Authentication with OpenID Connect in Angular

Dr. Philippe De Ryck

https://Pragmatic Web Security.com

Dr. Philippe De Ryck

- Deep understanding of the web security landscape
- Google Developer Expert (not employed by Google)
- Course curator of the SecAppDev course (https://secappdev.org)

Pragmatic Web Security

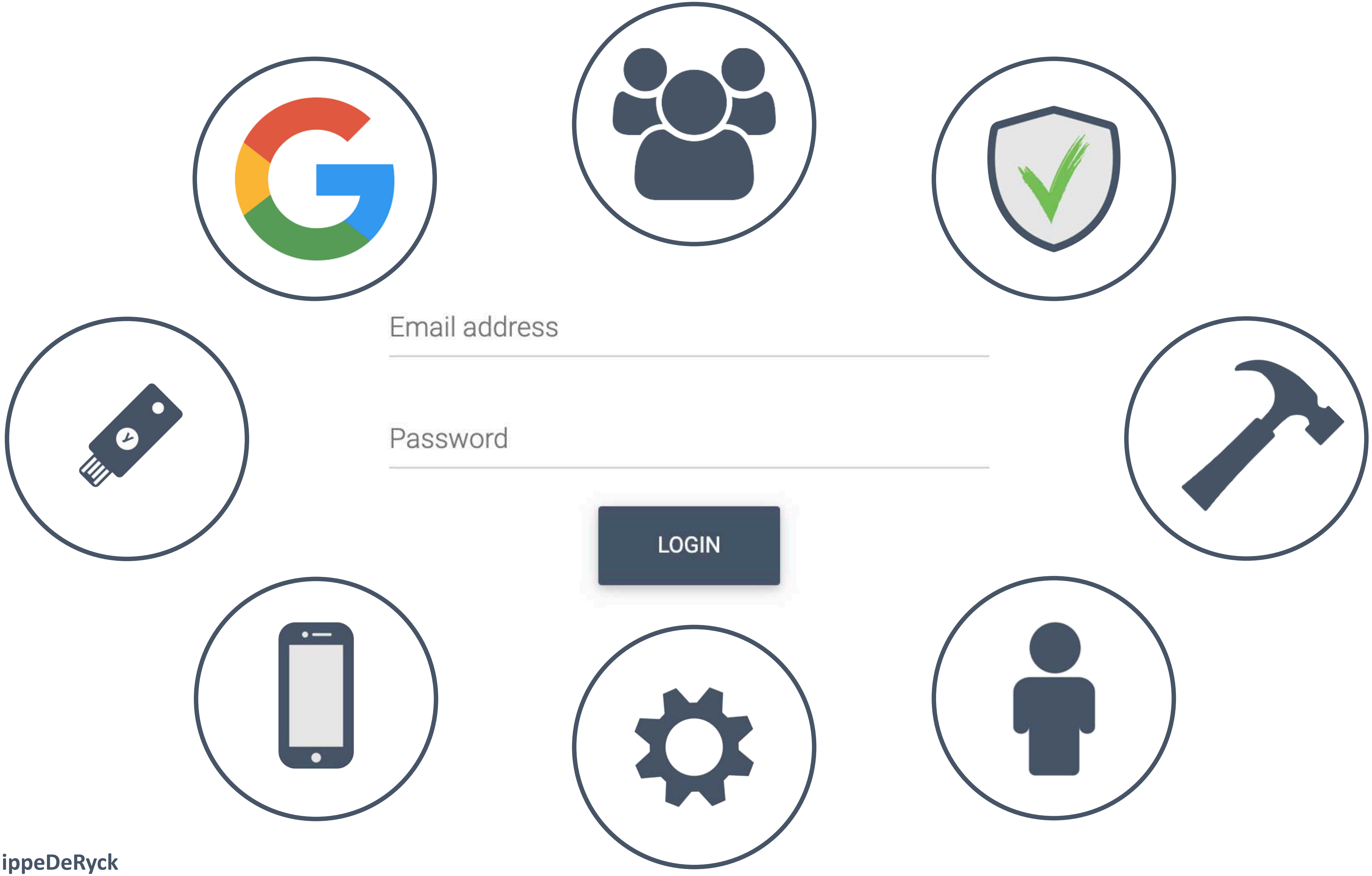
High-quality security training for developers and managers

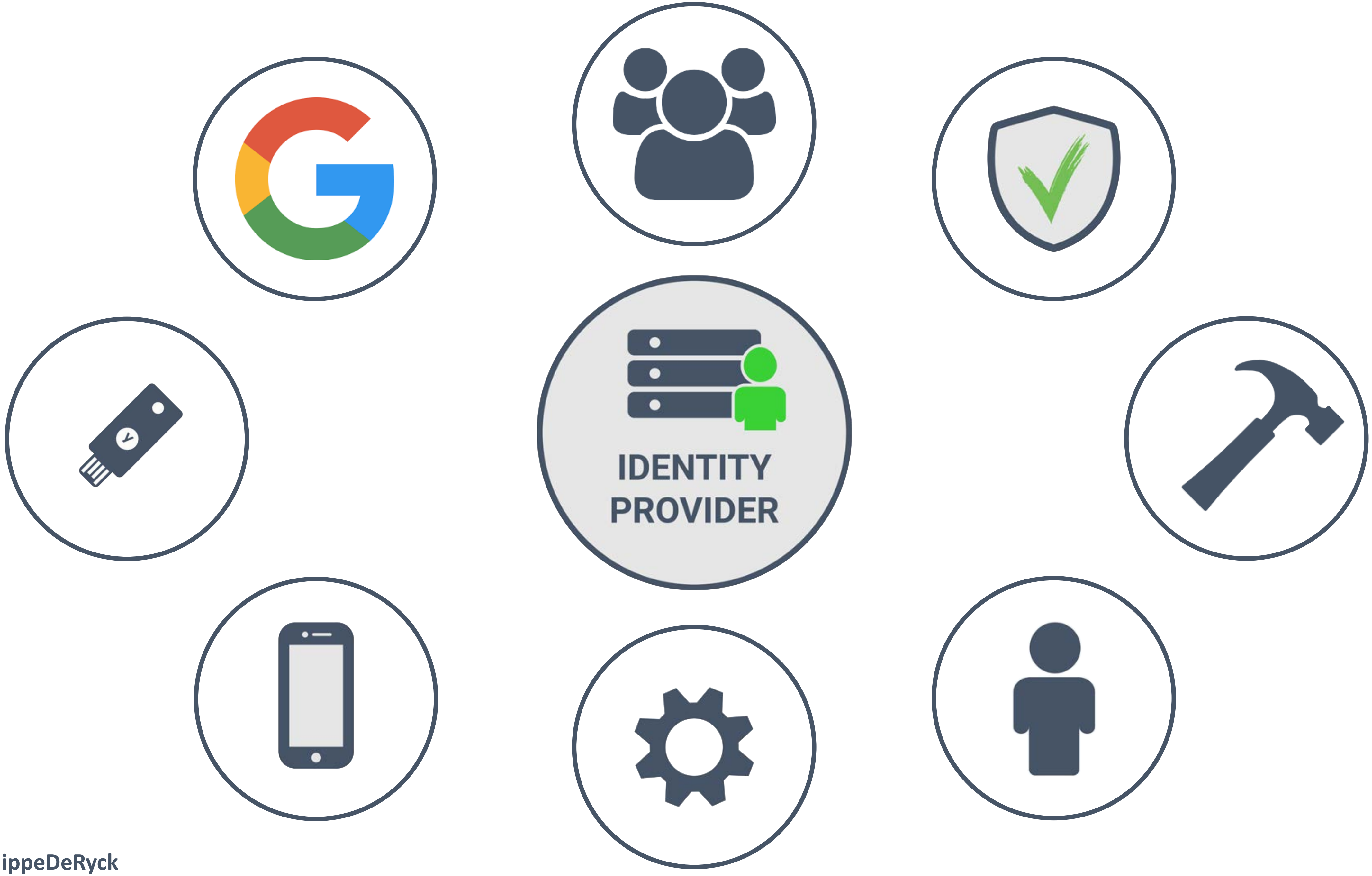
Custom courses covering web security, API security, Angular security, …

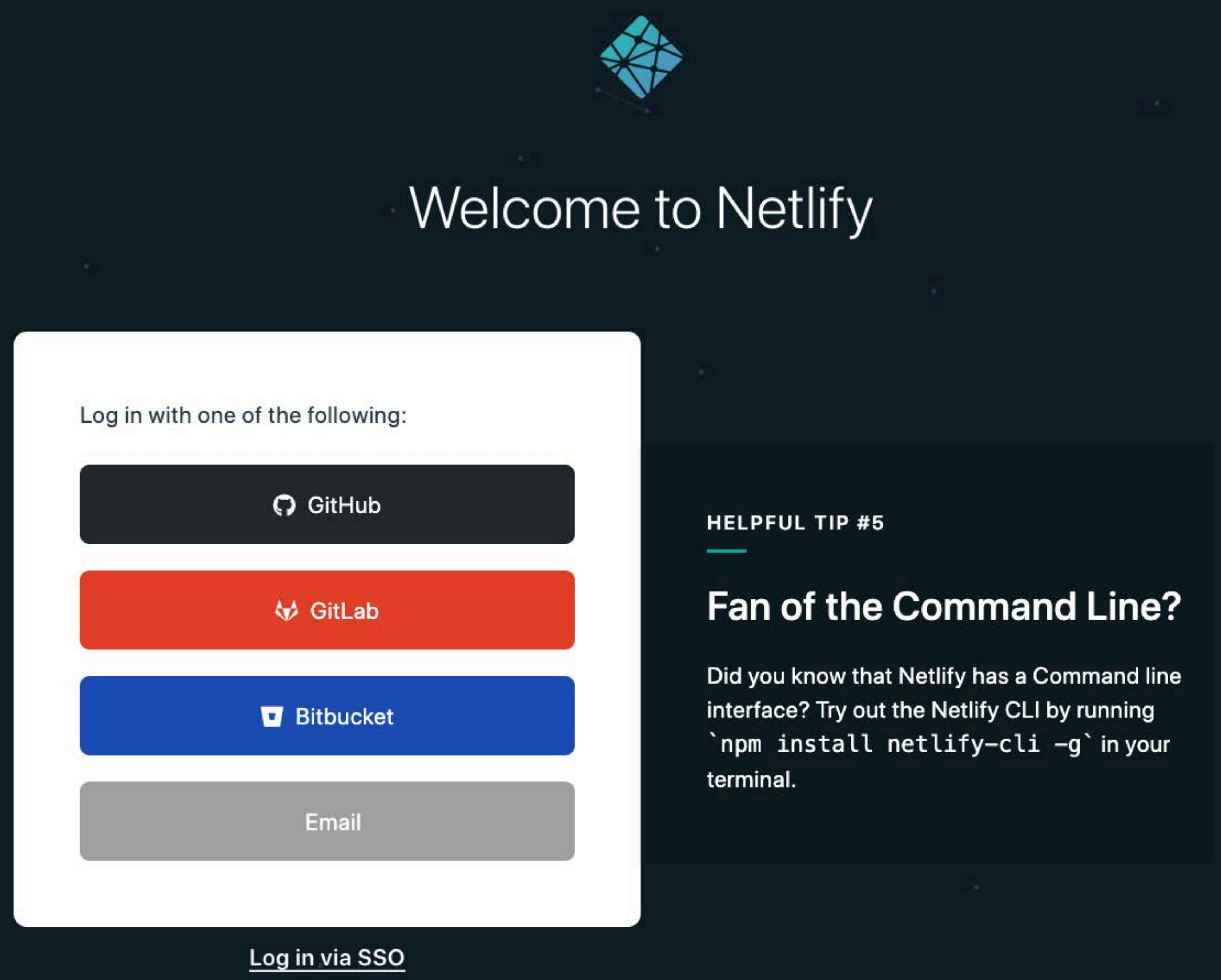
Consulting services on security, OAuth 2.0, OpenID Connect, …

@PhilippeDeRyck

https://PragmaticWebSecurity.com


Email address
Password
LOGIN


IDENTITY PROVIDER



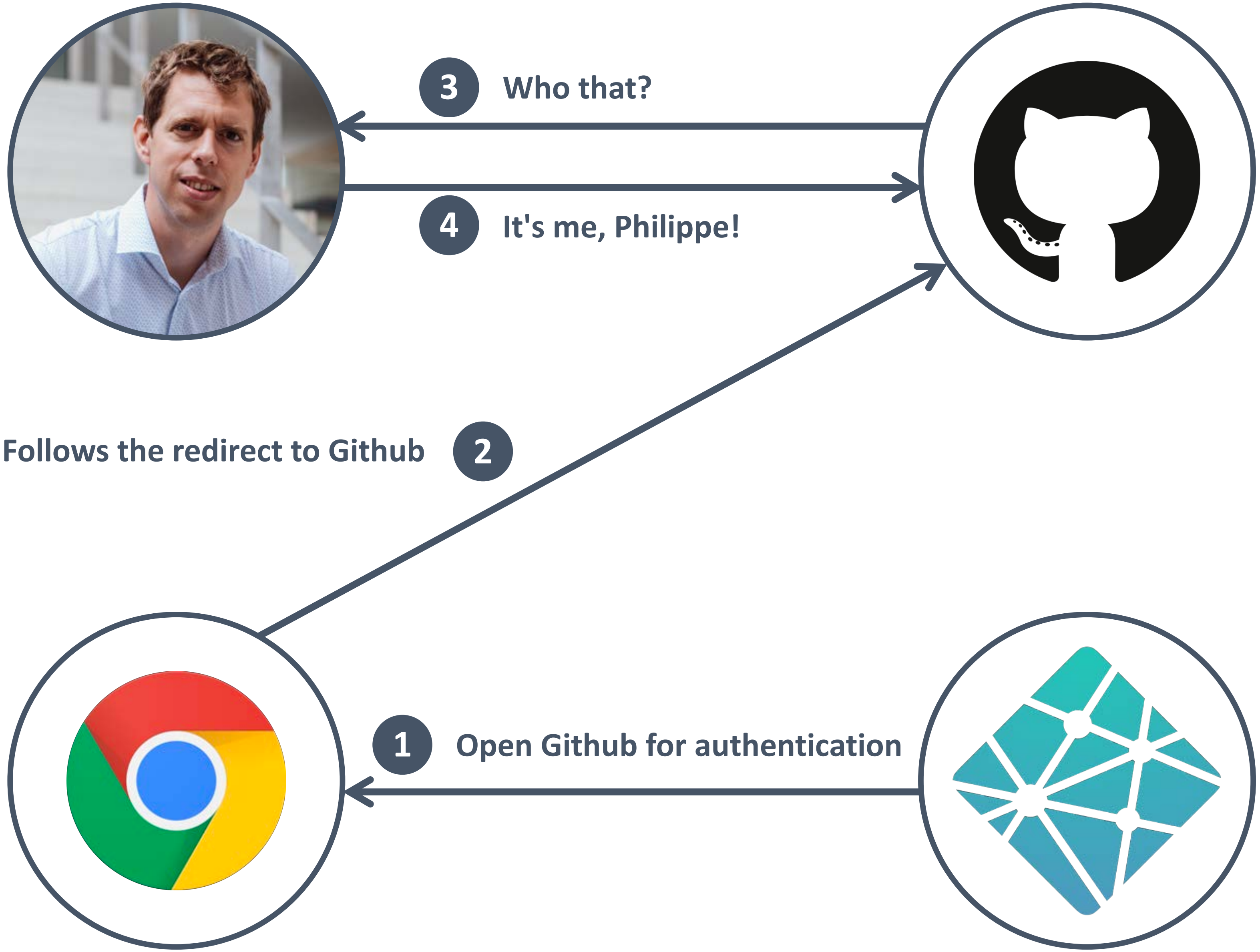
Welcome to Netlify

Log in with one of the following:

HELPFUL TIP #5

Fan of the Command Line?

Did you know that Netlify has a Command line interface? Try out the Netlify CLI by running `npm install netlify-cli -g` in your terminal.

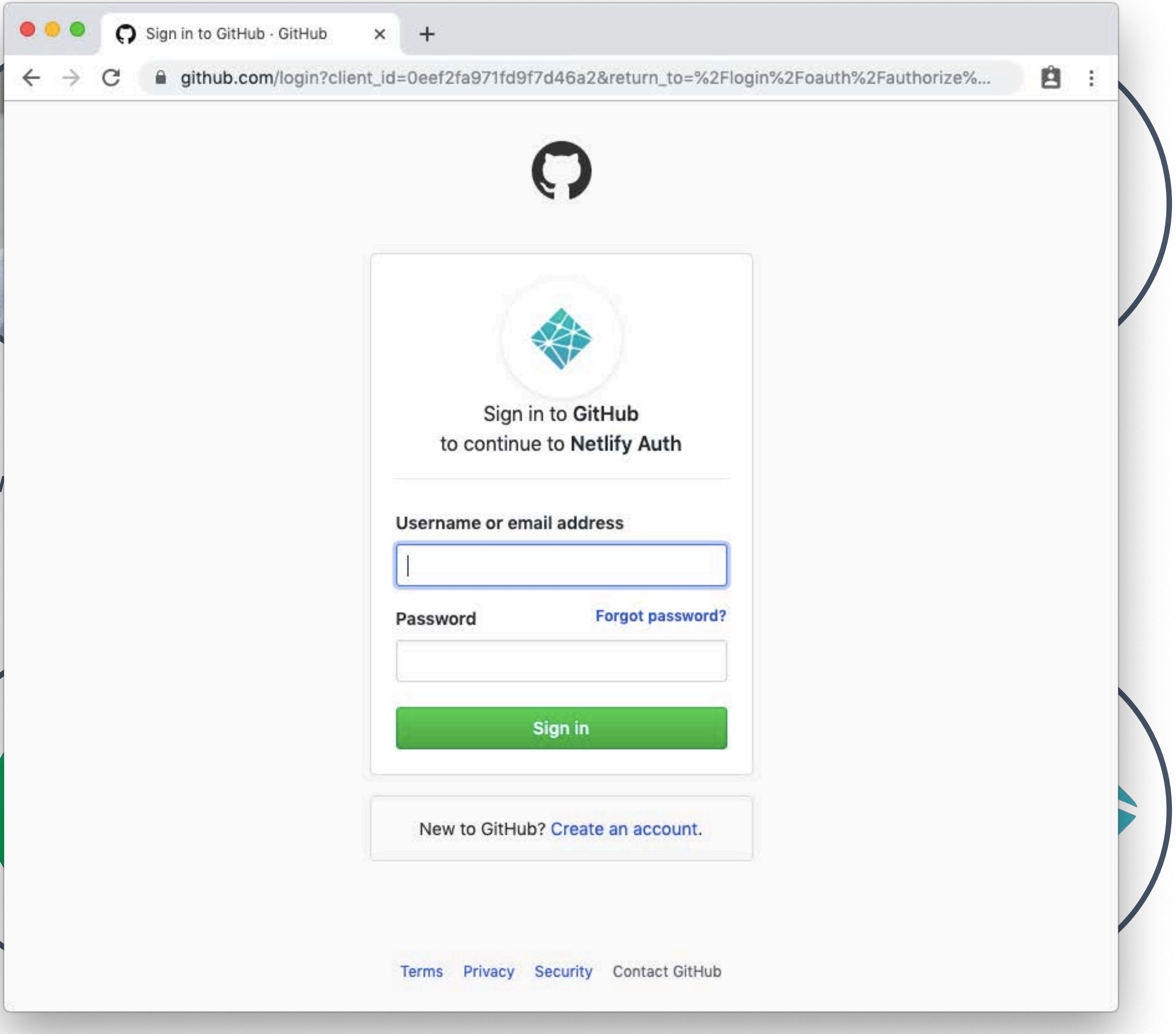


3 Who that?

4 It's me, Philippe!

Follows the redirect to Github 2

1 Open Github for authentication



Sign in to GitHub · GitHub

github.com/login?client_id=0eef2fa971fd9f7d46a2&return_to=%2Flogin%2Foauth%2Fauthorize%...

Sign in to **GitHub**
to continue to **Netlify Auth**

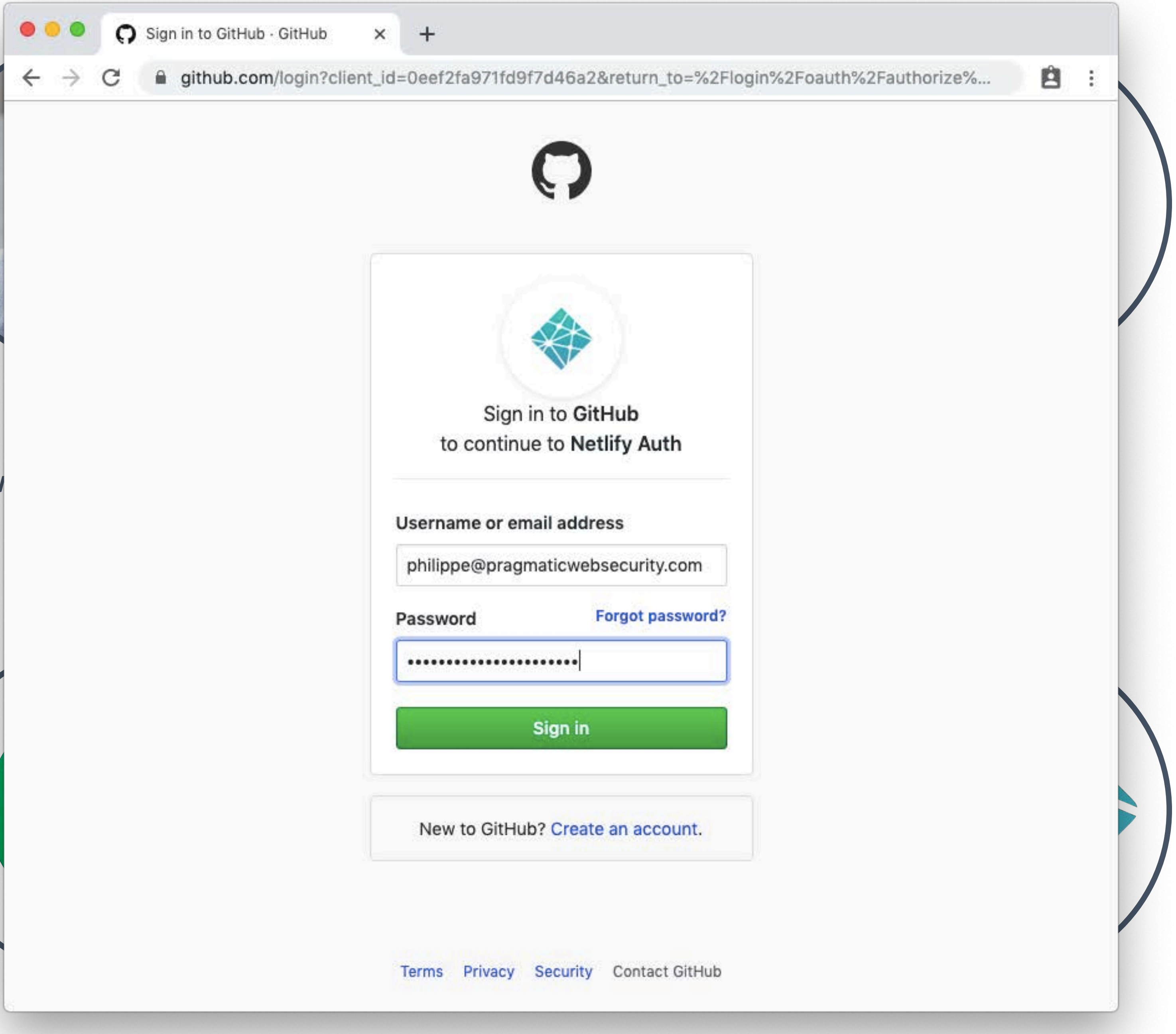
Username or email address

Password **Forgot password?**

New to GitHub? Create an account.

Follov

Follov



Sign in to GitHub · GitHub

github.com/login?client_id=0eef2fa971fd9f7d46a2&return_to=%2Flogin%2Foauth%2Fauthorize%...

Sign in to **GitHub**
to continue to **Netlify Auth**

Username or email address

philippe@pragmaticwebsecurity.com

Password **Forgot password?**

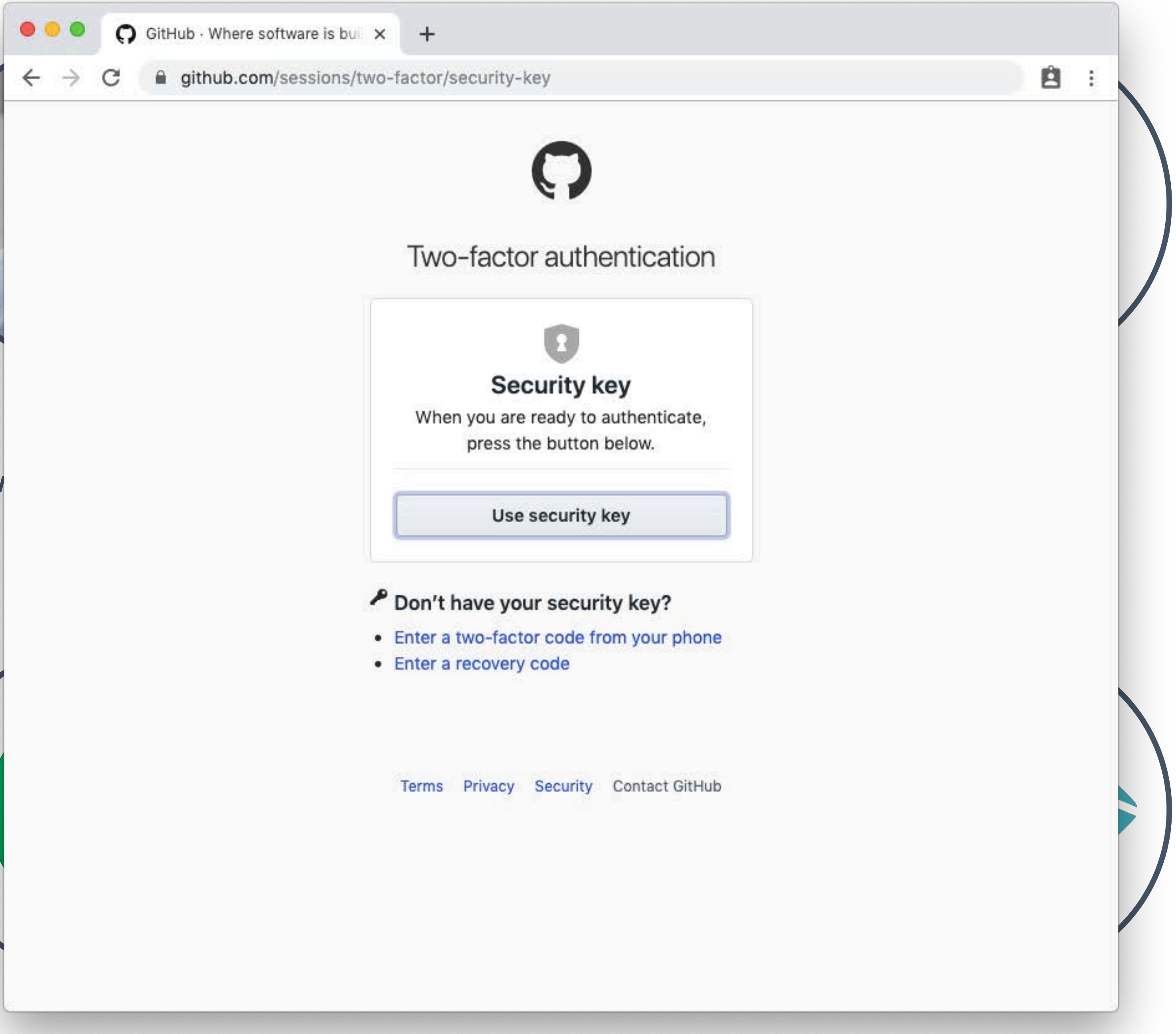
••••••••••••••••••••••

Sign in

New to GitHub? Create an account.

Terms Privacy Security Contact GitHub

Follov



GitHub · Where software is bui
github.com/sessions/two-factor/security-key

Two-factor authentication

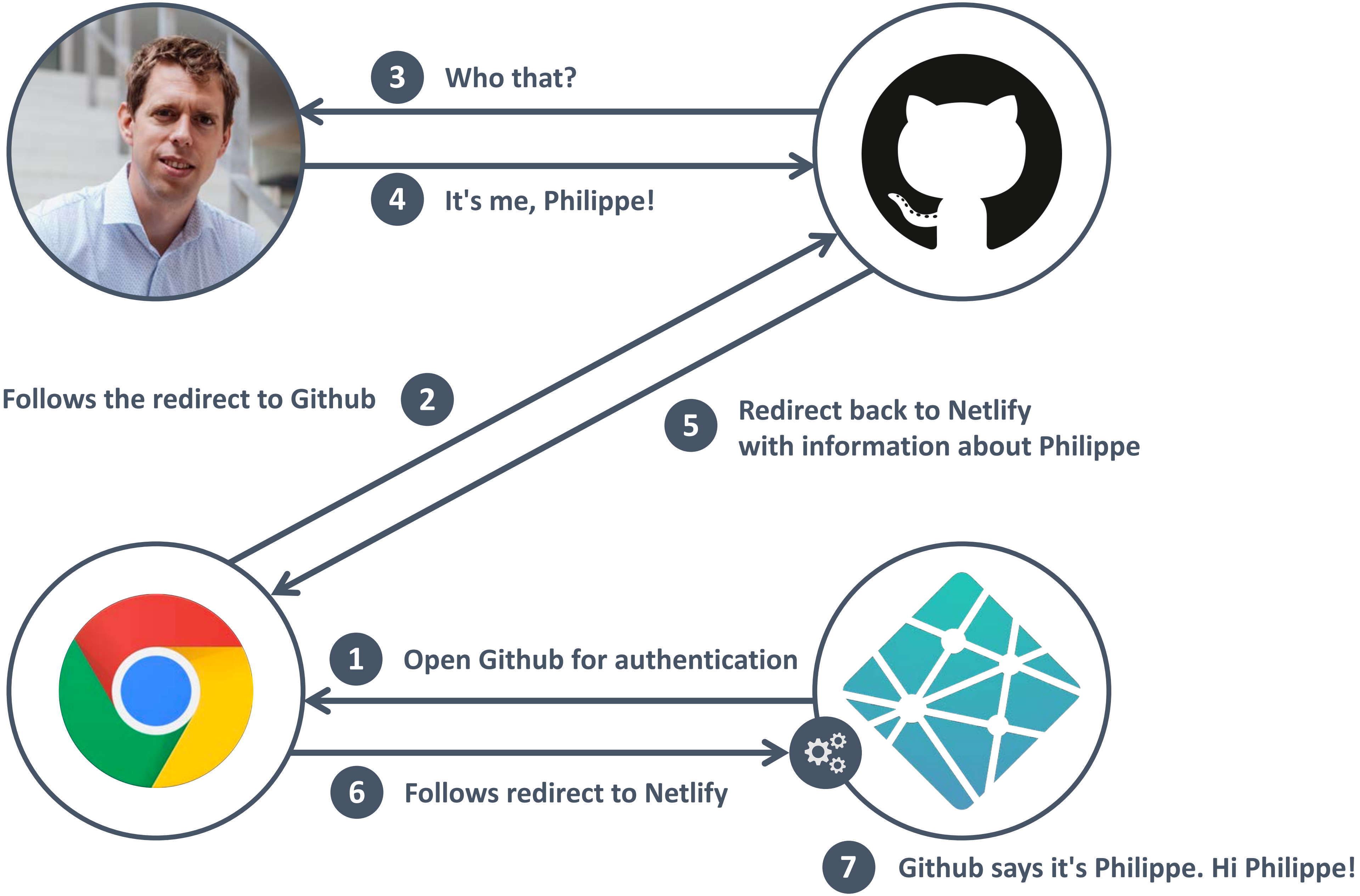
Security key

When you are ready to authenticate, press the button below.

Don't have your security key?

- Enter a two-factor code from your phone
- Enter a recovery code

Terms
Privacy
Security
Contact GitHub



3 Who that?

4 It's me, Philippe!

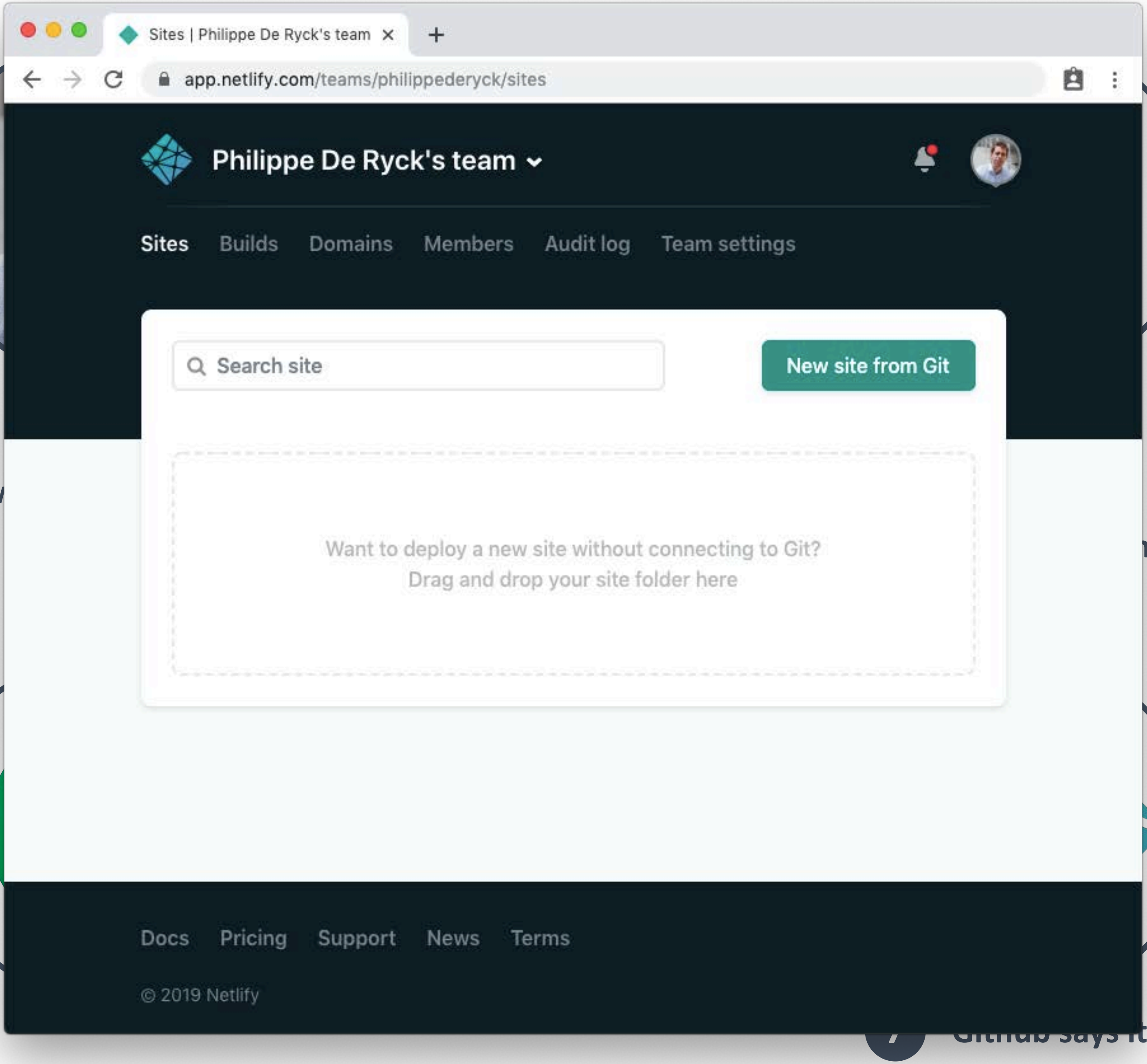
Follows the redirect to Github 2

5 Redirect back to Netlify
with information about Philippe

1 Open Github for authentication

6 Follows redirect to Netlify

7 Github says it's Philippe. Hi Philippe!

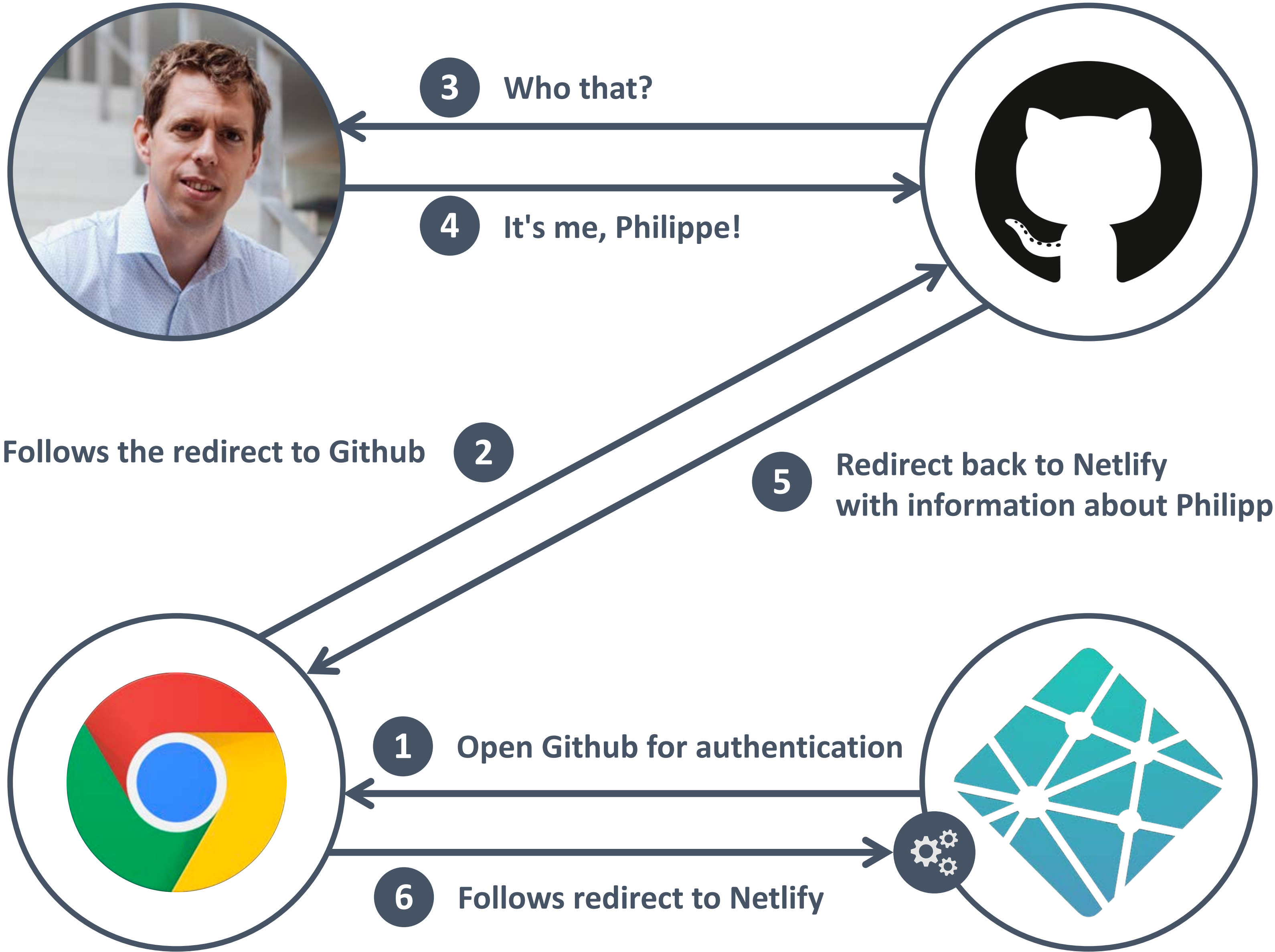


Want to deploy a new site without connecting to Git?
Drag and drop your site folder here

Follov

hilippe

Github says it's Philippe. Hi Philippe!



3 Who that?

4 It's me, Philippe!

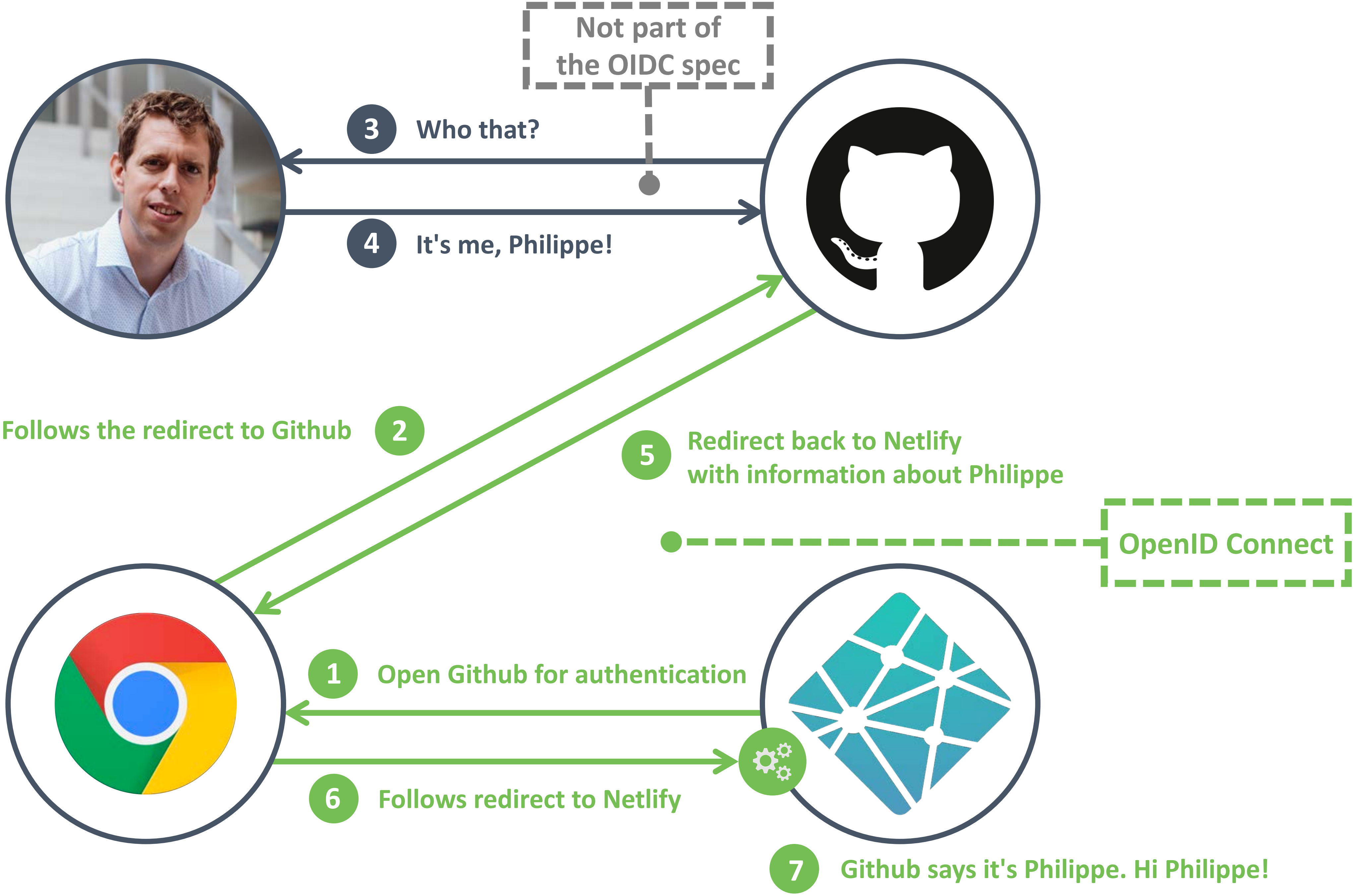
Follows the redirect to Github 2

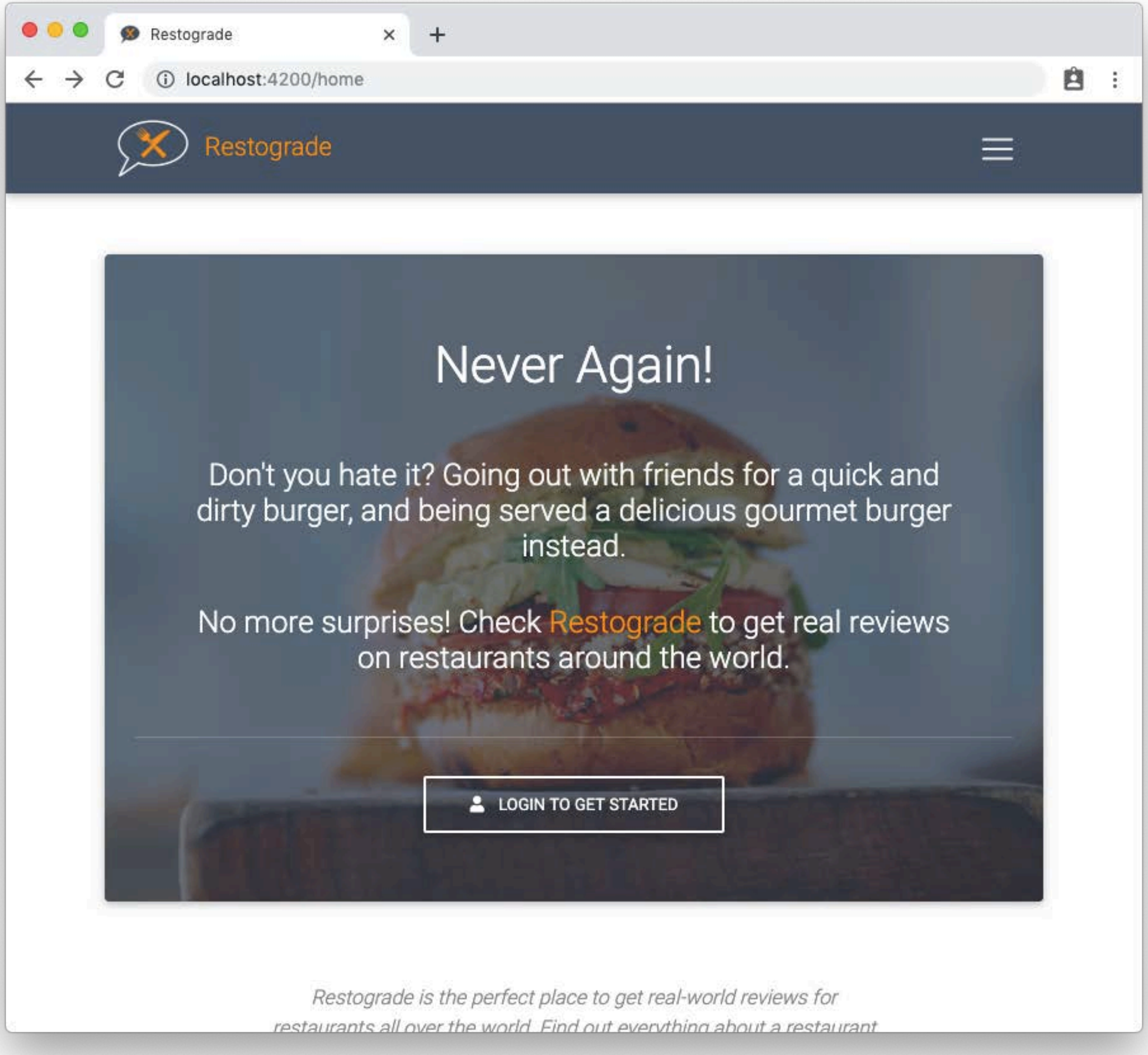
5 Redirect back to Netlify
with information about Philippe

1 Open Github for authentication

6 Follows redirect to Netlify

7 Github says it's Philippe. Hi Philippe!


Not part of the OIDC spec
3 Who that?
4 It's me, Philippe!
Follows the redirect to Github 2
5 Redirect back to Netlify with information about Philippe
OpenID Connect
1 Open Github for authentication
6 Follows redirect to Netlify
7 Github says it's Philippe. Hi Philippe!

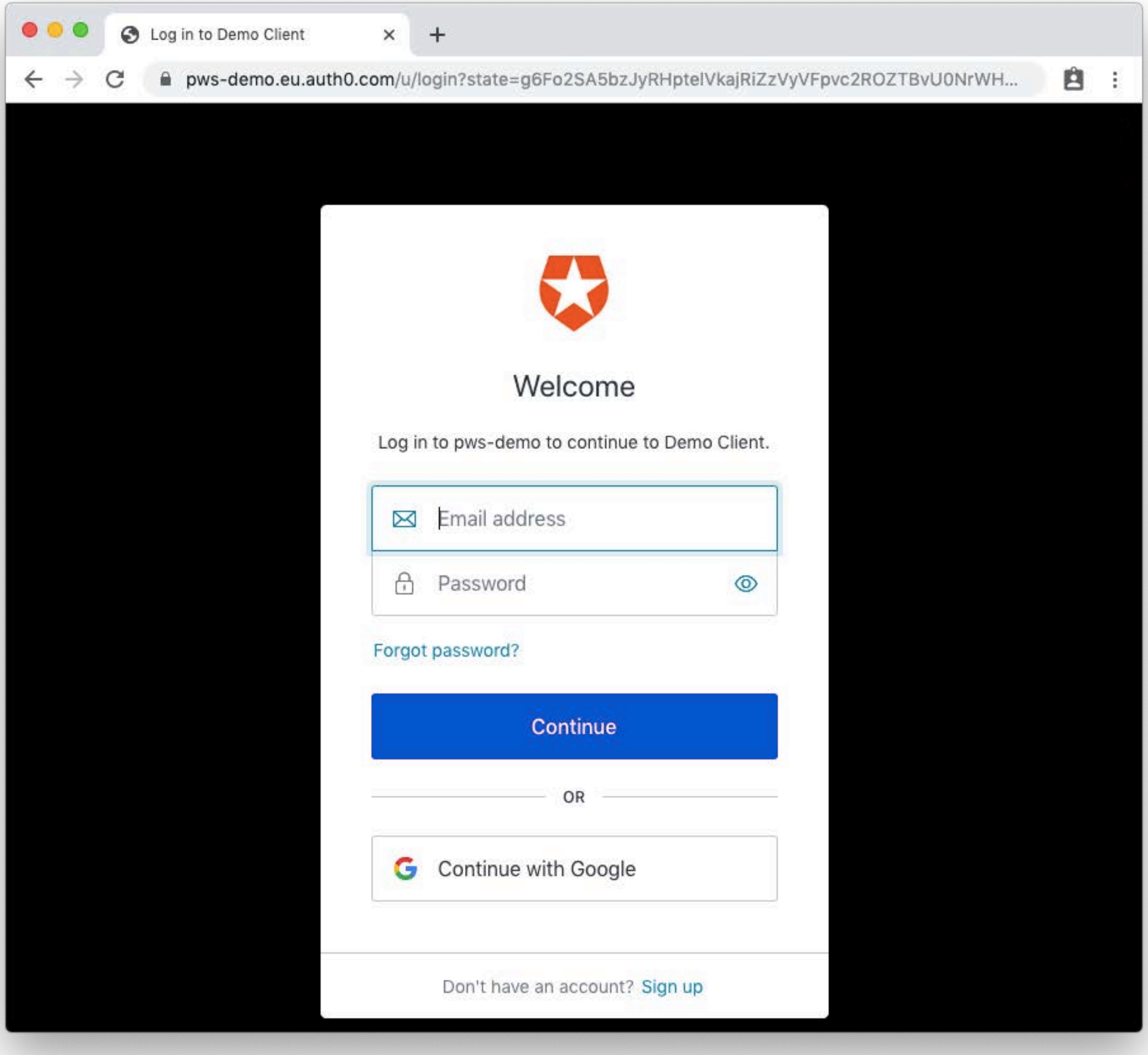


Never Again!

Don't you hate it? Going out with friends for a quick and dirty burger, and being served a delicious gourmet burger instead.

No more surprises! Check Restograde to get real reviews on restaurants around the world.

Restograde is the perfect place to get real-world reviews for restaurants all over the world. Find out everything about a restaurant

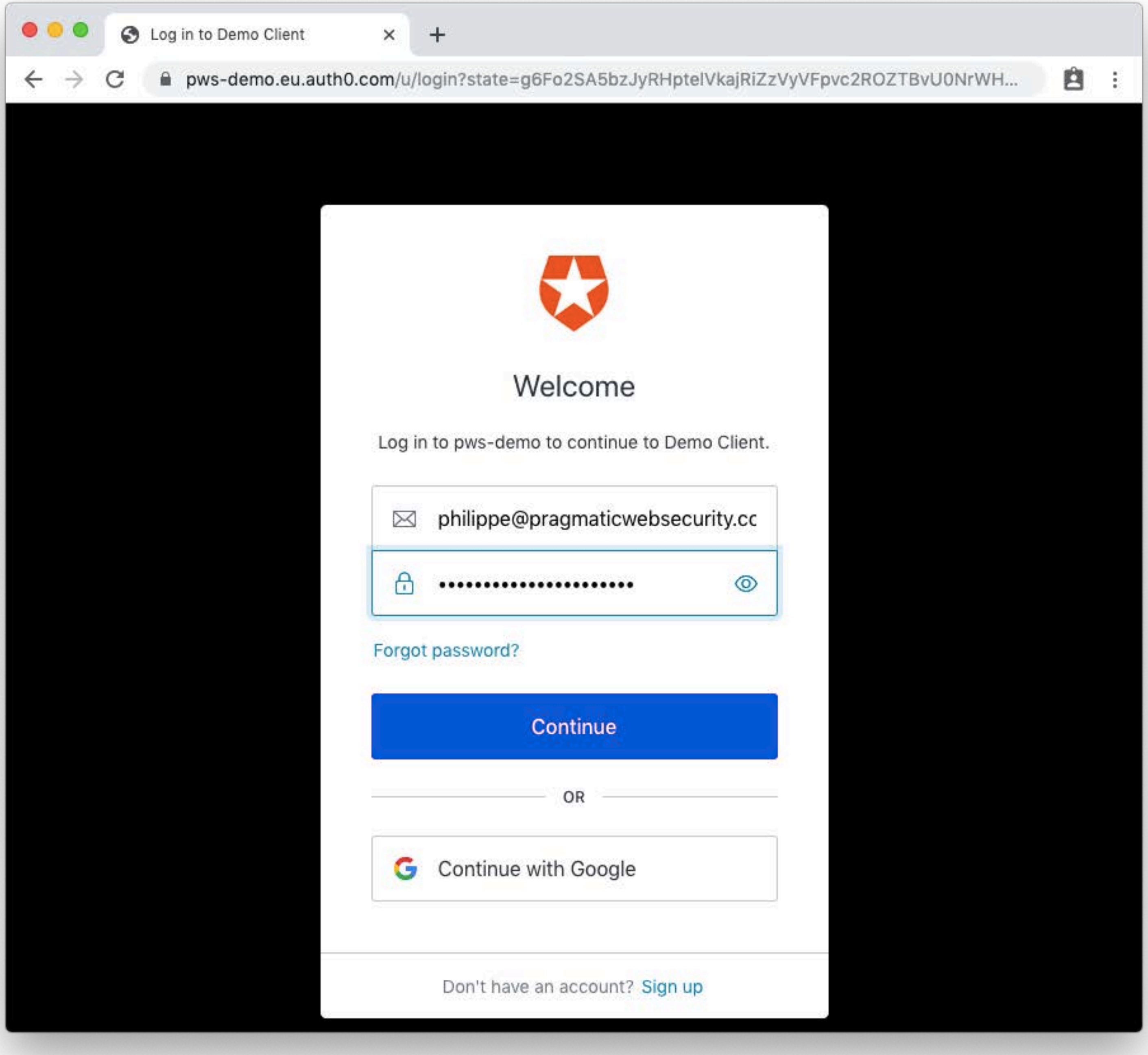


Log in to Demo Client
pws-demo.eu.auth0.com/u/login?state=g6Fo2SA5bzJyRHptelVkajRiZzVyVFpvc2ROZTBvU0NrWH...

Welcome

Log in to pws-demo to continue to Demo Client.

Email address
Password
Forgot password?
Continue
OR
Continue with Google
Don't have an account? Sign up



Log in to Demo Client

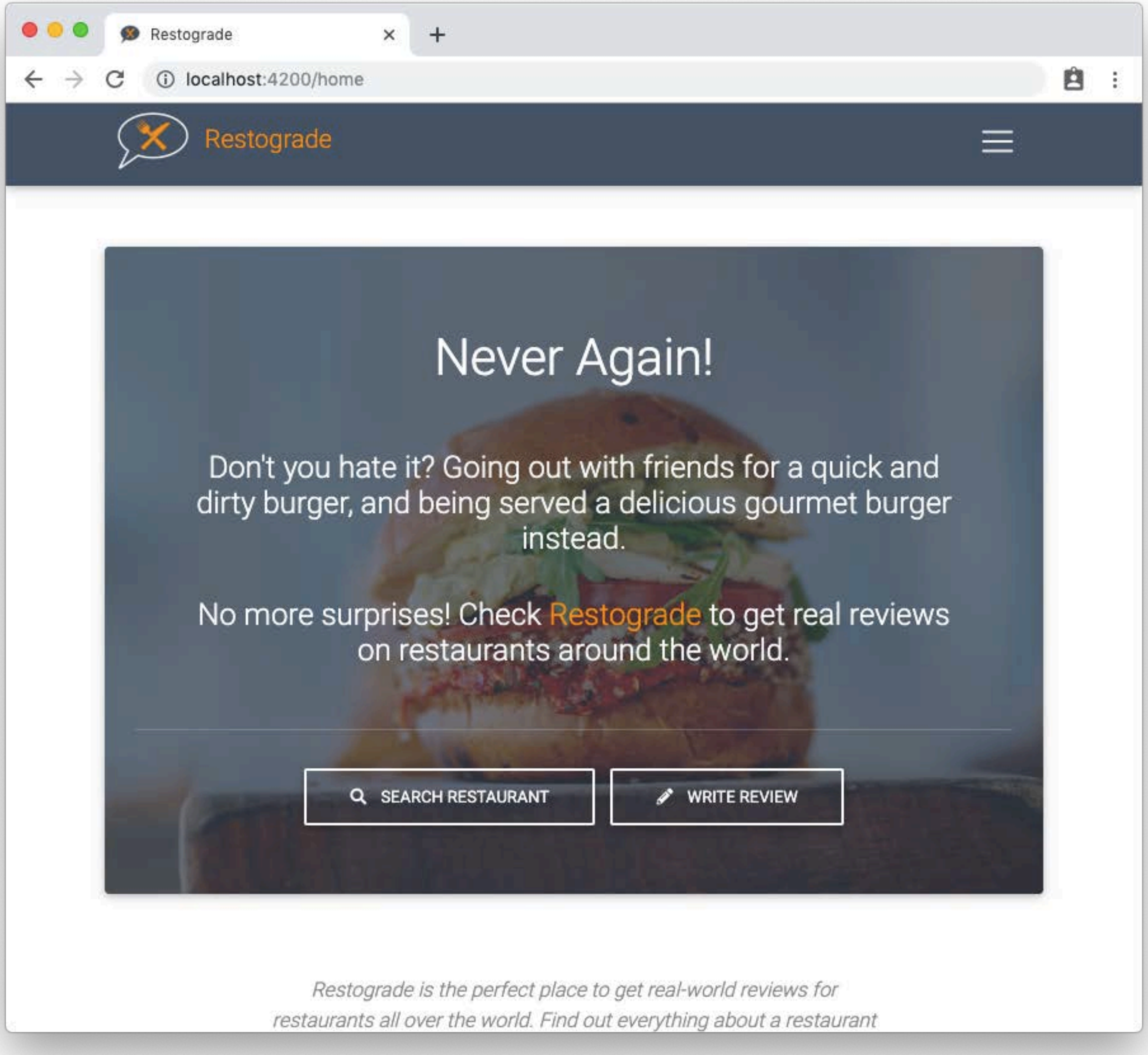
pws-demo.eu.auth0.com/u/login?state=g6Fo2SA5bzJyRHptelVkajRiZzVyVFpvc2ROZTBvU0NrWH...

Welcome

Log in to pws-demo to continue to Demo Client.

philippe@pragmaticwebsecurity.cc

••••••••••••••••••••••

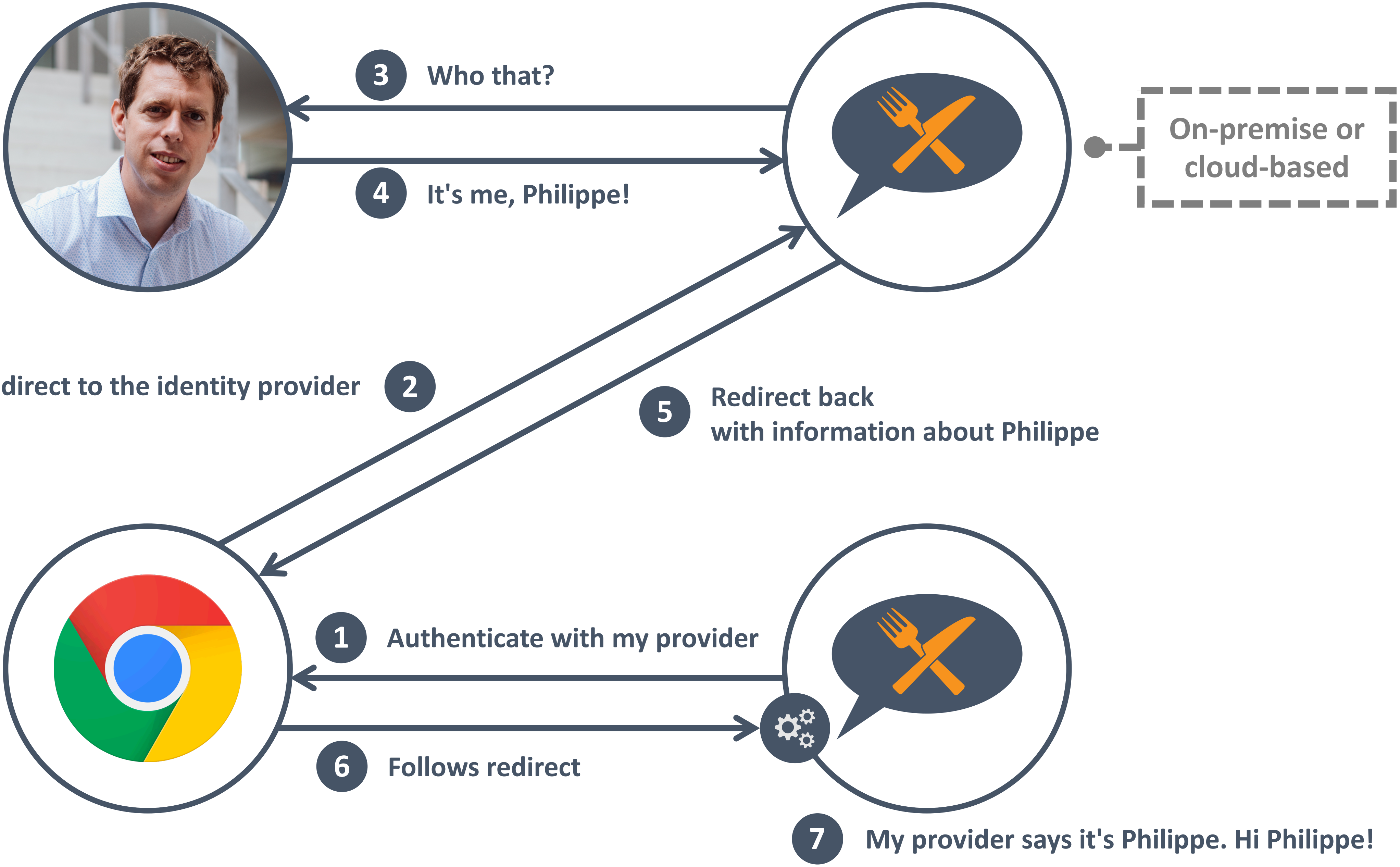


Never Again!

Don't you hate it? Going out with friends for a quick and dirty burger, and being served a delicious gourmet burger instead.

No more surprises! Check Restograde to get real reviews on restaurants around the world.

Restograde is the perfect place to get real-world reviews for restaurants all over the world. Find out everything about a restaurant



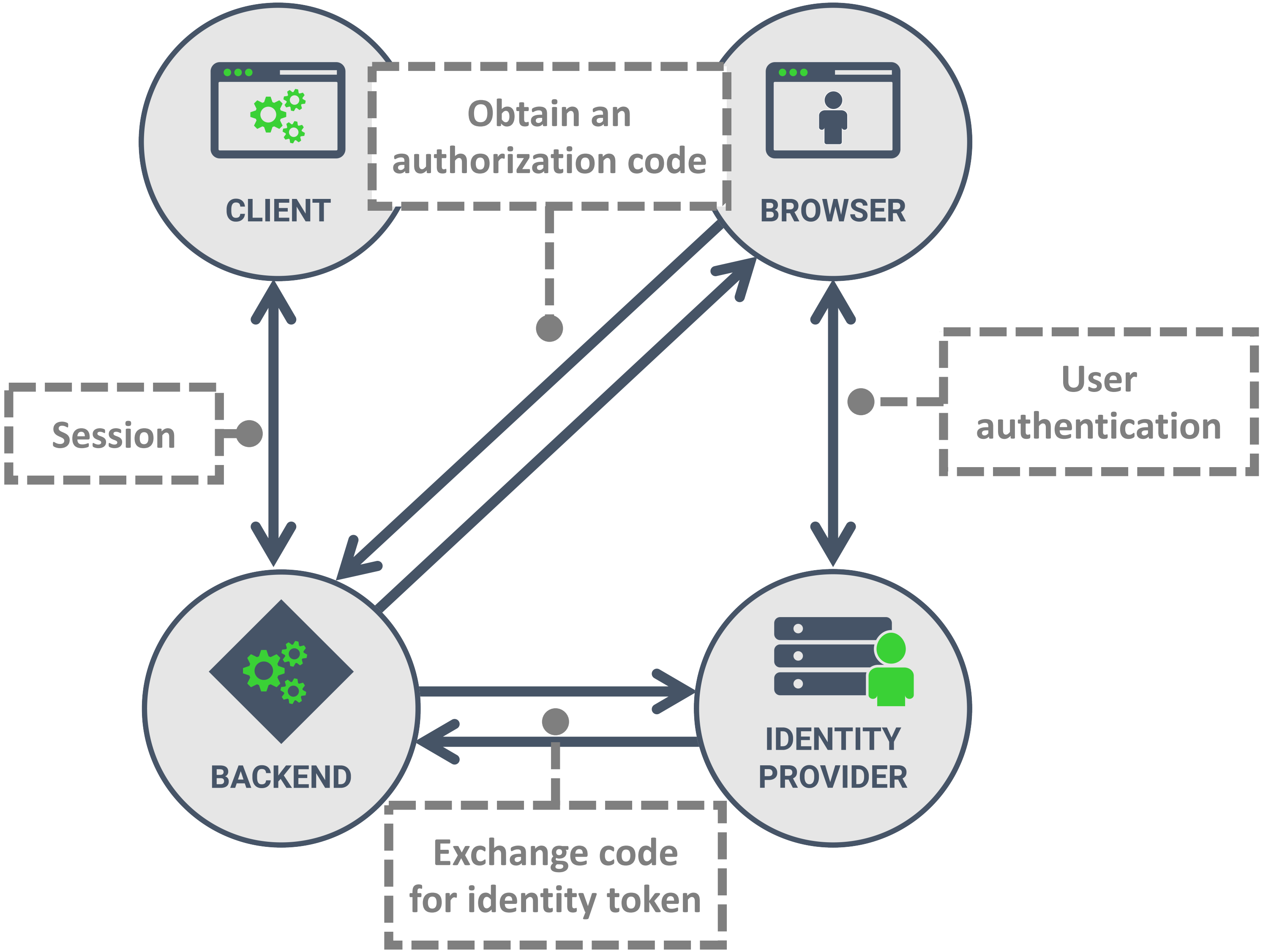
3 Who that?
4 It's me, Philippe!
On-premise or cloud-based
Follows the redirect to the identity provider 2
5 Redirect back with information about Philippe
1 Authenticate with my provider
6 Follows redirect
7 My provider says it's Philippe. Hi Philippe!

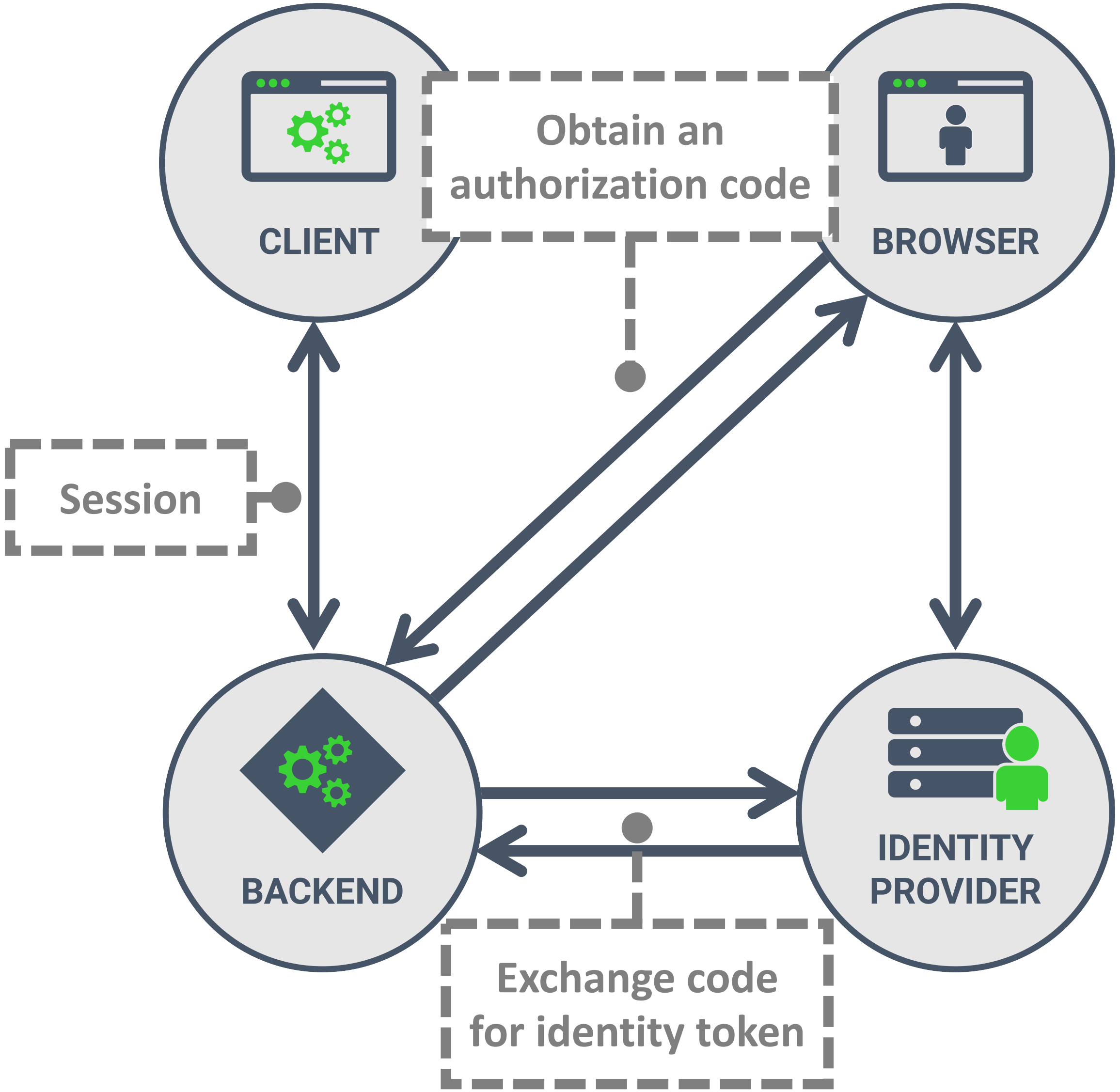
Delegate authentication with OpenID Connect

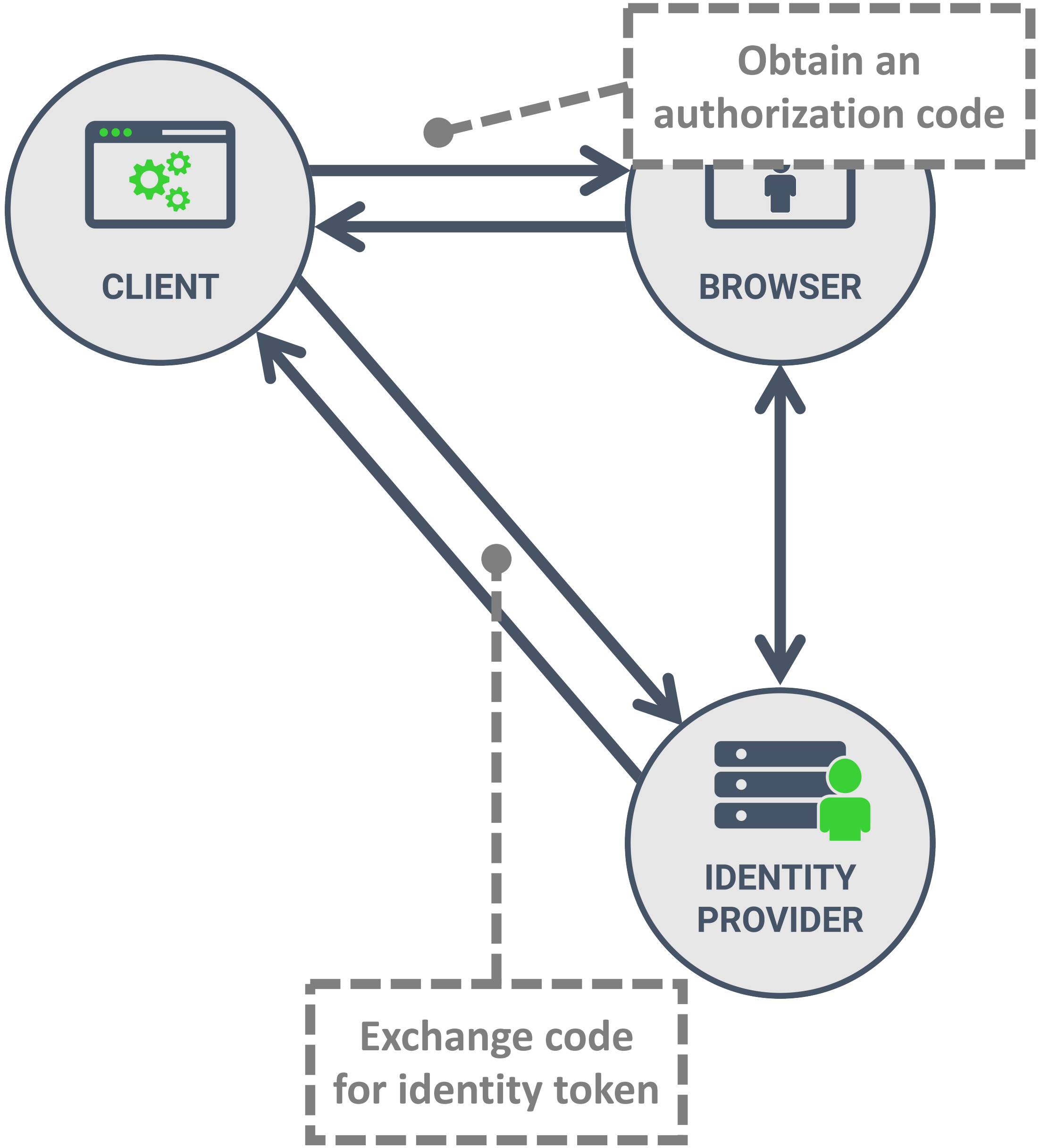
Building a secure custom authentication mechanism is hard

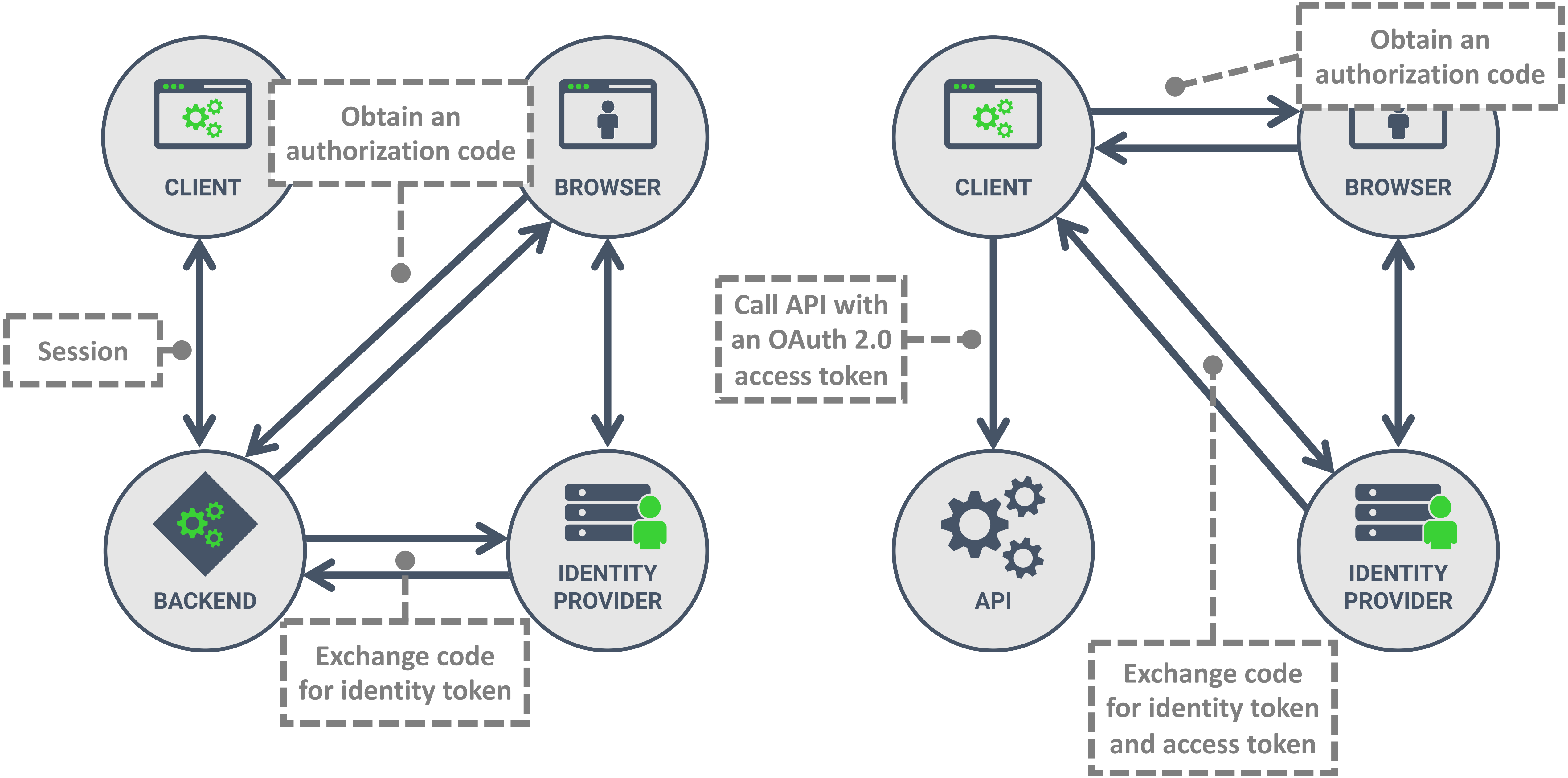
Identity providers are specialized in managing & authenticating users

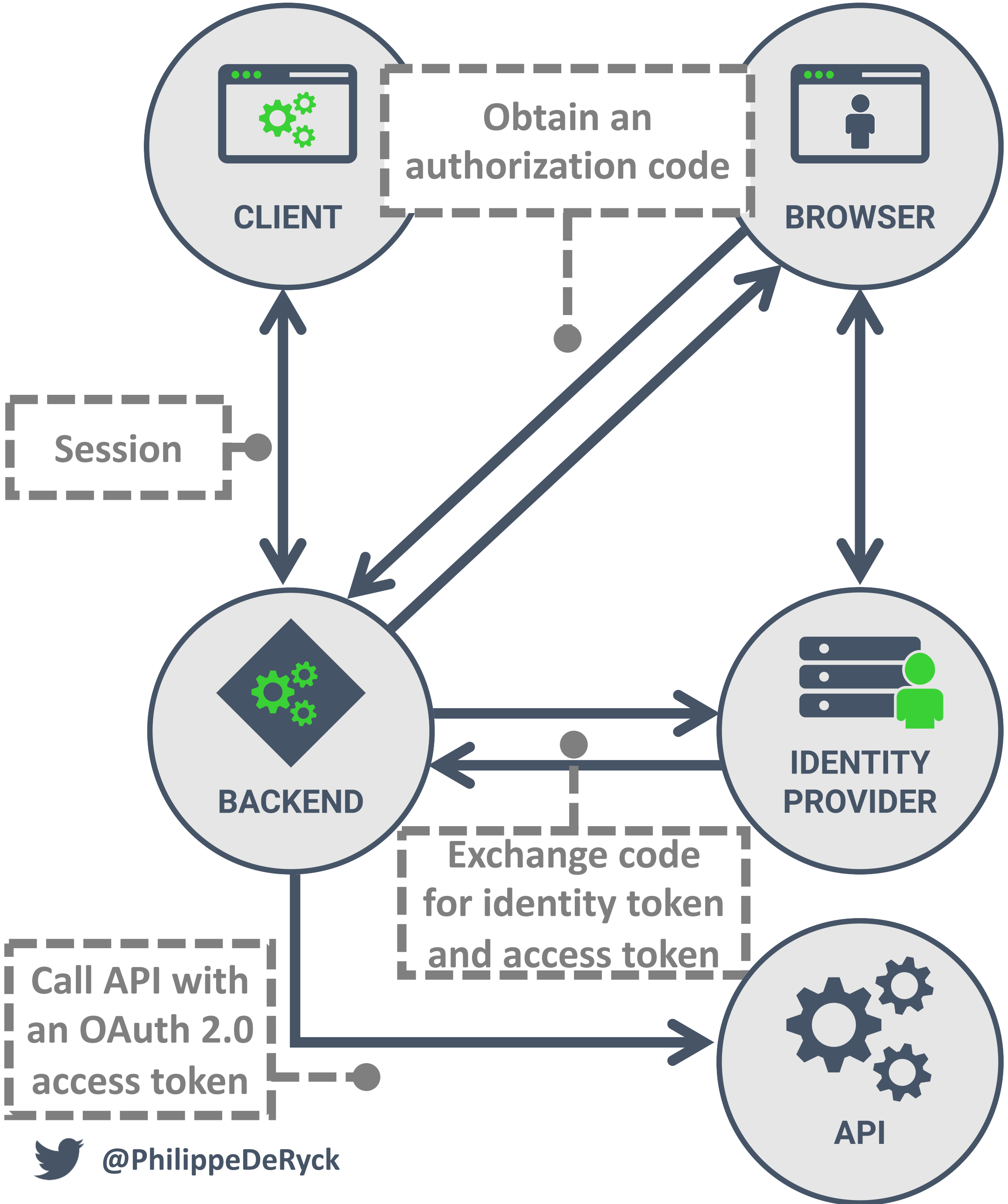
Offloading authentication makes sense, even in a non-SSO scenario

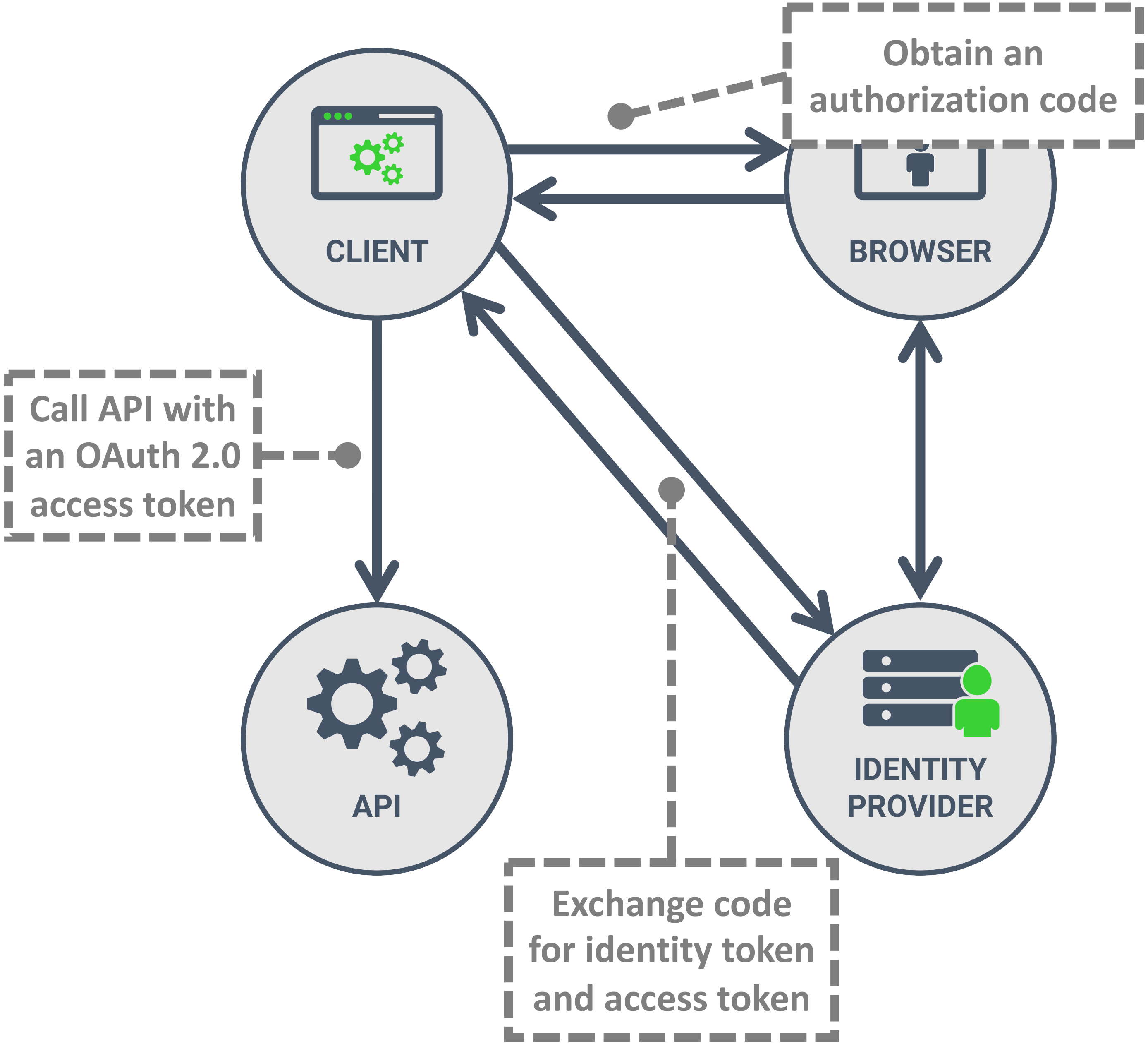

CLIENT
Obtain an authorization code
BROWSER
Session
User authentication
BACKEND
IDENTITY PROVIDER
Exchange code for identity token

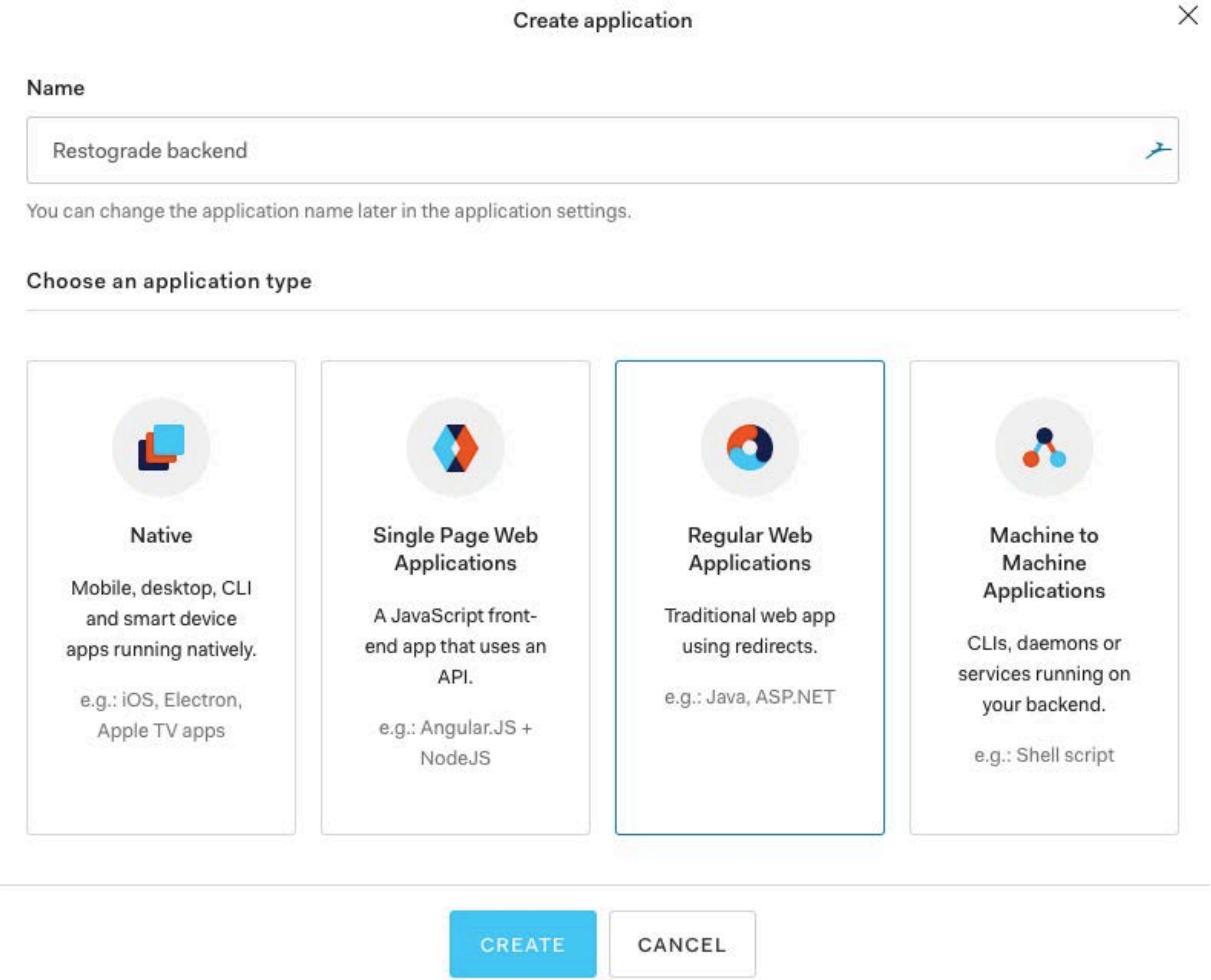

CLIENT
Obtain an authorization code
BROWSER
Session
BACKEND
IDENTITY PROVIDER
Exchange code for identity token


Obtain an authorization code
CLIENT
BROWSER
IDENTITY PROVIDER
Exchange code for identity token


CLIENT
Obtain an authorization code
BROWSER
Session
BACKEND
IDENTITY PROVIDER
Exchange code for identity token
CLIENT
Obtain an authorization code
BROWSER
Call API with an OAuth 2.0 access token
API
IDENTITY PROVIDER
Exchange code for identity token and access token


CLIENT
Obtain an authorization code
BROWSER
Session
BACKEND
IDENTITY PROVIDER
Exchange code for identity token and access token
Call API with an OAuth 2.0 access token
API


Obtain an authorization code
CLIENT
BROWSER
Call API with an OAuth 2.0 access token
API
IDENTITY PROVIDER
Exchange code for identity token and access token



Create application

Name

Restograde backend

You can change the application name later in the application settings.

Choose an application type

Native

Mobile, desktop, CLI and smart device apps running natively.

e.g.: iOS, Electron, Apple TV apps

Single Page Web Applications

A JavaScript front-end app that uses an API.

e.g.: Angular.JS + NodeJS

Regular Web Applications

Traditional web app using redirects.

e.g.: Java, ASP.NET

Machine to Machine Applications

CLIs, daemons or services running on your backend.

e.g.: Shell script

Redirect from Netlify to Github

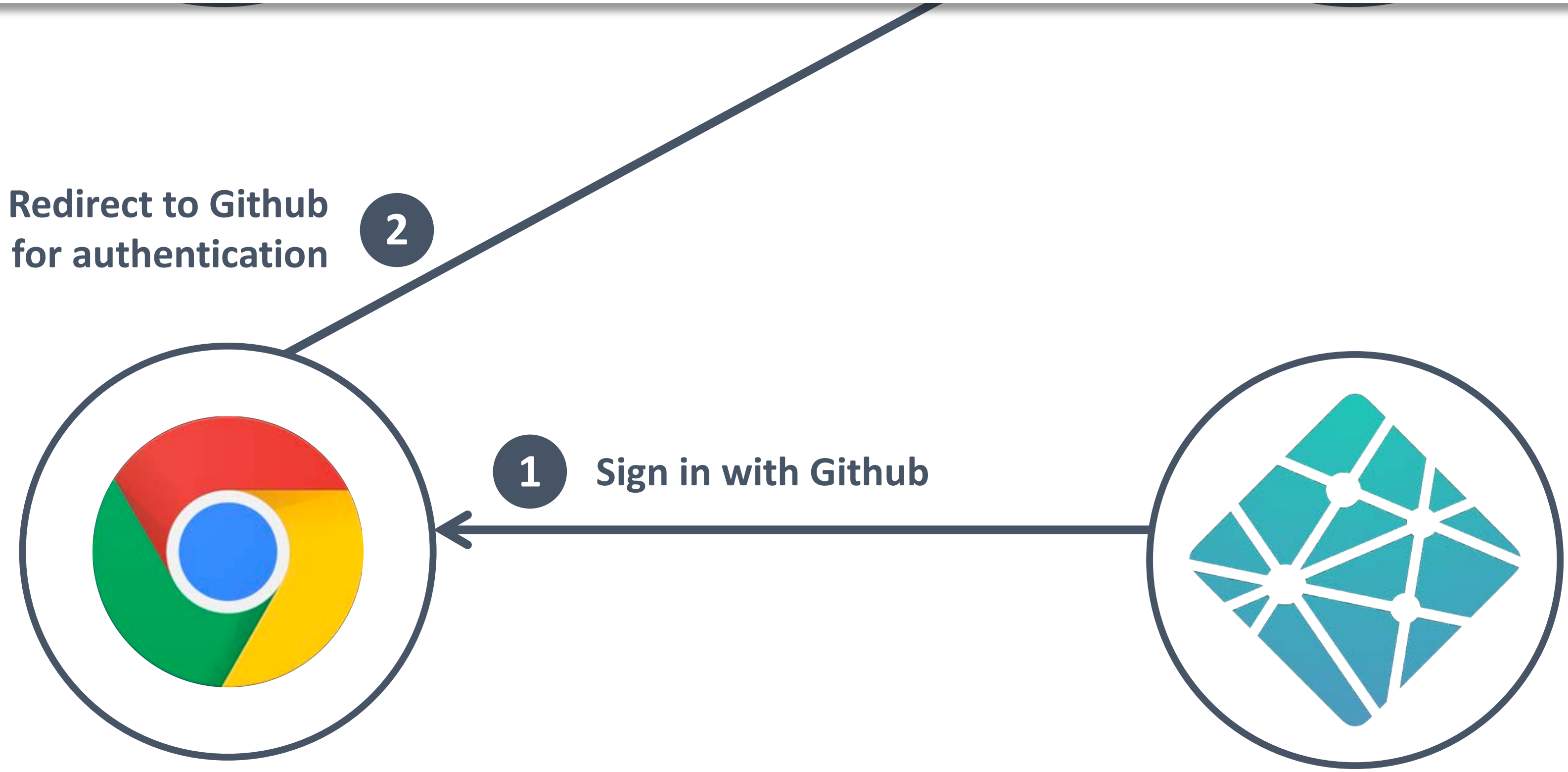
1 2

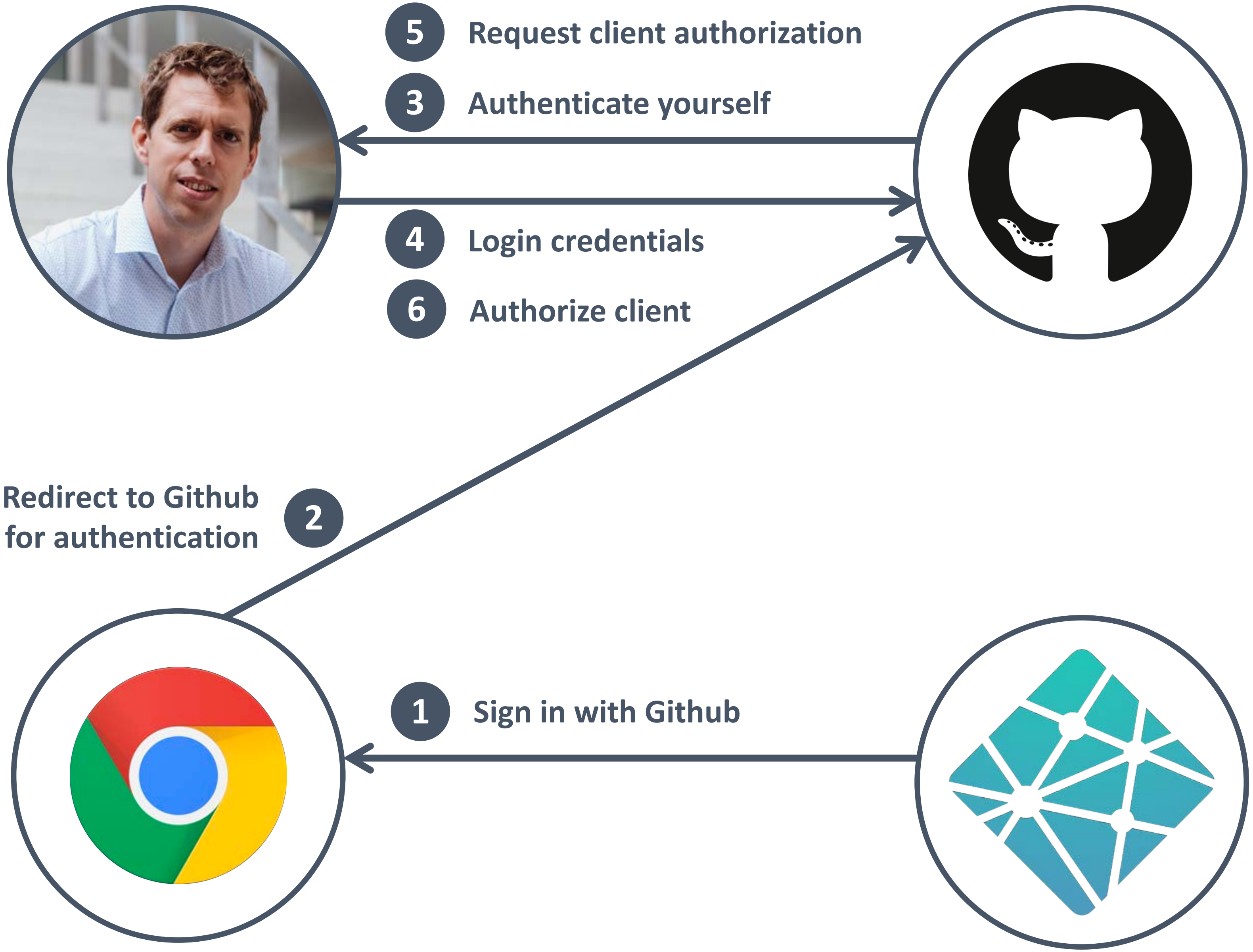
```
https://github.com/openid-connect/auth
  ?response_type=id_token code
  &client_id=NetlifyClient
  &scope=openid email profile
  &redirect_uri=https://netlify.com/codeCallback
  &state=s0wzojm2w8c23xzprkk6
  &nonce=Bh91lG2QLb1jAiaha372
```

GitHub's OIDC endpoint

Indicates the OIDC hybrid flow

Requests access to user's identity information





5 Request client authorization

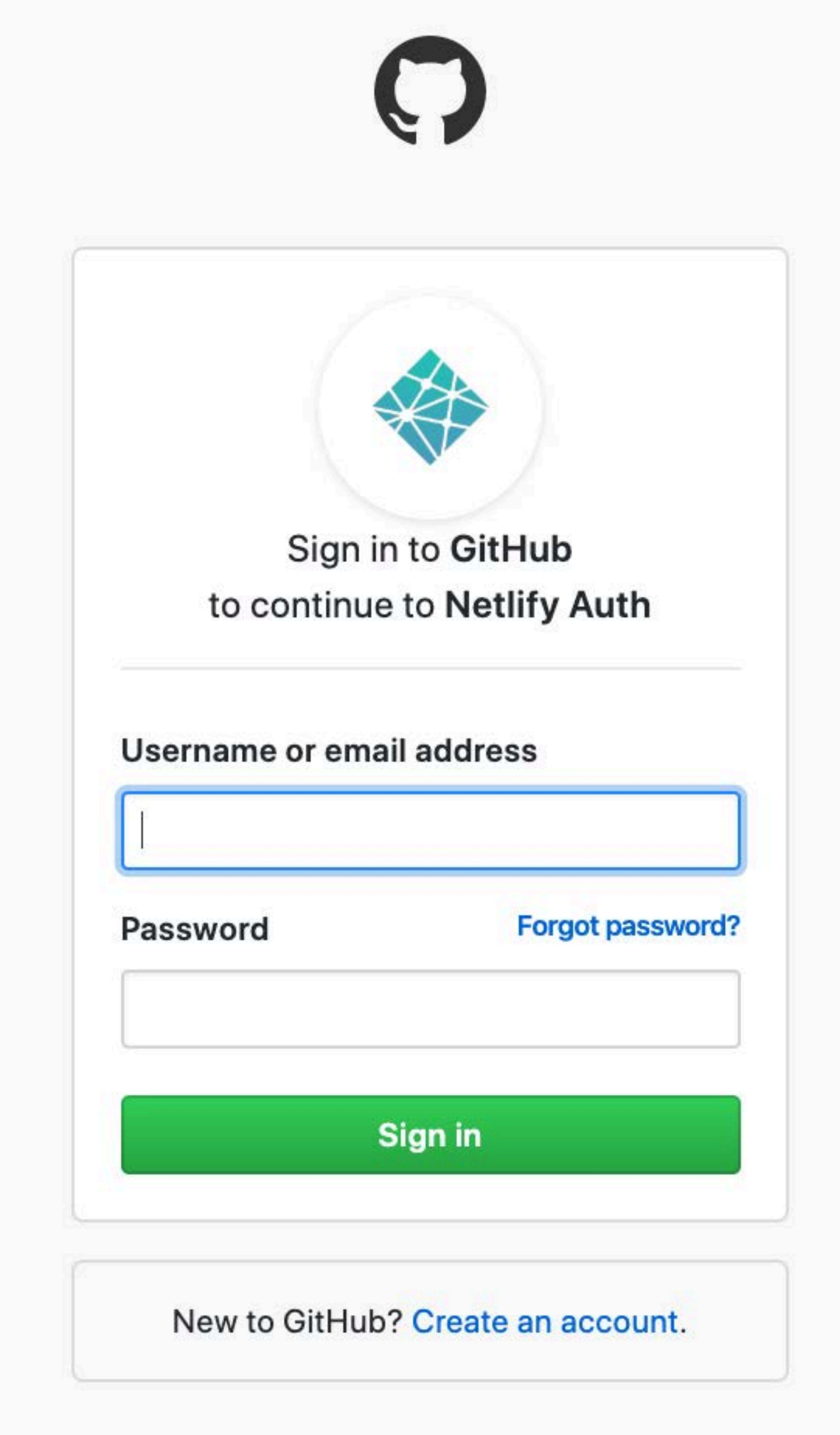
3 Authenticate yourself

4 Login credentials

6 Authorize client

Redirect to Github
for authentication 2

1 Sign in with Github



Sign in to GitHub
to continue to **Netlify Auth**

Username or email address

Password Forgot password?

Sign in

New to GitHub? Create an account.

Redirect from Github to Netlify

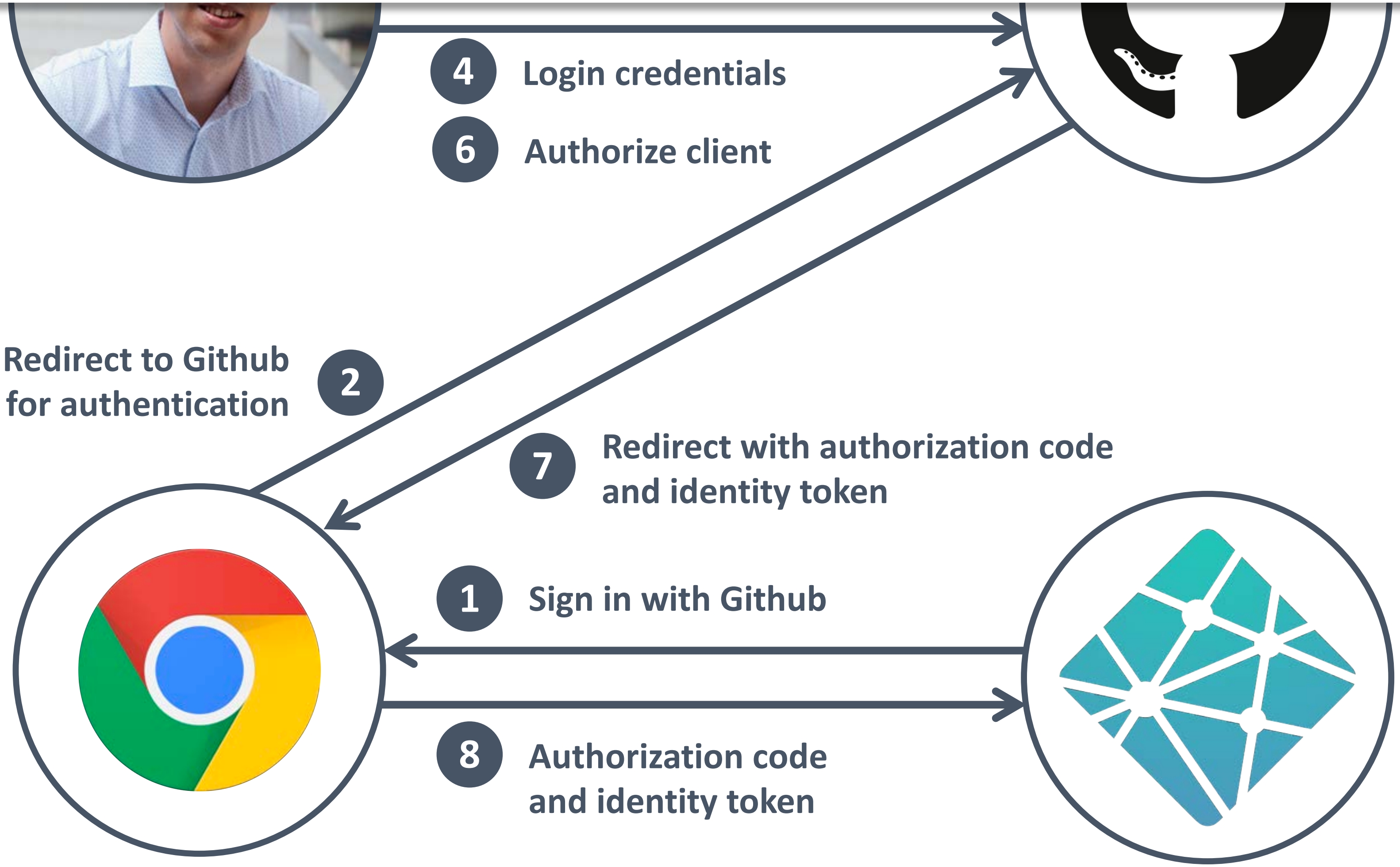
7 8

```
https://netlify.com/codeCallback
   ?code=q3AKQ...0X4UeQ
   &id_token=eyJhbGciO...du6TY9w
   &state=s0wzojm2w8c23xzprkk6
```

Approved redirect URI

Authorization code

JWT containing authentication information



4 Login credentials

6 Authorize client

Redirect to Github for authentication 2

7 Redirect with authorization code and identity token

1 Sign in with Github

8 Authorization code and identity token

THE IDENTITY TOKEN CONTAINS INFORMATION ABOUT THE USER'S AUTHENTICATION

8

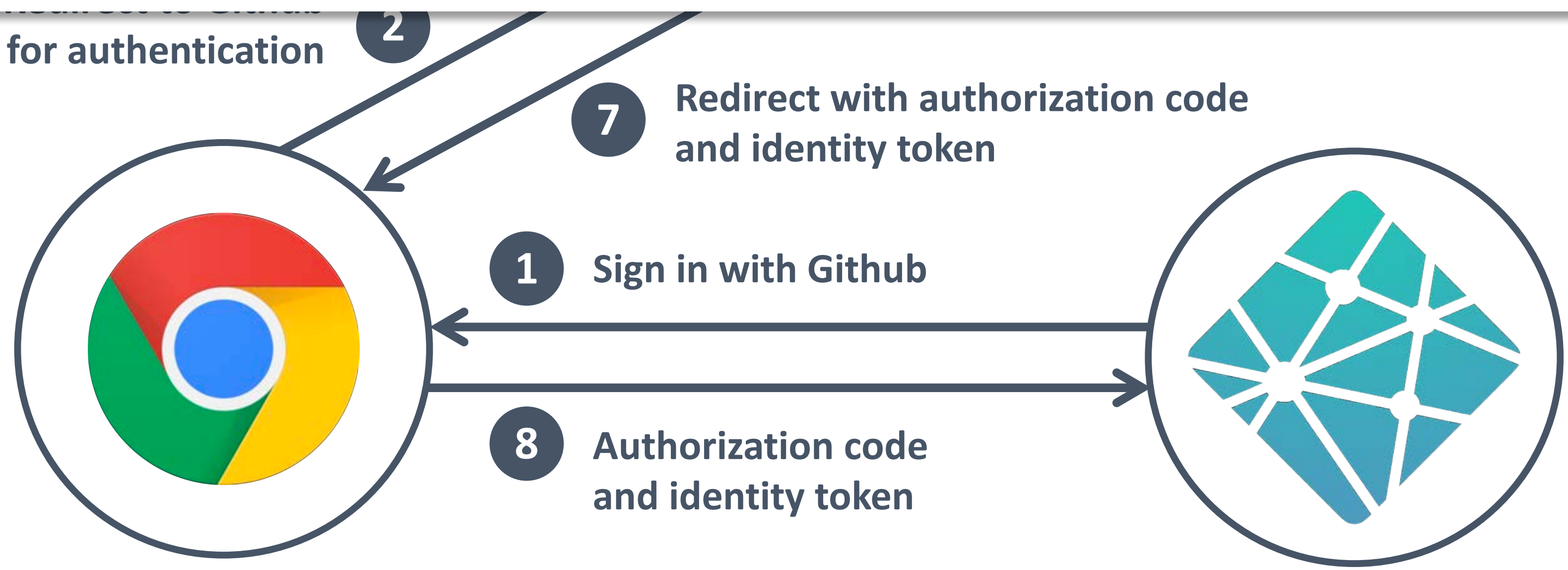
```
{
  "name": "Philippe De Ryck",
  "email": "philippe@pragmaticwebsecurity.com",
  "email_verified": true,
  "iss": "https://github.com",
  "aud": "NetlifyClient",
  "iat": "1550400912",
  "exp": "1550422512",
  "sub": "github|bBFd87uO9PDaVpOjZRB7",
}
```

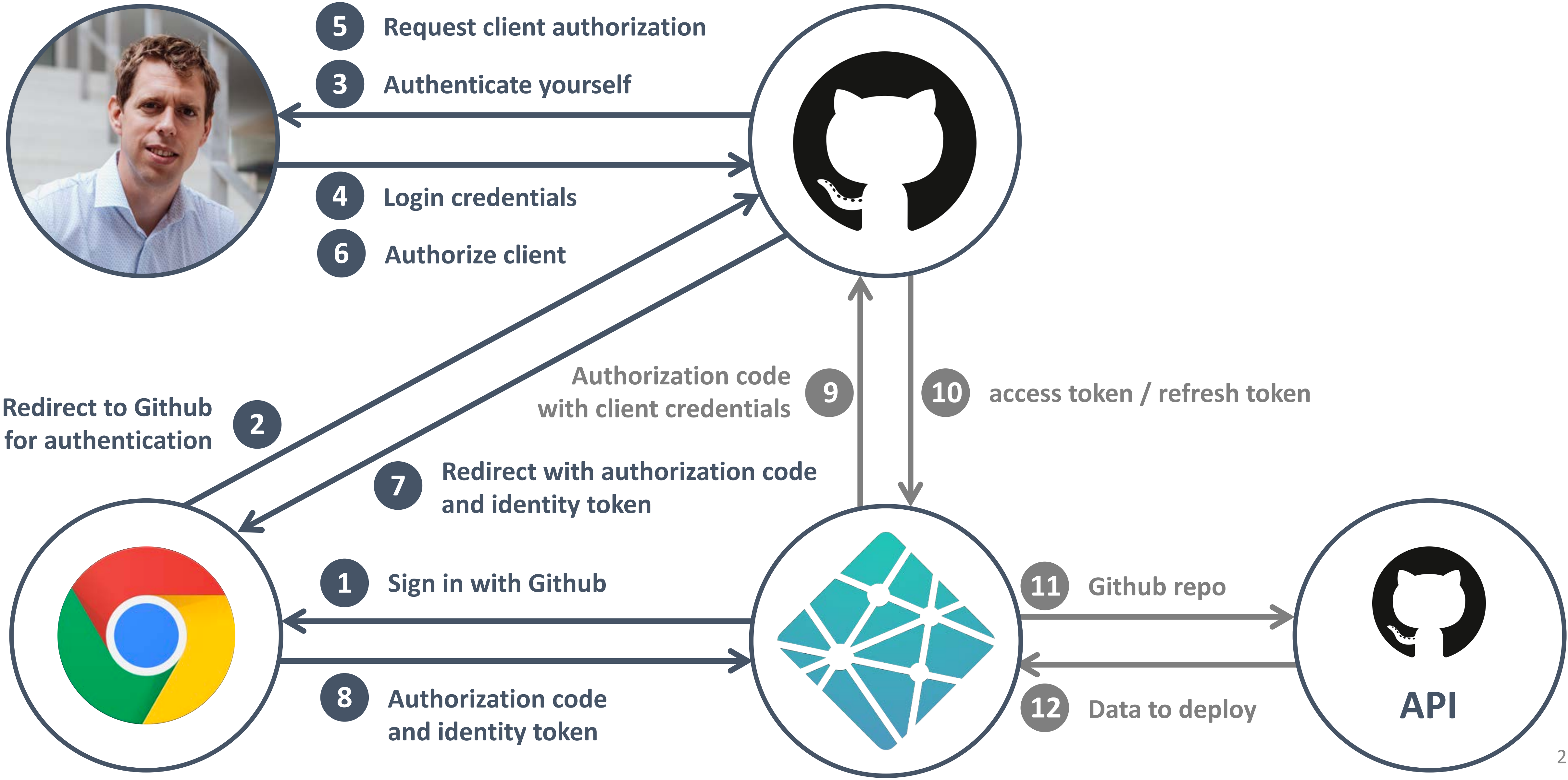
Profile information about the user

The identifier of the issuer of the token

The intended audience for this token

The unique ID of the user within the issuer


for authentication
2
7
Redirect with authorization code and identity token
1
Sign in with Github
8
Authorization code and identity token



5 Request client authorization

3 Authenticate yourself

4 Login credentials

6 Authorize client

Redirect to Github for authentication 2

Authorization code with client credentials 9

10 access token / refresh token

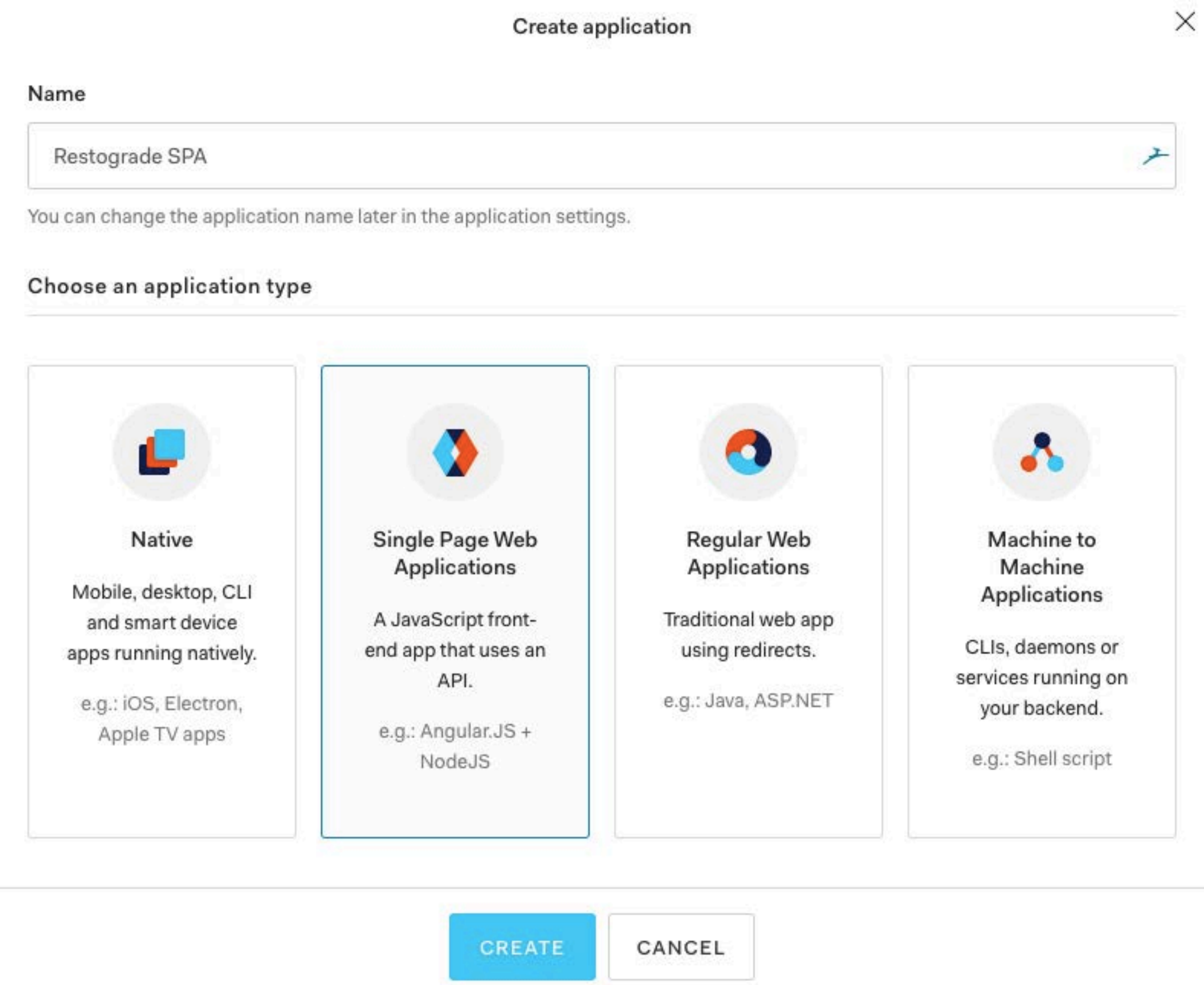
7 Redirect with authorization code and identity token

1 Sign in with Github

8 Authorization code and identity token

11 Github repo

12 Data to deploy



Create application

Name

Restograde SPA

You can change the application name later in the application settings.

Choose an application type

Native

Mobile, desktop, CLI and smart device apps running natively.

e.g.: iOS, Electron, Apple TV apps

Single Page Web Applications

A JavaScript front-end app that uses an API.

e.g.: Angular.JS + NodeJS

Regular Web Applications

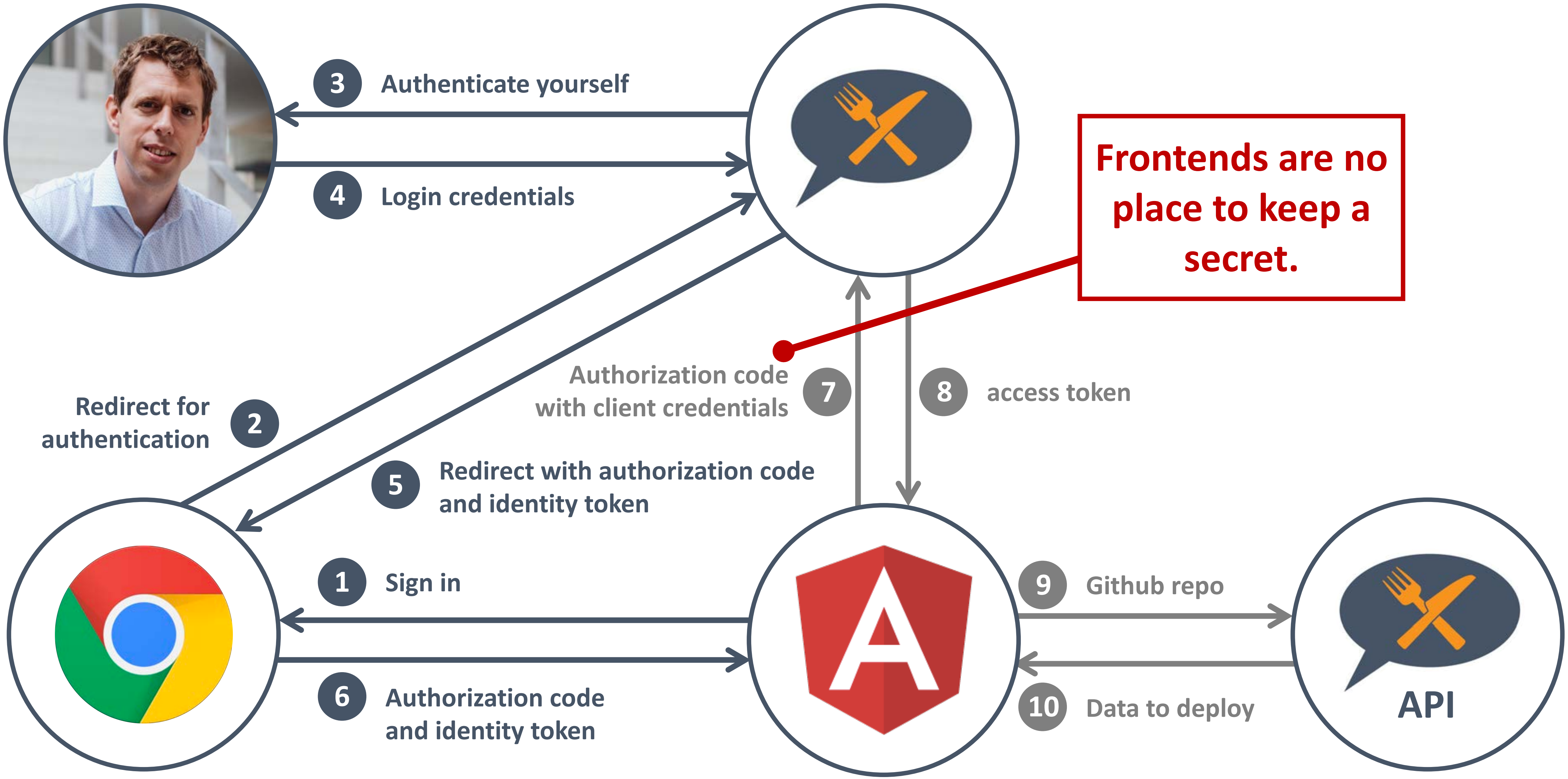
Traditional web app using redirects.

e.g.: Java, ASP.NET

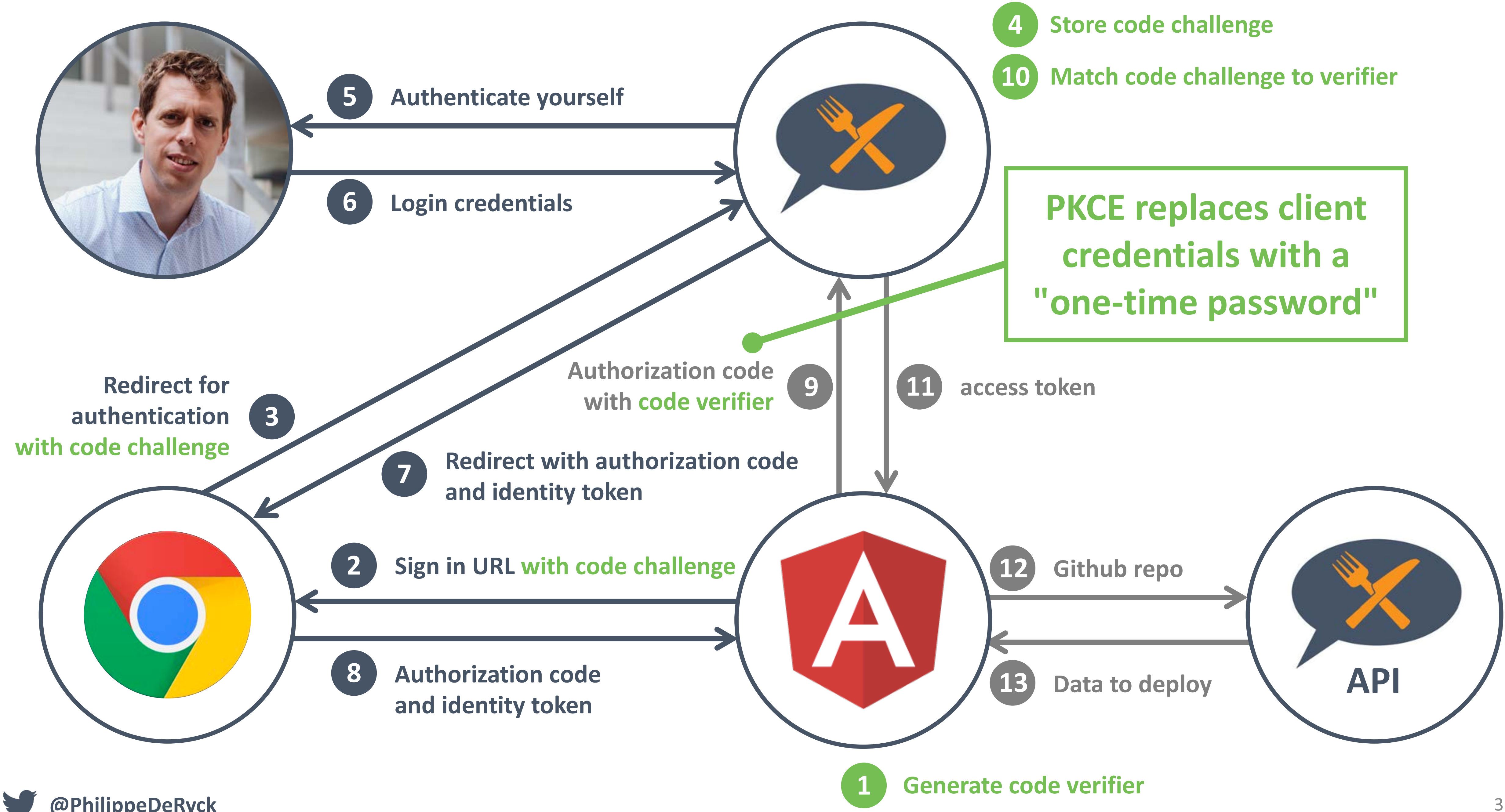
Machine to Machine Applications

CLIs, daemons or services running on your backend.

e.g.: Shell script


3 Authenticate yourself
4 Login credentials
Redirect for authentication 2
Authorization code with client credentials 7
8 access token
5 Redirect with authorization code and identity token
1 Sign in
6 Authorization code and identity token
9 Github repo
10 Data to deploy
API

Frontends are no place to keep a secret.



4 Store code challenge

10 Match code challenge to verifier

5 Authenticate yourself

6 Login credentials

PKCE replaces client credentials with a "one-time password"

Redirect for authentication with code challenge 3

Authorization code with code verifier 9

11 access token

7 Redirect with authorization code and identity token

2 Sign in URL with code challenge

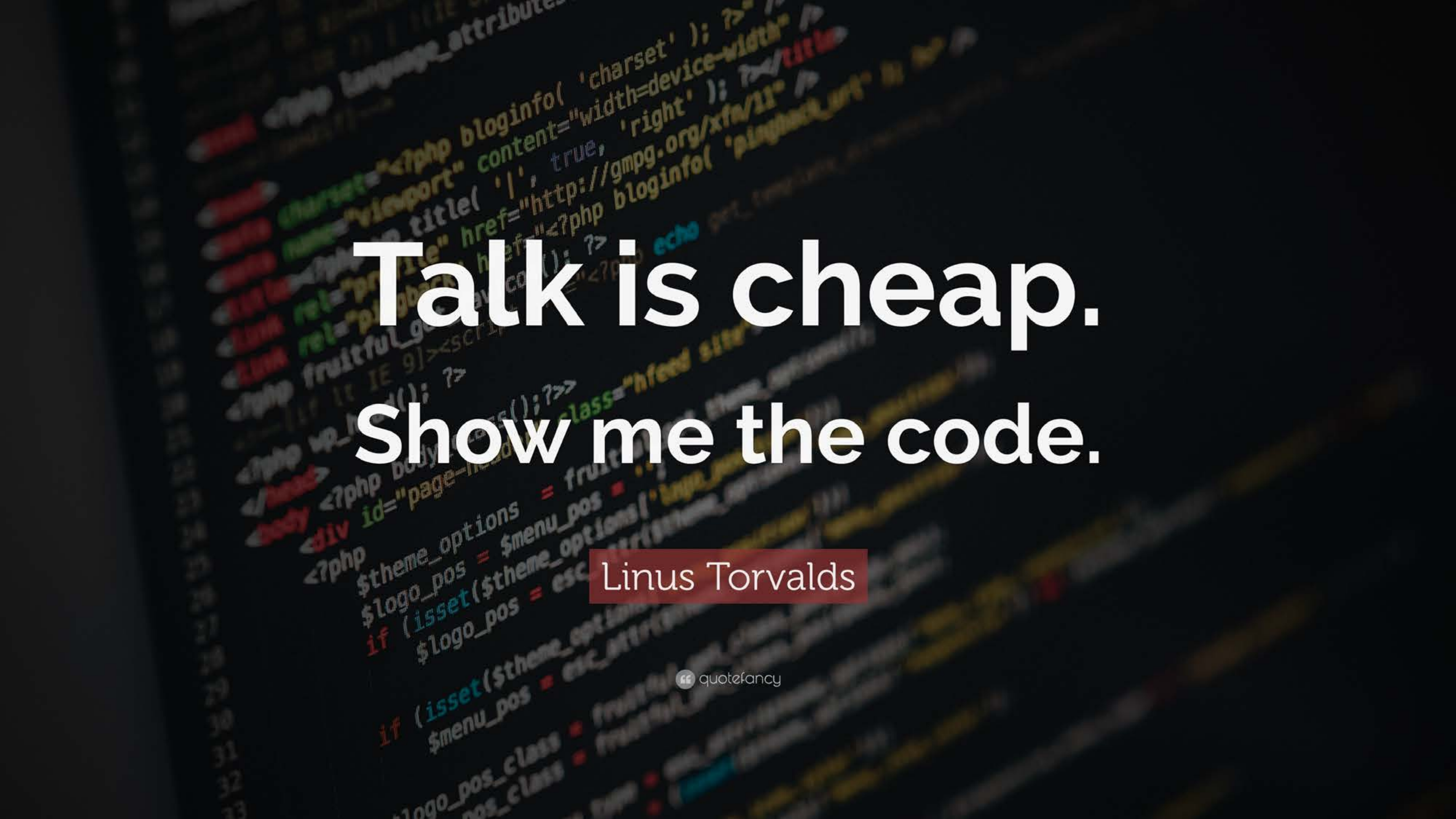
8 Authorization code and identity token

12 Github repo

13 Data to deploy

API

1 Generate code verifier



Talk is cheap.
Show me the code.

Linus Torvalds

```
npm install angular-oauth2-oidc
```

```
this.oauthService.initCodeFlow();
```

```
npm install @auth0/auth0-spa-js
```

```
this.auth0Client$.subscribe((client: Auth0Client) => {
  client.loginWithRedirect()
});
```

```
npm install keycloak-js
```

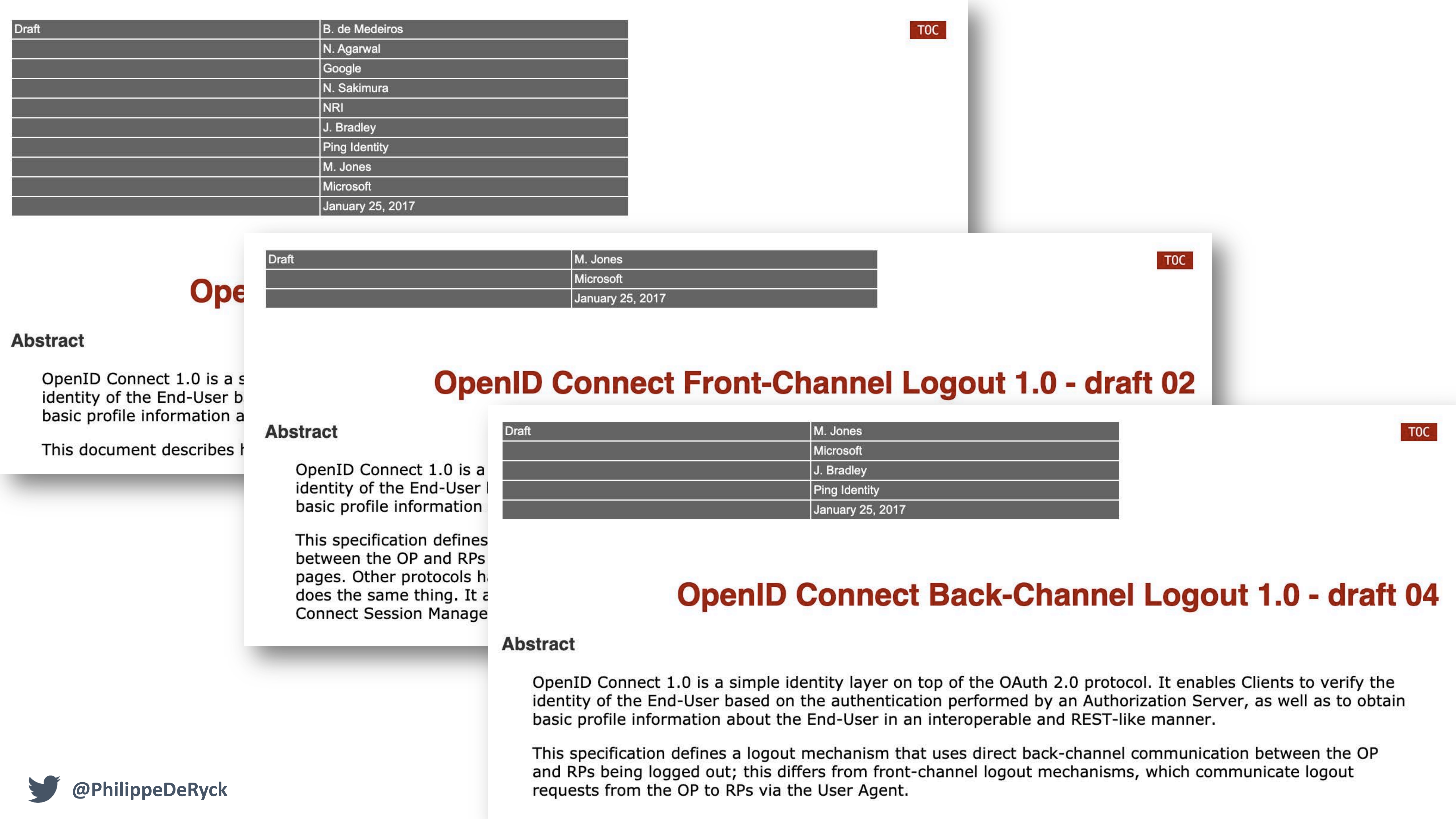
```
keycloak.init({
  flow: 'hybrid',
  promiseType: 'native',
})
```

Use the right OIDC flow for your application

Both a backend and a frontend can use the OIDC hybrid flow

Backends require client authentication & frontends require PKCE

OIDC is typically used along with OAuth 2.0 to enable API access



Draft	B. de Medeiros
	N. Agarwal
	Google
	N. Sakimura
	NRI
	J. Bradley
	Ping Identity
	M. Jones
	Microsoft
	January 25, 2017

TOC

Ope

Abstract

OpenID Connect 1.0 is a s
identity of the End-User b
basic profile information a

This document describes h

Draft	M. Jones
	Microsoft
	January 25, 2017

TOC

OpenID Connect Front-Channel Logout 1.0 - draft 02

Abstract

OpenID Connect 1.0 is a
identity of the End-User
basic profile information

This specification defines
between the OP and RPs
pages. Other protocols h
does the same thing. It a
Connect Session Manage

Draft	M. Jones
	Microsoft
	J. Bradley
	Ping Identity
	January 25, 2017

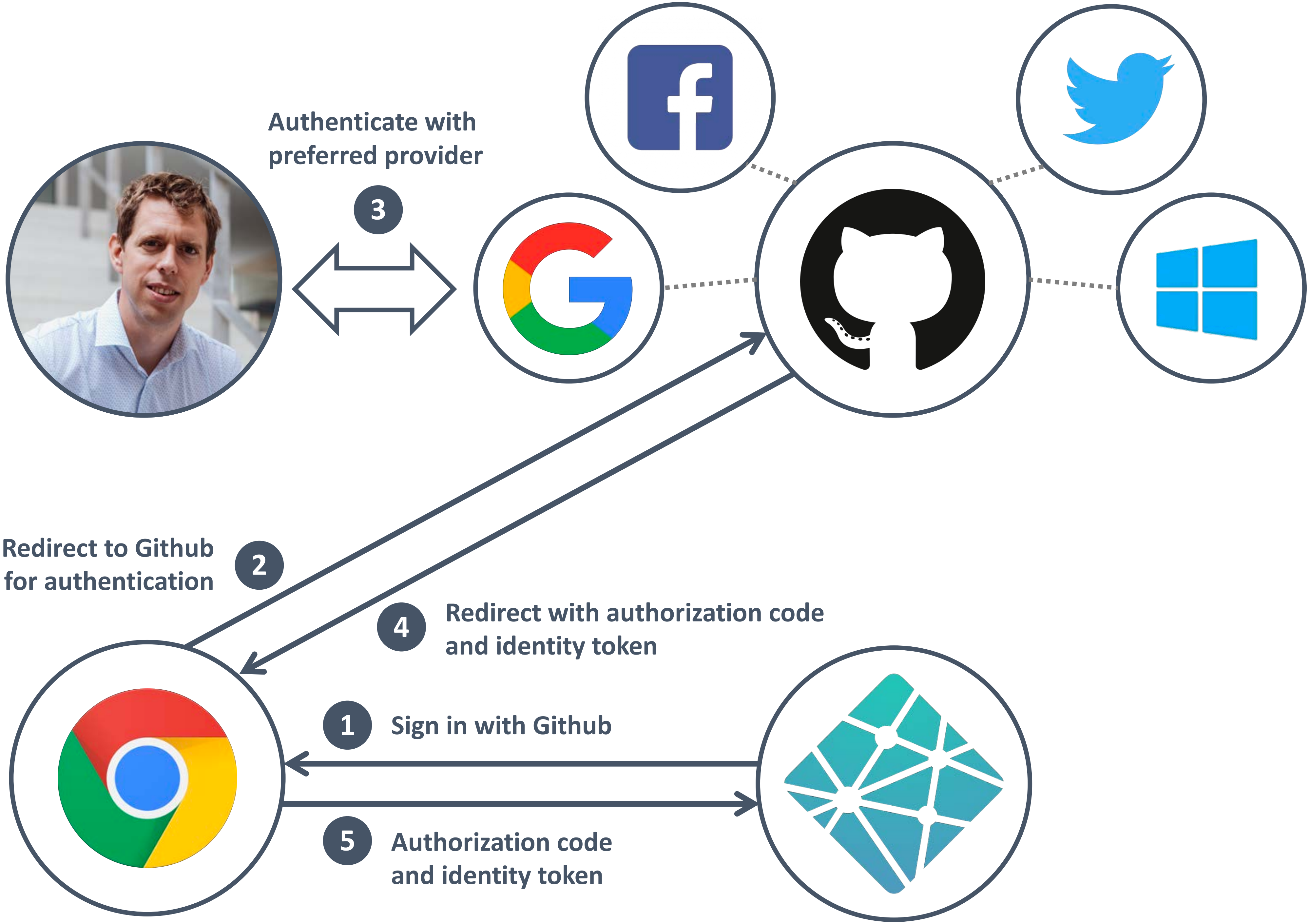
TOC

OpenID Connect Back-Channel Logout 1.0 - draft 04

Abstract

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

This specification defines a logout mechanism that uses direct back-channel communication between the OP and RPs being logged out; this differs from front-channel logout mechanisms, which communicate logout requests from the OP to RPs via the User Agent.



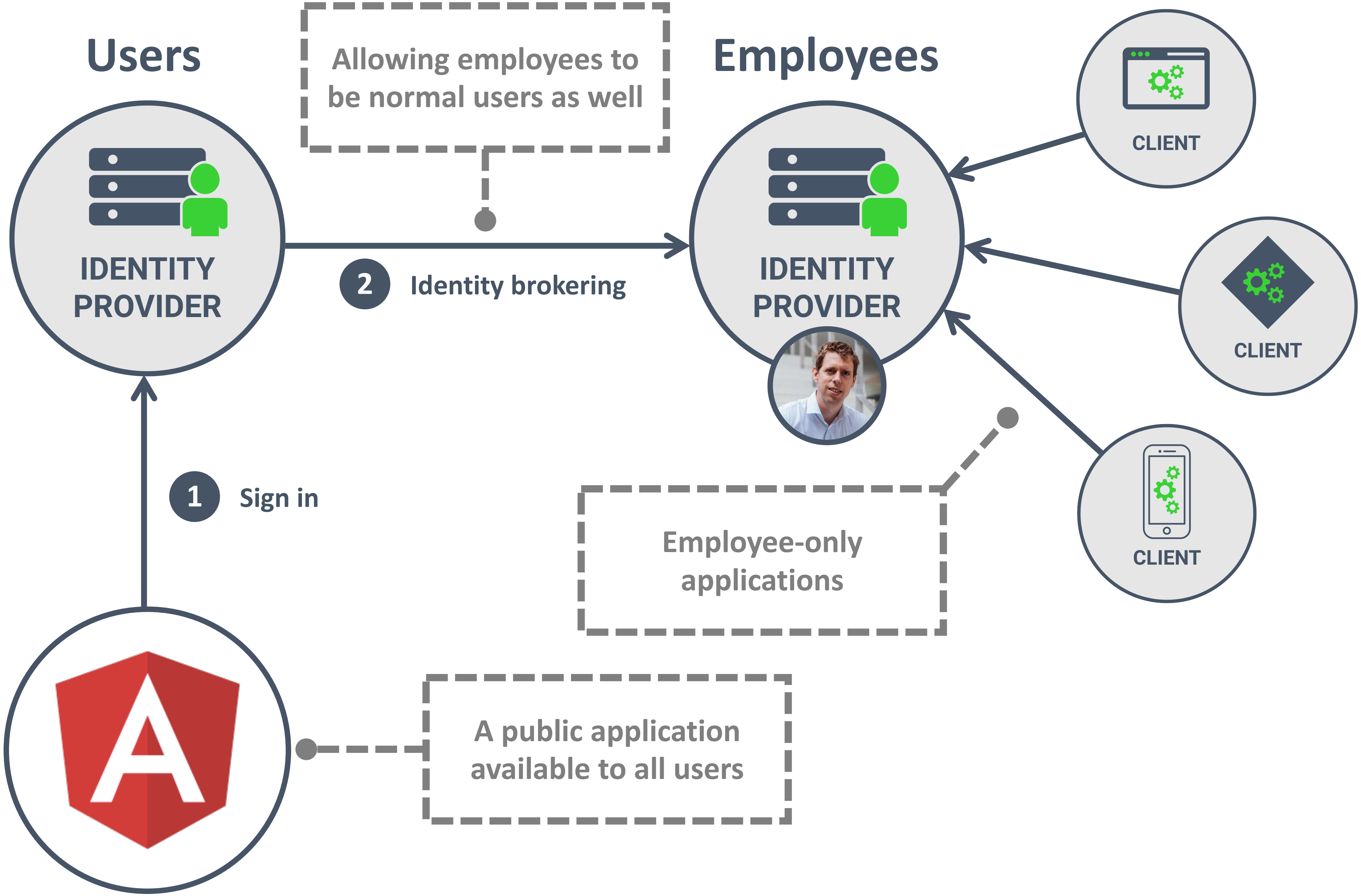
1 Sign in with Github

2 Redirect to Github for authentication

3 Authenticate with preferred provider

4 Redirect with authorization code and identity token

5 Authorization code and identity token



Users

Allowing employees to be normal users as well

Employees

IDENTITY PROVIDER

2 Identity brokering

IDENTITY PROVIDER

CLIENT

CLIENT

CLIENT

1 Sign in

Employee-only applications

A public application available to all users

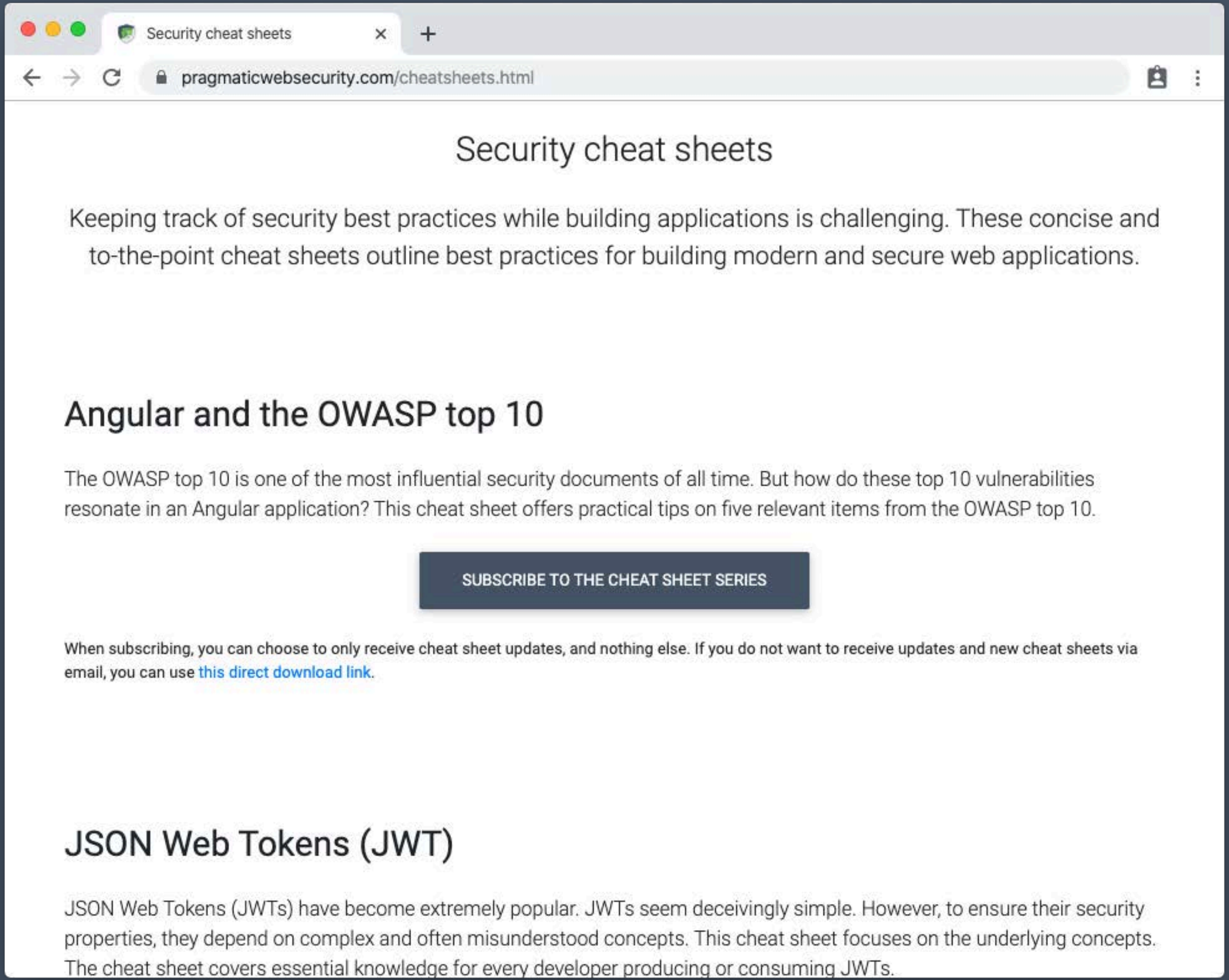
OIDC IS MORE THAN AUTHENTICATION ALONE

OIDC also includes support for session management and logout

Identity brokering enables the chaining of multiple identity providers

Identity brokering is a crucial concept in enterprise architectures

Free security cheat sheets for modern applications



Security cheat sheets

Keeping track of security best practices while building applications is challenging. These concise and to-the-point cheat sheets outline best practices for building modern and secure web applications.

Angular and the OWASP top 10

The OWASP top 10 is one of the most influential security documents of all time. But how do these top 10 vulnerabilities resonate in an Angular application? This cheat sheet offers practical tips on five relevant items from the OWASP top 10.

SUBSCRIBE TO THE CHEAT SHEET SERIES

When subscribing, you can choose to only receive cheat sheet updates, and nothing else. If you do not want to receive updates and new cheat sheets via email, you can use this direct download link.

JSON Web Tokens (JWT)

JSON Web Tokens (JWTs) have become extremely popular. JWTs seem deceivingly simple. However, to ensure their security properties, they depend on complex and often misunderstood concepts. This cheat sheet focuses on the underlying concepts. The cheat sheet covers essential knowledge for every developer producing or consuming JWTs.

https://cheatsheets.pragmaticwebsecurity.com/

SecAppDev

March 9th – 13th, 2020
Leuven, Belgium

A week-long course on Secure Application Development

Taught by experts from around the world

38 in-depth lectures and 3 one-day workshops

https://secappdev.org

A yearly initiative from the SecAppDev.org non-profit, since 2005

Thank you!

Follow me on Twitter to stay up to date on web security best practices

@PhilippeDeRyck