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 available electronically at:

Copyright © 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 extent permitted by applicable law, this material is provided AS IS AND WITH
The Printer Working Group

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 Transport Layer Security (TLS) Authentication .......... 13
4 Implementation Recommendations ................................ 14
  4.1 Client Implementation Recommendations .................. 14
    4.1.1 General Recommendations .................................. 14
    4.1.2 Handling Authentication Failure ........................... 14
    4.1.3 OAuth2 Recommendations .................................... 14
  4.2 Printer Implementation Recommendations .................. 14
    4.2.1 Handling Authentication Failure ........................... 14
    4.2.2 OAuth2 Recommendations .................................... 14
5 Internationalization Considerations ............................. 15
6 Security Considerations .............................................. 15
  6.1 Human-readable Strings ........................................... 15
  6.2 Client Security Considerations .................................. 16
  6.3 Printer Security Considerations ............................... 16
7 References ..................................................................... 17
  7.1 Normative References .............................................. 17
  7.2 Informative References ............................................ 19
8 Authors' Addresses ..................................................... 20
9 Change History .......................................................... 21
  9.1 January 23, 2018 ...................................................... 21
  9.2 December 5, 2017 ..................................................... 21
  9.3 August 3, 2017 ........................................................ 21

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
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/


Overview of IPP Authentication Methods
4 Rationale for IPP Authentication Methods

5 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.

5.1 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 authorize access to capabilities such as operations, resources, and attributes. As 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.

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, as well as a discussion of each method's advantages and shortcomings.
5.1.1 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 5.1.2.

Figure 5.1: Sequence diagram for the 'none' IPP Authentication Method
5.1.2 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 5.2: Sequence diagram for the 'requesting-user-name' IPP Authentication Method
5.1.3 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 5.3: Sequence diagram for the 'basic' IPP Authentication Method
5.1.4 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-Authenticate" 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 5.4: Sequence diagram for the 'digest' IPP Authentication Method](image-url)
5.1.5 The 'negotiate' IPP Authentication Method

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

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

The 'oauth' IPP Authentication method uses the OAHTTP "oauth2" authentication scheme [RFC6749][RFC6749] and the OAuth2 Bearer Token [RFC6750][RFC5849].

Figure 5.6: Sequence diagram for the 'oauth' IPP Authentication Method
156 Transport Layer Security (TLS) Authentication
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.
8 Implementation Recommendations

8.1 Client Implementation Recommendations

8.1.1 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.

8.1.2 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.

8.1.3 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.

○ Information Disclosure

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

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

○ Printer Implementation Recommendations
8.1.6 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.

8.1.7 OAuth2 Recommendations

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.

TBD

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
9 Security Considerations

Provide security considerations for this document.

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

9.1 Client Security Considerations

An IPP Client SHOULD follow 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 server certificate SHOULD be validated and matched to the originating host and against the host name or IP 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.

1. Validating the Printer identity (am I talking to whom I think I’m talking to?) → look in 8010 / 8011 for guidance or references to guidance

2. Printer Security Considerations

An IPP Printer SHOULD follow the recommendations below.

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

2. 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).

3. Certificates

   1. What is an acceptable certificate?

   2. How long is a self-signed certificate expected to last?

   3. How long should a CA issued certificate last? (e.g. recent work on short lives CA certificates...)

   4. Let’s Encrypt and IPP (and OAuth2 or in general?)

   4. Point to best practice documents

10 References

10.1 Normative References


10.2 Informative References


11 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:

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

12.1 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.

12.2 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.

12.3 August 3, 2017

Initial revision.