



The Printer Working Group

January 23, 2018  
White Paper

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

3 Status: Interim

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-20180123.odt>

11 <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20171205.odt>

12 <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20180123.pdf>

13 <http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20171205.pdf>

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

15 Title: IPP Authentication Methods (*IPPAUTH*)

16 The material contained herein is not a license, either expressed or implied, to any IPR  
17 owned or controlled by any of the authors or developers of this material or the Printer  
18 Working Group. The material contained herein is provided on an "AS IS" basis and to the  
19 maximum extent permitted by applicable law, this material is provided AS IS AND WITH



## The Printer Working Group

20 ALL FAULTS, and the authors and developers of this material and the Printer Working  
21 Group and its members hereby disclaim all warranties and conditions, either expressed,  
22 implied or statutory, including, but not limited to, any (if any) implied warranties that the  
23 use of the information herein will not infringe any rights or any implied warranties of  
24 merchantability or fitness for a particular purpose.

25	<b>Table of Contents</b>	
26	1 Introduction.....	5
27	2 Terminology.....	5
28	2.1 Protocol Roles Terminology.....	5
29	2.2 Other Terms Used in This Document.....	5
30	2.3 Acronyms and Organizations.....	5
31	3 Overview of IPP Authentication Methods.....	6
32	3.1 Client Authentication Methods.....	6
33	3.1.1 The 'none' IPP Authentication Method.....	7
34	3.1.2 The 'requesting-user-name' IPP Authentication Method.....	8
35	3.1.3 The 'basic' IPP Authentication Method.....	9
36	3.1.4 The 'digest' IPP Authentication Method.....	10
37	3.1.5 The 'negotiate' IPP Authentication Method.....	11
38	3.1.6 The 'oauth' IPP Authentication Method.....	12
39	3.1.7 Transport Layer Security (TLS) Authentication.....	13
40	4 Implementation Recommendations.....	14
41	4.1 Client Implementation Recommendations.....	14
42	4.1.1 General Recommendations.....	14
43	4.1.2 Handling Authentication Failure.....	14
44	4.1.3 OAuth2 Recommendations.....	14
45	4.2 Printer Implementation Recommendations.....	14
46	4.2.1 Handling Authentication Failure.....	14
47	4.2.2 OAuth2 Recommendations.....	14
48	5 Internationalization Considerations.....	15
49	6 Security Considerations.....	15
50	6.1 Human-readable Strings.....	15
51	6.2 Client Security Considerations.....	16
52	6.3 Printer Security Considerations.....	16
53	7 References.....	17
54	7.1 Normative References.....	17
55	7.2 Informative References.....	19
56	8 Authors' Addresses.....	20
57	9 Change History.....	21
58	9.1 January 23, 2018.....	21
59	9.2 December 5, 2017.....	21
60	9.3 August 3, 2017.....	21

## 61 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

## 62 **1 Introduction**

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

## 70 **2 Terminology**

### 71 **2.1 Protocol Roles Terminology**

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

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

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

### 79 **2.2 Other Terms Used in This Document**

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

### 81 **2.3 Acronyms and Organizations**

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

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

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

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

86 | **3 Overview of IPP Authentication Methods**

## 87 | 4 ~~Rationale for IPP Authentication Methods~~

88 | **5 This white paper describes how various HTTP based**  
89 | **authentication systems integrate into IPP communications**  
90 | **between a Client and a Printer. Although the authentication**  
91 | **protocols themselves do not need to change to be integrated**  
92 | **into IPP communications, the IPP Client is not a Web browser,**  
93 | **so some considerations must be made by IPP Client**  
94 | **implementors. The “uri-authentication-supported” attribute**  
95 | **[RFC8011] Printer Description attribute indicates the**  
96 | **authentication systems supported by the Printer.**

### 97 | 5.1 Client Authentication Methods

98 | ~~An IPP Printer specifies its supported authentication methods via several IPP attributes.~~  
99 | ~~The “uri-authentication-supported” attribute [RFC8011] indicates the authentication method~~  
100 | ~~used for a corresponding URI in “printer-uri-supported” [RFC8011]. The “xri-authentication”~~  
101 | ~~member attribute of “printer-xri-supported” [RFC3380] specifies the same corresponding~~  
102 | ~~values, if the Printer implements the “printer-xri-supported” attribute.~~

103 | ~~A Printer uses the “authenticated identity” or the “most authenticated user” [RFC8011] to~~  
104 | ~~authorize access to capabilities such as operations, resources, and attributes. As in most~~  
105 | ~~other contexts, authentication is the process of establishing some level of trust that an~~  
106 | ~~entity is who or what they are claiming to be.~~

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

112 | Each of the authentication method keywords currently registered for “uri-authentication-  
113 | supported” is described below, with an accompanying sequence diagram for illustration  
114 | purposes, ~~as well as a discussion of each method's advantages and shortcomings.~~

115 **5.1.1 The 'none' IPP Authentication Method**

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

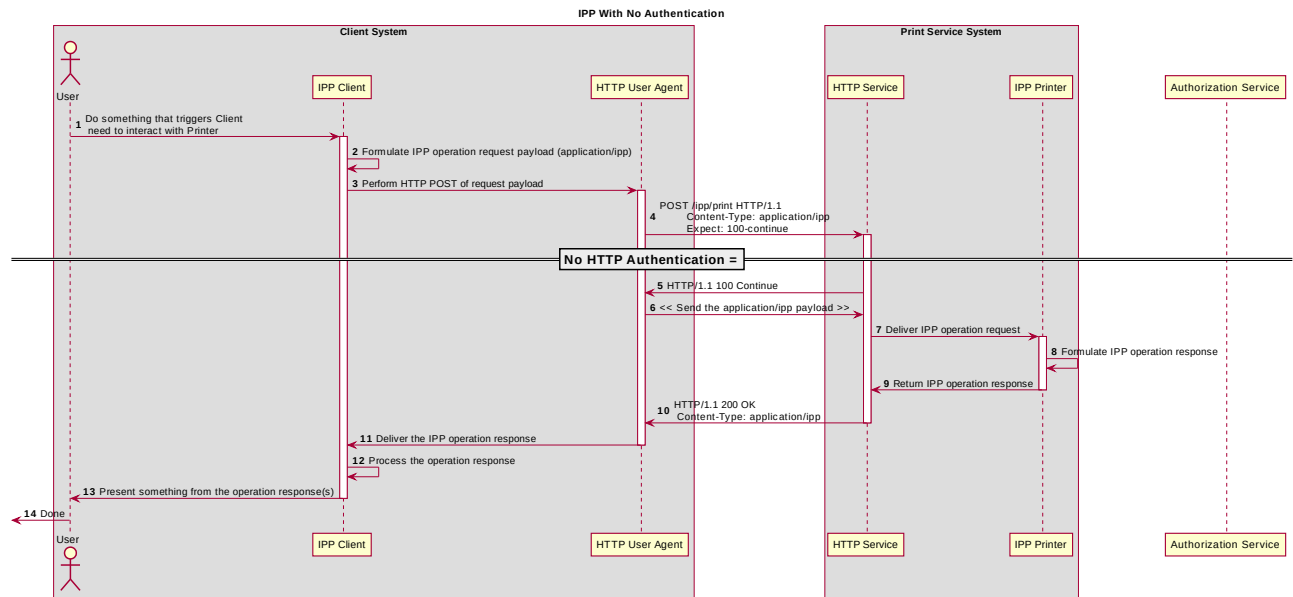


Figure 5.1: Sequence diagram for the 'none' IPP Authentication Method

120 This method is not recommended unless the Printer's operator has the objective of  
 121 providing an anonymous print service. In most cases, the Client SHOULD provide the  
 122 "requesting-user-name" operation attribute, as described in section 5.1.2.



123 **5.1.2 The 'requesting-user-name' IPP Authentication Method**

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

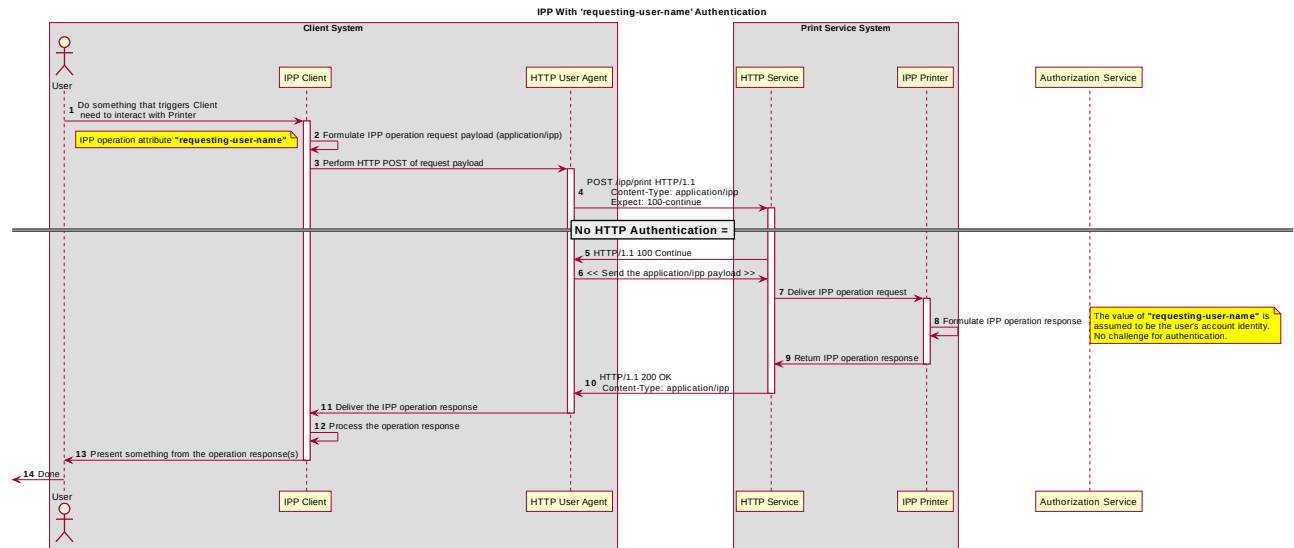


Figure 5.2: Sequence diagram for the 'requesting-user-name' IPP Authentication Method

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

130 **5.1.3 The 'basic' IPP Authentication Method**

131 | The 'basic' IPP Authentication Method uses HTTP **B**asic authentication scheme  
 132 | [RFC7617]. It is employed in IPP in much the same way that it is employed in conventional  
 133 | HTTP workflows using a Web browser. **W**hen the IPP Client encounters an HTTP 401  
 134 | Unauthorized response, it evaluates whether it supports the authentication method  
 135 | identified by the value of the “WWW-Authenticate” header in the response. In this case, if  
 136 | it supports 'basic', it will present UI asking the User to provide username and password  
 137 | credentials that may be used to authenticate with the HTTP Server providing access to the  
 138 | IPP Printer. If the HTTP Server successfully authenticates that set of credentials, then the  
 139 | IPP operation request is passed on to the IPP Printer, which responds as usual.

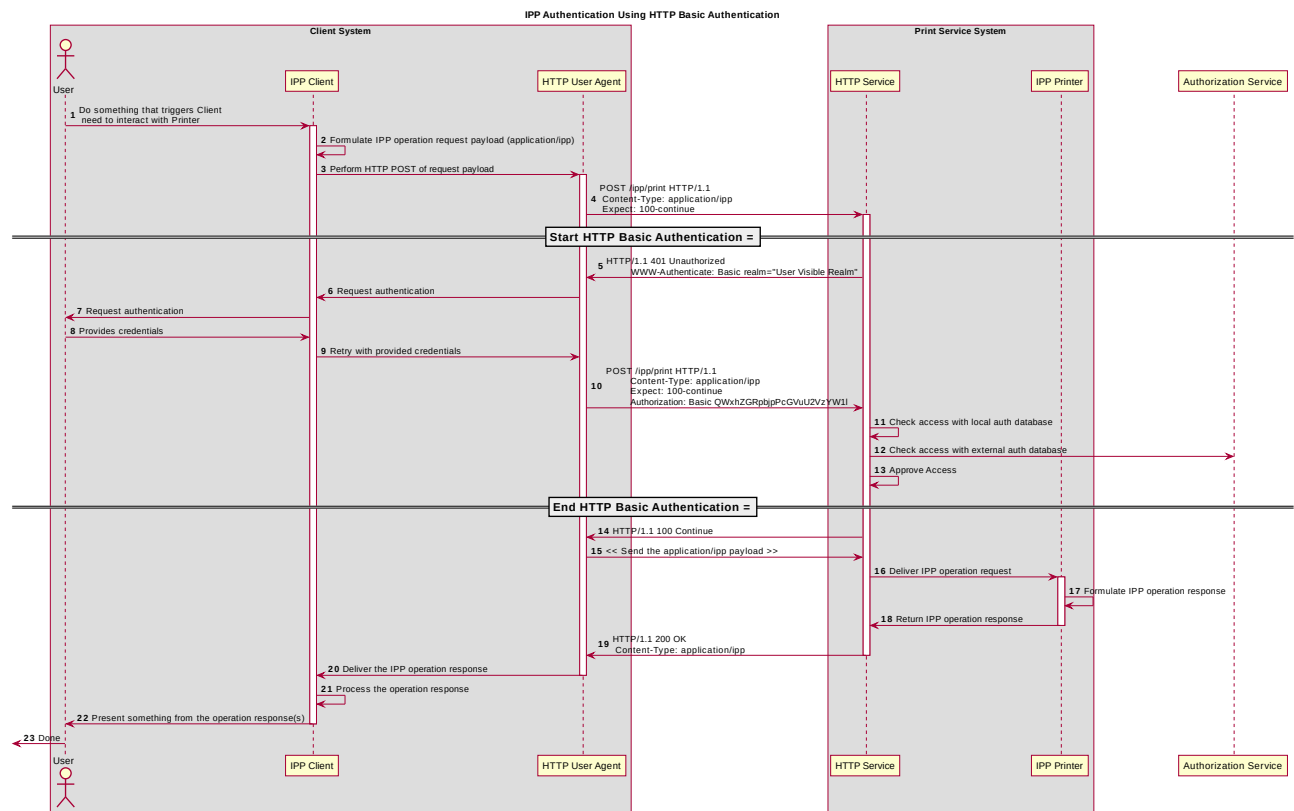


Figure 5.3 : Sequence diagram for the 'basic' IPP Authentication Method

140 **5.1.4 The 'digest' IPP Authentication Method**

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

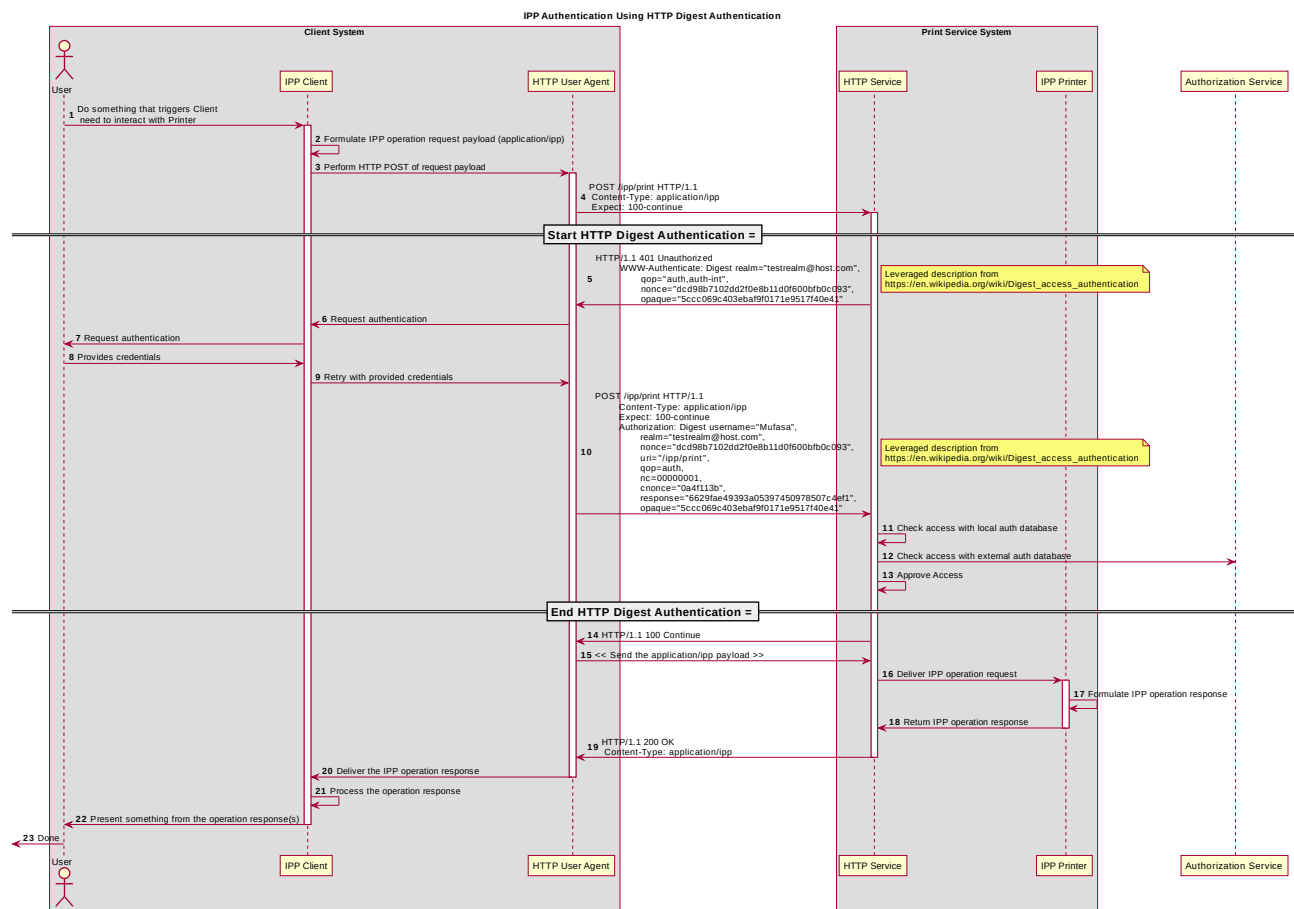


Figure 5.4 : Sequence diagram for the 'digest' IPP Authentication Method

150 **5.1.5 The 'negotiate' IPP Authentication Method**

151 The 'negotiate' IPP Authentication method uses the HTTP ~~N“negotiate”~~ authentication  
 152 scheme [RFC4559][RFC4559].

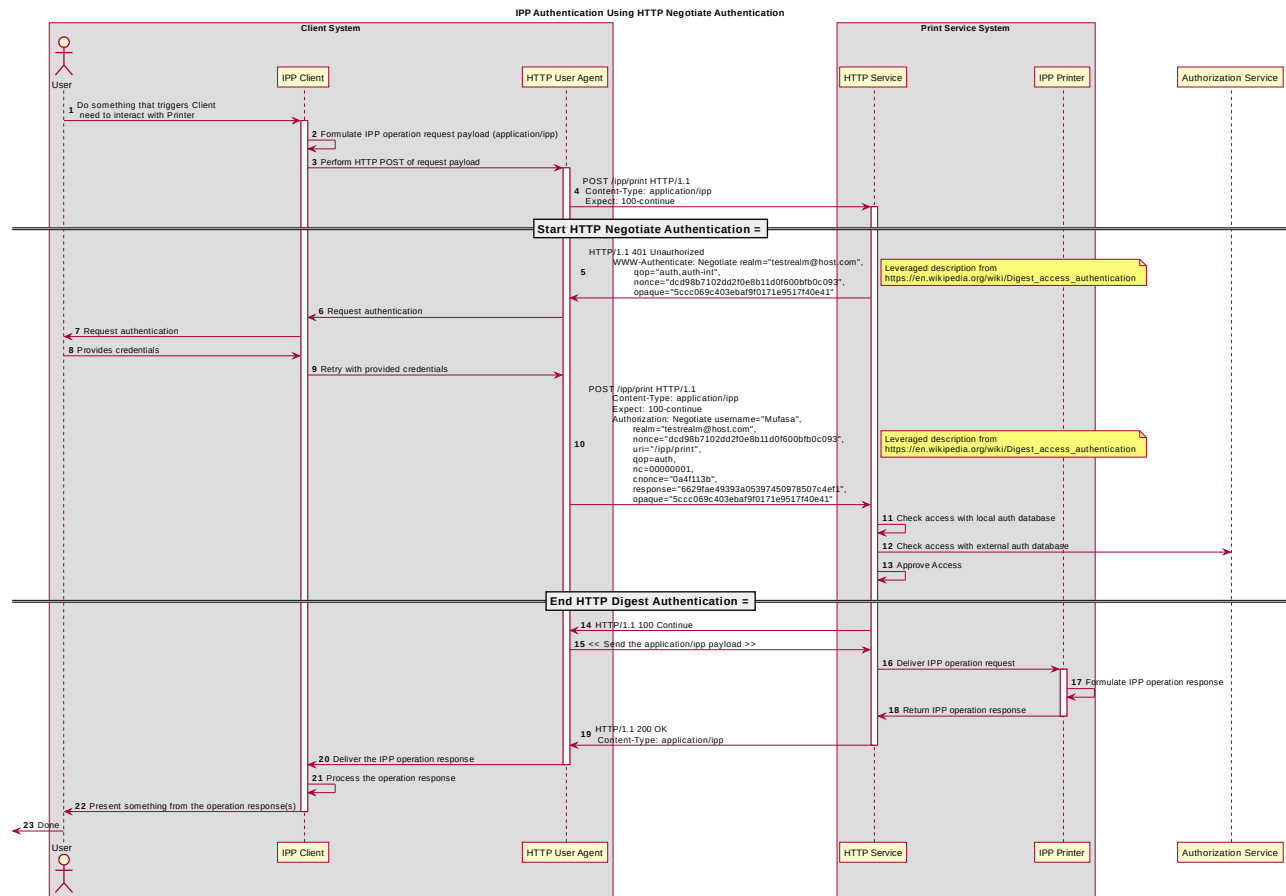


Figure 5.5 : Sequence diagram for the 'negotiate' IPP Authentication Method

153 **5.1.6 The 'oauth' IPP Authentication Method**

154 The 'oauth' IPP Authentication method uses the OAuth2 authentication scheme  
 155 [RFC6749] and the OAuth2 Bearer Token [RFC6750].

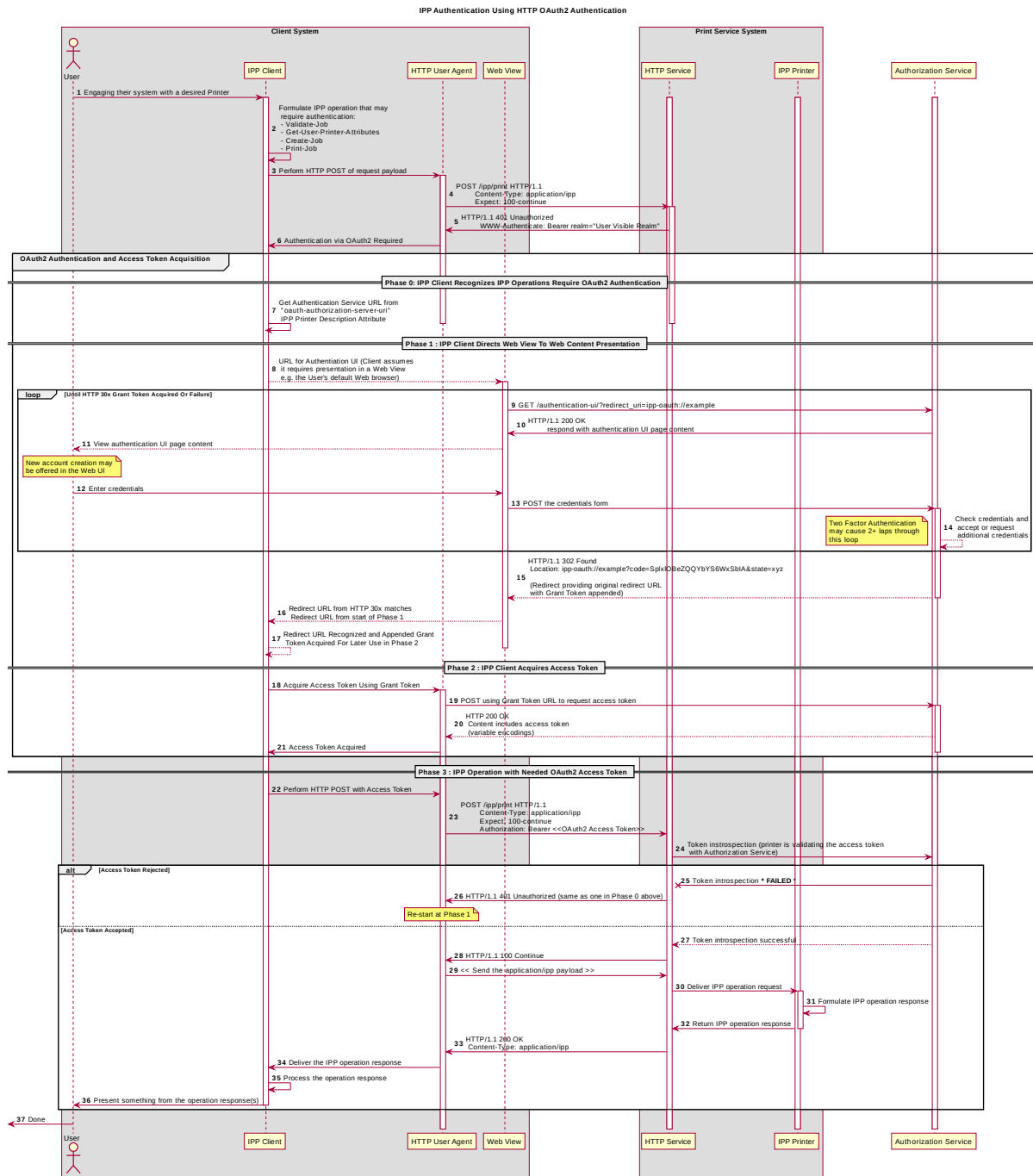


Figure 5.6 : Sequence diagram for the 'oauth' IPP Authentication Method

156 | [Transport Layer Security \(TLS\) Authentication](#)

157 | **6 Implementation Recommendations**

158 | **7 While Transport Layer Security (TLS) [RFC5246] is the**  
159 | **commonly used protocol for encrypting an IPP connection**  
160 | **[RFC8010][RFC8011], the authentication facilities of TLS are**  
161 | **commonly employed in scenarios where client authentication**  
162 | **is provided via a client certificate.**

## 163 | **8 Implementation Recommendations**

### 164 | **8.1 Client Implementation Recommendations**

#### 165 | **8.1.1 General Recommendations**

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

#### 169 | **8.1.2 Handling Authentication Failure**

170 | If a Printer rejects authentication credentials provided by a Client in response to an  
171 | authentication challenge following an IPP operation request, the Printer MAY return an IPP  
172 | operation response. If it does not, and the connection is left open, it SHOULD treat the  
173 | connection the same way it handles a stalled connection, and close it after a reasonably  
174 | brief amount of time.

#### 175 | **8.1.3 OAuth2 Recommendations**

176 | A Client that supports OAuth2 authentication SHOULD incorporate the following  
177 | considerations into their implementation:

178 | User experience considerations

179 | The OAuth2 authorization service may have a complicated user presentation. If possible,  
180 | select a presentation alternative that is the least complicated.

181 |       ○ Information Disclosure

182 | ~~8.1.4 If the native app uses an embedded web view, then the native app might have~~  
183 | ~~access to the web view (directly or indirectly). That means the native app might have~~  
184 | ~~access to the controls and the information in that web view. That may or may not be~~  
185 | ~~desirable...~~

186 | ~~8.1.5 RFC 7636 (PKCE) and RFC 8252 (native apps OAuth2 recommendations) should~~  
187 | ~~be examined for further recommendations to be leveraged here and calling out specific~~  
188 | ~~sections of those that pertain to the use cases that are relevant to PWG / IPP (e.g. printer~~  
189 | ~~discovery UI, print dialog UI)~~

190 |       ○ Printer Implementation Recommendations



### 191 | **8.1.6 Handling Authentication Failure**

192 | If a Printer receives an IPP operation request, challenges the Client for authentication, and  
193 | the authentication process fails, the Printer SHOULD send an appropriate IPP operation  
194 | response indicating the cause of the failure.

### 195 | **8.1.7 OAuth2 Recommendations**

196 | A Printer that incorporates OAuth2 authentication into its solution SHOULD direct a Client  
197 | to an authentication page that facilitates an appropriate presentation on even limited Client  
198 | systems such as smart phones.

199 | **TBD**

### 200 | Internationalization Considerations

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

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

- 207 | • Unicode Bidirectional Algorithm [UAX9] – left-to-right, right-to-left, and vertical
- 208 | • Unicode Line Breaking Algorithm [UAX14] – character classes and wrapping
- 209 | • Unicode Normalization Forms [UAX15] – especially NFC for [RFC5198]
- 210 | • Unicode Text Segmentation [UAX29] – grapheme clusters, words, sentences
- 211 | • Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization
- 212 | • Unicode Collation Algorithm [UTS10] – sorting
- 213 | • Unicode Locale Data Markup Language [UTS35] – locale databases

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

- 216 | • Unicode Character Encoding Model [UTR17] – multi-layer character model
- 217 | • Unicode in XML and other Markup Languages [UTR20] – XML usage
- 218 | • Unicode Character Property Model [UTR23] – character properties

- 219 • Unicode Conformance Model [UTR33] – Unicode conformance basis

## 220 | **9 Security Considerations**

221 | ~~Provide security considerations for this document.~~

222 | Human-readable Strings

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

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

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


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

### 229 | **9.1 Client Security Considerations**

230 An IPP Client SHOULD follow the recommendations below

231 1. A Client SHOULD securely store at rest any personally identifiable information (PII)  
232 and authentication credentials such as passwords.

233 2. A Client SHOULD only respond to an authentication challenge over a secure  
234 connection (TLS) [RFC8010][RFC8011] unless TLS is not supported over that  
235 transport (e.g. IPP USB).

236 3. A Client SHOULD validate the identity of the Printer by whatever means are  
237 available for that connection type. If the connection is secured via TLS [RFC8010],  
238 the server certificate SHOULD be validated and matched to the originating host and  
239 against the host name or IP addresses from the IPP URI for the target Printer. If the  
240 connection is not secured via TLS, other means may be needed. 

241 4. A Client SHOULD provide a means to allow the User to examine a Printer's  
242 provided identity.

243 5. A Client SHOULD provide one or more means of notification when it is engaging  
244 with a previously encountered Printer whose identity has changed.

245 6. OAuth2 Considerations

- 246 | 1. The recommendations in “Proof Key for Code Exchange by OAuth Public  
247 | Clients” [RFC7636] SHOULD be followed, since the threats described therein  
248 | has been observed in practice.
- 249 | 2. The recommendations in “OAuth 2 for Native Apps” [RFC8252] should be  
250 | followed if the print system provides its own user interface presentation and  
251 | controls for handling the OAuth2 authentication steps, to mitigate the risks  
252 | described therein.
- 253 | 1. ~~Validating the Printer identity (am I talking to whom I think I'm talking to?) → look in~~  
254 | ~~8010 / 8011 for guidance or references to guidance~~

255 | 2. Printer Security Considerations

256 | An IPP Printer SHOULD follow the recommendations below.

- 257 | 1. A Printer SHOULD securely store at rest any personally identifiable information (PII)  
258 | and authentication credentials such as passwords that are local to the Printer.
- 259 | 2. A Printer SHOULD only challenge a Client for authentication over a secure  
260 | connection (TLS) [RFC8010][RFC8011] unless TLS is not supported over that  
261 | transport (e.g. IPP USB).-
- 262 | 3. **Certificates**
- 263 | 1. **What is an acceptable certificate?**
- 264 | 2. **How long is a self-signed certificate expected to last?**
- 265 | 3. **How long should a CA issued certificate last? (e.g. recent work on short lives CA**  
266 | **certificates...)**
- 267 | 4. **Let's Encrypt and IPP (and OAuth2 or in general?)**
- 268 | 4. **Point to best practice documents**

269 | **10 References**

270 | **10.1 Normative References**

- 271 | [IANA-HTTP-AUTH] Hypertext Transfer Protocol (HTTP) Authentication Scheme Registry,  
272 | Internet Assigned Numbers Authority,  
273 | [https://www.iana.org/assignments/http-authschemes/http-](https://www.iana.org/assignments/http-authschemes/http-authschemes.xml)  
274 | [authschemes.xml](https://www.iana.org/assignments/http-authschemes/http-authschemes.xml)
- 275 | [ISO10646] "Information technology -- Universal Coded Character Set (UCS)",  
276 | ISO/IEC 10646:2011

- 277 [PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP Version 2.0, 2.1,  
278 and 2.2", PWG 5100.12-2015, October 2015,  
279 <http://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.pdf>
- 280 [PWG5100.13] M. Sweet, I. McDonald, P. Zehler, "IPP: Job and Printer Extensions -  
281 Set 3 (JPS3)", PWG 5100.13-2012, July 2012,  
282 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-  
283 20120727-5100.13.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf)
- 284 [PWG5100.14] M. Sweet, I. McDonald, A. Mitchell, J. Hutchings, "IPP Everywhere",  
285 5100.14-2013, January 2013,  
286 [http://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-  
287 5100.14.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-5100.14.pdf)
- 288 [PWG5100.19] S. Kennedy, "IPP Implementor's Guide v2.0", PWG 5100.19-2015,  
289 August 2015, [http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-  
290 20150821-5100.19.pdf](http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-20150821-5100.19.pdf)
- 291 [PWG5100.SYSTEM] I. McDonald, "IPP System Service v1.0", PWG 5100.SYSTEM, TBD,  
292 <http://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippssystem10-20170719.pdf>
- 293 [RFC2817] R. Khare, S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC  
294 2817, May 2000, <https://www.ietf.org/rfc/rfc2817.txt>
- 295 ~~[RFC3380] T. Hastings, R. Herriot, C. Kugler, H. Lewis, "Internet Printing Protocol  
296 (IPP): Job and Printer Set Operations", RFC 3380, September 2002,  
297 <https://www.ietf.org/rfc/rfc3380.txt>~~
- 298 [RFC3629] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC  
299 3629, November 2003, <https://www.ietf.org/rfc/rfc3629.txt>
- 300 ~~[RFC4559] K. Jaganathan, L. Zhu, J. Brezak, "SPNEGO-based Kerberos and  
301 NTLM HTTP Authentication in Microsoft Windows", RFC 4559, June  
302 2006, <https://www.ietf.org/rfc/rfc4559.txt>~~
- 303 [RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange",  
304 RFC 5198, March 2008, <https://www.ietf.org/rfc/rfc5198.txt>
- 305 ~~[RFC5246] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol  
306 Version 1.2", August 2008, <https://www.ietf.org/rfc/rfc5246.txt>~~
- 307 ~~[RFC6749] D. Hardt, Ed., "The OAuth 2.0 Authorization Framework", RFC 6749,  
308 October 2012, <https://www.ietf.org/rfc/rfc6749.txt>~~
- 309 ~~[RFC6750] M. Jones, D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer  
310 Token Usage", RFC 6750, October 2012,  
311 <https://www.ietf.org/rfc/rfc6750.txt>~~

- 312 | [RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1):  
313 Message Syntax and Routing", RFC 7230, June 2014,  
314 <https://www.ietf.org/rfc/rfc7230.txt>
- 315 | [RFC7616] R. Shekh-Yusef, D. Ahrens, S. Bremer, "HTTP Digest Access  
316 Authentication", RFC 7616, September 2015,  
317 <https://www.ietf.org/rfc/rfc7616.txt>
- 318 | [RFC7617] J. Reschke, "The 'Basic' HTTP Authentication Scheme", RFC 7617,  
319 September 2015, <https://www.ietf.org/rfc/rfc7617.txt>
- 320 | ~~[RFC7636] N. Sakimura, Ed., J. Bradley, N. Agarwal, "Proof Key for Code  
321 Exchange by OAuth Public Clients", RFC 7636, September 2015,  
322 <https://www.ietf.org/rfc/rfc7636.txt>~~
- 323 | [RFC8010] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1: Encoding and  
324 Transport", RFC 8010, January 2017,  
325 <https://www.ietf.org/rfc/rfc8010.txt>
- 326 | [RFC8011] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1: Model and  
327 Semantics", RFC 8011, January 2017,  
328 <https://www.ietf.org/rfc/rfc8011.txt>
- 329 | ~~[RFC8252] W. Denniss, J. Bradley, "OAuth 2.0 for Native Apps", RFC 8252,  
330 October 2017, <https://www.ietf.org/rfc/rfc8252.txt>~~
- 331 | [UAX9] Unicode Consortium, "Unicode Bidirectional Algorithm", UAX#9, May  
332 2016, <http://www.unicode.org/reports/tr9>
- 333 | [UAX14] Unicode Consortium, "Unicode Line Breaking Algorithm", UAX#14,  
334 June 2016, <http://www.unicode.org/reports/tr14>
- 335 | [UAX15] Unicode Consortium, "Normalization Forms", UAX#15, February 2016,  
336 <http://www.unicode.org/reports/tr15>
- 337 | [UAX29] Unicode Consortium, "Unicode Text Segmentation", UAX#29, June  
338 2016, <http://www.unicode.org/reports/tr29>
- 339 | [UAX31] Unicode Consortium, "Unicode Identifier and Pattern Syntax",  
340 UAX#31, May 2016, <http://www.unicode.org/reports/tr31>
- 341 | [UNICODE] The Unicode Consortium, "Unicode® 10.0.0", June 2017,  
342 <http://unicode.org/versions/Unicode10.0.0/>
- 343 | [UTS10] Unicode Consortium, "Unicode Collation Algorithm", UTS#10, May  
344 2016, <http://www.unicode.org/reports/tr10>

- 345 [UTS35] Unicode Consortium, “Unicode Locale Data Markup Language”,  
346 UTS#35, October 2016, <http://www.unicode.org/reports/tr35>
- 347 [UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, June  
348 2016, <http://www.unicode.org/reports/tr39>

## 349 **10.2 Informative References**

- 350 [UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2016,  
351 <http://www.unicode.org/faq/security.html>
- 352 [UTR17] Unicode Consortium “Unicode Character Encoding Model”, UTR#17,  
353 November 2008, <http://www.unicode.org/reports/tr17>
- 354 [UTR20] Unicode Consortium “Unicode in XML and other Markup Languages”,  
355 UTR#20, January 2013, <http://www.unicode.org/reports/tr20>
- 356 [UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23,  
357 May 2015, <http://www.unicode.org/reports/tr23>
- 358 [UTR33] Unicode Consortium “Unicode Conformance Model”, UTR#33,  
359 November 2008, <http://www.unicode.org/reports/tr33>

## 360 **11 Authors' Addresses**

361 Primary authors (using Address style):

362 Smith Kennedy  
363 [HP Inc.](#)  
364 11311 Chinden Blvd.  
365 Boise ID 83714  
366 smith.kennedy@hp.com

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

369 Mike Sweet – Apple Inc.  
370 Zapp Brannigan - Democratic Order of Planets

## 371 | **12 Change History**

### 372 | **12.1 January 23, 2018**

373 | Updated as per email feedback and discussion:

- 374 | • Fixed some editorial issues with naming HTTP Basic, HTTP Digest, and HTTP  
375 | Negotiate, and some names of sections.
- 376 | • Added mention of “printer-xri-supported”.
- 377 | • Added additional references.
- 378 | • Added additional sub-sections to capture Client and Printer recommendations for  
379 | appropriate behavior when authentication is unsuccessful since the negative cases  
380 | can vary widely.

### 381 | **12.2 December 5, 2017**

382 | Updated as per feedback from the November 2017 PWG vF2F and subsequent work with  
383 | IPP WG members on specific details:

- 384 | • Corrected OAuth2 sequence diagram to more correctly describe the sequence of  
385 | operations and actors involved in an OAuth2 authenticated IPP Printer scenario.
- 386 | • Added Implementation Recommendations that were revealed during the course of  
387 | correcting the OAuth2 sequence diagram.

### 388 | **12.3 August 3, 2017**

389 | Initial revision.