

OAuth Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 27, 2018

D. Hardt  
Amazon  
May 26, 2018

Reciprocal OAuth  
draft-ietf-oauth-reciprocal-00

## Abstract

There are times when a user has a pair of protected resources that would like to request access to each other. While OAuth flows typically enable the user to grant a client access to a protected resource, granting the inverse access requires an additional flow. Reciprocal OAuth enables a more seamless experience for the user to grant access to a pair of protected resources.

## 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 <https://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 November 27, 2018.

## Copyright Notice

Copyright (c) 2018 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 (<https://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

Internet-Draft

I-D

May 2018

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## 1. Introduction

In the usual three legged, authorization code grant, the OAuth flow enables a resource owner (user) to enable a client (party A) to be granted authorization to access a protected resource (party B). If party A also has a protected resource that the user would like to let party B access, then a second complete OAuth flow, but in the reverse direction, must be performed. In practice, this is a complicated user experience as the user is at Party A, but the OAuth flow needs to start from Party B. This requires the second flow to send the user back to party B, which then sends the user to Party A as the first step in the flow. At the end, the user is at Party B, even though the original flow started at Party A.

Reciprocal OAuth simplifies the user experience by eliminating the redirections in the second OAuth flow. After the initial OAuth flow, party A obtains consent from the user to grant party B access to a protected resource at party A, and then passes an authorization code to party B using the access token party A obtained from party B to provide party B the context of the user. Party B then exchanges the authorization code for an access token per the usual OAuth flow.

### 1.1. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [BCP 14](#), [RFC 2119](#) [[RFC2119](#)].

## 2. Reciprocal Scope Request

When party B is providing an authorization response per [[RFC6749](#)] 4.1.2, party B MAY include an additional query component in the redirection URI to indicate the scope requested in the reciprocal grant.

reciprocal OPTIONAL. The scope of party B's reciprocal access request per [[RFC6749](#)] 3.3.

If party B does not provide a reciprocal parameter in the

authorization response, the reciprocal scope will be a value previously preconfigured by party A and party B.

### [3.](#) Reciprocal Authorization Flow

The reciprocal authorization flow starts after the client (party A) has obtained an access token from the authorization server (party B) per [\[RFC6749\]](#) 4.1 Authorization Code Grant.

#### [3.1.](#) User Consent

Party A obtains consent from the user to grant Party B access to protected resources at party A. The consent represents the scopes party B had preconfigured at party A.

#### [3.2.](#) Reciprocal Authorization Code

Party A generates an authorization code representing the access granted to party B by the user. Party A then makes a request to party B's token endpoint authenticating per [\[RFC6749\]](#) 2.3 and sending the following parameters using the "application/x-www-form-urlencoded" format per [\[RFC6749\] Appendix B](#) with a character encoding of UTF-8 in the HTTP request entity-body:

grant\_type REQUIRED. Value MUST be set to "urn:ietf:params:oauth:grant-type:reciprocal".

code REQUIRED. The authorization code generated by party A.

client\_id REQUIRED, party A's client ID.

access\_token REQUIRED, the access token obtained from Party B. Used to provide user context.

For example, the client makes the following HTTP request using TLS (with extra line breaks for display purposes only):

```
POST /token HTTP/1.1
Host: server.example.com
```

Authorization: Basic ej4hsyfishwssjduisdhkjsdksusdhkjsdjk  
Content-Type: application/x-www-form-urlencoded

grant\_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Areciprocal&code=hasdyubas

Party B MUST verify the authentication provided by Party A per  
[\[RFC6749\]](#) 2.3

Party B MUST then verify the access token was granted to the client  
identified by the client\_id.

Hardt

Expires November 27, 2018

[Page 3]

---

Internet-Draft

I-D

May 2018

Party B MUST respond with either an HTTP 200 (OK) response if the  
request is valid, or an HTTP 400 "Bad Request" if it is not.

Party B then plays the role of the client to make an access token  
request per [\[RFC6749\]](#) 4.1.3.

#### [4.](#) IANA Considerations

TBD.

#### [5.](#) Acknowledgements

TBD.

#### [6.](#) 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,  
<<https://www.rfc-editor.org/info/rfc2119>>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework",  
[RFC 6749](#), DOI 10.17487/RFC6749, October 2012,  
<<https://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,  
<<https://www.rfc-editor.org/info/rfc6750>>.

[Appendix A](#). Document History

[A.1. draft-ietf-oauth-reciprical-00](#)

- o Initial version.

Author's Address

Dick Hardt  
Amazon

Email: [dick.hardt@gmail.com](mailto:dick.hardt@gmail.com)