Mastering OAuth 2.0

Ben Ramsey
Day Camp 4 Developers
2 June 2017

HI, I'M BEN.

I'm a web craftsman, author, and speaker. I build a platform for professional photographers at ShootProof. I enjoy APIs, open source software, organizing user groups, good beer, and spending time with my family. Nashville, TN is my home.

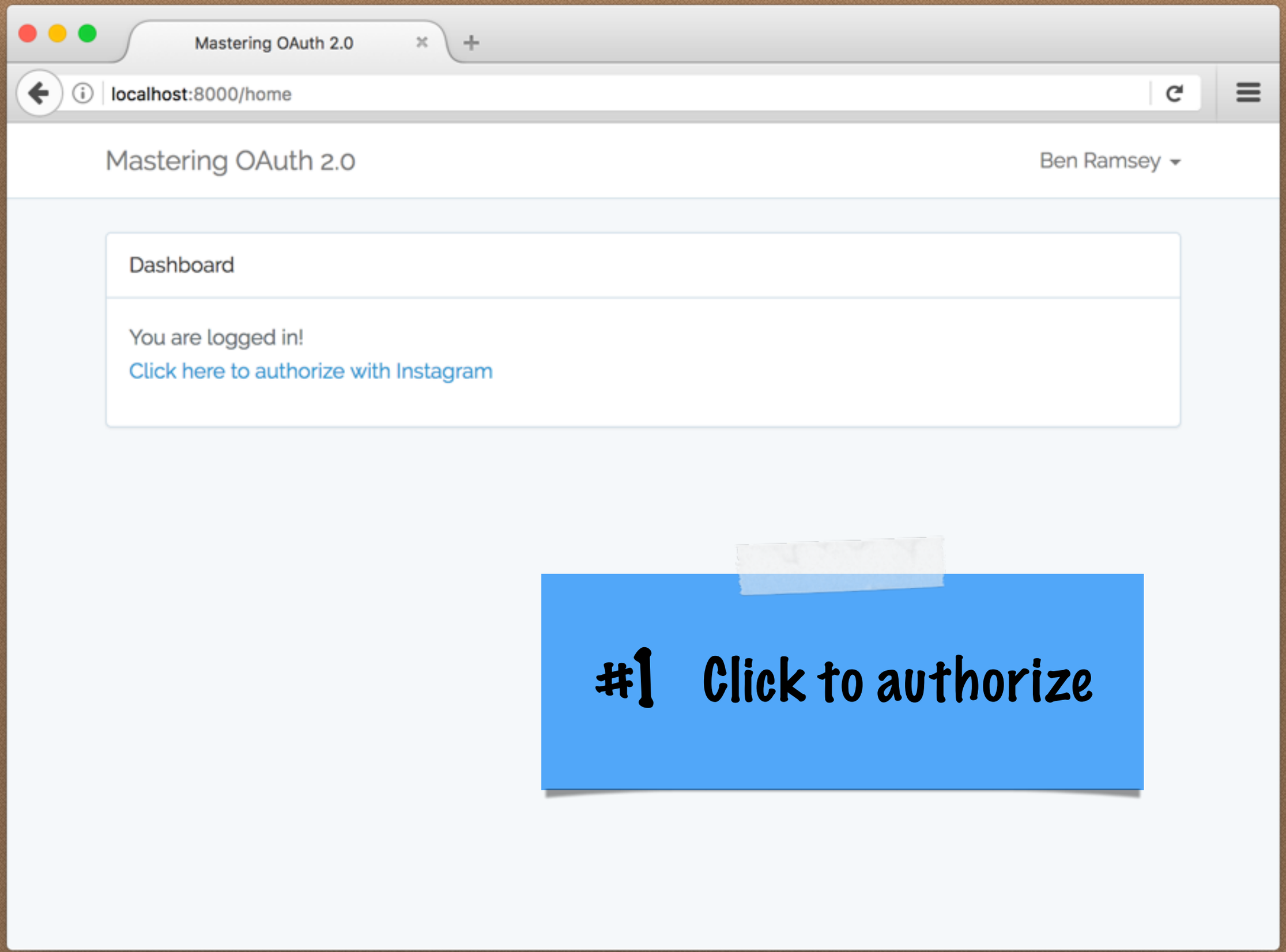
- ***Zend PHP Certification Study Guide***
- **Nashville PHP & Atlanta PHP user groups**
- **array_column()**
- **league/oauth2-client**
- **ramsey/uuid**

OAuth 2.0


THE LEAGUE OF
EXTRAORDINARY PACKAGES


OAUTH
OAUTH

Instagram Demo



#1 Click to authorize

Authorization Request — In...

https://www.instagram.com/oauth/authorize?state=211dd4a7d45650253669d507245c7f3b&scope=basic&respons

Instagram

This app is in sandbox mode and can only be authorized by sandbox users.

Hi **ramseyben,** **Mastering OAuth 2.0** is requesting to do the following:

Access your basic information Your media & profile info

Not ramseyben?

Cancel Authorize

You should only authorize third-party appli
how and when they will use your data. You
your profile page and clicking "revoke" in th

#2 Log in on site and grant permission

#3 Redirect back with auth code

#4 Exchange code for access token

Mastering OAuth 2.0

localhost:8000/home

Mastering OAuth 2.

Ben Ramsey

#5 Use access token to get data

Dashboard

You are logged in!

Hello, Ben Ramsey

I was once PHPamous. Now, I'm just a normal guy.

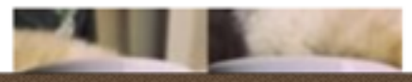
Forget Instagram token

Your Instagram Media







GitHub - ramsey/oauth2-ex...

GitHub, Inc. (US) https://github.com/ramsey/oauth2-example/tree/dc4d

Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

ramsey / oauth2-example

Watch 2 Star 7 Fork 1

Code Issues 0 Pull requests 0 Projects 0 Insights

Full Laravel source application for example in "Mastering OAuth 2.0" articles and talks.

7 commits

1 contributor

Tag: dc4d New pull req file Clone or download

ramsey Update readme mmit 3e5590d 5 minutes ago

app		7 months ago
bootstrap	True North PHP 2016 Example Application	7 months ago
config	True North PHP 2016 Example Application	7 months ago
database	True North PHP 2016 Example Application	7 months ago
public	True North PHP 2016 Example Application	7 months ago
resources	True North PHP 2016 Example Application	7 months ago
routes	True North PHP 2016 Example Application	7 months ago
storage	True North PHP 2016 Example Application	7 months ago
tests	True North PHP 2016 Example Application	7 months ago

bram.se/dc4d-oauth2-app

Preparing for OAuth

1. Register your application with the service
2. Let the service know your domains or redirect URLs
3. Configure your application to use the client ID and client secret given to you by the service

! No two OAuth 2.0 providers are alike!

Instagram

https://www.instagram.com

Instagram

Sign up to see photos and videos from your friends.

Log in with Facebook

OR

samwise@example.com

Samwise Gamgee

samwisegamgee4497

••••••••••

Sign up

By signing up, you agree to our Terms & Privacy Policy.

Instagram Developer Docu...

https://www.instagram.com/developer/clients/register/

Instagram | Sandbox Invites | Manage Clients | samwisegamgee4497

Search Documentation

- Overview
- Authentication
- Login Permissions
- Permissions Review
- Sandbox Mode
- Secure Requests
- Endpoints
- Rate Limits
- Subscriptions
- Embedding
- Mobile Sharing
- Libraries
- Support
- Changelog
- Platform Policy

Register new Client ID

Details | Security

Application Name: Mastering OAuth 2.0

*Do not use **Instagram**, **IG**, **insta** or **gram** in your app name. Make sure to adhere to the API Terms of Use and Brand Guidelines .*

Description: Teaching OAuth 2.0 principles.

Company Name:

Website URL: http://example.com

Valid redirect URIs: http://localhost:8000/instagram × Press Enter to confirm.

The redirect_uri specifies where we redirect users after they have chosen whether or not to authenticate your application.

Privacy Policy URL:

Contact email:

Description: Teaching OAuth 2.0 principles.

Company Name:

Website URL: http://example.com

Valid redirect URIs: http://localhost:8000/instagram ×

The redirect_uri specifies where we redirect users after they have chosen whether
application.

Privacy Policy URL:

Contact email:

Instagram Developer Docu...

https://www.instagram.com/developer/clients/e4bf73d6c24b4ce09db0549b31c255e5/edit/

Instagram | Sandbox Invites | Manage Clients | samwisegamgee4497

Search Documentation

- Overview
- Authentication
- Login Permissions
- Permissions Review
- Sandbox Mode
- Secure Requests
- Endpoints
- Rate Limits
- Subscriptions
- Embedding
- Mobile Sharing
- Libraries
- Support
- Changelog
- Platform Policy

Manage Client: Mastering OAuth 2.0

Client ID e4bf73d6c24b4ce09db0549b31c255e5

Client Secret [redacted] RESET SECRET

Client Status Sandbox Mode

Details | Security | Sandbox | Permissions | Migrations

Application Name: Mastering OAuth 2.0

*Do not use **Instagram**, **IG**, **insta** or **gram** in your app name. Make sure to adhere to the API Terms of Use and Brand Guidelines .*

Description: Teaching OAuth 2.0 principles.

Company Name:

Website URL: http://example.com

Privacy Policy URL:

Contact email:

Manage Client: Mastering OAut

Client ID	e4bf73d6c24b4ce09db0549b31c255e5
Client Secret	[redacted]

RESET S

Client Status Sandbox Mode

Details | Security | Sandbox | Permissions | Migrations

Application Name: Mastering OAuth 2.0

*Do not use **Instagram**, **IG**, **insta** or **gram** in your app name. Make sure to adhere to Guidelines .*

Description: Teaching OAuth 2.0 principles.

Integrating with the Provider

```
composer require league/oauth2-instagram
```

```php
use League\OAuth2\Client\Provider\Instagram;

$provider = new Instagram([
    'clientId' => 'CLIENT_ID',
    'clientSecret' => 'CLIENT_SECRET',
    'redirectUri' => 'https://example.com/redirect',
]);
```

Authorization Request

1. Generate authorization URL
2. Store *state* to session
3. Prompt user to authorize or redirect them

```php
$authUrl = $provider->getAuthorizationUrl();

$request->session()->put(
    'instagramState',
    $provider->getState()
);

return redirect()->away($authUrl);
```

Redirection Endpoint

1. Receive authorization code
2. Check state
3. Exchange code for an access token

```php
$state = $request->session()->get('instagramState');

if ($request->state !== $state) {
  abort(400, 'Invalid state');
}

if (!$request->has('code')) {
  abort(400, 'Authorization code not available');
}
```

```php
$token = $provider->getAccessToken(
  'authorization_code',
  [
    'code' => $request->code,
  ]
);

$request->session()->put('instagramToken', $token);

return redirect()->action('HomeController@index');
```

Expiring & Refreshing Tokens

1. Check for expiration & refresh token
2. Request access token using refresh token

```php
if ($token->hasExpired() && $token->getRefreshToken()) {
    $newToken = $provider->getAccessToken('refresh_token', [
        'refresh_token' => $token->getRefreshToken(),
    ]);

    $request->session()->put('accessToken', $newToken);
}
```

! Instagram does not support refresh tokens

Using Access Tokens

1. getAuthenticatedRequest() returns a PSR-7 RequestInterface object
2. Use your favorite HTTP request library to make a request

```php
$feedRequest = $provider->getAuthenticatedRequest(
  'GET',
  'https://api.instagram.com/v1/users/self/media/recent',
  $instagramToken
);
```

```php
$client = new \GuzzleHttp\Client();
$feedResponse = $client->send($feedRequest);

$instagramFeed = json_decode(
  $feedResponse->getBody()->getContents()
);
```

A Brief History of Web Authorization

What is OAuth 2.0?

“However, as a rich and highly extensible framework with many optional components, on its own, this specification is likely to produce a wide range of non-interoperable implementations.”

RFC 6749, Section 1.8

1. Resource owner
2. Resource server
3. Client
4. Authorization server

```
composer require league/oauth2-client
```

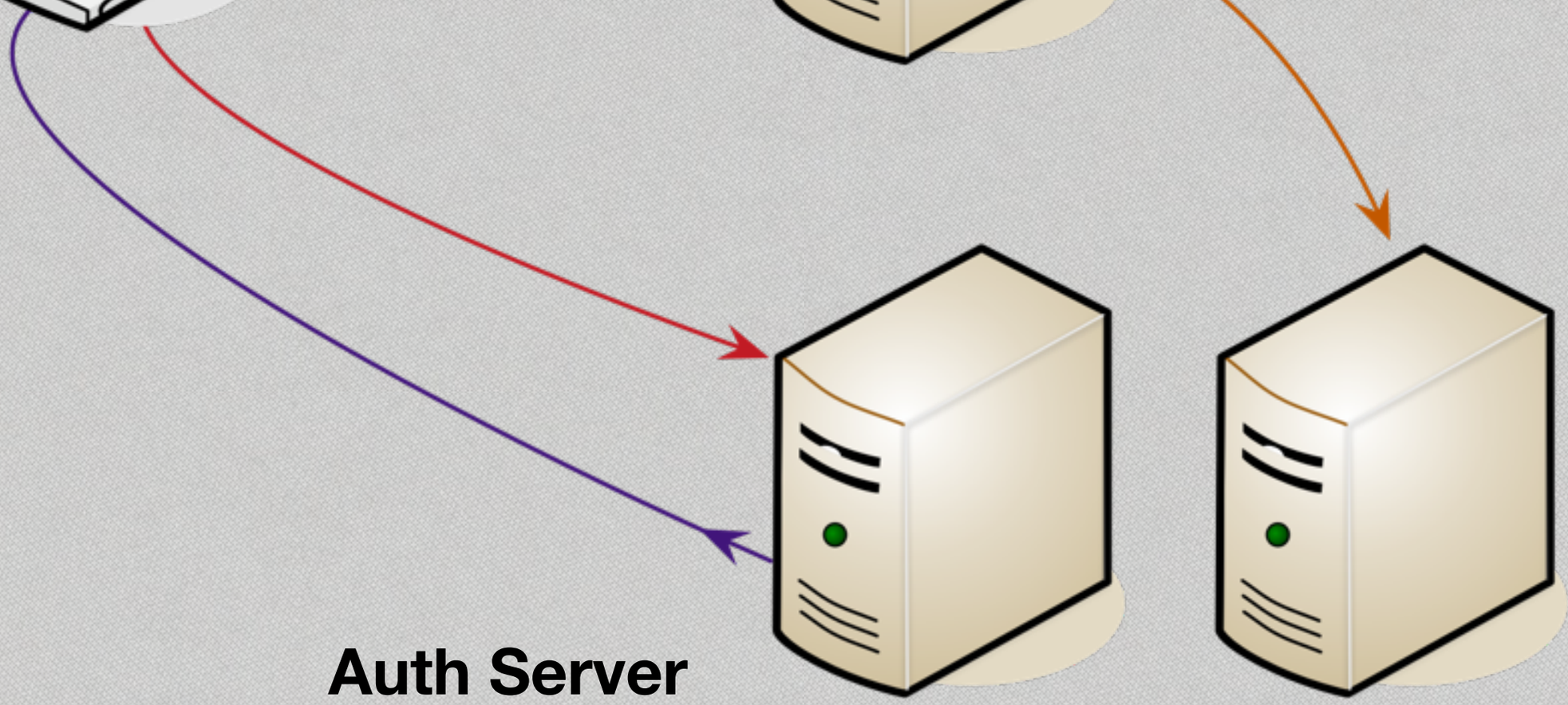
```php
use League\OAuth2\Client\Provider\GenericProvider;

$provider = new GenericProvider([
  'clientId' => 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',
  'clientSecret' => 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',
  'redirectUri' => 'https://you.example.com/redirect-url',
  'urlAuthorize' => 'https://them.example.net/authorize',
  'urlAccessToken' => 'https://them.example.net/token',
  'urlResourceOwnerDetails' =>
    'https://them.example.net/api/me'
]);
```

Authorization Code

1. Commonly referred to as *three-legged*
2. Used in our Instagram example
3. Very common grant type

Resource Owner

Client



Auth Server

Resource Server

Resource Owner

Step 1

Client

Auth Server

Resource Server

Resource Owner

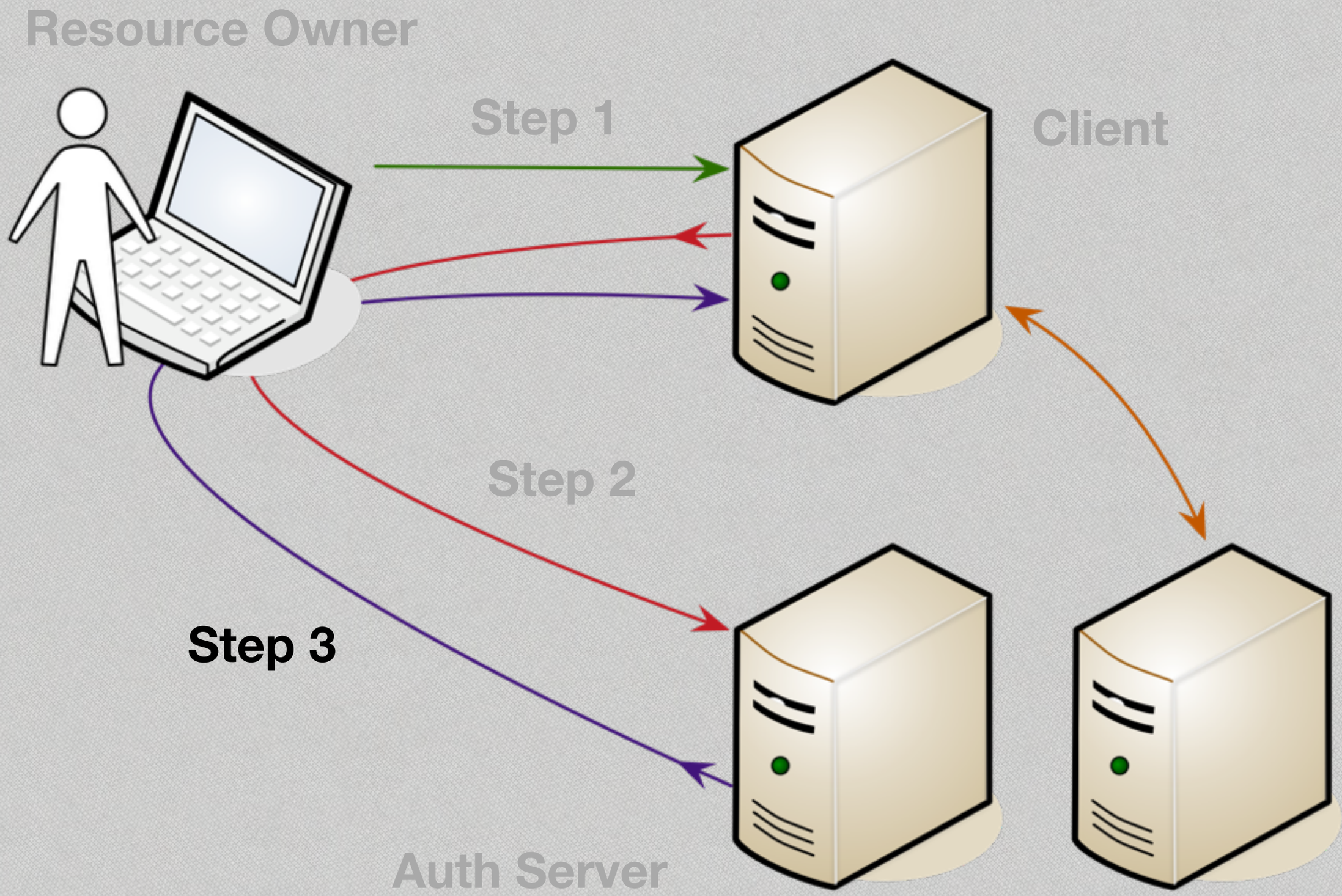
Step 1

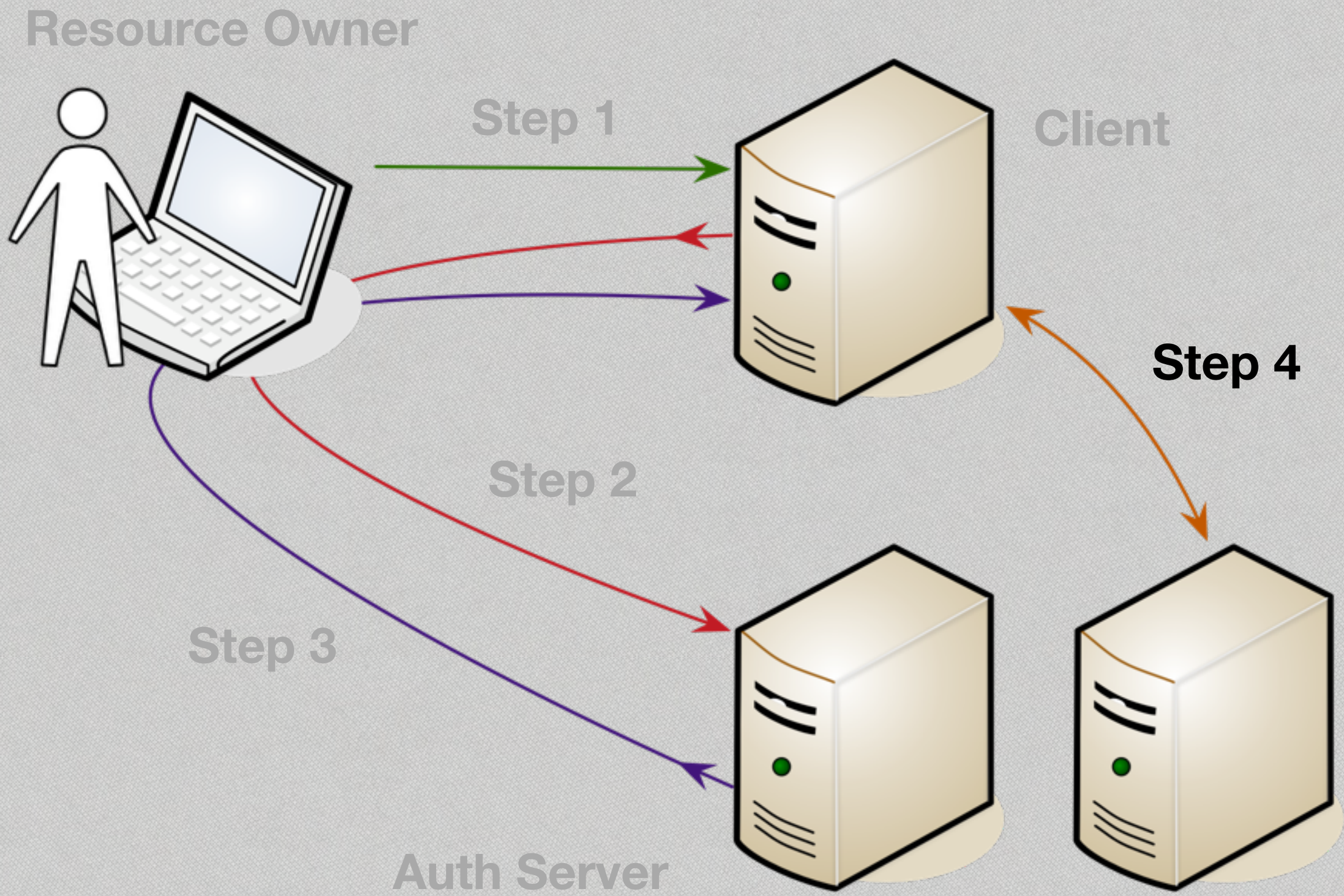
Client

Step 2

Auth Server

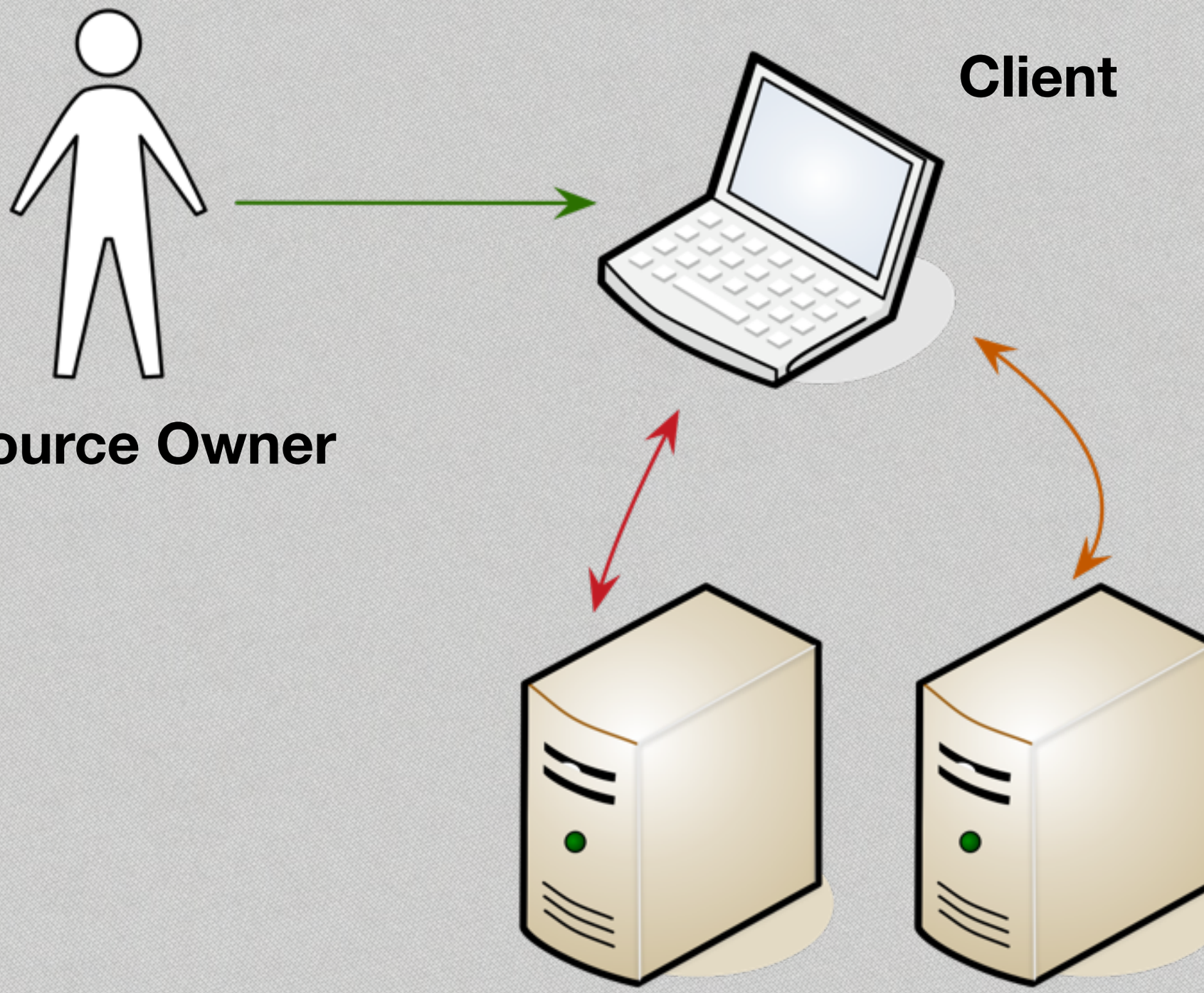
Resource Server

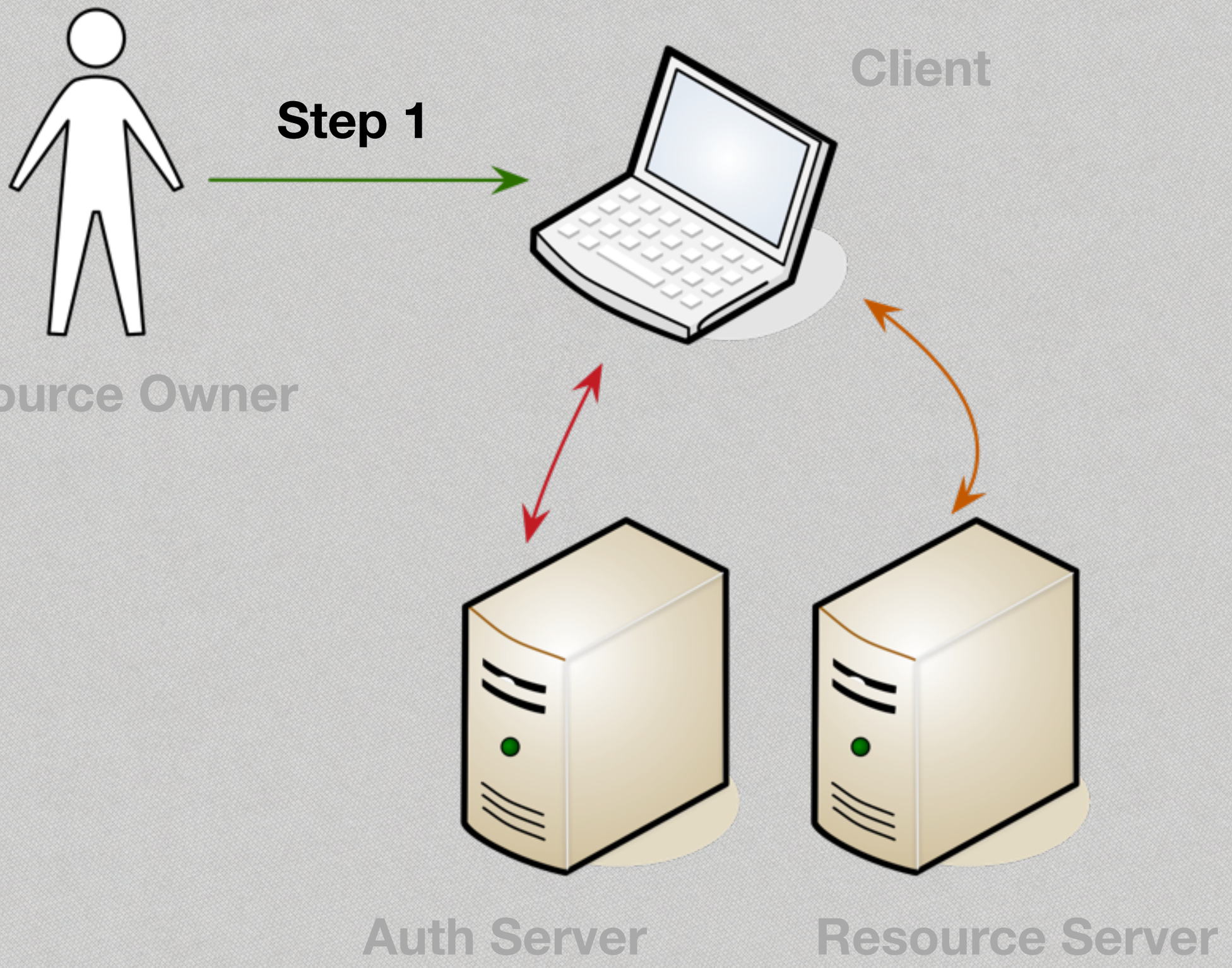

Resource Owner
Step 1
Client
Step 2
Step 3
Auth Server
Resource Server

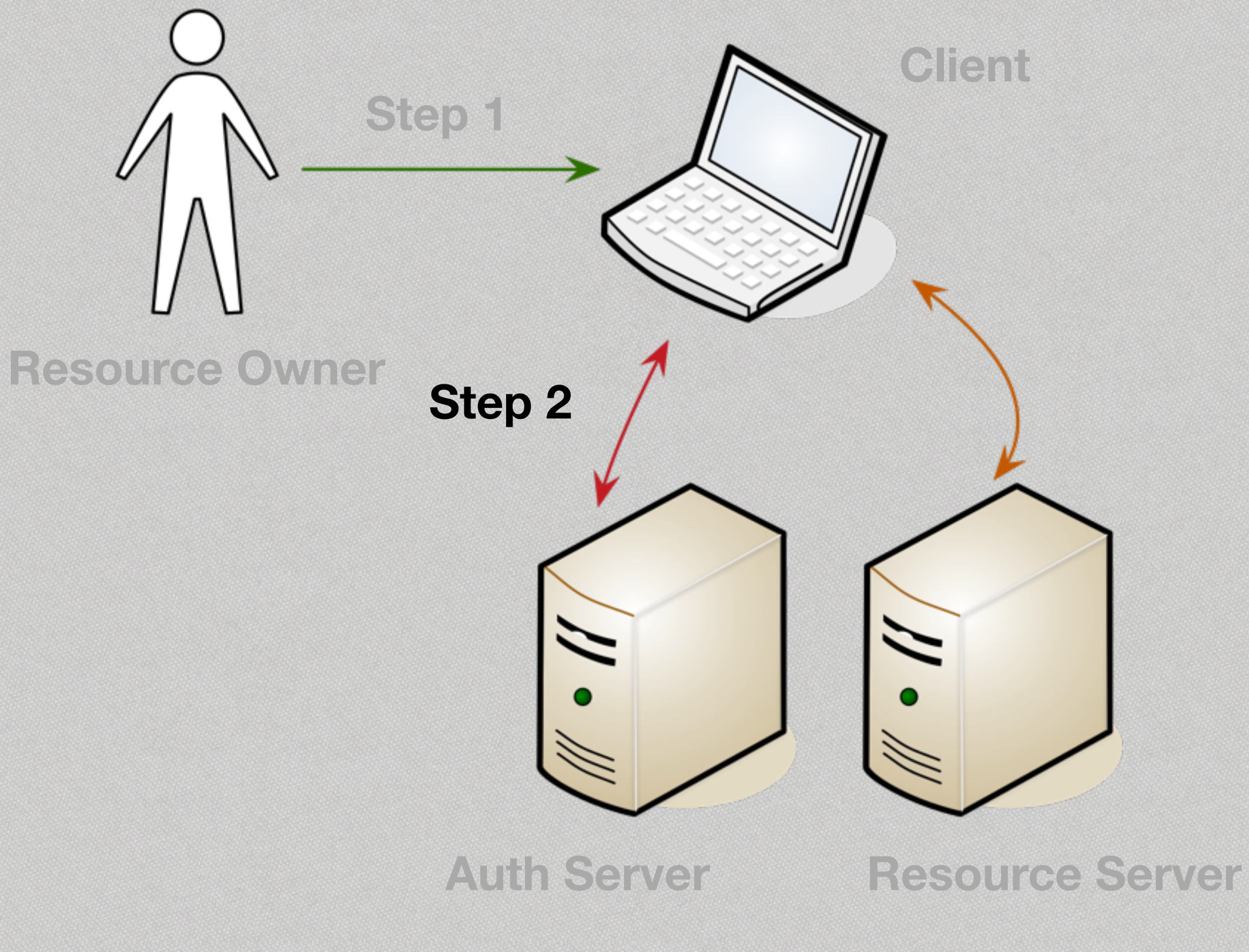

Resource Owner
Step 1
Client
Step 4
Step 2
Step 3
Auth Server
Resource Server

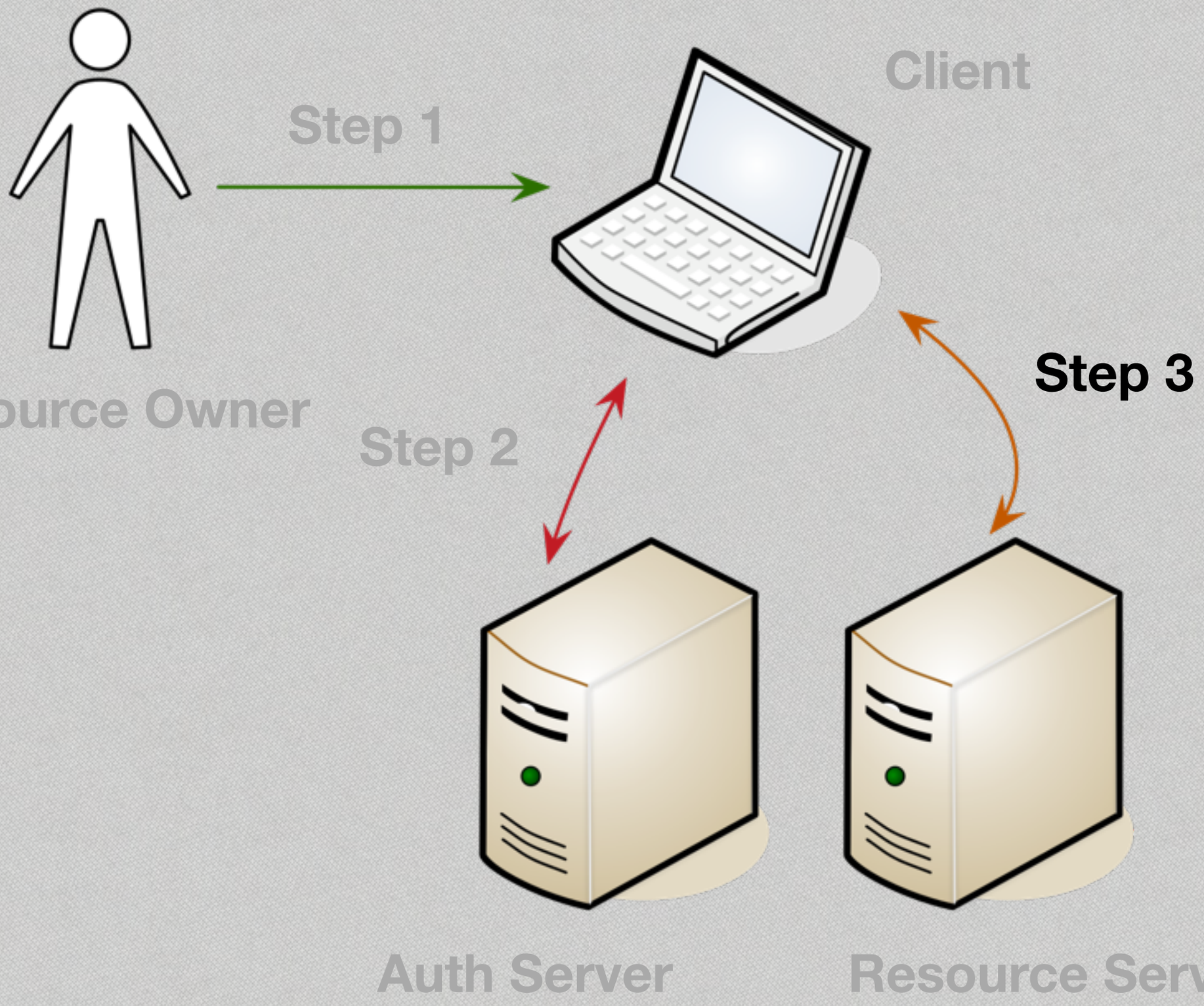
Resource Owner Password Credentials

1. Gives username and password to client
2. Client exchanges them for access token
3. Use with extreme caution


Client
Resource Owner
Auth Server
Resource Server


Step 1
Client
Resource Owner
Auth Server
Resource Server


Client
Step 1
Resource Owner
Step 2
Auth Server
Resource Server

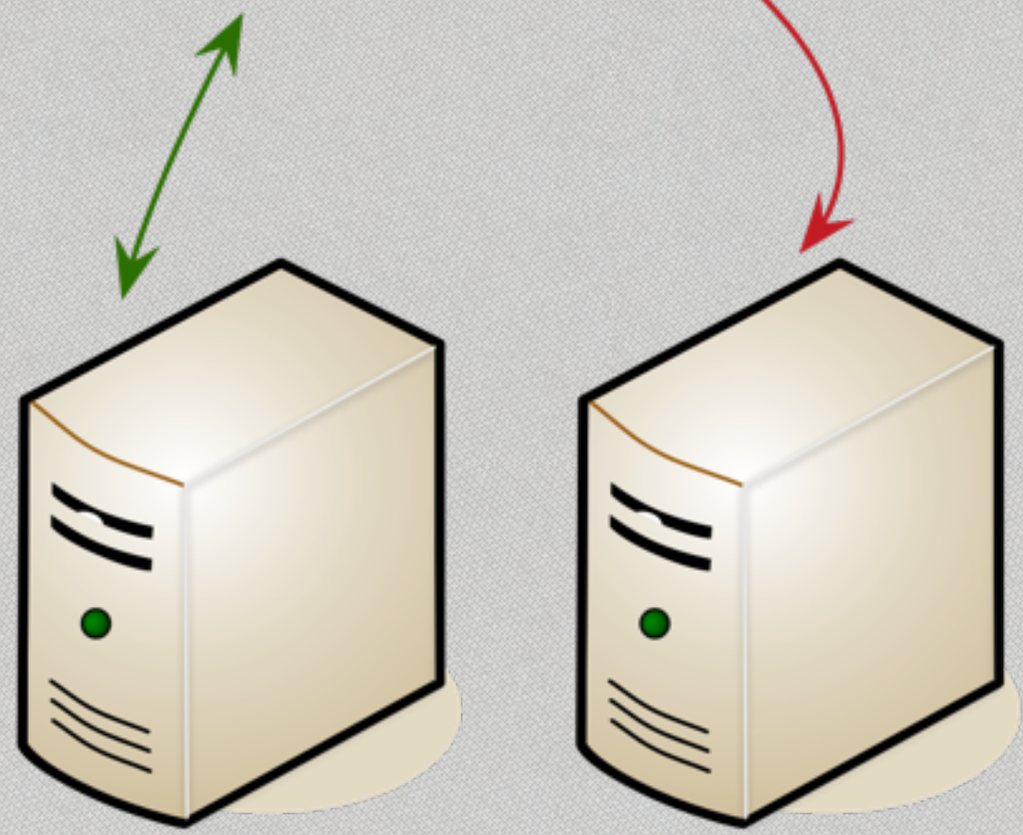

Client
Step 1
Resource Owner
Step 2
Step 3
Auth Server
Resource Server

```php
$accessToken = $provider->getAccessToken('password', [
    'username' => 'demouser',
    'password' => 'testpass'
]);
```

Client Credentials

1. Client is the resource owner
2. Credentials are stored in the client (usually safely on the server)

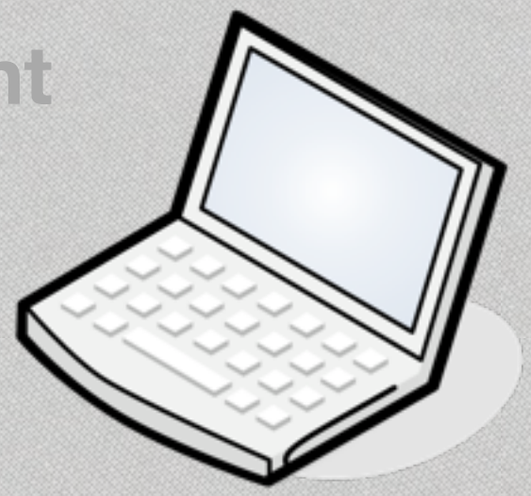
Client



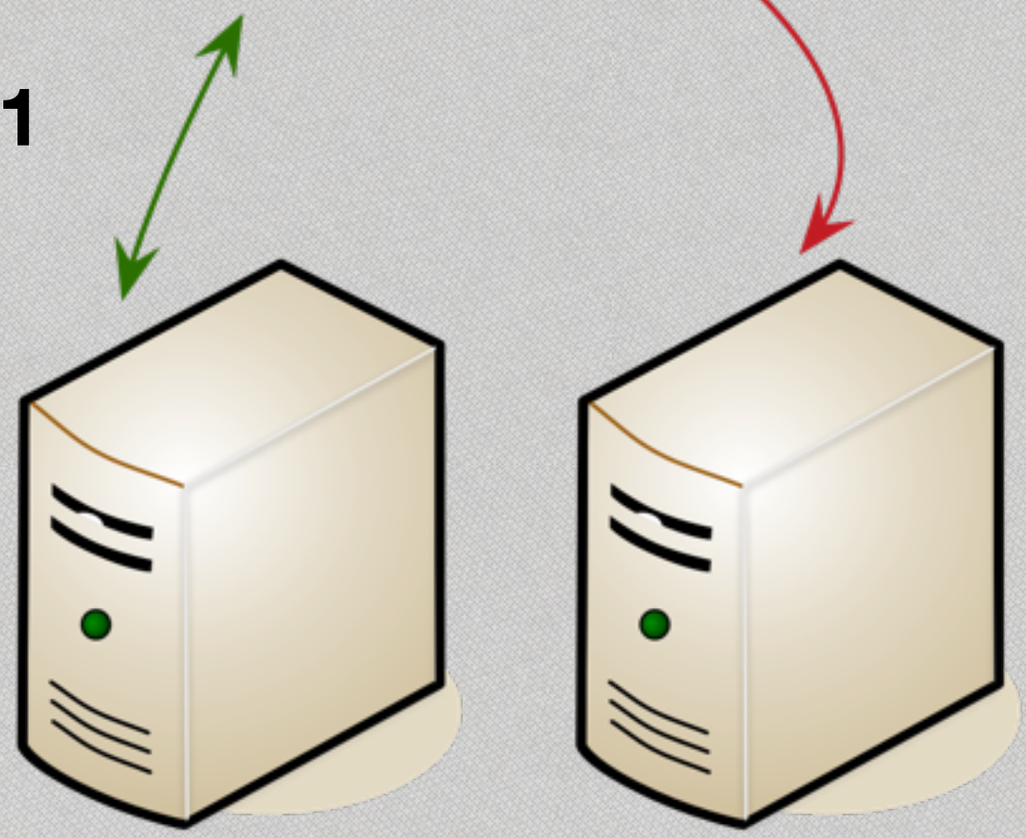
Auth Server

Resource Server

Client



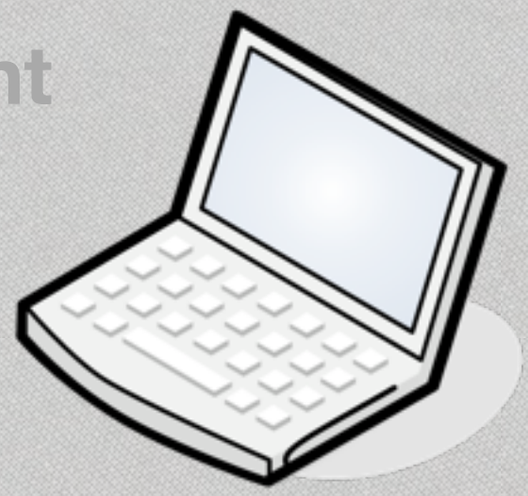
Step 1



Auth Server

Resource Server

Client



Step 1

Step 2

Auth Server

Resource Server

```php
$accessToken = $provider->getAccessToken(
    'client_credentials'
);
```

Implicit

1. Relies on client-side redirection using a client ID and a known redirection URL
2. league/oauth2-client cannot support this

Toward a More Secure Web

Next steps…

1. league/oauth2-client
2. league/oauth2-instagram
3. OAuth 2.0 with Instagram Example App
4. OAuth 2.0 specifications
5. oauth2-client provider packages
6. “Mastering OAuth 2.0” in *Web Security 2016*
7. Book: *Integrating Web Services with OAuth and PHP*

Next steps…server

league/oauth2-server

THANK YOU.
ANY QUESTIONS?

If you want to talk more, feel free to contact me.

benramsey.com

@ramsey

github.com/ramsey

ben@benramsey.com

This presentation was created using Keynote. The text is set in Chunk Five, Helvetica Neue, and Marker Felt. The source code is set in Menlo. The iconography is provided by Font Awesome.

Unless otherwise noted, all photographs are used by permission under a Creative Commons license. Please refer to the Photo Credits slide for more information.

Ramsey, Ben. “Mastering OAuth 2.0.” Day Camp 4 Developers. Web conference. 2 Jun. 2017. Conference presentation.

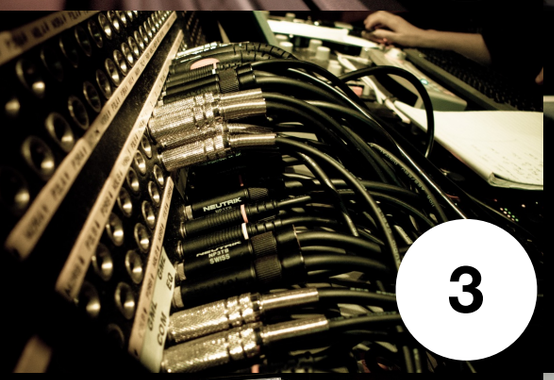


Photo Credits

1. “Untitled” by MICHΛΞL
2. “Master” by Giuditta
3. “Untitled” by MICHΛΞL
4. “Untitled” by MICHΛΞL
5. “Untitled” by MICHΛΞL
6. “master gain” by Chris Blakeley
7. “Mixing board” by Kevin Jaako