



Alex Bilbie
University of Lincoln

@alexbilbie

Story time!

I'm a **user** of a web
service

I own **resources** on
the web service

For example,
personal details

Welcome to Facebook – Log In, Sign Up or Learn More

Welcome to Facebook – Log In, ...

www.facebook.com

Google

facebook

Email

☐ Keep me logged in

Password

[Forgot your password?](#)

Log In

Facebook helps you connect and share with the people in your life.



Sign Up

It's free and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am:

Birthday:

Why do I need to provide my birthday?

Sign Up

Create a Page for a celebrity, band or business.

English (UK) English (US) Cymraeg Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी ...

Facebook © 2011 · English (US) Mobile · Find Friends · Badges · People · Pages · About · Advertising · Create a Page · Developers · Careers · Privacy · Terms · Help

These **resources**¹ are
stored on a **resource**
server²

1. personal details
2. facebook.com

The resource server
exposes user
resources over an **API**

I visit a 3rd party web
application

The 3rd party web
app is called a **client**

The **client**¹ wants to
use my **resources**²

1. 3rd party web app
2. personal details

But the resource
server's API requires
user **authorisation**

How?

Give the client my
password

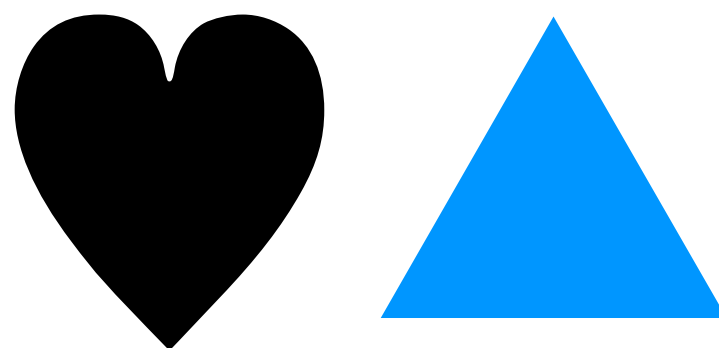
~~Give the client my
password~~

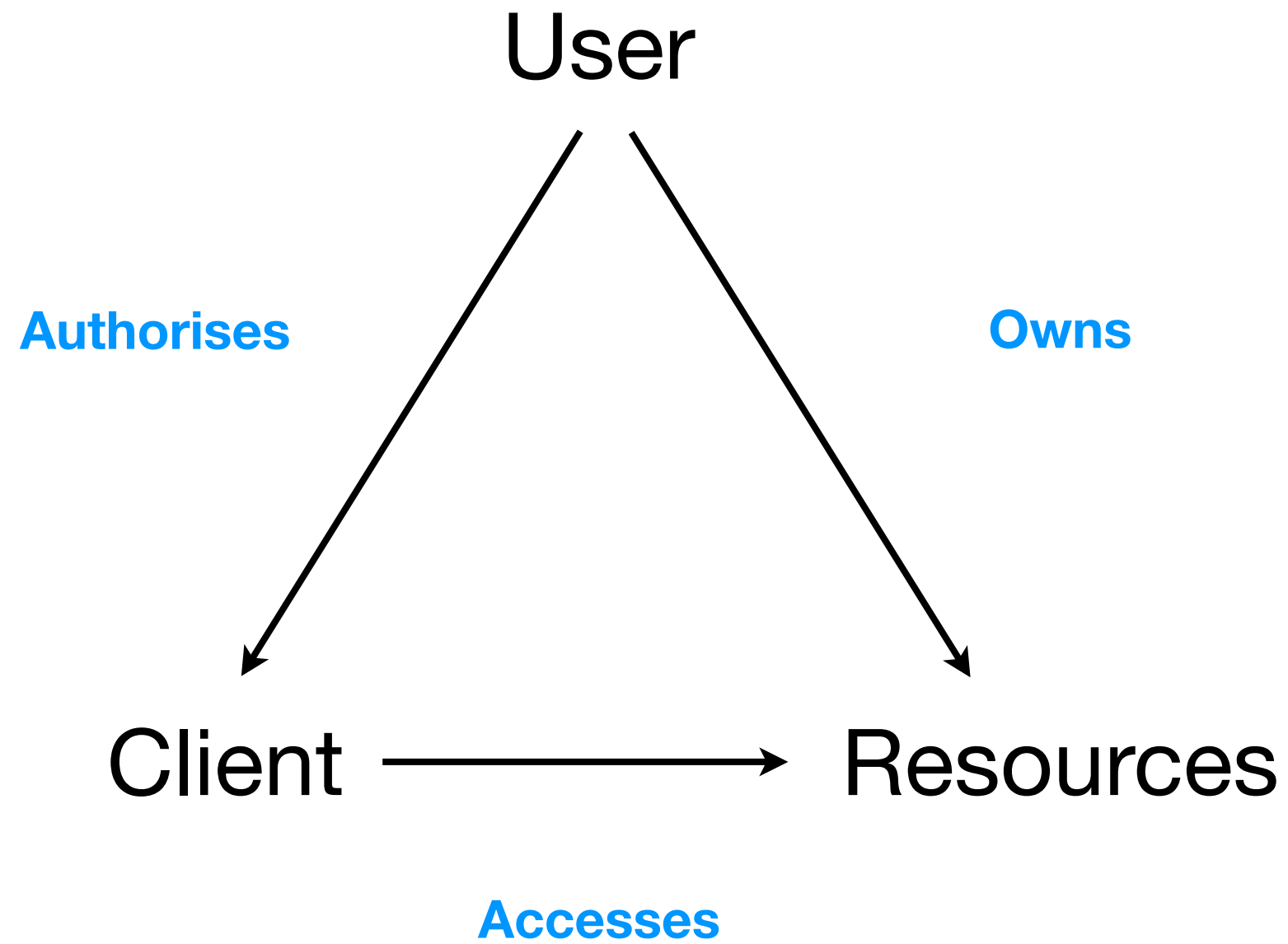
So what then?

OAuth

“An **open protocol** to allow **secure API authorisation** in a **simple** and **standard** method from desktop and web applications.”

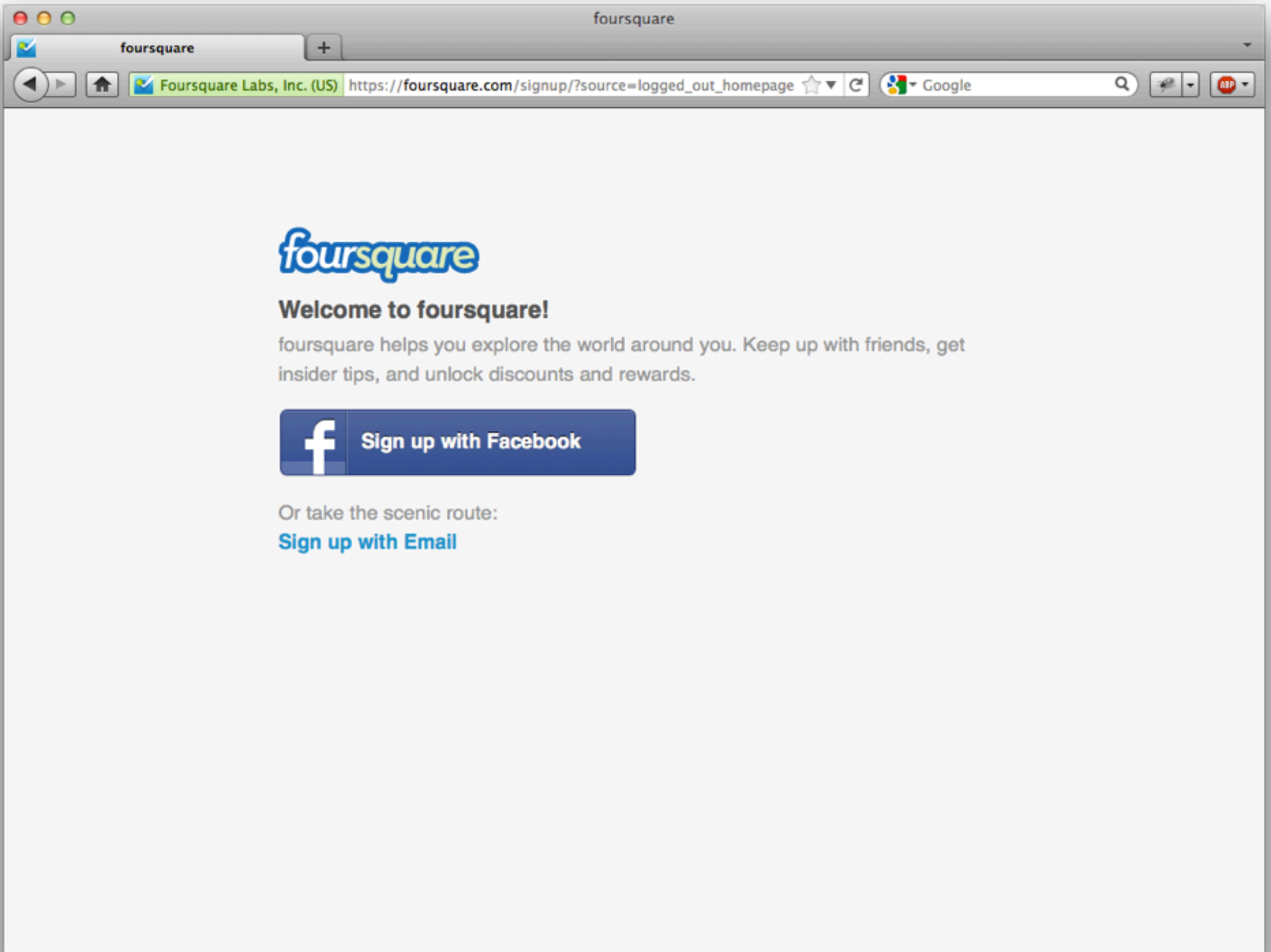
oauth.net





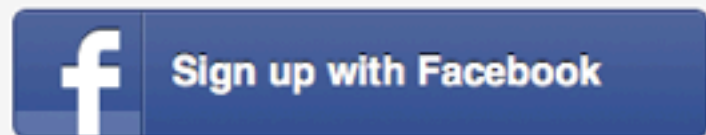
The **flow**

User clicks “sign in” in
the client application



Welcome to foursquare!

foursquare helps you explore the world around you. Keep up with friends, get insider tips, and unlock discounts and rewards.



Or take the scenic route:

[Sign up with Email](#)

The user is **redirected** to
the resource server and
asked to sign in

Log In | Facebook

facebook.com https://www.facebook.com/login.php?api_key=0&skip_api_login=1&displ: ☆ ABP ▼

f Facebook

You must log in to see this page.

Email:

Password:

☐ Keep me logged in

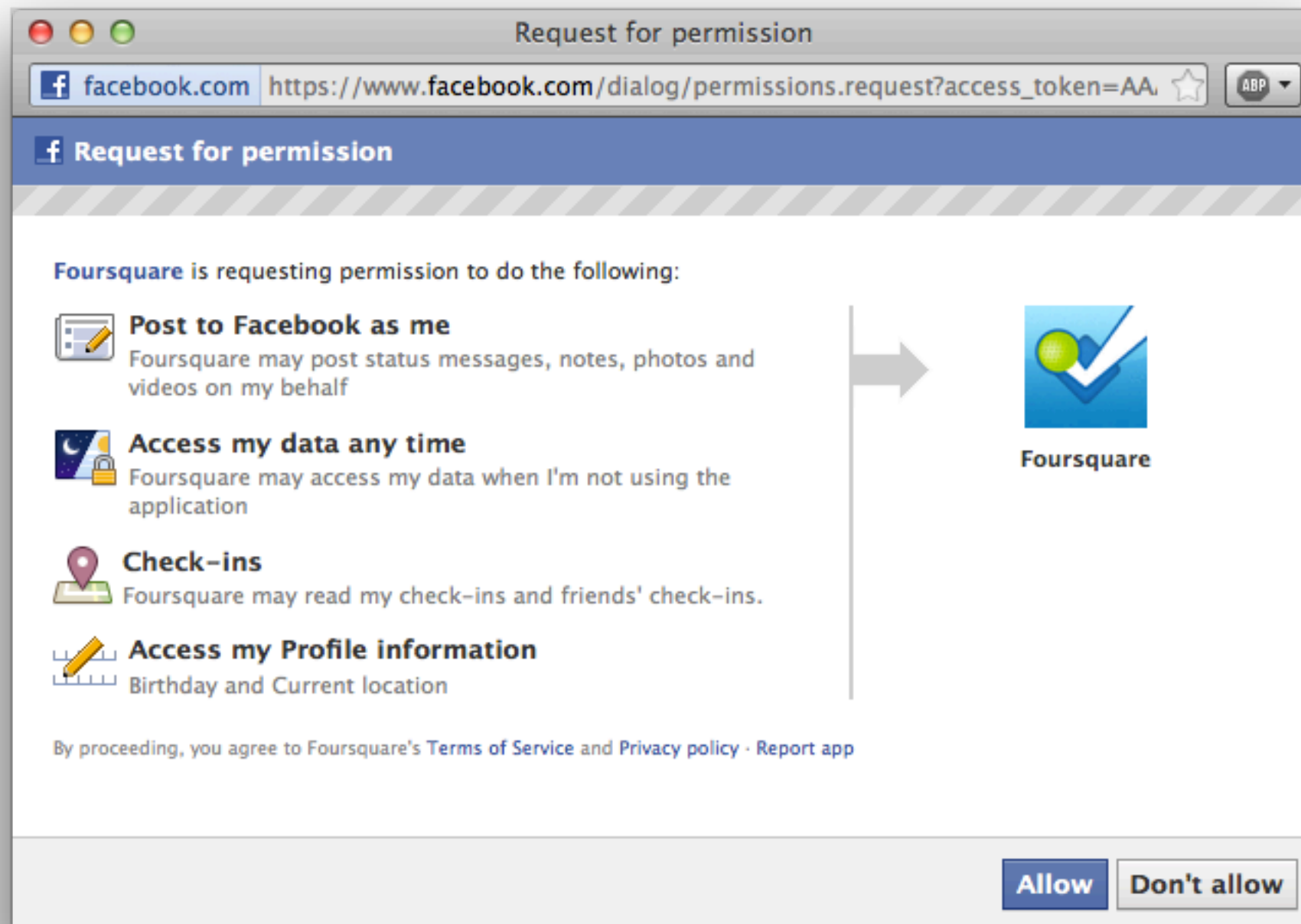
[Forgot your password?](#)

[Sign up for Facebook](#) **Log In** Cancel

GET /authorise?
response_type=code&client_id=12345&redirect_uri=
http://client.tld/
redirect&scope=name,email,birthday HTTP/1.1

Host: resource-server.tld

The resource server clearly
tells the user the **specific**
data the client wants to
access



User **authorises** the application
and is redirected back to client
with a authorisation code in the
query string

HTTP/1.1 302 Found

Location: <http://client.tld/redirect?code=78dsf9sudfo9s>

Client exchanges the
authorisation code for an
access token

POST /token HTTP/1.1

Host: resource-server.tld

Content-type: application/x-www-form-urlencoded

code=78dsf9sudfo9s&client_id=12345&client_secret=12345&redirect_uri=http://client.tld/redirect

HTTP/1.1 200 OK

Content-type: application/json

```
{  
    access_token: "aLKJHskjhda8s13jsi9sis",  
    valid_until: 1320759526  
}
```

The access token can then be used as **authorisation** by the client to access the **specified** resources for a specific length of time

Advantages

No password sharing



<- Happy security conscious user

Developers just need to
implement **a redirect**
and a **POST request**



<- Happy developers

Users can **revoke**
access tokens for
specific clients

App settings

(1) Twitter / HomeApp settings

facebook.comhttps://www.facebook.com/settings?tab=applicationsGoogle
















facebookSearchAlex BilbieFind friendsHome

GeneralSecurityNotificationsAppsMobilePaymentsFacebook Adverts

You can also visit your [privacy preferences](#) or edit your [Timeline](#) to control who sees the info there.

App settings

You have authorised these apps to interact with your Facebook account:

 Meetup	Sunday	Edit	×
 Spotify	04 November	Edit	×
 Diaspora	03 November	Edit	×
 Movember Connect Application	01 November	Edit	×
 The Guardian	31 October	Edit	×
 Hipster	10 October	Edit	×
 Foursquare	10 October	Edit	×
 fdCal	More than 6 months ago	Edit	×
 Xbox LIVE	More than 6 months ago	Edit	×
 iPhoto Uploader	More than 6 months ago	Edit	×
 Gist	More than 6 months ago	Edit	×
 Gowalla	More than 6 months ago	Edit	×
 UserVoice	More than 6 months ago	Edit	×
 the BBC website	More than 6 months ago	Edit	×
 Yahoo!	More than 6 months ago		

Chat (8)

Nefarious clients can have
their credentials **revoked** and
all associated access tokens
destroyed immediately





I E T F[®]

Currently version **1.0a**

Incn.eu/giy

Version 2.0
is almost finished

[Incn.eu/bkw](http://incn.eu/bkw)

OAuth 2.0

- Simpler
- Requires all communication over SSL
- New flows
- Better UX

Who's using OAuth?

Google

Microsoft®

YAHOO!

foursquare

twitter

Salesforce

github
SOCIAL CODING

facebook

Google

v1.0a and v2.0

YAHOO!

v1.0a

twitter

v1.0a

github
SOCIAL CODING

v2.0 (prev v1.0a)

Microsoft®

v2.0

foursquare

v2.0 (prev v1.0a)

Salesforce

v2.0 (prev v1.0a)

facebook

v2.0

And in **HE**?



UNIVERSITY OF
LINCOLN

THE UNIVERSITY OF
WARWICK



UNIVERSITY OF
LINCOLN

LINKED OPEN DATA DATA.LINCOLN.AC.UK

[Home](#) [Documentation](#) [Licence](#)

Get the data!

API methods with a symbol require authentication.

[Events](#) [Calendars](#) [Locations](#) [People](#) [Courses](#) [Energy](#) [Bibliographic](#) [URL Shortening](#) [Authentication](#)

Events

Upcoming events

Returns a user's upcoming events. Does not include any events that have already started when request was made.

Endpoint

<https://nucleus.online.lincoln.ac.uk/events/agenda>

HTTP method

GET

Required parameters

access_token A valid OAuth access token

Optional parameters

calendar_id Limits results to events from a specific calendar

type Event type - set to 'academic', 'assignment', 'library' or 'user'. Default is all event types.

freebusy Set to 1 to hide the title of the event

location_id Valid campus_id, building_id or room_id. Comma separated for multiple locations.

user_id Returns upcoming events for a specific user (autonomous access tokens only)

limit The number of results to return (default 15)

Events occurring at a specific time

Returns all of a user's events occurring at a specific time.

documents

people

location

calendars

data.lincoln.ac.uk

bibliographic

energy

printing

events

Internal and external authorisation

Single Sign-On

Blackboard	(SAML)
Zendesk	(SAML)
Get Satisfaction	(OAuth)
WordPress	(OAuth)
Exchange	(ADFS)
Sharepoint	(ADFS)
Gmail	(SAML)
+ OAuth clients (internal + external)	

Open source 2.0 server

Incn.eu/ar6

Any questions?

Thank you

@alexbilbie