



April 30, 2018
White Paper

The Printer Working Group

IPP Authentication Methods (IPPAUTH)

Status: Interim

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

This document is a White Paper. For [thea](#) definition of a "White Paper", see: <http://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf>

<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-ippauth-20180430.odt>

<http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20180430.pdf>[20180123.odt](http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-ippauth-20180123.odt)

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

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

Title: IPP Authentication Methods (*IPPAUTH*)

The material contained herein is not a license, either expressed or implied, to any IPR owned or controlled by any of the authors or developers of this material or the Printer Working Group. The material contained herein is provided on an "AS IS" basis and to the maximum

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

extent permitted by applicable law, this material is provided AS IS AND WITH ALL FAULTS, and the authors and developers of this material and the Printer Working Group and its members hereby disclaim all warranties and conditions, either expressed, implied or statutory, including, but not limited to, any (if any) implied warranties that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

Table of Contents

1.Introduction.....	5
2.Terminology.....	5
2.1.Protocol Roles Terminology.....	5
2.2.Other Terms Used in This Document.....	5
2.3.Acronyms and Organizations.....	5
3.Overview of IPP Authentication Methods.....	6
3.1.Client Authentication Methods.....	6
3.1.1.The 'none' IPP Authentication Method.....	7
3.1.2.The 'requesting-user-name' IPP Authentication Method.....	8
3.1.3.The 'basic' IPP Authentication Method.....	9
3.1.4.The 'digest' IPP Authentication Method.....	10
3.1.5.The 'negotiate' IPP Authentication Method.....	11
3.1.6.The 'oauth' IPP Authentication Method.....	12
3.1.7.X.509 Certificate Authentication Via TLS.....	14
4.Implementation Recommendations.....	15
4.1.Client Implementation Recommendations.....	15
4.1.1.General Recommendations.....	15
4.1.2.Handling Authentication Failure.....	15
4.1.3.OAuth2 Recommendations.....	15
4.2.Printer Implementation Recommendations.....	15
4.2.1.Handling Authentication Failure.....	15
4.2.2.OAuth2 Recommendations.....	15
5.Internationalization Considerations.....	16
6.Security Considerations.....	16
6.1.Human-readable Strings.....	16
6.2.Client Security Considerations.....	17
6.3.Printer Security Considerations.....	17
7.References.....	18
7.1.Normative References.....	18
7.2.Informative References.....	21
8.Authors' Addresses.....	21
9.Change History.....	22
9.1.April 30, 2018.....	22
9.2.January 23, 2018.....	22
9.3.December 5, 2017.....	22
9.4.August 3, 2017.....	23

List of Figures

Figure 1: Sequence diagram for the 'none' IPP Authentication Method.....	7
--	---

Figure 2: Sequence diagram for the 'requesting-user-name' IPP Authentication Method....8
Figure 3: Sequence diagram for the 'basic' IPP Authentication Method.....9
Figure 4: Sequence diagram for the 'digest' IPP Authentication Method.....10
Figure 5: Sequence diagram for the 'negotiate' IPP Authentication Method.....11
Figure 6: Sequence diagram for the 'oauth' IPP Authentication Method.....12
Figure 7: Sequence diagram for the hybrid 'oauth' / 'digest' IPP Authentication Method...13
Figure 8: Sequence diagram for X.509 Certificate Authentication Via TLS.....14

List of Tables

1. Introduction

The Internet Printing Protocol (hereafter, IPP) uses HTTP as its underlying transport [RFC8010]. When an IPP Printer is configured to limit access to its services to only those Clients operated by an authorized User, it challenges the User's Client by employing one of the IPP-employs various different HTTP authentication methods. But ~~since~~ an IPP Client isn't usually a typical HTTP User Agent (e.g. it isn't a commonly used Web browser). This white paper examines the common HTTP authentication methods employed today and outlines, ~~some~~ limits, constraints and conventions that ought to be considered when implementing support for one of these different HTTP authentication methods to ensure a high quality printing user experience. -

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/>

Overview of IPP Authentication Methods

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

2.4. Client Authentication Methods

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

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

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

2.4.1. The 'none' IPP Authentication Method

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

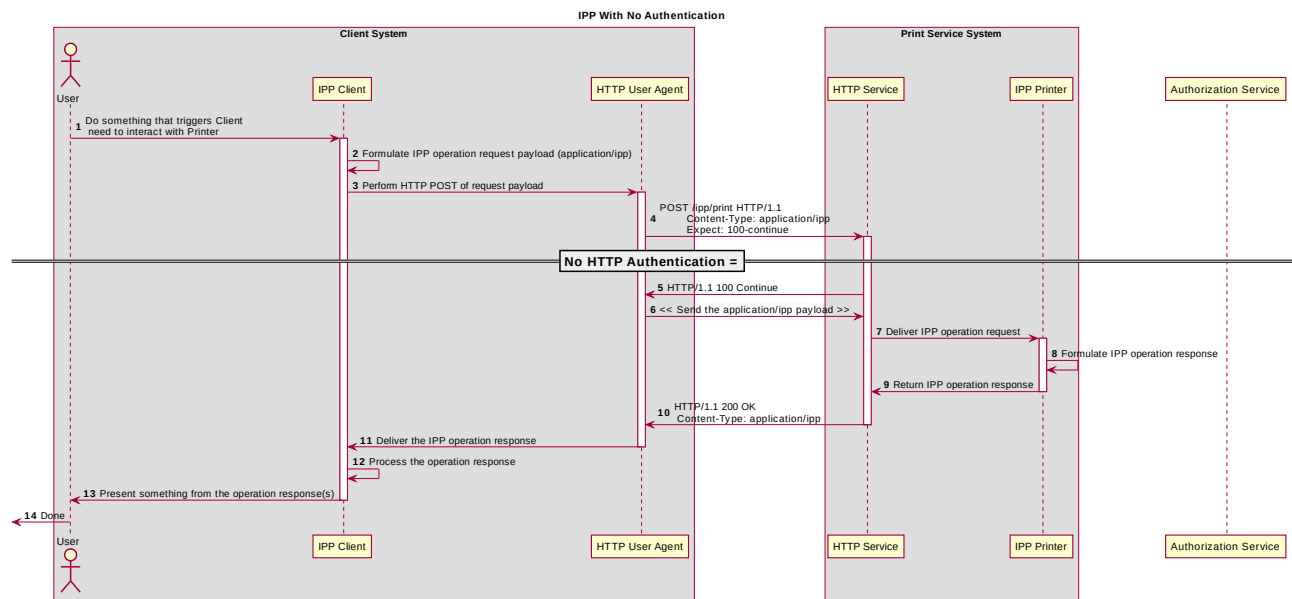


Figure 1: Sequence diagram for the 'none' IPP Authentication Method

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

~~This method is not recommended unless the Printer's operator has the objective of providing an anonymous print service. In most cases, the Client SHOULD provide the "requesting-user-name" operation attribute, as described in section~~ Error: Reference source not found.

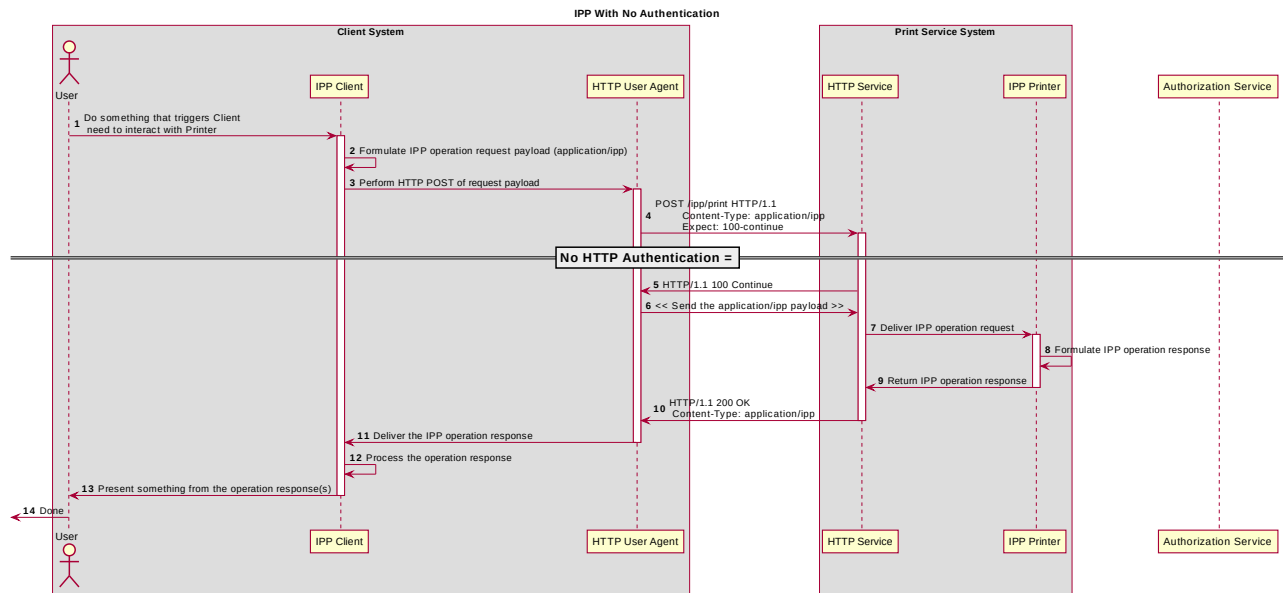


Figure 2: Sequence diagram for the 'none' IPP Authentication Method

The 'requesting-user-name' IPP Authentication Method

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

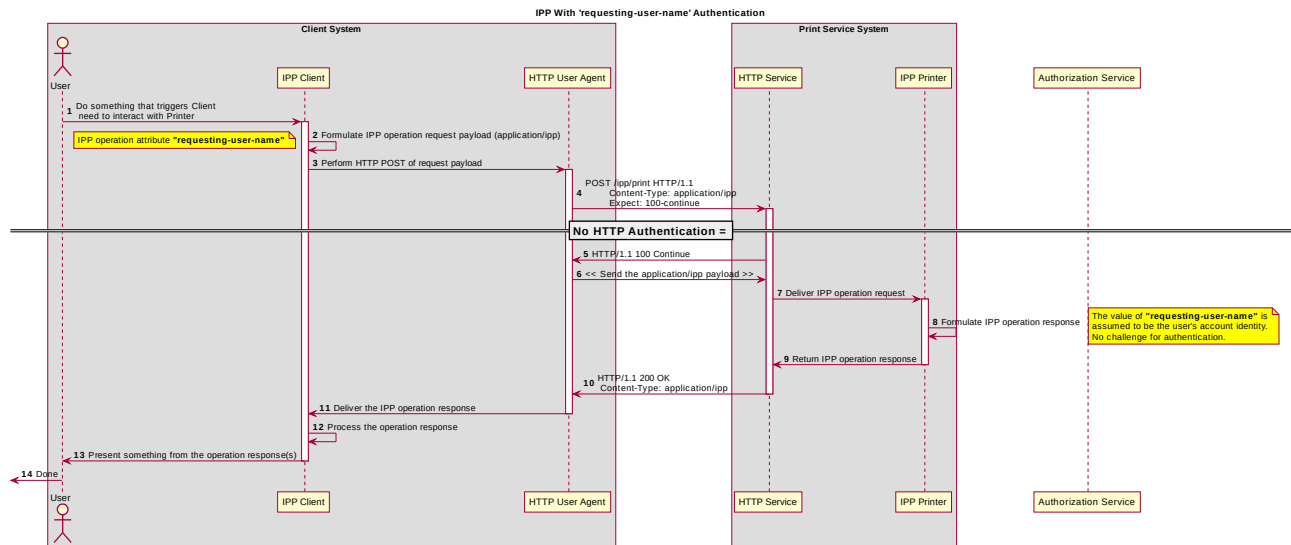


Figure 3: Sequence diagram for the 'requesting-user-name' IPP Authentication Method

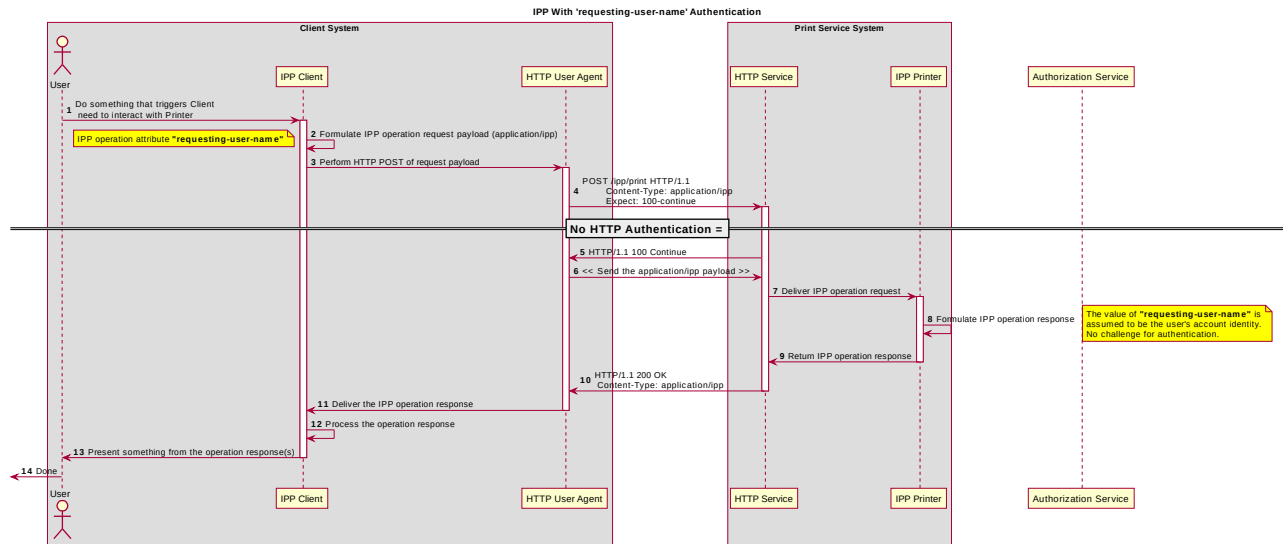


Figure 4: Sequence diagram for the 'requesting-user-name' IPP Authentication Method

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

2.4.2. The 'basic' IPP Authentication Method

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

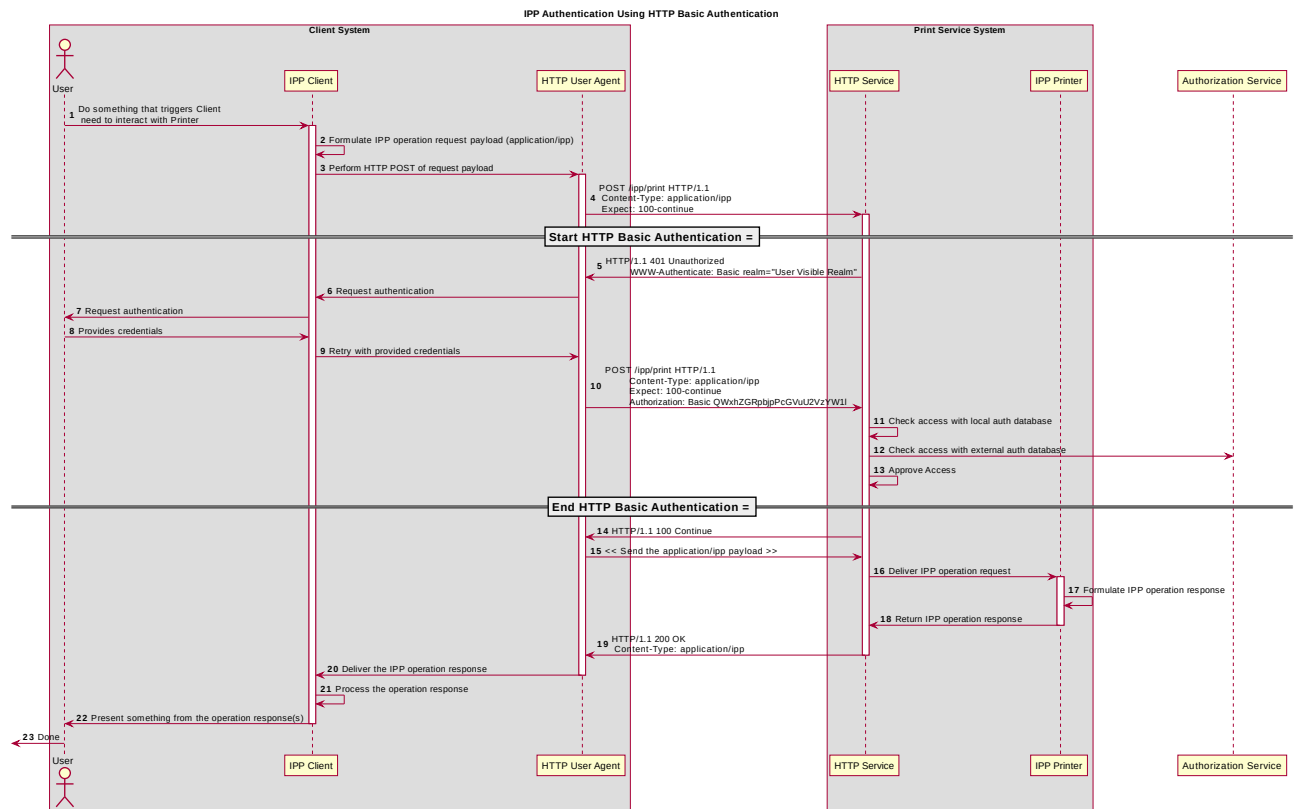


Figure 5: Sequence diagram for the 'basic' IPP Authentication Method

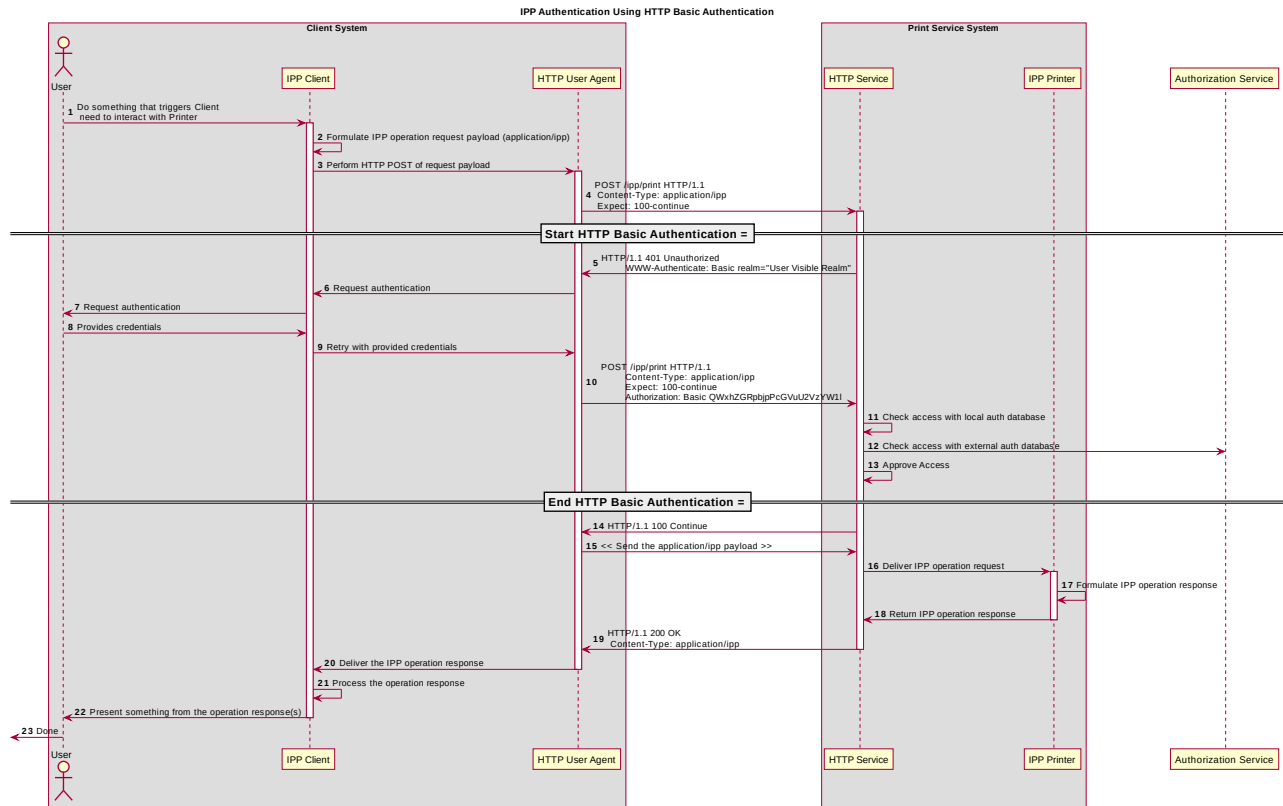
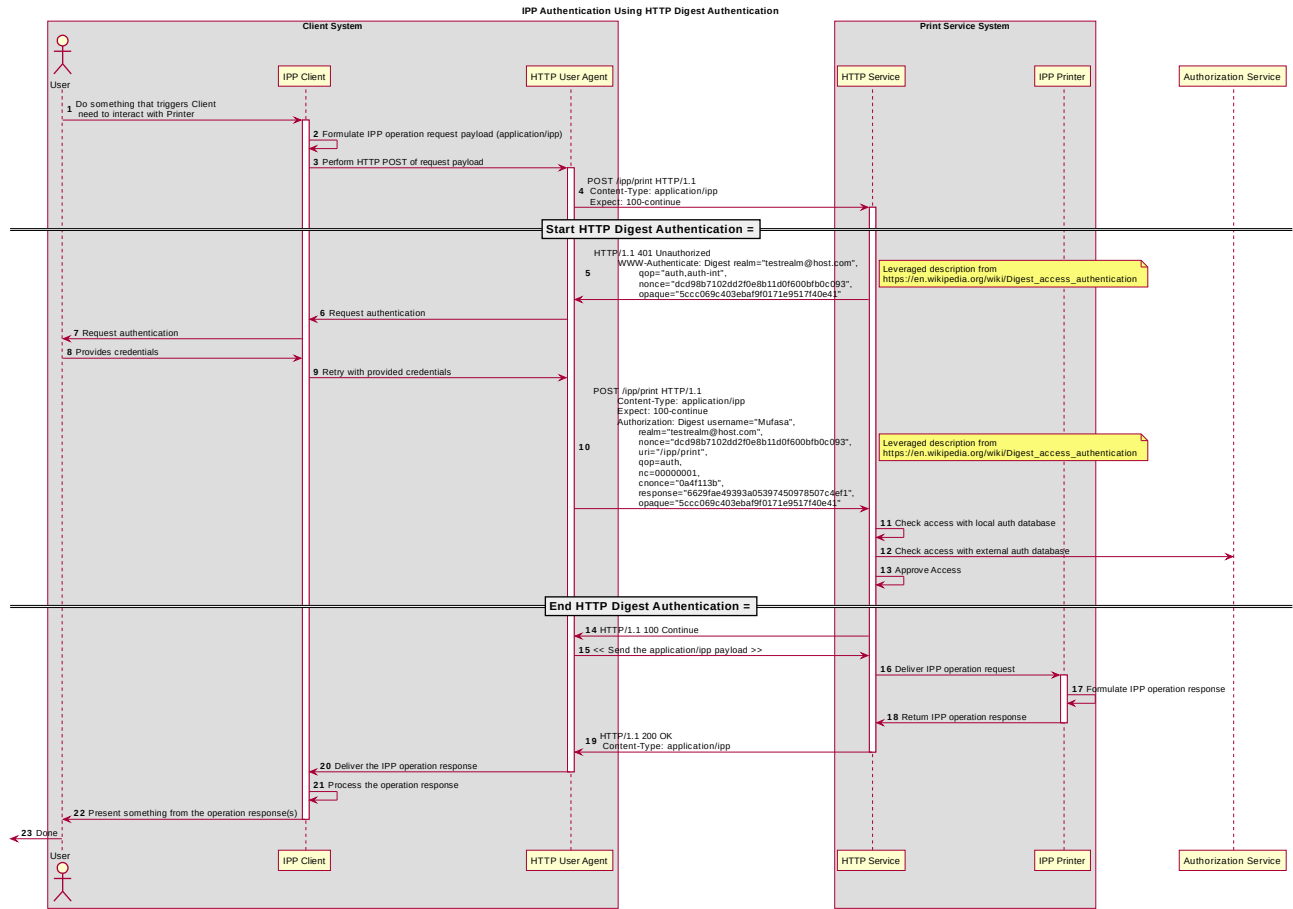


Figure 6 : Sequence diagram for the 'basic' IPP Authentication Method

The 'digest' IPP Authentication Method

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



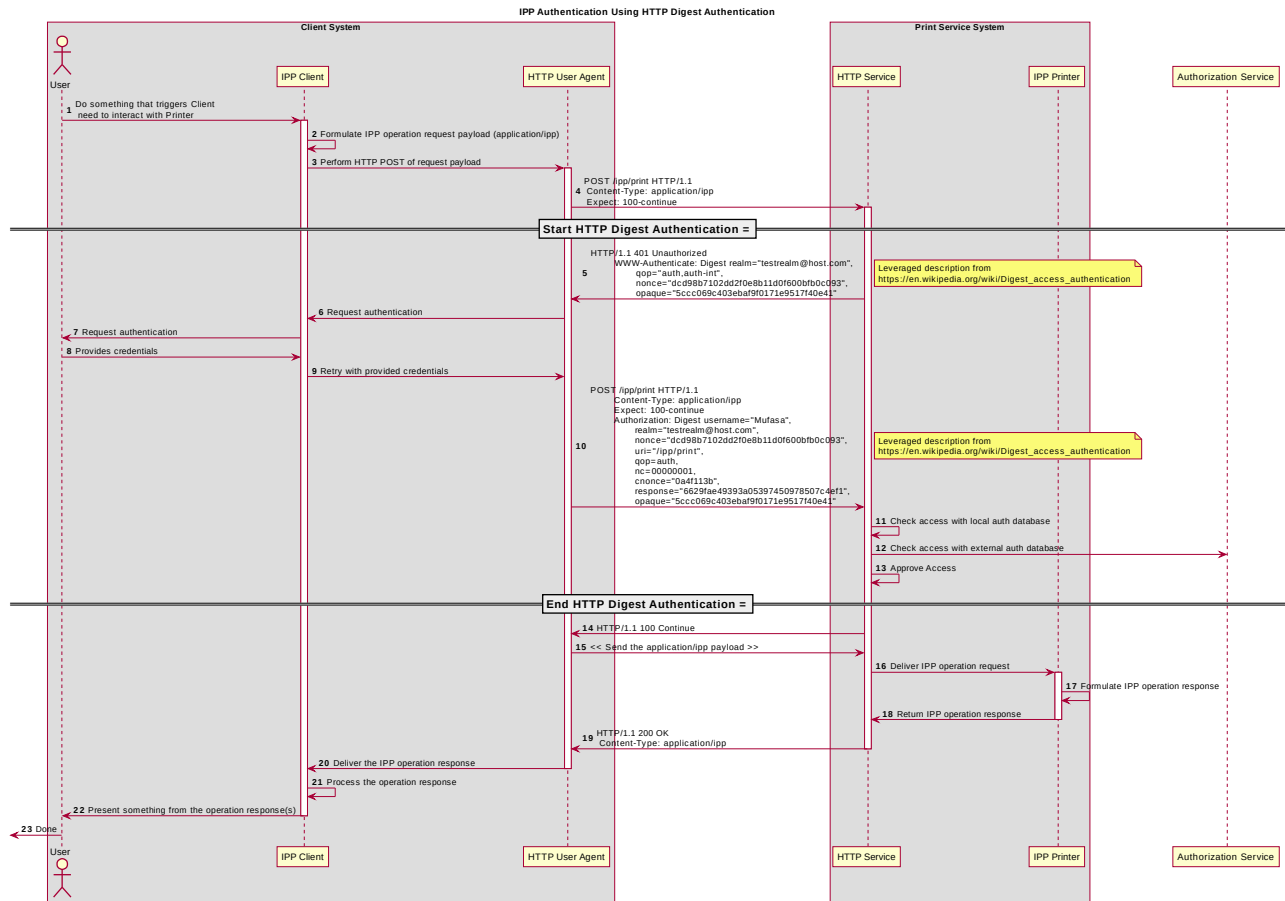


Figure 8 : Sequence diagram for the 'digest' IPP Authentication Method

The 'negotiate' IPP Authentication Method

The 'negotiate' IPP Authentication method uses the HTTP Negotiate authentication scheme [RFC4559].

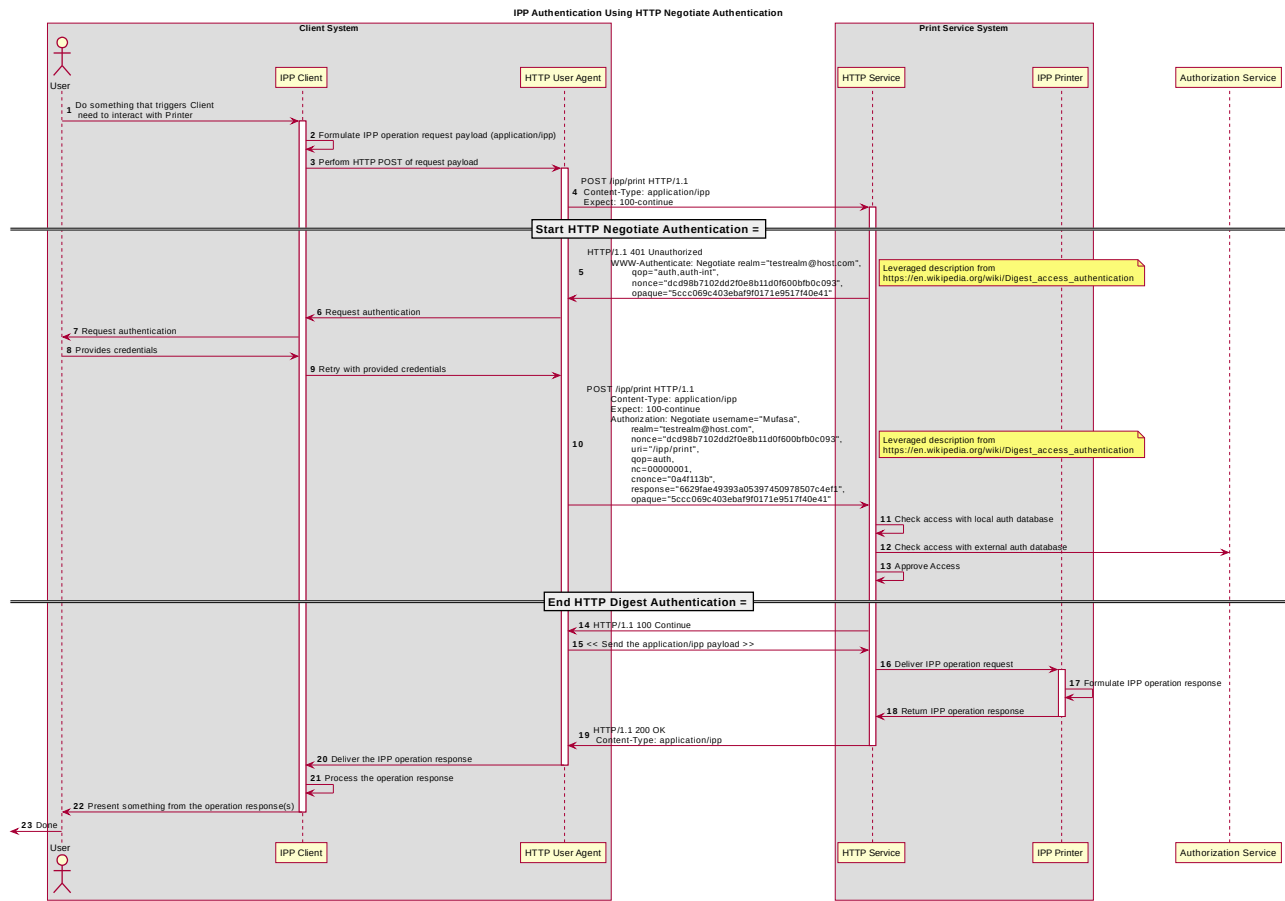


Figure 9: Sequence diagram for the 'negotiate' IPP Authentication Method

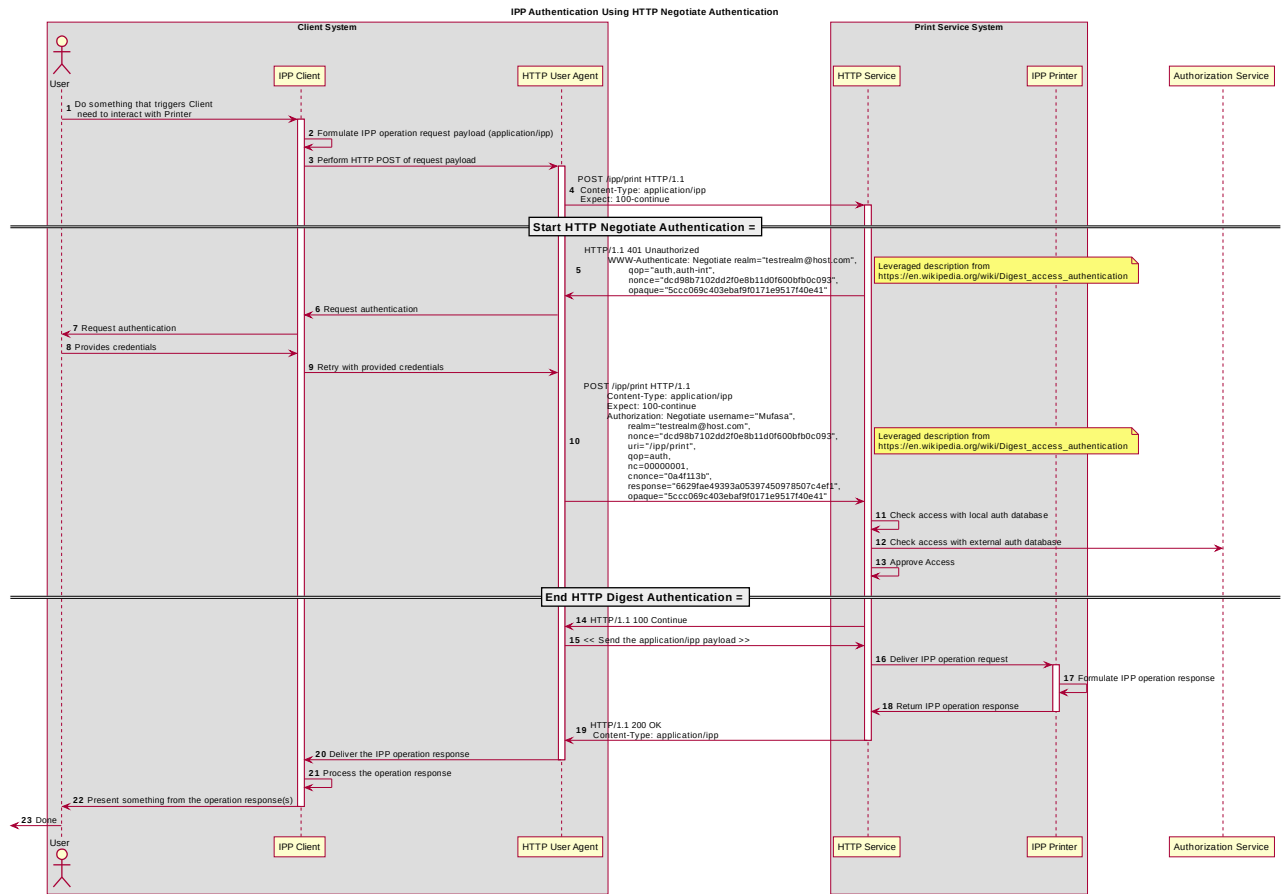


Figure 10 : Sequence diagram for the 'negotiate' IPP Authentication Method

2.4.3. The 'oauth' IPP Authentication Method

The 'oauth' IPP Authentication method uses the OAuth2 authentication scheme [RFC6749][RFC6749] and the OAuth2 Bearer Token [RFC6750]. A conventional OAuth2 authentication workflow integrated into an IPP Print flow is described in Error: Reference source not found.

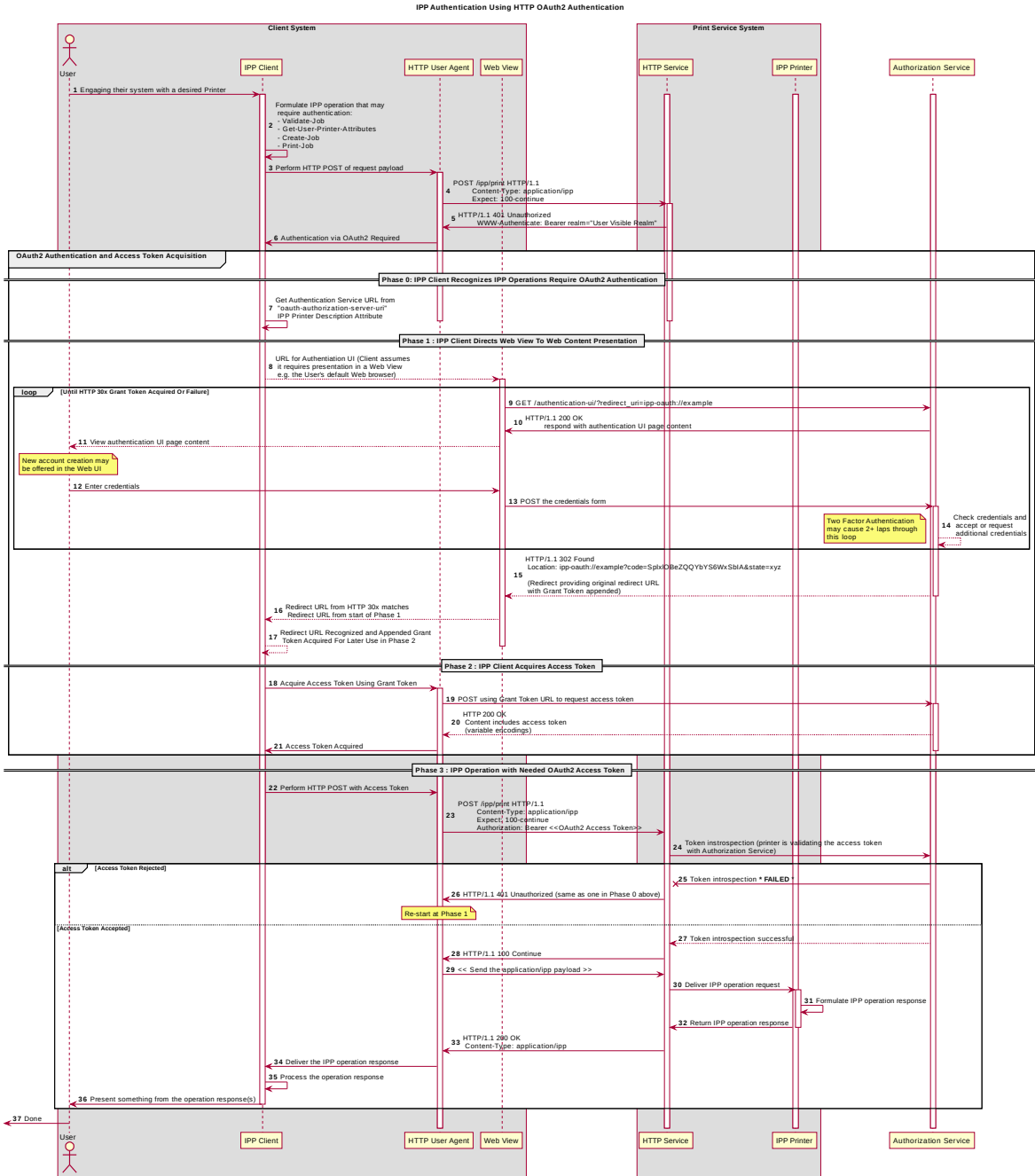


Figure 11: Sequence diagram for the 'oauth' IPP Authentication Method

In the OAuth2 process, the user experience for servicing the authentication challenge is commonly provided by "web content" (HTML etc.) presented in a "web view" (embeddable web browser). Since this can be awkward or disorienting in a print workflow, a hybrid of 'oauth' and 'basic' or 'digest' can be employed, as outlined in Figure 12.

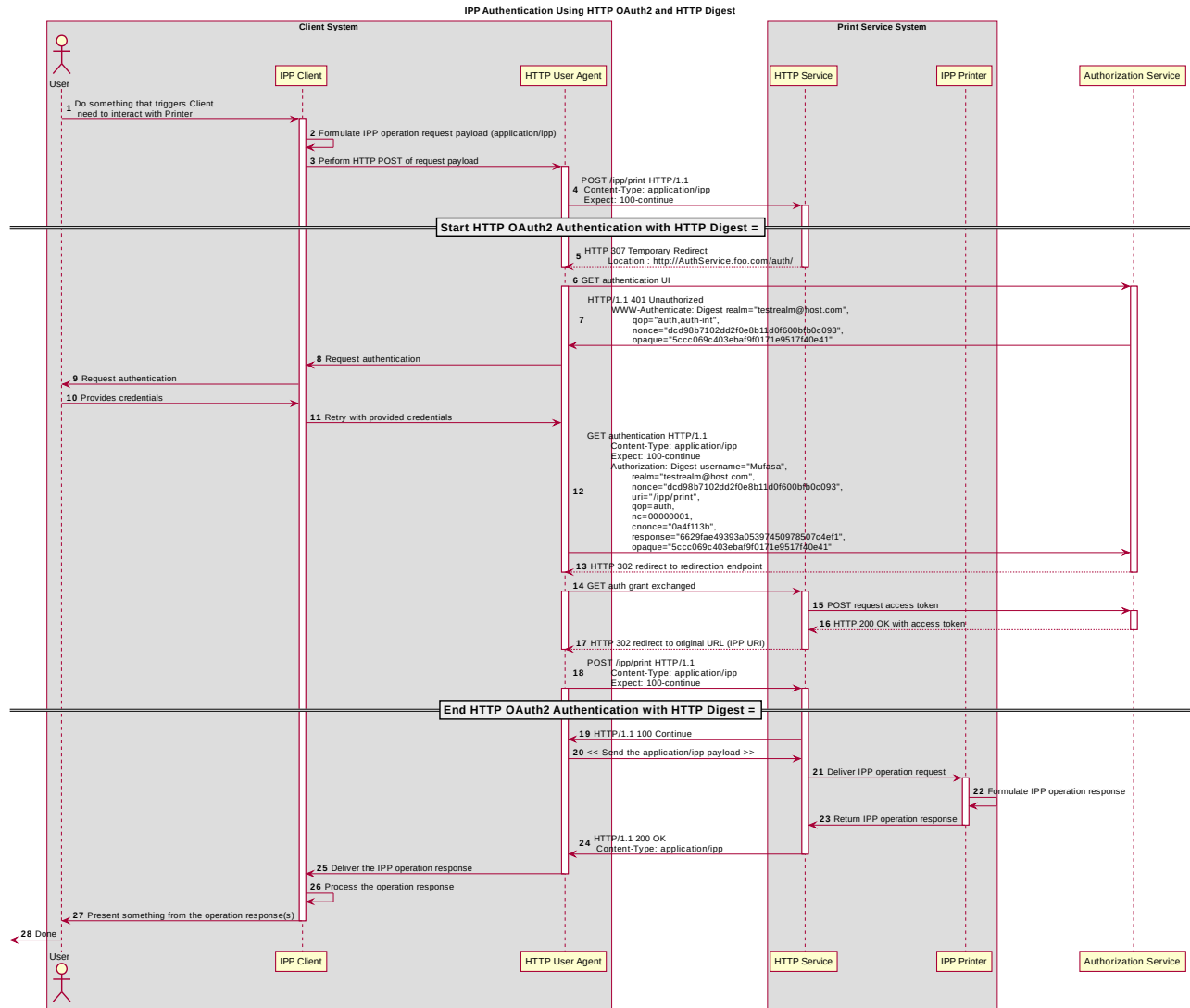


Figure 12: Sequence diagram for the hybrid 'oauth' / 'digest' IPP Authentication Method

2.4.4. X.509 Certificate Authentication Via TLS

Client X.509 certificate authentication in an HTTP session is achieved using the client authentication facilities of Transport Layer Security (TLS) [RFC5246], the commonly used protocol for encrypting an HTTP or IPP connection [RFC8010][RFC8011]. In this

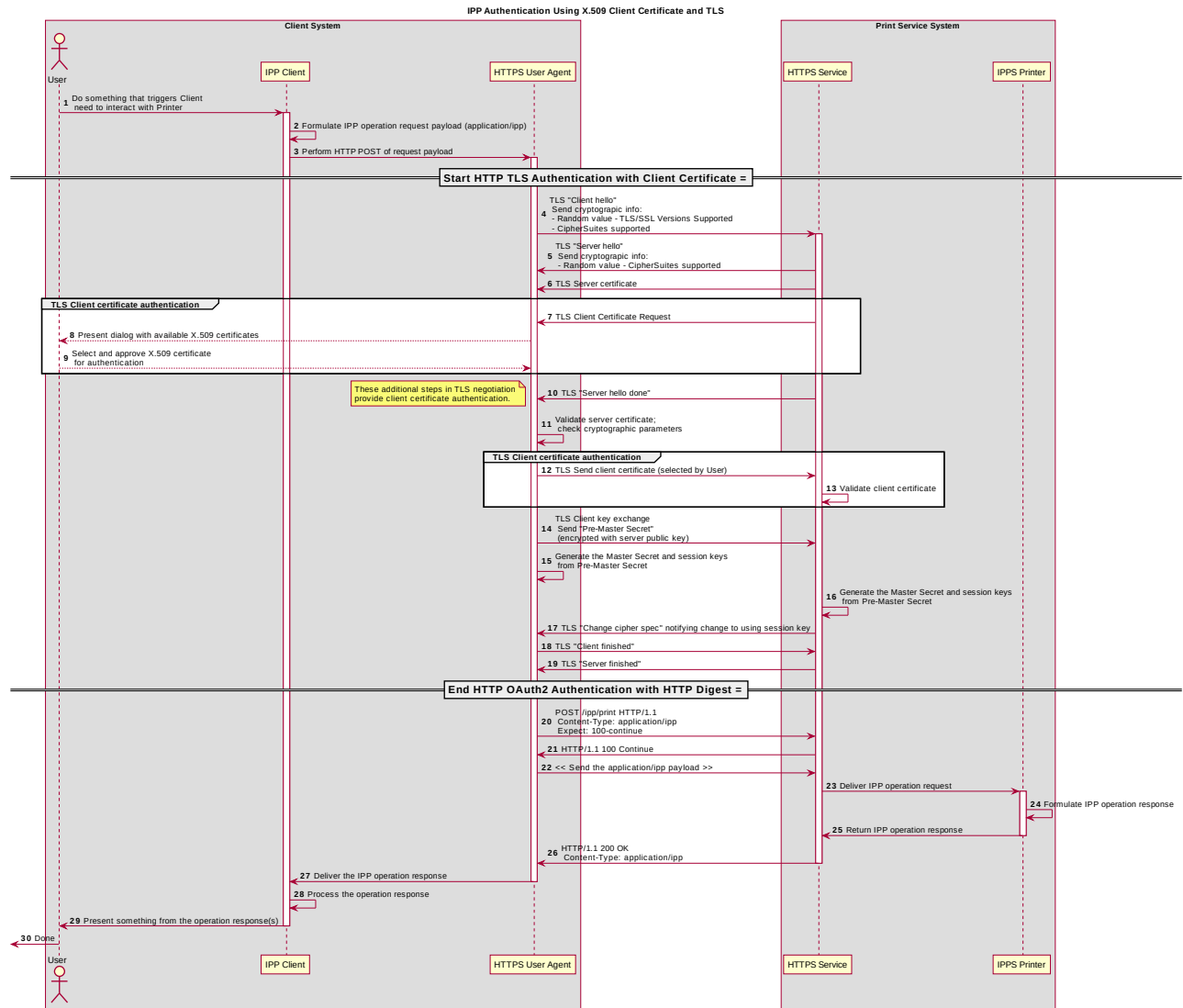


Figure 13: Sequence diagram for X.509 Certificate Authentication Via TLS

1.1.1 ~~Transport Layer Security (TLS) Authentication~~

- ~~3. While Transport Layer Security (TLS) [RFC5246] is the commonly used protocol for encrypting an IPP connection [RFC8010][RFC8011], the authentication facilities of TLS are commonly employed in scenarios where client authentication is provided via a client certificate.~~

4.

1.1.2 Implementation Recommendations

Provide possible technical solutions/approaches in this section. Include pros and cons for each technical solution or approach. Include references to specific protocols and/or data models when appropriate. Include mapping and gateway considerations when appropriate.

4.1. Client Implementation Recommendations

4.1.1. General Recommendations

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

4.1.2. Handling Authentication Failure

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

4.1.3. OAuth2 Recommendations


~~A Client that supports OAuth2 authentication SHOULD incorporate the following considerations into their implementation:~~

~~User experience considerations~~

The OAuth2 authorization service may have a complicated user presentation. If possible, select a presentation alternative that is the least complicated or the most similar to the user experience provided for older authentication methods (HTTP Basic or HTTP Digest) that may be more familiar to the user.

4.2. Printer Implementation Recommendations

4.2.1. Handling Authentication Failure

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

4.2.2. OAuth2 Recommendations

To align with existing Client authentication user experience for HTTP Basic or HTTP Digest authentication, the OAuth2 Authentication Server SHOULD use HTTP Basic or HTTP Digest authentication rather than presenting an authentication dialog page using its own web content. If that isn't practical, an OAuth2 Authorization Service used in an IPP printing workflow. A Printer that incorporates OAuth2 authentication into its solution SHOULD direct a Client to an authentication page that facilitates an appropriate presentation on even limited Client systems such as smart phones.-

5. 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

Security Considerations

5.1. 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

5.2. Client Security Considerations

An IPP Client SHOULD follow ~~these recommendations:~~the recommendations below

1. A Client SHOULD securely store at rest any personally identifiable information (PII) and authentication credentials such as passwords.
2. A Client SHOULD only respond to an authentication challenge over a secure connection (TLS) [RFC8010][RFC8011] unless TLS is not supported over that transport (e.g. IPP USB).
3. A Client SHOULD validate the identity of the Printer by whatever means are available for that connection type. If the connection is secured via TLS [RFC8010], the Client SHOULD validate the server's TLS certificate, match it server certificate ~~SHOULD be validated and matched~~ to the originating host, and cross-check it to match -and-against the host name or IP address in~~addresses from~~ the IPP URI for the target Printer. If the connection is not secured via TLS, other means may be needed. 
4. A Client SHOULD provide a means to allow the User to examine a Printer's provided identity.
5. A Client SHOULD provide one or more means of notification when it is engaging with a previously encountered Printer whose identity has changed.
6. OAuth2 Considerations
 1. The recommendations in “Proof Key for Code Exchange by OAuth Public Clients” [RFC7636] SHOULD be followed, since the threats described therein has been observed in practice.
 2. The recommendations in “OAuth 2 for Native Apps” [RFC8252] should be followed if the print system provides its own user interface presentation and controls for handling the OAuth2 authentication steps, to mitigate the risks described therein.

5.3. Printer Security Considerations

An IPP Printer:

~~An IPP Printer SHOULD follow the recommendations below.~~

~~A Printer~~ SHOULD securely store at rest any personally identifiable information (PII) and authentication credentials such as passwords that are local to the Printer.

1. ~~A Printer~~ SHOULD only challenge a Client for authentication over a secure connection (TLS) [RFC8010][RFC8011] unless TLS is not supported over that transport (e.g. IPP USB).
1. **Certificates**
2. SHOULD support User-provisioned X.509 certificates:
 1. **What is an acceptable certificate?**
 2. The certificate persists across power cycles
 3. **How long is a self-signed certificate expected to last?**
 4. The certificate MUST NOT be automatically renewed or replaced
 5. **How long should a CA issued certificate last? (e.g. recent work on short lives CA certificates...)**
 6. The certificate has a maximum expiration of 1 year from the date of issuance
2. SHOULD support self-generated self-signed X.509 certificates:
 7. **Let's Encrypt and IPP (and OAuth2 or in general?)**
 8. The certificate persists across power cycles
 1. The certificate has a minimum default expiration of 5 years from the date of issuance / generation
 2. The certificate is automatically renewed (regenerated), using a new private key if the previous certificate has expired
 3. The certificate is generated using the mDNS, DHCP and/or manually-configured DNS hostname(s) and regenerated whenever these change
 4. The Printer MUST be able to generate RSA certificates with a key length of 2048 bits using SHA-256 hash
 5. The Printer SHOULD be able to generate ECDSA certificates using the secp256r1(P-256), secp384r1 (P-384), or secp521r1 (P-521) curves and a SHA-256 hash.
 6. The Printer MUST NOT generate self-signed certificates using a SHA-1 hash
3. **Point to best practice documents**
4. References

5.4. Normative References

[IANA-HTTP-AUTH] Hypertext Transfer Protocol (HTTP) Authentication Scheme Registry, Internet Assigned Numbers Authority,

<https://www.iana.org/assignments/http-authschemes/http-authschemes.xml>

- [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>
- [PWG5100.14] 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, [M. Sweet](#), "IPP System Service v1.0", PWG 5100.SYSTEM, TBD, <https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippsystem10-2018042520170719.pdf>
- [RFC2817] R. Khare, S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC 2817, May 2000, <https://www.ietf.org/rfc/rfc2817.txt>
- [RFC3380] T. Hastings, R. Herriot, C. Kugler, H. Lewis, "Internet Printing Protocol (IPP): Job and Printer Set Operations", RFC 3380, September 2002, <https://www.ietf.org/rfc/rfc3380.txt>
- [RFC3629] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629, November 2003, <https://www.ietf.org/rfc/rfc3629.txt>
- [RFC4559] K. Jaganathan, L. Zhu, J. Brezak, "SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows", RFC 4559, June 2006, <https://www.ietf.org/rfc/rfc4559.txt>
- [RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, March 2008, <https://www.ietf.org/rfc/rfc5198.txt>
- [RFC5246] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008, <https://www.ietf.org/rfc/rfc5246.txt>
- [RFC6749] D. Hardt, Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012, <https://www.ietf.org/rfc/rfc6749.txt>
- [RFC6750] M. Jones, D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, October 2012, <https://www.ietf.org/rfc/rfc6750.txt>

- [RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, June 2014, <https://www.ietf.org/rfc/rfc7230.txt>
- [RFC7616] R. Shekh-Yusef, D. Ahrens, S. Bremer, "HTTP Digest Access Authentication", RFC 7616, September 2015, <https://www.ietf.org/rfc/rfc7616.txt>
- [RFC7617] J. Reschke, "The 'Basic' HTTP Authentication Scheme", RFC 7617, September 2015, <https://www.ietf.org/rfc/rfc7617.txt>
- [RFC7636] N. Sakimura, Ed., J. Bradley, N. Agarwal, "Proof Key for Code Exchange by OAuth Public Clients", RFC 7636, September 2015, <https://www.ietf.org/rfc/rfc7636.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>
- [RFC8252] W. Denniss, J. Bradley, "OAuth 2.0 for Native Apps", RFC 8252, October 2017, <https://www.ietf.org/rfc/rfc8252.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>

5.5. Informative References

- [UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2016, <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>

6. Authors' Addresses

Primary authors ~~(using Address style)~~:

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

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

~~Michael Sweet~~

~~Mike Sweet — Apple Inc.
Apple Inc.
One Apple Park Way
MS 111-HOMC
Cupertino, CA 95014
msweet@apple.com~~

~~Zapp Brannigan — Democratic Order of Planets~~

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

~~Ira McDonald — High North, Inc.~~

7. Change History

7.1. April 30, 2018

Changed to Apache OpenOffice template. Added Mike Sweet as a co-author since he has contributed a great deal of content to the document. Resolved all “to-do” highlighted areas

and resolved issues identified in the February 2018 vF2F minutes (<https://ftp.pwg.org/pub/pwg/ipp/minutes/ippv2-f2f-minutes-20180207.pdf>):

- [Added sequence diagram for X.509 client authentication](#)
- [Added sequence diagram for hybrid 'oauth' / 'digest' authentication](#)
- [Many other changes](#)

7.2. January 23, 2018

Updated as per email feedback and discussion:

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

7.3. December 5, 2017

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

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

7.4. August 3, 2017

Initial revision.