Individual   W. Mills
Internet-Draft   Yahoo! Inc.
Intended status: Informational   October 17, 2012
Expires: April 20, 2013

                   Link Type Registrations for OAuth 2
                      draft-wmills-oauth-lrdd-06.txt

Abstract

   Defines link type registrations for the OAuth 2 authentication
   framework and OAuth 1.0a.

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on April 20, 2013.

Table of Contents

1. Introduction

This document defines the link type [RFC5988] registrations for the
OAuth 2 [I-D.ietf-oauth-v2] authentication framework and for OAuth
1.0a [RFC5849]. These link types are used during the endpoint
discovery process using Web Host Metadata [RFC6415] and Webfinger
[I-D.ietf-appsawg-webfinger] by clients needing to discover the
authorization, token, and initiation endpoints for a service or site.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

The reader is assumed to be familiar with the terms used in the OAuth
2 and OAuth 1.0a specifcations.

3. **OAuth 2 Link Types**

   OAuth 2 [I-D.ietf-oauth-v2] defines two endpoints which a site or
   domain might need to advertize via a mechanism such as Webfinger
   [I-D.ietf-appsawg-webfinger]. These are the user authorization
   endpoint (usually expected to be a web page the user interacts with)
   and the token endpoint used for obtaining tokens used to access
   protected resources. These are described in detail in the OAuth 2
   specification.

3.1. **OAuth 2 Authorization Endpoint**

   This link type indicates an OAuth 2 authorization endpoint to be used
   for user authentication/authorization to grant access to a protected
   resource.

3.2. **OAuth 2 Token Endpoint**

   The OAuth 2 token endpoint to be used for obtaining tokens to access
   protected services. This link type has two link-extensions:

      grant-types: A space separated list of OAuth 2 grant types (see
         section 4 of [I-D.ietf-oauth-v2]) that can be used at the token
         endpoint to obtain a token. This is not an exclusive list, it
         provides a hint to the application of what SHOULD be valid. A
         token endpoint MAY support additional grant types not
         advertised by a discovery service. The client MAY use this to
         determine the grant types available for use.

      token-types: A space separated list of OAuth 2 token types (see
         section 7.1 of [I-D.ietf-oauth-v2]) that may be issued by the
         token endpoint. It is possible for a token endpoint to issue
         multiple tokens, and types may vary based on scope or other
         factors. This is not an exclusive list, it provides a hint to
         the application of what SHOULD be valid, and it MAY be used by
         a client to determine if the client supports one or more of the
         token type(s) available.

[4](#). **OAuth 1.0a Link Types**

   The OAuth 1.0a [[RFC5849](#)] protocol defines three endpoints that a site
   supporting OAuth 1.0a might advertize via a mechanism like Webfinger:
   the request initiation endpoint, the authorization endpoint, and the
   token endpoint. These are descibed in detail in the OAuth 1.0a
   specification.

[4.1](#). **OAuth 1.0a Request Initiation Endpoint**

   The OAuth 1.0a endpoint used to initiate the sequence, this short
   lived request is what the user approves to grant access to the
   resource.

[4.2](#). **OAuth 1.0a Authorization Endpoint**

   The OAuth 1.0a authorization endpoint used to approve an access
   request. This is expected to be a user facing web interface.

[4.3](#). **OAuth 1.0a Token Endpoint**

   The OAuth 1.0a token API endpoint used to exchange an approved access
   request for a token, used by the client once the resource owner has
   approved the access request.

5. Security Considerations

   This document is informational, defining values in existing
   registries, and as such has no security properties to discuss.

6. IANA Considerations

6.1. Link Type Registration

   Pursuant to [RFC5988] The following link type registrations [[will
   be]] registered by mail to link-relations@ietf.org.

6.1.1. OAuth 2 Authorization Endpoint

   o Relation Name: oauth2-authorize

   o Description: An OAuth 2 authorization endpoint to be used for user
      authentication/authorization to grant access to a protected
      resource.

   o Reference: Section 3.1 of [[This Document]]

   o Notes:

   o Application Data: N/A

6.1.2. OAuth 2 Token Endpoint

   o Relation Name: oauth2-token

   o Description: The OAuth 2 token endpoint to be used for obtaining
      tokens use to access a protected resource.

   o Reference: Section 3.2 of [[This Document]]

   o Notes: This link type has two link extension parameters: "grant-
      types" and "token-types".

   o Application Data: N/A

6.1.3. OAuth 1.0a Request Initiation Endpoint

   o Relation Name: oauth-initiate

   o Description: The OAuth 1.0a request initiation endpoint used to
      get an access request.

   o Reference: Section 4.1 of [[This Document]]

   o Notes:

   o Application Data: N/A

6.1.4. OAuth 1.0a Authorization Endpoint

o Relation Name: oauth-authorize

o Description: The OAuth 1.0a authorization endpoint used to approve
   an access request.

o Reference: Section 4.2 of [[This Document]]

o Notes:

o Application Data: N/A

6.1.5. OAuth 1.0a Token Endpoint

o Relation Name: oauth-token

o Description: The OAuth 1.0a token API endpoint used to exchange an
   approved access request for a token, used by the client once the
   resource owner has approved the access request.

o Reference: Section 4.3 of [[This Document]]

o Notes:

o Application Data: N/A

7. References

7.1. Normative References

[I-D.ietf-oauth-v2]
          Hardt, D., "The OAuth 2.0 Authorization Framework",
          draft-ietf-oauth-v2-31 (work in progress), August 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5849] Hammer-Lahav, E., "The OAuth 1.0 Protocol", RFC 5849,
          April 2010.

[RFC5988] Nottingham, M., "Web Linking", RFC 5988, October 2010.

7.2. Informative References

[I-D.ietf-appsawg-webfinger]
          Jones, P., Salgueiro, G., and J. Smarr, "WebFinger",
          draft-ietf-appsawg-webfinger-00 (work in progress),
          July 2012.

[RFC6415] Hammer-Lahav, E. and B. Cook, "Web Host Metadata",
          RFC 6415, October 2011.

Appendix A. Document History

[[to be removed by RFC editor before publication as an RFC]]

-06

o Restructured the link extensions dscription into the prose,
   simplifying the IANA section.

-05

o Changed the references to [[this document]] in the IANA parts.

o Added a small ammount of text.

-04

o Fixed the title.

o Removed the examples.

-03

o Corrected more typos and fixed the XRD for the examples, and small
   changes in the prose.

-02

o Corrected typos. Added and example.

-01

o Editorial changes, corrected authenticate to authrorize is most
   places, and added examples.

-00

o Initial revision

Author's Address

   William J. Mills
   Yahoo! Inc.

   Phone:
   Email: wmills_92105@yahoo.com