SINGLE SIGN ON USING OAUTH2

The Spring Boot way

Marc Thomas - Lead Developer @connect_agency
Twitter: @mtdevuk
Blog: http://mtdevuk.com
GitHub: https://github.com/marcthomas2013

AGENDA

- Single Sign On
- OAuth2
  - What is it? How it works
- Social OAuth Integrations
- Spring Boot
- Implementing OAuth2 authorisation with Spring Boot

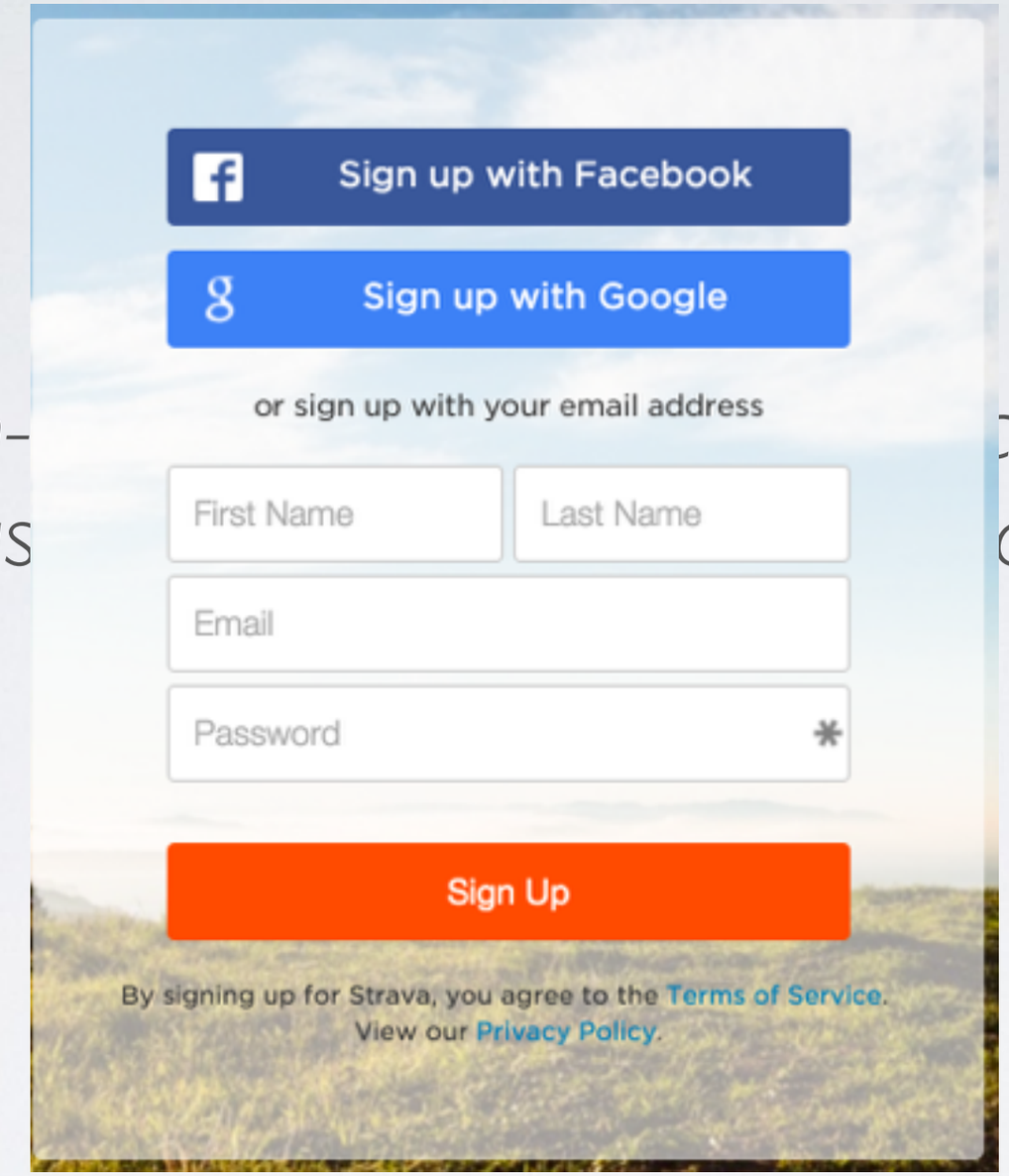
"Single sign-on (SSO) is a user authentication process using one username and password to access multiple applications."

gn-on (SSO) is a user authentication process
e username and password to access multiple
applications."

gn-on (SSO) is a user authenticat
e username and password to acce
applications."

gn-on (SSO) is a user authenticat
e username and password to acce
applications."

gn-on (SSO) is a user authenticat
e username and password to acce
applications."


Sign up with Facebook
Sign up with Google
or sign up with your email address
First Name
Last Name
Email
Password
Sign Up
By signing up for Strava, you agree to the Terms of Service.
View our Privacy Policy.

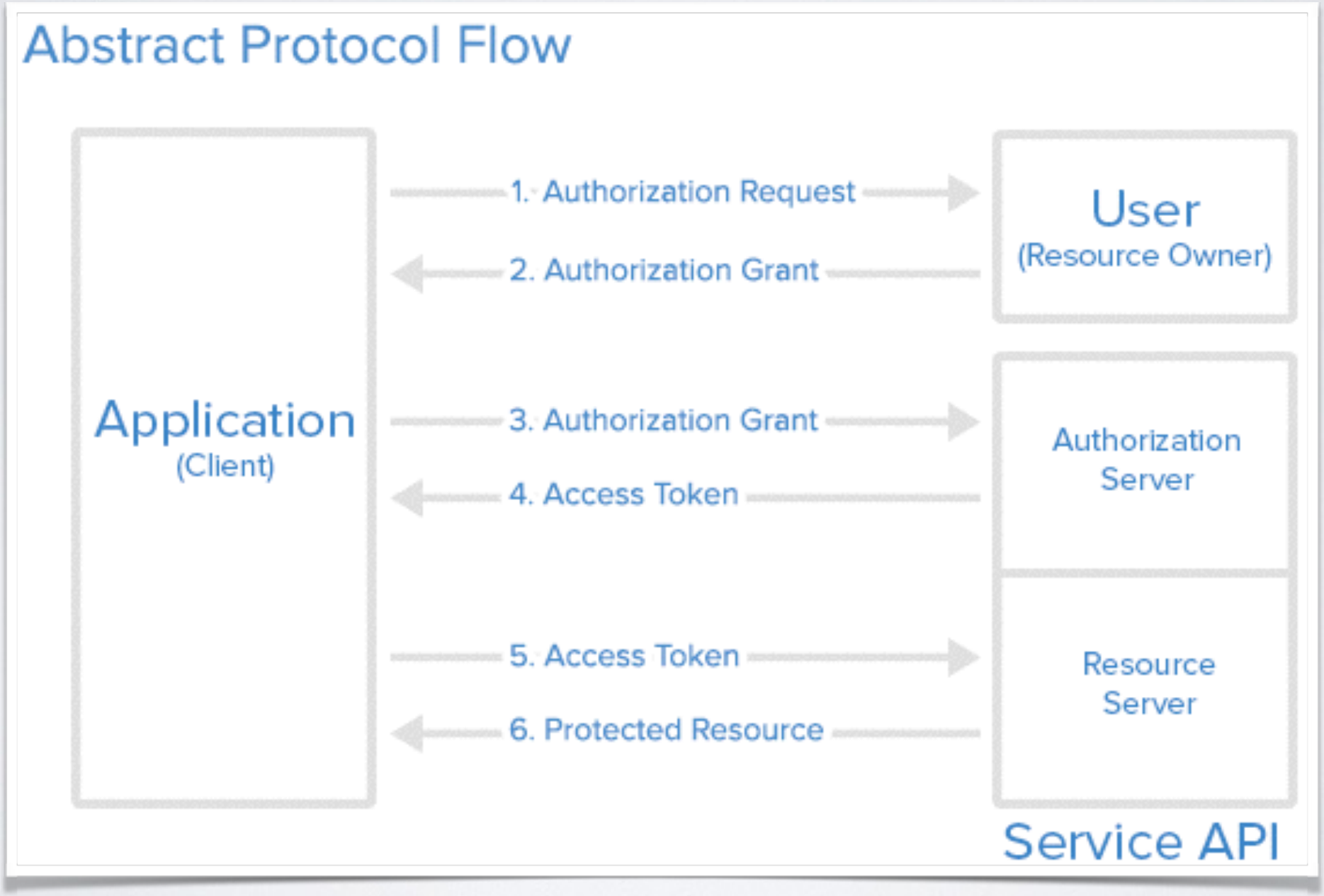
OAUTH2

- Authorisation protocol and not Authentication
- When used the application delegates authentication to a 3rd party - Facebook, Google, Twitter
- Authorises the registered app access to the user account details
- Supports Web, Desktop and Mobile
- RFC - https://tools.ietf.org/html/rfc6749
- Don't use for sensitive data

OAUTH2 ROLES

- Resource Owner - User of the application
- Resource Server - Access User's information
- Authorisation Server - Issues authentication token
  - Resource & Authorisation Server tend to be the same in practice
  - GitHub, Facebook, Google, etc.
- Client - Your application

OAUTH2 PROCESS



https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

OAUTH2 PROCESS

Authorize application

Meetup Demo by @marcthomas2013 would like permission to access your account

Review permissions

Public data only
Limited access to your public data ...

Authorize application

Meetup Demo

No description

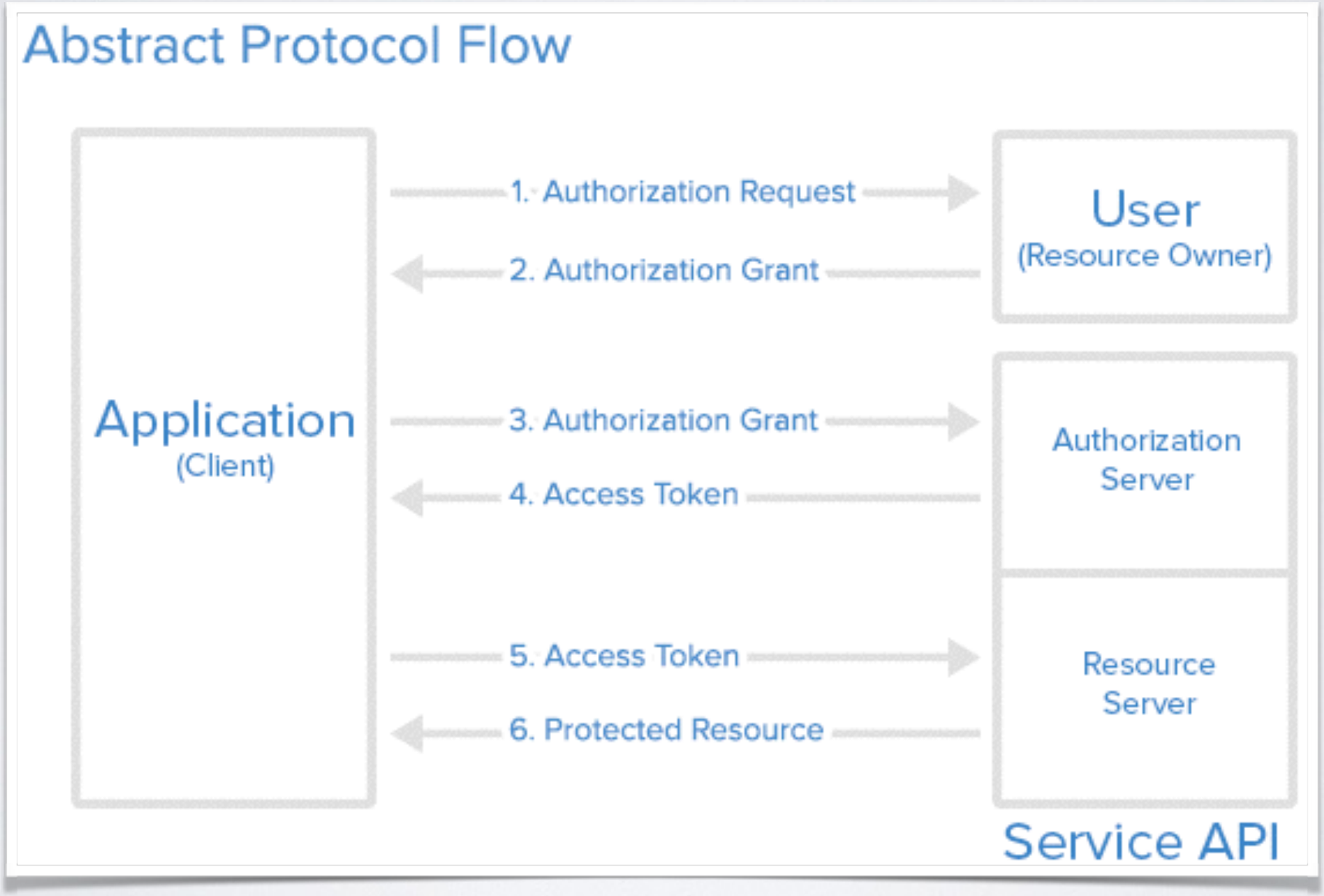
Visit application's website

Learn more about OAuth

Service API

https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

OAUTH2 PROCESS



https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

GITHUB EXAMPLE

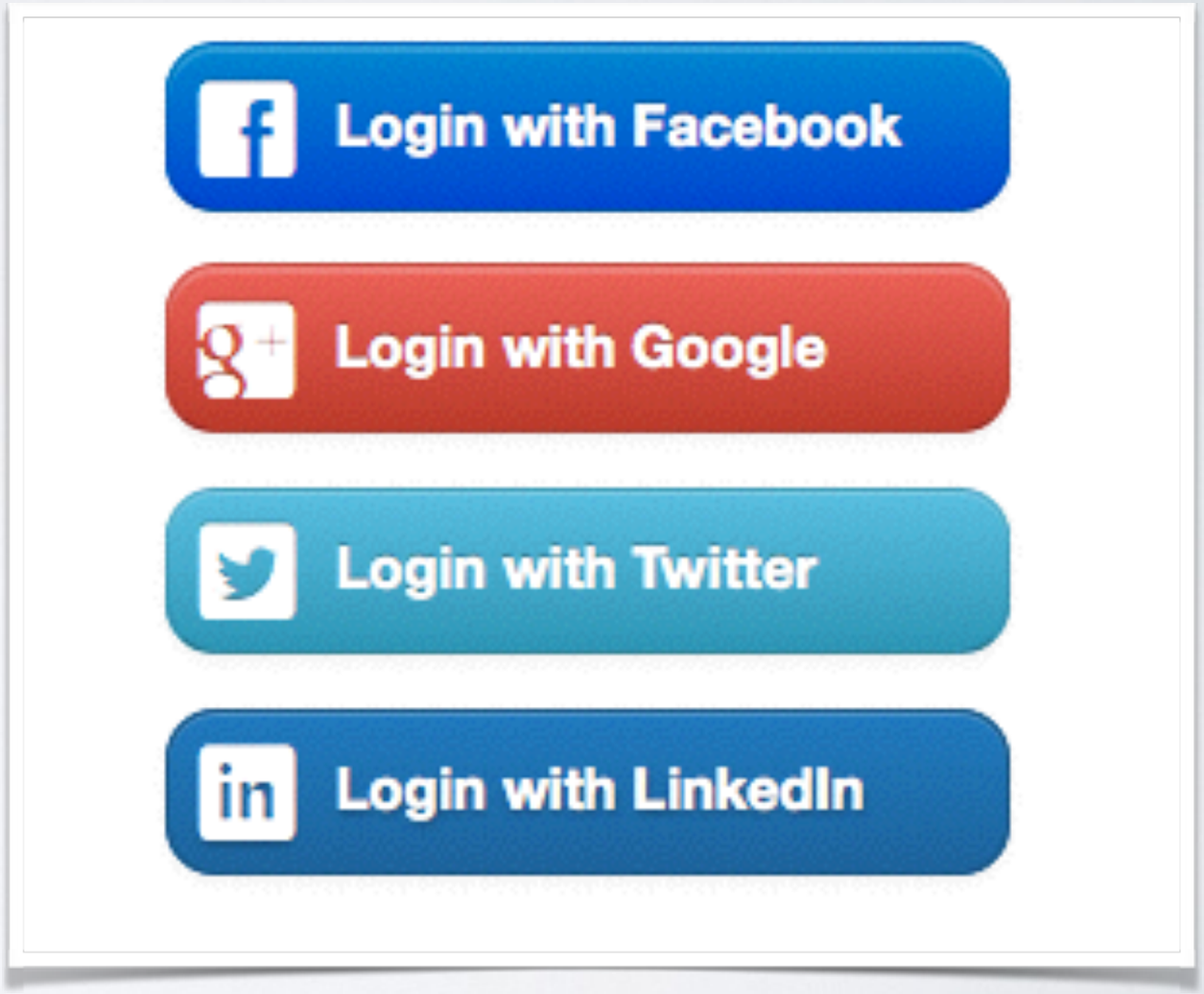
- Access resource
  - curl https://api.github.com/user
- Login to the resource
  - curl https://api.github.com/user --user ‘‘marcthomas2013"
- Create an OAUTH token instead
  - curl https://api.github.com/authorizations --user "marcthomas2013" --data ‘{‘‘scopes":["gist"],"note":"Meetup"}'
- Use the token
  - curl https://api.github.com/user?access_token=OAUTH_TOKEN
  - curl -H "Authorization: token OAUTH-TOKEN" https://api.github.com/user

OAUTH2 TOKENS

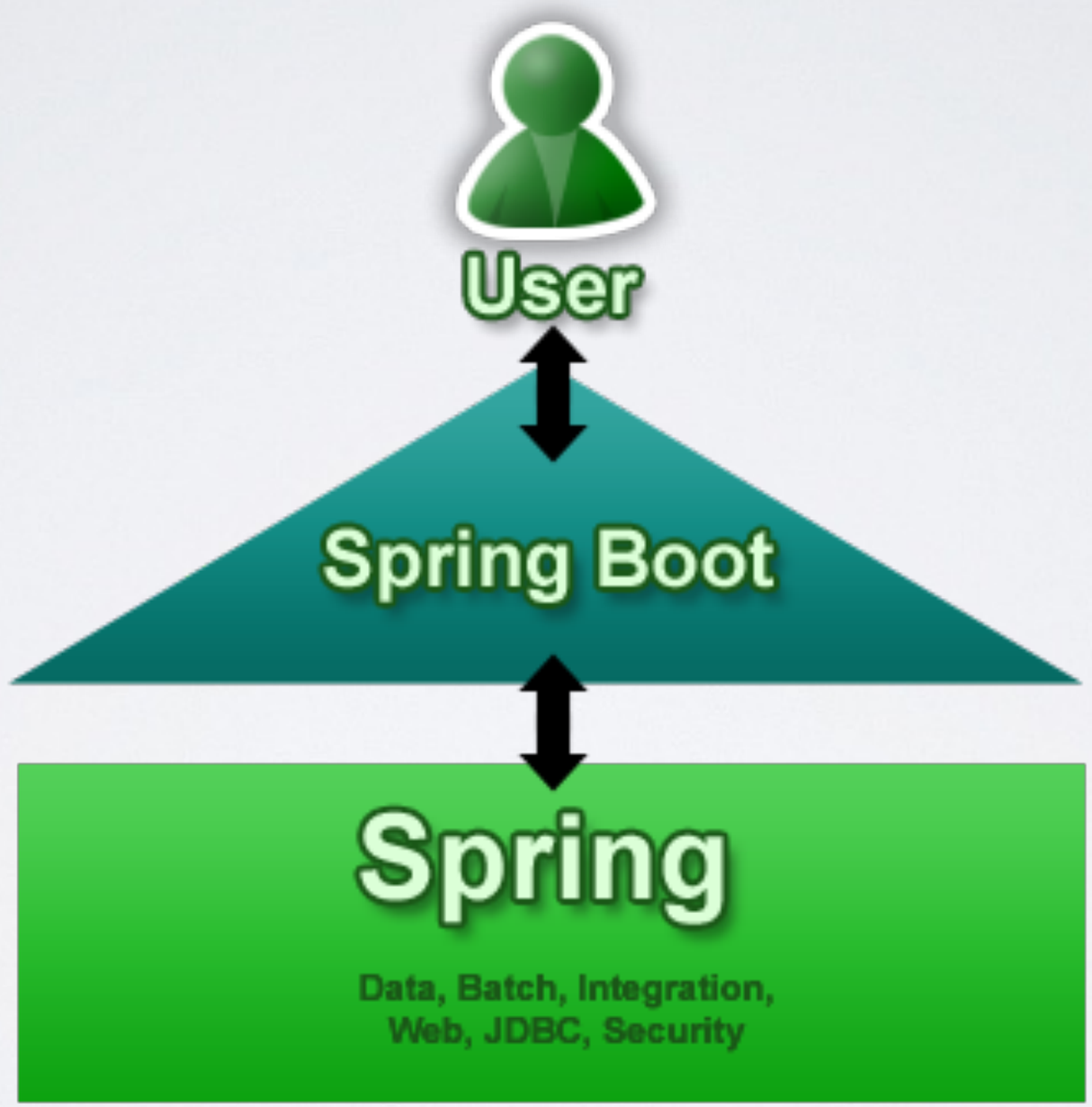
- Lightweight - UUID
- Like cookies
- Represent authentication
- Need to use HTTPS for token interactions
- Opaque to clients

SOCIAL INTEGRATIONS

- Google
- Twitter
- Facebook
- LinkedIn
- GitHub
- Many others…



SPRING BOOT


User
Spring Boot
Spring
Data, Batch, Integration,
Web, JDBC, Security

RUN THROUGH SPRING BOOT CODE

- Add spring-boot-starter-security to add authentication to the web app
- Add spring-security-oauth2 to add oauth2 support to the project
- Add annotation @EnableOAuth2Sso to the application for OAuth2 support
- Register the application in GitHub
  - Settings->Applications->Developer Applications
  - Copy the clientId and clientSecret into application.properties

RESOURCES

- Code from this demo
  - https://github.com/marcthomas2013
- GitHub APIs
  - https://gist.github.com/caspyin/2288960
  - https://developer.github.com/v3/oauth/
- Spring OAuth
  - http://spring.io/guides/tutorials/spring-boot-oauth2/