Making OAuth Work on the Open Web

Aaron Parecki • IIW 27 • October 2018
IndieAuth

OAuth for the open web

IndieAuth is a decentralized identity protocol built on top of OAuth 2.0.

Read more about how IndieAuth solves OAuth for the open web.

Read the Spec

The latest version of the IndieAuth spec is available at:

indieauth.spec.indieweb.org

The January 2018 published version is also available at:
Challenges with OAuth 2.0 for the Open Web:

- Client registration is impractical with thousands of authorization servers
- User IDs need to be globally unique
- Discovery: How does the app know where to send the user to authenticate?
IndieAuth builds on OAuth 2.0:

- Client IDs are URLs
- User IDs are URLs
- Discovery of the authorization server happens by looking at the User’s URL
IndieAuth

W3C Working Group Note 23 January 2018

This version:
https://www.w3.org/TR/2018/NOTE-indieauth-20180123/

Latest published version:
https://www.w3.org/TR/indieauth/

Latest editor's draft:
https://indieauth.spec.indieweb.org/

Test suite:
https://indieauth.rocks/

Editor:
Aaron Parecki

Repository:
Github
Issues
Commits

Please check the errata for any errors or issues reported since publication.
The app https://indielogin.com/ would like to sign you in as https://wordpress.avocado.lol/.


You will be redirected to https://indielogin.com/redirect/indieauth after authenticating.
Success! You logged in as https://wordpress.avocado.lol/

{
    "me": "https://wordpress.avocado.lol/
}

Start Over
Hi, I’m Aaron, co-founder of IndieWebCamp. I maintain oauth.net, write and consult about OAuth, and am the editor of several W3C specifications. I record videos for local conferences and help run a podcast studio in Portland.

I wrote 100 songs in 100 days! I’ve been tracking my location since 2008, and write down everything I eat and drink. I’ve spoken at conferences around the world about owning your data, OAuth, quantified self, and explained why R is a vowel. Read more.
Quill

Quill is a simple app for posting text notes to your website.

To use Quill, sign in with your domain. Your website will need to support Micropub for creating new posts.

https://aaronparecki.co Sign In
<!doctype html>
<html>
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Aaron Parecki</title>
    <link rel="authorization_endpoint" href="https://aaronparecki.com/auth">
    <link rel="token_endpoint" href="https://aaronparecki.com/auth/token">
    <link rel="micropub" href="https://aaronparecki.com/micropub">
    <link rel="microsub" href="https://aperture.p3k.io/microsub/1">
    <link rel="feed" href="/syndicated" />
    <link rel="feed" href="/all" />
    <link rel="alternate" type="application/jf2feed+json" href="/primary.jf2" >
    <link rel="alternate" type="application/json" href="/feed.json" >
    <link rel="alternate" type="application/atom+xml" href="/feed.xml" >
    <link rel="EditURI" type="application/rsd+xml" title="RSD" href="https://xmlrpc.p3k.io/aaronparecki.com/xmlrpc?rsd" />
    <script type="application/ld+json">
      {
        "@context": "http://schema.org",
        "@type": "WebSite",
        "url": "https://aaronparecki.com/",
        "potentialAction": {
          "@type": "SearchAction",
          "target": "https://aaronparecki.com/search?q={search_term_string}"
        }
      }
    </script>
  </head>
</html>
This app is requesting the following scopes. You can edit the scopes that will be granted to this application.

**Publishing**
- create
  - Allows the application to create posts and upload to the Media Endpoint
- update
  - Allows the application to update posts
- delete
  - Allows the application to delete posts
- media
  - Allows the application to upload to the Media Endpoint

**Reading**
- read
  - Allows the application to read content from channels
- follow
  - Allows the application to follow and unfollow feeds
- mute
  - Allows the application to mute and unmute users
- block
  - Allows the application to block and unblock users
- channels
  - Allows the application to manage your channels

▶ Channels

✅ Approve
Hello from IIW! This is a post from Quill to demonstrate IndieAuth.

e.g. web, personal

github.com/aaronpk
twitter.com/aaronpk
Hello from IIW! This is a post from Quill to demonstrate IndieAuth.

Hello from IIW! This is a post from Quill to demonstrate IndieAuth.

Have you written a response to this? Let me know the URL:

Send Webmention

Posted in /notes using quill.p3k.io

Hi, I'm Aaron, co-founder of IndieWebCamp. I maintain oauth.net, write and consult about OAuth, and use the alias @aaronp. Follow me on Mastodon.
Indigenous - Social timeline

Make the web social again

DOWNLOAD FOR IOS

DOWNLOAD FOR ANDROID

Indigenous allows you to engage with the Internet as you do on social media sites, but posts it all on your website. Use the built-in reader to read and respond to posts across the internet. Indigenous doesn’t track or store any of your information. You choose a service you trust or host it yourself.
Indigenous - Social timeline

Make the web social again

DOWNLOAD FOR IOS

DOWNLOAD FOR ANDROID
{
  "name": "Indigenous for iOS",
  "icons": [{
    "src": "img/app-icon.png",
    "sizes": "167x167",
    "type": "image/png"
  }],
  "prefer_related_applications": true,
  "related_applications": [{
    "platform": "itunes",
  }]
}
IndieAuth Authentication Flow Diagram

Browser

Client

User URL

Authorization Endpoint

Token Endpoint

User enters their profile URL

Client fetches URL to discover rel=authorization_endpoint and rel=token_endpoint

Client builds authorization request and redirects to authorization_endpoint

User visits their authorization endpoint and sees the authorization request

Authorization endpoint fetches client information (name, icon)

User authenticates, and approves the request. Authorization endpoint issues code, builds redirect back to client.

User's browser is redirected to client with an authorization code

Client exchanges authorization code for an access token by making a POST request to the token_endpoint

Token endpoint verifies code and returns canonical user profile URL with an access token

Client initiates login session and the user is logged in
To set up your website manually, you’ll need to choose an IndieAuth server such as https://indieauth.com and add a few links to your home page. Add a link to the indieauth.com authorization endpoint in an HTML <link> tag so that apps will know where to send you to log in.

```
<link rel="authorization_endpoint" href="https://indieauth.com/auth">
```

Then tell indieauth.com how to authenticate you by linking to either a GitHub account or email address.

```
<a href="https://github.com/username" rel="me">GitHub</a>
<a href="mailto:you@example.com" rel="me">Email</a>
```
OAuth for the Open Web

Sat, Jul 7, 2018 9:30am - 07:00

OAuth has become the de facto standard for authorization and authentication on the Web.