OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2016

N. Sakimura
Nomura Research Institute

November 04, 2015

OAuth Response Metadata
draft-sakimura-oauth-meta-05

Abstract

This specification defines an extensible metadata that may be inserted into the OAuth 2.0 responses to assist the clients to process those responses. It is expressed either as a link header, or query parameters. It will allow the client to learn where the members in the response could be used. Since it is just additional response header/query parameters, any client that does not understand this extension should not break and work normally while supporting clients can utilize the metadata to take the advantage of the extension.

Table of Contents

1. Introduction 2
2. Requirements 2
3. Authorization Response 2
4. Token Endpoint Response 3
5. IANA Considerations 4
5.1. Link Type Registration 4
6. Security Considerations 4
6.1. Query Parameter Tampering 4
7. Acknowledgements 4
8. Document History 4
9. References 5
9.1. Normative References 5
9.2. Informational References 6
Author's Address 6

1. Introduction

Although OAuth 2.0 [RFC6749] has been known for its REST friendliness, OAuth itself is not RESTful, as it heavily relies on out-of-band information to drive the interactions. This situation can be eased by hypertext-enabling the endpoint responses through the introduction of data structure that represents such hypertext and other metadata. This specification defines methods to represent such metadata in the authorization and token endpoints.

2. Requirements

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 RFC 2119 [RFC2119].

3. Authorization Response

The Authorization response of the implementation of this specification MUST return the following query parameter in the redirect URI.

turi REQUIRED if the response contains code. Token Endpoint URI.
The value of this parameter is the URI of the Token Endpoint that the code can be sent to obtain the access token.

ruri REQUIRED if the response contains an Access Token. Resource URI. The value of this parameter is the URI of the Resource Endpoint that the Access Token can be used at.

duri OPTIONAL. Discovery Endpoint URI. The URI of from which the discovery document can be obtained.

If the discovery document also includes Token Endpoint URI or Resource Endpoint, the value of the turi or ruri takes precedence.

The following is an example of such resopnse. Line breaks are for display purposes only.

```
HTTP/1.1 302 Found
Location: https://client.example.com/cb?code=SplxlOBeZQQYbYS6WxSbIA
    &turi=https%3A%2F%2Fexample.com%2Ftoken
    &duri=https%3A%2F%2Fexample.com%2Fdisco
    &state=xyz
```

4. Token Endpoint Response

Token Endpoints that implements this specification MUST return the following relation (rel) and the corresponding URI value as defined in [RFC5988] in the Access Token Response defined in [RFC6749].

ruri REQUIRED if the response contains a bearer Access Token. Resource URI. The value of this parameter is the URI of the Resource Endpoint that the Access Token can be used at.

turi OPTIONAL. Token Endpoint URI. The value of this parameter is the URI of the Token Endpoint that the Refresh Token can be sent to obtain a new Access Token.

duri OPTIONAL. Discovery Endpoint URI. The URI of from which the discovery document can be obtained.

Following is an example of an HTTPS response.

```
HTTP/1.1 200 OK
Link: <https://example.com/userinfo>; rel="ruri",
 <https://example.com/disco>; rel="duri"
Content-Type: application/JSON; charset=utf-8

{
        "access_token":"aCeSsToKen"
}
```

5. IANA Considerations

5.1. Link Type Registration

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

- Relation Name: turl
- Description: An OAuth 2.0 Token Endpoint specified in section 3.2 of [RFC6749].
- Reference: This specification
- Relation Name: rurl
- Description: An OAuth 2.0 Resource Endpoint specified in section 3.2 of [RFC6750].
- Reference: This specification

6. Security Considerations

6.1. Query Parameter Tampering

The query response parameters may be tampered by the man-in-the-browser.

7. Acknowledgements

Members of OAuth WG helped to form this specification. Notabely: Hannes tschofenig, John Bradley, Justin Richer, Kaoru Maeda, Masashi Kurabayashi, Nov Matake, Michael B. Jones, Phil Hunt, William Dennis, (add yourselves).

8. Document History

-05

- Factored out JSON Meta and now using query param and Web Linking.

-04

- Date refresh.

-03

- Date refresh.

-02

- Added Mike Kelly as an author.
- xref fix.
- Introduced "operations" as in draft-ietf-scim-api-00#section-3.5.
- Updated the informative reference to HAL.
- Added description to OAuth Token Endpoint hrefs.
- Added content-type to the example.
- Added Area and Working Group.

-01

- Some format changes, reference fix, and typo fixes.
- Changed 'items' to 'elements' to match the JSON terminology.

-00

- Initial Draft

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, DOI 10.17487/RFC2616, June 1999, <http://www.rfc-editor.org/info/rfc2616>.

[RFC5988] Nottingham, M., "Web Linking", RFC 5988, DOI 10.17487/RFC5988, October 2010, <http://www.rfc-editor.org/info/rfc5988>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <http://www.rfc-editor.org/info/rfc6749>.

[RFC6750] Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, DOI 10.17487/RFC6750, October 2012, <http://www.rfc-editor.org/info/rfc6750>.

9.2. Informational References

[HAL] Kelly, M., "JSON Hypermedia API Language", February 2013.

[oauth-lrdd] Mills, W., "Link Type Registrations for OAuth 2", October 2012.

[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, DOI 10.17487/RFC4627, July 2006, <http://www.rfc-editor.org/info/rfc4627>.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/RFC6570, March 2012, <http://www.rfc-editor.org/info/rfc6570>.

Author's Address

Nat Sakimura
Nomura Research Institute

Email: sakimura@gmail.com