Link Type Registry for OAuth 2
draft-wmills-oauth-lrdd-02.txt

Abstract

Defines link type registrations for the OAuth 2 authentication framework.

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 March 30, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
# Table of Contents

1. Introduction ................................................. 3  
2. Terminology .................................................. 4  
3. Security Considerations ................................. 5  
4. IANA Considerations ....................................... 6  
   4.1. Link Type Registration ................................. 6  
   4.1.1. OAuth 2 Authorization Endpoint .................... 6  
   4.1.2. OAuth 2 Token Endpoint ............................ 6  
   4.1.3. OAuth 1.0a Request Initiation Endpoint .......... 7  
   4.1.4. OAuth 1.0a Authorization Endpoint ............... 7  
   4.1.5. OAuth 1.0a Token Endpoint ...................... 7  
5. Examples ....................................................... 8  
   5.1. Host-Meta Example ................................... 8  
   5.2. WebFinger Example .................................. 8  
6. References ................................................... 10  
   6.1. Normative References ................................. 10  
   6.2. Informative References .............................. 10  
Appendix A. Document History ............................. 11  
Author’s Address ............................................. 12
1. Introduction

This document defines the link type [RFC5988] registrations for the OAuth 2 [I-D.ietf-oauth-v2] authentication framework. It also defines link type registrations for OAuth 1.0a [RFC5849]. These link types are used during the endpoint discovery process using Web Host Metadata [RFC6415] and Webfinger [I-D.jones-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 2.0 specification [I-D.ietf-oauth-v2].

In examples, "C:" and "S:" indicate lines sent by the client and server respectively. Line breaks have been inserted for readability.

Note that the IMAP SASL specification requires base64 encoding message, not this memo.
3. Security Considerations

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

4.1. Link Type Registration

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

4.1.1. OAuth 2 Authorization Endpoint

- Relation Name: oauth2-authorize
- Description: An OAuth 2.0 authorization endpoint.
- Reference: [I-D.ietf-oauth-v2]
- Notes: This link type indicates an OAuth 2.0 authorization endpoint that can be used for user authentication/authorization for the endpoint providing the link.
- Application Data: [optional]

4.1.2. OAuth 2 Token Endpoint

- Relation Name: oauth2-token
- Description: The OAuth token endpoint used to get tokens for access.
- Reference: [I-D.ietf-oauth-v2]
- Notes: The OAuth 2.0 token endpoint to be used for obtaining tokens to access the endpoint providing the link.
- Application Data: This link type has two link-extensions:

  - grant-types: A space separated list of OAuth 2.0 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 if the client supports one or more of the grant types available.

  - token-types: A space separated list of OAuth 2.0 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.

4.1.3. OAuth 1.0a Request Initiation Endpoint

- Relation Name: oauth-initiate
- Description: The OAuth 1.0a request initiation endpoint used to get an access request.
- Reference: [RFC5849]
- Notes: The OAuth 1.0a endpoint used to initiate the sequence, this temporary request is what the user approves to grant access to the resource.
- Application Data:

4.1.4. OAuth 1.0a Authorization Endpoint

- Relation Name: oauth-authorize
- Description: The OAuth 1.0a authorization endpoint used to approve an access request.
- Reference: [RFC5849]
- Notes:
- Application Data:

4.1.5. OAuth 1.0a Token Endpoint

- Relation Name: oauth-token
- Description: The OAuth 1.0a token endpoint used to exchange an approved access request for a token.
- Reference: [RFC5849]
- Notes:
- Application Data:
5. Examples

We provide here both a Host-Meta example and a WebFinger example so that we have both XRD and JSON usages.

5.1. Host-Meta Example

The following might be returned from a fetch of https://www.example.com/.well-known/host-meta if OAuth 2 is supported and advertised.

```xml
<?xml version='1.0' encoding='UTF-8'?>
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'
     xmlns:hm='http://host-meta.net/xrd/1.0'>
  <!-- Host-wide Information -->
  <Subject>example.com</Subject>

  <Link rel='oauth2-authorize'
        href='http://login.example.com/oauth2/authorize' />
  <Link rel='oauth2-token'
        href='http://login.example.com/oauth2/token'
        grant-types='code password' token-types='bearer' />
</XRD>
```

Figure 1: Example of a Host-Meta type query result

5.2. WebFinger Example

Below we have an example of a server souporting WebFinger advertising the OAuth 2 endpoints as a result of a query against "acct:carol@example.com".
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8

{
    "subject" : "acct:carol@example.com",
    "links" :
        [ 
            { 
                "rel" : "oauth2-authorize",
                "href" : "http://login.example.com/oauth2/authorize"
            },
            { 
                "rel" : "oauth2-token",
                "href" : "https://login.example.com/oauth2/token",
                "properties" :
                    { 
                        "grant-types" : "code password",
                        "token-types" : "bearer"
                    }
            }
        ]
}

Figure 2: Example of a WebFinger type query result
6. References

6.1. 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

April 2010.


6.2. Informative References

[I-D.jones-appsawg-webfinger]
Jones, P., Salgueiro, C., and J. Smarr, "WebFinger",
draft-jones-appsawg-webfinger-06 (work in progress),
June 2012.

RFC 6415, October 2011.
Appendix A. Document History

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

-02

- Corrected typos. Added an example.

-01

- Editorial changes, corrected authenticate to authorize in most places, and added examples.

-00

- Initial revision
Author’s Address

William J. Mills
Yahoo! Inc.

Phone:
Email: wmills_92105@yahoo.com