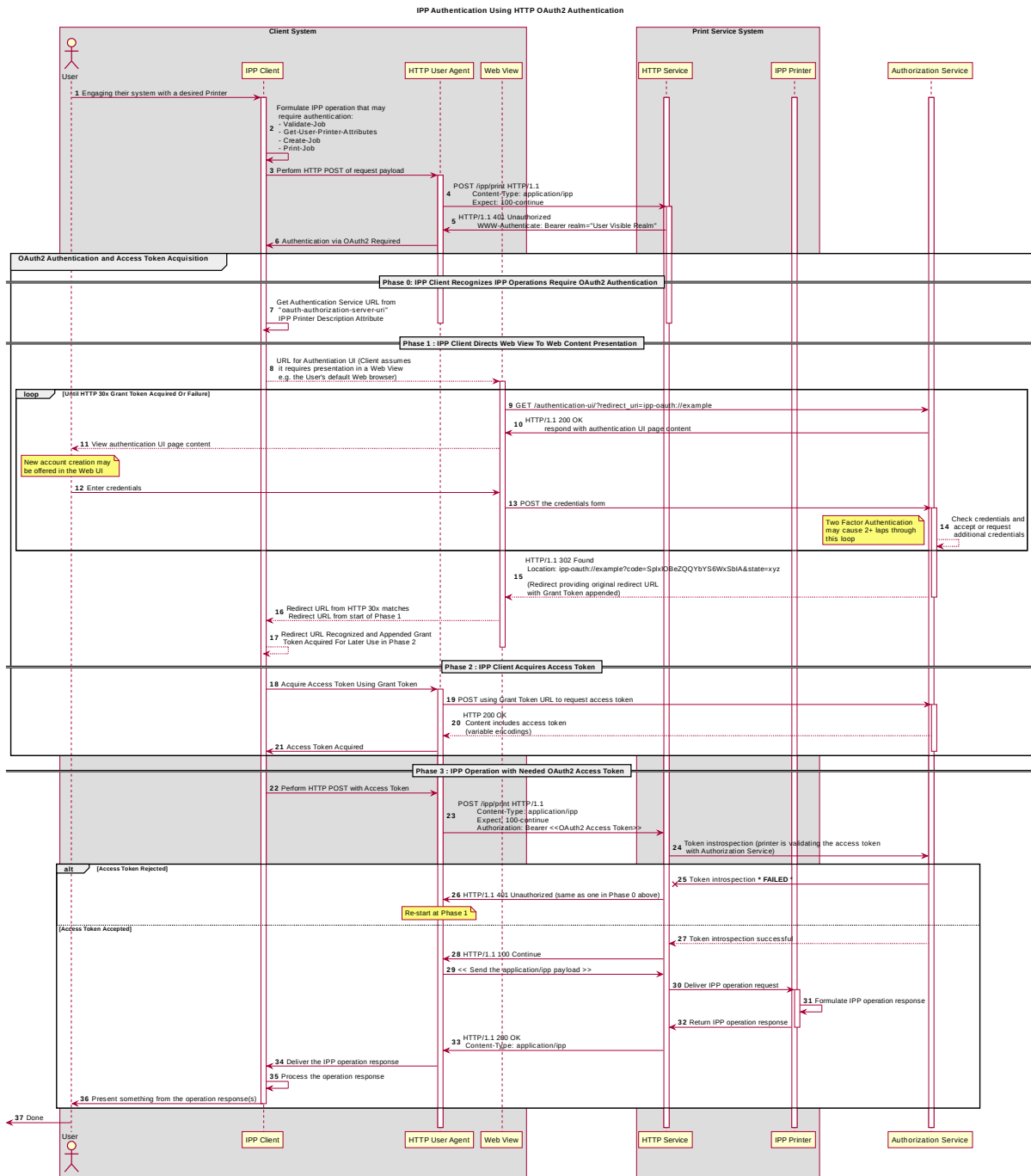
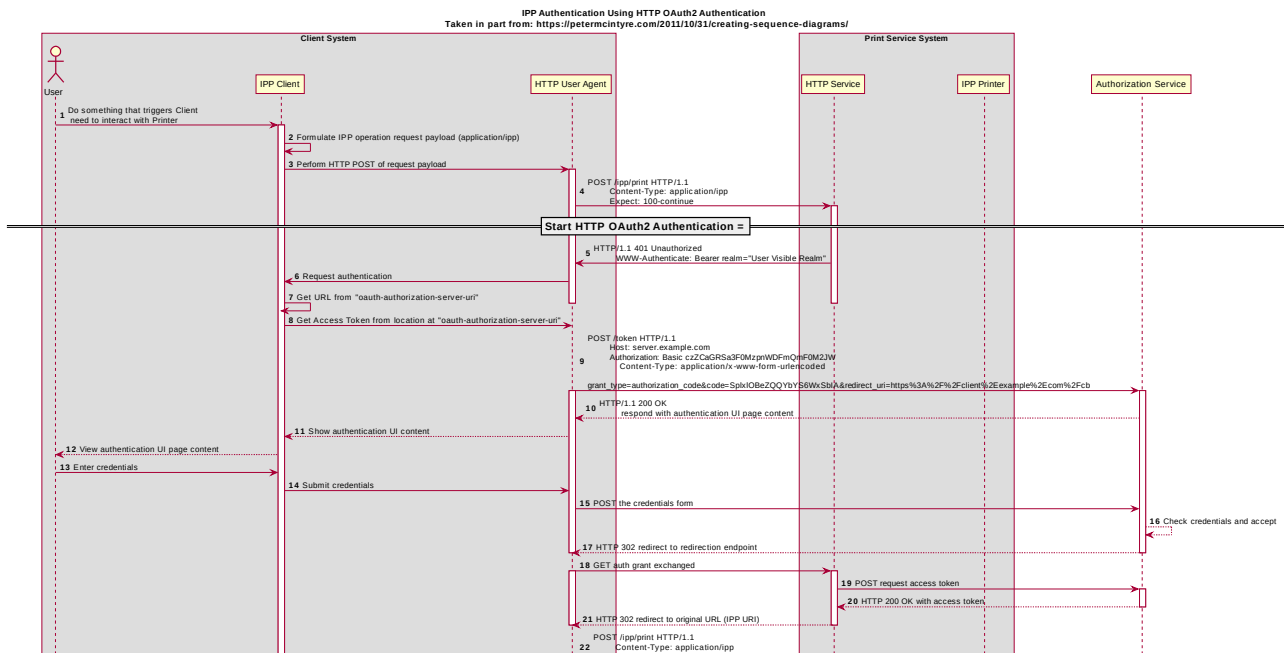


Figure 2.6 : Sequence diagram for the 'oauth' IPP Authentication Method



140 | Implementation Recommendations

## 141 | **2.2 Client Implementation Recommendations**

### 142 | **2.2.1 General Recommendations**

143 | A Client SHOULD as a general principle limit the number of additional windows presented  
144 | to the user during the course of an authentication workflow, to avoid causing a fragmented,  
145 | disruptive user experience.

### 146 | **2.2.2 OAuth2 Recommendations**

147 | A Client that supports OAuth2 authentication

148 |     ○ User experience considerations

149 |     ○ Information Disclosure

150 |         ▪ If the native app uses an embedded web view, then the native app might  
151 | have access to the web view (directly or indirectly). That means the native  
152 | app might have access to the controls and the information in that web view.  
153 | That may or may not be desirable...

154 |         ▪ RFC 7636 (PKCE) and RFC 8252 (native apps OAuth2 recommendations)  
155 | should be examined for further recommendations to be leveraged here and  
156 | calling out specific sections of those that pertain to the use cases that are  
157 | relevant to PWG / IPP (e.g. printer discovery UI, print dialog UI)

## 158 | **2.3 Printer Implementation Recommendations**

159 | TBD

160 | TBD?

161 | Internationalization Considerations

162 | For interoperability and basic support for multiple languages, conforming implementations  
163 | MUST support the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8)

164 [RFC3629] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for  
165 Network Interchange [RFC5198].

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

- 168 • Unicode Bidirectional Algorithm [UAX9] – left-to-right, right-to-left, and vertical
- 169 • Unicode Line Breaking Algorithm [UAX14] – character classes and wrapping
- 170 • Unicode Normalization Forms [UAX15] – especially NFC for [RFC5198]
- 171 • Unicode Text Segmentation [UAX29] – grapheme clusters, words, sentences
- 172 • Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization
- 173 • Unicode Collation Algorithm [UTS10] – sorting
- 174 • Unicode Locale Data Markup Language [UTS35] – locale databases

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

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

## 181 **3 Security Considerations**

182 Provide security considerations for this document.

### 183 **3.1 Human-readable Strings**

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

- 186 • Unicode Security Mechanisms [UTS39] – detecting and avoiding security attacks

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

- 189 • Unicode Security FAQ [UNISECFAQ] – common Unicode security issues

## 190 | **3.2 Client Security Considerations**

191 | An IPP Client SHOULD follow the recommendations below

- 192 | 1. A Client SHOULD securely store at rest any personally identifiable information (PII)  
193 | and authentication credentials such as passwords.
- 194 | 2. A Client SHOULD only respond to an authentication challenge over a secure  
195 | connection (TLS) [RFC8010][RFC8011] unless TLS is not supported over that  
196 | transport (e.g. IPP USB).
- 197 | 3. A Client SHOULD provide a means to allow the User to examine a Printer's  
198 | provided identity.
- 199 | 4. A Client SHOULD provide one or more means of notification when it is engaging  
200 | with a previously encountered Printer whose identity has changed.
- 201 | 5. Validating the Printer identity (am I talking to whom I think I'm talking to?) → look in  
202 | 8010 / 8011 for guidance or references to guidance

## 203 | **3.3 Printer Security Considerations**

204 | An IPP Printer SHOULD follow the recommendations below.

- 205 | 1. A Printer SHOULD securely store at rest any personally identifiable information (PII)  
206 | and authentication credentials such as passwords that are local to the Printer.
- 207 | 2. A Printer SHOULD only challenge a Client for authentication over a secure  
208 | connection (TLS) [RFC8010][RFC8011] unless TLS is not supported over that  
209 | transport (e.g. IPP USB).
- 210 | 3. Certificates
  - 211 | 1. What is an acceptable certificate?
  - 212 | 2. How long is a self-signed certificate expected to last?
  - 213 | 3. How long should a CA issued certificate last? (e.g. recent work on short lives CA  
214 | certificates...)
  - 215 | 4. Let's Encrypt and IPP (and OAuth2 or in general?)
- 216 | 4. Point to best practice documents

## 217 | 4 References

### 218 4.1 Normative References

- 219 [IANA-HTTP-AUTH] Hypertext Transfer Protocol (HTTP) Authentication Scheme Registry,  
220 Internet Assigned Numbers Authority,  
221 [https://www.iana.org/assignments/http-authschemes/http-](https://www.iana.org/assignments/http-authschemes/http-authschemes.xml)  
222 [authschemes.xml](https://www.iana.org/assignments/http-authschemes/http-authschemes.xml)
- 223 [ISO10646] "Information technology -- Universal Coded Character Set (UCS)",  
224 ISO/IEC 10646:2011
- 225 [PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP Version 2.0, 2.1,  
226 and 2.2", PWG 5100.12-2015, October 2015,  
227 <http://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.pdf>
- 228 [PWG5100.13] M. Sweet, I. McDonald, P. Zehler, "IPP: Job and Printer Extensions -  
229 Set 3 (JPS3)", PWG 5100.13-2012, July 2012,  
230 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-](http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf)  
231 [20120727-5100.13.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf)
- 232 [PWG5100.14] M. Sweet, I. McDonald, A. Mitchell, J. Hutchings, "IPP Everywhere",  
233 5100.14-2013, January 2013,  
234 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-](http://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-5100.14.pdf)  
235 [5100.14.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-5100.14.pdf)
- 236 [PWG5100.19] S. Kennedy, "IPP Implementor's Guide v2.0", PWG 5100.19-2015,  
237 August 2015, [http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-](http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-20150821-5100.19.pdf)  
238 [20150821-5100.19.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-20150821-5100.19.pdf)
- 239 [PWG5100.SYSTEM] I. McDonald, "IPP System Service v1.0", PWG 5100.SYSTEM, TBD,  
240 <http://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippssystem10-20170719.pdf>
- 241 [RFC2817] R. Khare, S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC  
242 2817, May 2000, <https://www.ietf.org/rfc/rfc2817.txt>
- 243 [RFC3629] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC  
244 3629, November 2003, <https://www.ietf.org/rfc/rfc3629.txt>
- 245 [RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange",  
246 RFC 5198, March 2008, <https://www.ietf.org/rfc/rfc5198.txt>
- 247 [RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1):  
248 Message Syntax and Routing", RFC 7230, June 2014,  
249 <https://www.ietf.org/rfc/rfc7230.txt>



- 250 [RFC7616] R. Shekh-Yusef, D. Ahrens, S. Bremer, “HTTP Digest Access  
251 Authentication”, RFC 7616, September 2015,  
252 <https://www.ietf.org/rfc/rfc7616.txt>
- 253 [RFC7617] J. Reschke, “The 'Basic' HTTP Authentication Scheme”, RFC 7617,  
254 September 2015, <https://www.ietf.org/rfc/rfc7617.txt>
- 255 [RFC8010] M. Sweet, I. McDonald, “Internet Printing Protocol/1.1: Encoding and  
256 Transport”, RFC 8010, January 2017,  
257 <https://www.ietf.org/rfc/rfc8010.txt>
- 258 [RFC8011] M. Sweet, I. McDonald, “Internet Printing Protocol/1.1: Model and  
259 Semantics”, RFC 8011, January 2017,  
260 <https://www.ietf.org/rfc/rfc8011.txt>
- 261 [UAX9] Unicode Consortium, “Unicode Bidirectional Algorithm”, UAX#9, May  
262 2016, <http://www.unicode.org/reports/tr9>
- 263 [UAX14] Unicode Consortium, “Unicode Line Breaking Algorithm”, UAX#14,  
264 June 2016, <http://www.unicode.org/reports/tr14>
- 265 [UAX15] Unicode Consortium, “Normalization Forms”, UAX#15, February 2016,  
266 <http://www.unicode.org/reports/tr15>
- 267 [UAX29] Unicode Consortium, “Unicode Text Segmentation”, UAX#29, June  
268 2016, <http://www.unicode.org/reports/tr29>
- 269 [UAX31] Unicode Consortium, “Unicode Identifier and Pattern Syntax”,  
270 UAX#31, May 2016, <http://www.unicode.org/reports/tr31>
- 271 [UNICODE] The Unicode Consortium, “Unicode® 10.0.0”, June 2017,  
272 <http://unicode.org/versions/Unicode10.0.0/>
- 273 [UTS10] Unicode Consortium, “Unicode Collation Algorithm”, UTS#10, May  
274 2016, <http://www.unicode.org/reports/tr10>
- 275 [UTS35] Unicode Consortium, “Unicode Locale Data Markup Language”,  
276 UTS#35, October 2016, <http://www.unicode.org/reports/tr35>
- 277 [UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, June  
278 2016, <http://www.unicode.org/reports/tr39>

## 279 4.2 Informative References

- 280 [UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2016,  
281 <http://www.unicode.org/faq/security.html>

- 282 [UTR17] Unicode Consortium “Unicode Character Encoding Model”, UTR#17,  
283 November 2008, <http://www.unicode.org/reports/tr17>
- 284 [UTR20] Unicode Consortium “Unicode in XML and other Markup Languages”,  
285 UTR#20, January 2013, <http://www.unicode.org/reports/tr20>
- 286 [UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23,  
287 May 2015, <http://www.unicode.org/reports/tr23>
- 288 [UTR33] Unicode Consortium “Unicode Conformance Model”, UTR#33,  
289 November 2008, <http://www.unicode.org/reports/tr33>

## 290 **5 Authors' Addresses**

291 Primary authors (using Address style):

292 Smith Kennedy  
293 11311 Chinden Blvd.  
294 Boise ID 83714  
295 smith.kennedy@hp.com

296 The authors would also like to thank the following individuals for their contributions to this  
297 whitepaper:

298 Mike Sweet – Apple Inc.  
299 Zapp Brannigan - Democratic Order of Planets

## 300 **6 Change History**

### 301 **6.1 December 5, 2017**

302 Updated as per feedback from the November 2017 PWG vF2F and subsequent work with  
303 IPP WG members on specific details

304 • Corrected OAuth2 sequence diagram to more correctly describe the sequence of  
305 operations and actors involved in an OAuth2 authenticated IPP Printer scenario.

306 • Added Implementation Recommendations that were revealed during the course of  
307 correcting the OAuth2 sequence diagram.

### 308 **6.2 August 3, 2017**

309 Initial revision.