IPP Authentication Methods
(IPPAUTH)

Status: Initial

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 available electronically at:


Copyright © 2017 The Printer Working Group. All rights reserved.
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 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.......................................................................................................................... 4
2 Terminology.......................................................................................................................... 4
  2.1 Protocol Roles Terminology............................................................................................. 4
  2.2 Other Terms Used in This Document.............................................................................. 4
  2.3 Acronyms and Organizations.......................................................................................... 4
3 Rationale for IPP Authentication Methods................................................................. 5
  3.1 Client Authentication Methods..................................................................................... 5
    3.1.1 The 'none' IPP Authentication Method..................................................................... 6
    3.1.2 The 'requesting-user-name' IPP Authentication Method........................................ 7
    3.1.3 The 'basic' IPP Authentication Method.................................................................... 8
    3.1.4 The 'digest' IPP Authentication Method................................................................. 9
    3.1.5 The 'negotiate' IPP Authentication Method............................................................. 10
    3.1.6 The 'oauth' IPP Authentication Method.................................................................... 11
4 Implementation Recommendations.................................................................................... 12
5 Internationalization Considerations.................................................................................. 12
6 Security Considerations..................................................................................................... 12
  6.1 Human-readable Strings................................................................................................. 13
7 References............................................................................................................................. 13
  7.1 Normative References..................................................................................................... 13
  7.2 Informative References.................................................................................................... 15
8 Authors' Addresses............................................................................................................... 15
9 Change History..................................................................................................................... 16
  9.1 August 3, 2017.................................................................................................................. 16

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

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, 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), some limits, constraints and conventions ought to be considered when implementing support for one of these different HTTP authentication methods.

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/](http://www.iana.org/)


3 Rationale for 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.

3.1 Client Authentication Methods

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

Each of the authentication method keywords currently registered for “uri-authentication-supported” is described below, with an accompanying sequence diagram for illustration purposes.
3.1.1 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'.

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

In the 'requesting-user-name' IPP Authentication Method [RFC8011], the Client MUST provides 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.

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".

Figure 3.2: Sequence diagram for the 'requesting-user-name' IPP Authentication Method
3.1.3 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 3.3: Sequence diagram for the 'basic' IPP Authentication Method
3.1.4 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 3.4: Sequence diagram for the 'digest' IPP Authentication Method
3.1.5 The 'negotiate' IPP Authentication Method

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

![Sequence diagram for the 'negotiate' IPP Authentication Method](image-url)
3.1.6 The 'oauth' IPP Authentication Method

The 'oauth' IPP Authentication method uses the HTTP "oauth" authentication scheme [RFC5849].

![Sequence diagram for the 'oauth' IPP Authentication Method](https://petermcintyre.com/2011/10/31/creating-sequence-diagrams/)

Figure 3.6: Sequence diagram for the 'oauth' IPP Authentication Method
4 Implementation Recommendations

TBD?

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

6 Security Considerations

Provide security considerations for this document.
6.1 Human-readable Strings

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


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

7 References

7.1 Normative References


7.2 Informative References


8 Authors' Addresses

Primary authors (using Address style):

Smith Kennedy
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:

Mike Sweet – Apple Inc.
Zapp Brannigan - Democratic Order of Planets
9 Change History

9.1 August 3, 2017

Initial revision.