OAuth: the spec, the dance, and drupal

Chris Christensen

@imetchrischris

AllPlayers.com

The Web: HTTP/1.0

- Client <-- --> Server
- GET, PUT, POST, DELETE, HEAD, ...
- Headers

Auth experience

- HTTP Basic Auth - IETF RFC 1945
  - Simple!
  - Plaintext (SSL can "help")
  - Relys on client/browser authentication popup

Example with Basic Auth:

```
curl -u "username:password" https://www.example.com/special
```

Auth experience

- Session Auth (cookies) IETF RFC 6265
  - "free" with most web frameworks
  - A session is usually tied to one user account and is normally authorized fully or not.

Example with cookies holding state through a session:

```
curl -c cookiejar.txt https://www.example.com/login
curl -b cookiejar.txt https://www.example.com/special
```

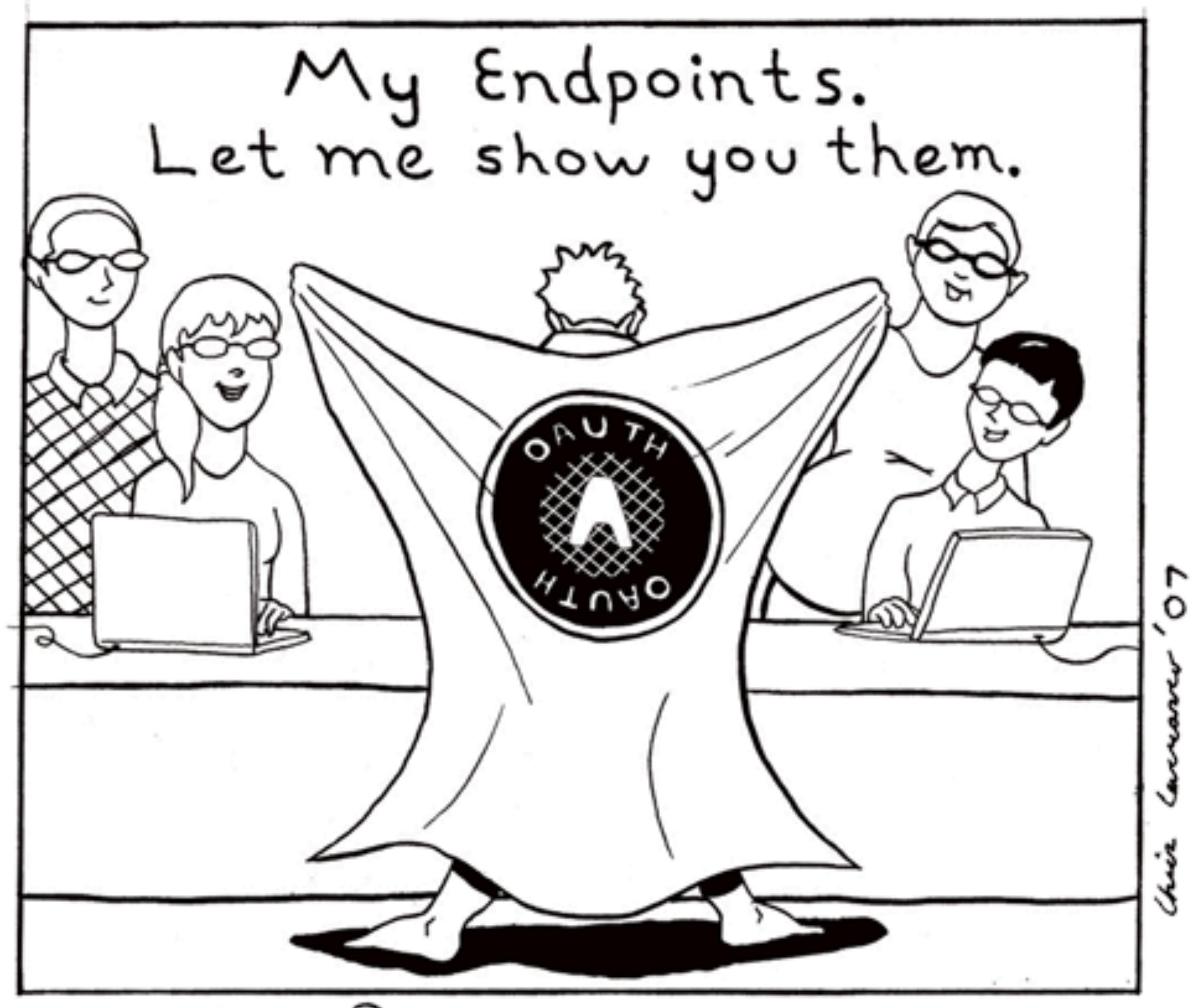
Auth experience

- OAuth IETF RFC 5849
  - "Valet key for the web" (limited access OAuth Token)
  - Scope access to resources

Example of a signed OAuth request:

```
<special signing sauce>
curl -v -H 'Authorization: OAuth
 oauth_consumer_key="zsQpwbL3AGRNV4272Xc8Msi3hxhQWGrS",
 oauth_signature_method="HMAC-SHA1",
 oauth_timestamp="1346887460",
 oauth_nonce="1548267549",
 oauth_version="1.0",
 oauth_token="wvokahqtGMLS5o4AvVvokGZaA9pZjBcW",
 oauth_signature="tvHRw2fLNxYE2FR62EfH6tAfBW4%3D"'
https://www.example.com/special
```

So what's so special about OAuth?



© hueniverse.com

So what's so special about OAuth?

- Each **client** is assigned **credentials** granted by a **resource owner** to access a **protected resource** on a **server**
    - Note: Client <-- (stuff) --> Server
    - Therefore the credentials granted to a *specific client* can be *managed/revoked* by the resource owner.

- An endpoint(s)/HTTP resource(s) can be **scoped** (to limit its functionality)
    - "I give you (Ms. client) access to my API, but read only."
    - "Access all of my public data (Mr. client)"
    - "(Mrs. Client) Is requesting access you your bank account, allow?"

What about that guy on the internet (Eran Hammer) that was like "OAuth 2.0 sucks" **!!rage quit!!** ?!!

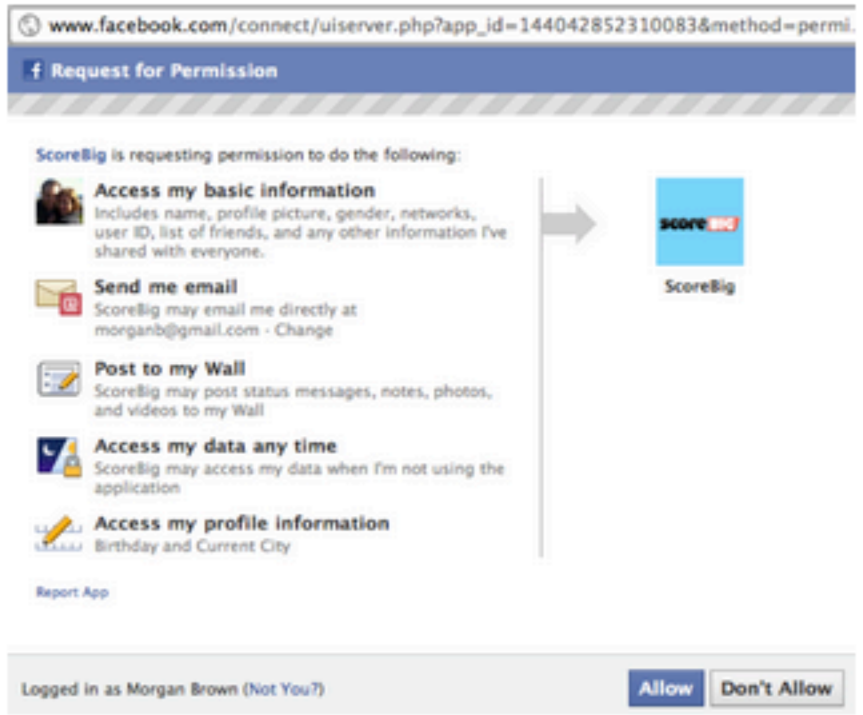
Agree or disgree ... most importantly: he's an expert and is prosthelytizing great information - **Listen to him!** (and read carefully)

The takeaway: dont throw the baby out with the bathwater and his commentary is directed at the 2.0 *draft*

Halt!

Let's Dance

What OAuth looks like



www.facebook.com/connect/uiserver.php?app_id=144042852310083&method=permi...

Request for Permission

ScoreBig is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

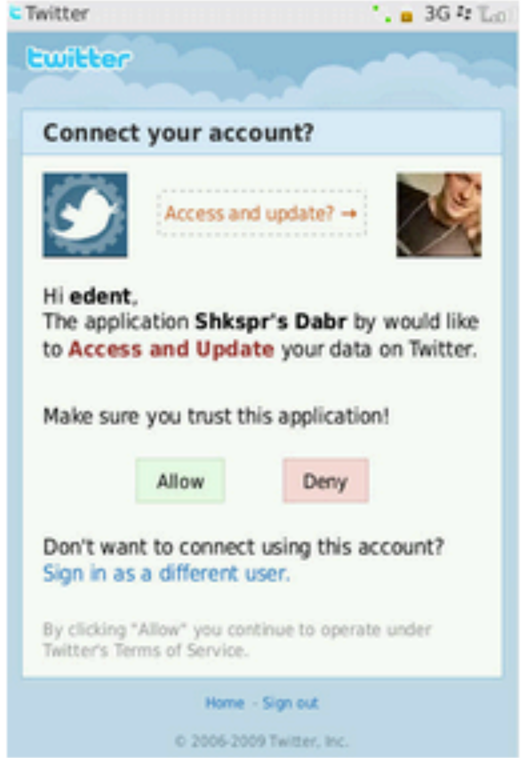
Send me email
ScoreBig may email me directly at morganb@gmail.com · Change

Post to my Wall
ScoreBig may post status messages, notes, photos, and videos to my Wall

Access my data any time
ScoreBig may access my data when I'm not using the application

Access my profile information
Birthday and Current City

Logged in as Morgan Brown (Not You?)



Connect your account?

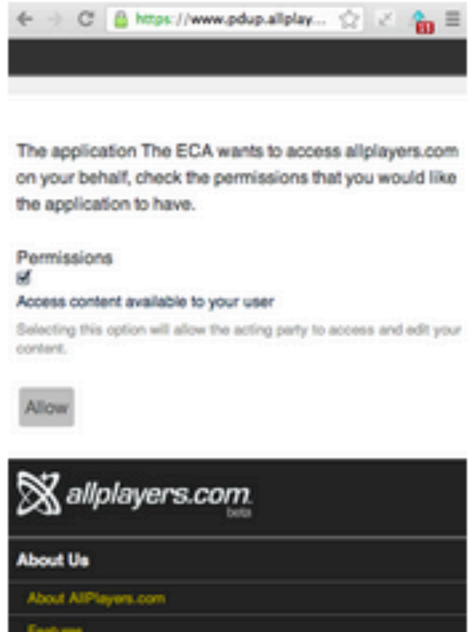
Hi **edent**,
The application **Shkspr's Dabr** by would like to **Access and Update** your data on Twitter.

Make sure you trust this application!

Don't want to connect using this account?
Sign in as a different user.

By clicking "Allow" you continue to operate under Twitter's Terms of Service.

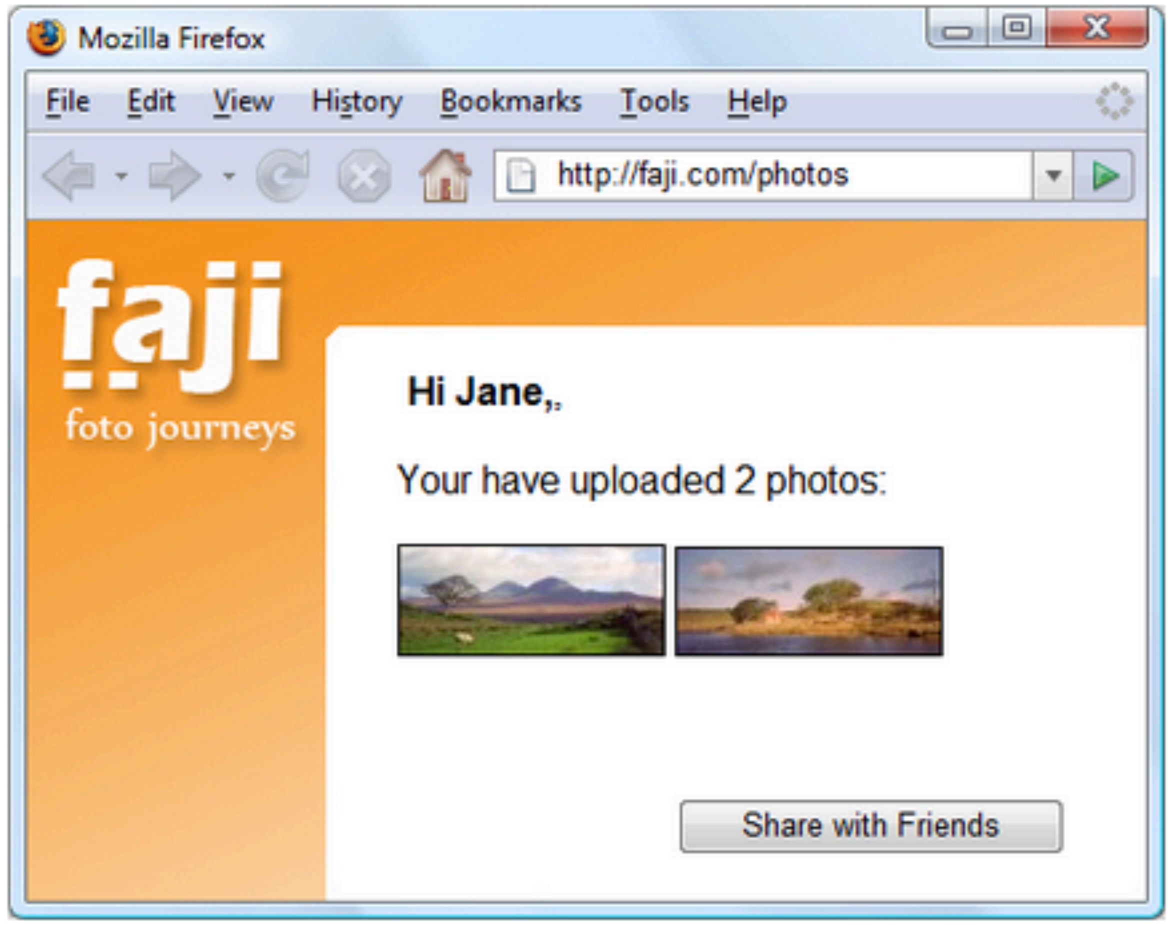
© 2006-2009 Twitter, Inc.



The application The ECA wants to access allplayers.com on your behalf, check the permissions that you would like the application to have.

Permissions
☑
Access content available to your user
Selecting this option will allow the acting party to access and edit your content.

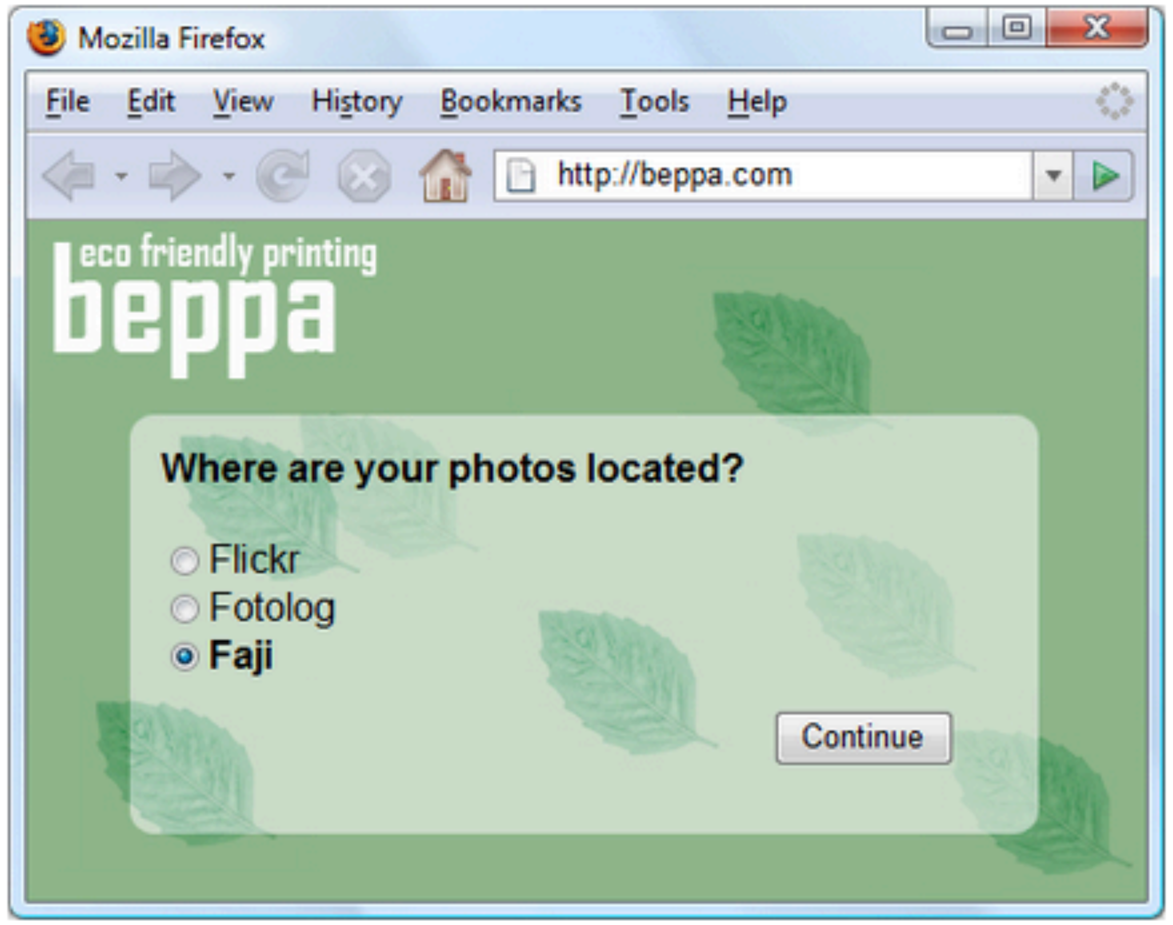
What OAuth looks like: Protocol workflow



http://faji.com/photos

Hi Jane,,

Your have uploaded 2 photos:

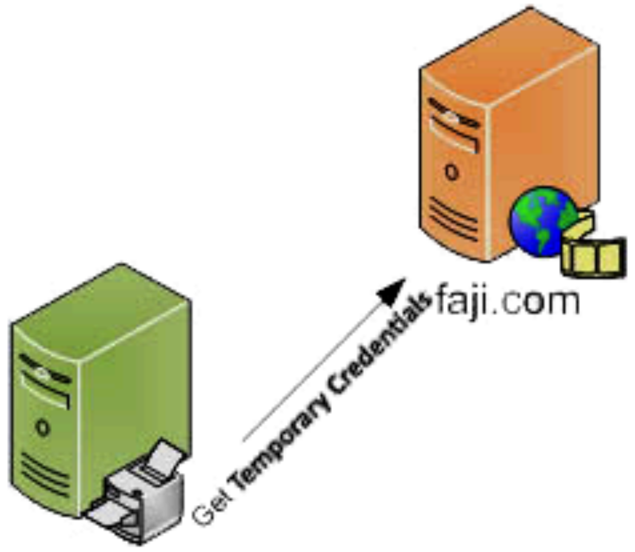


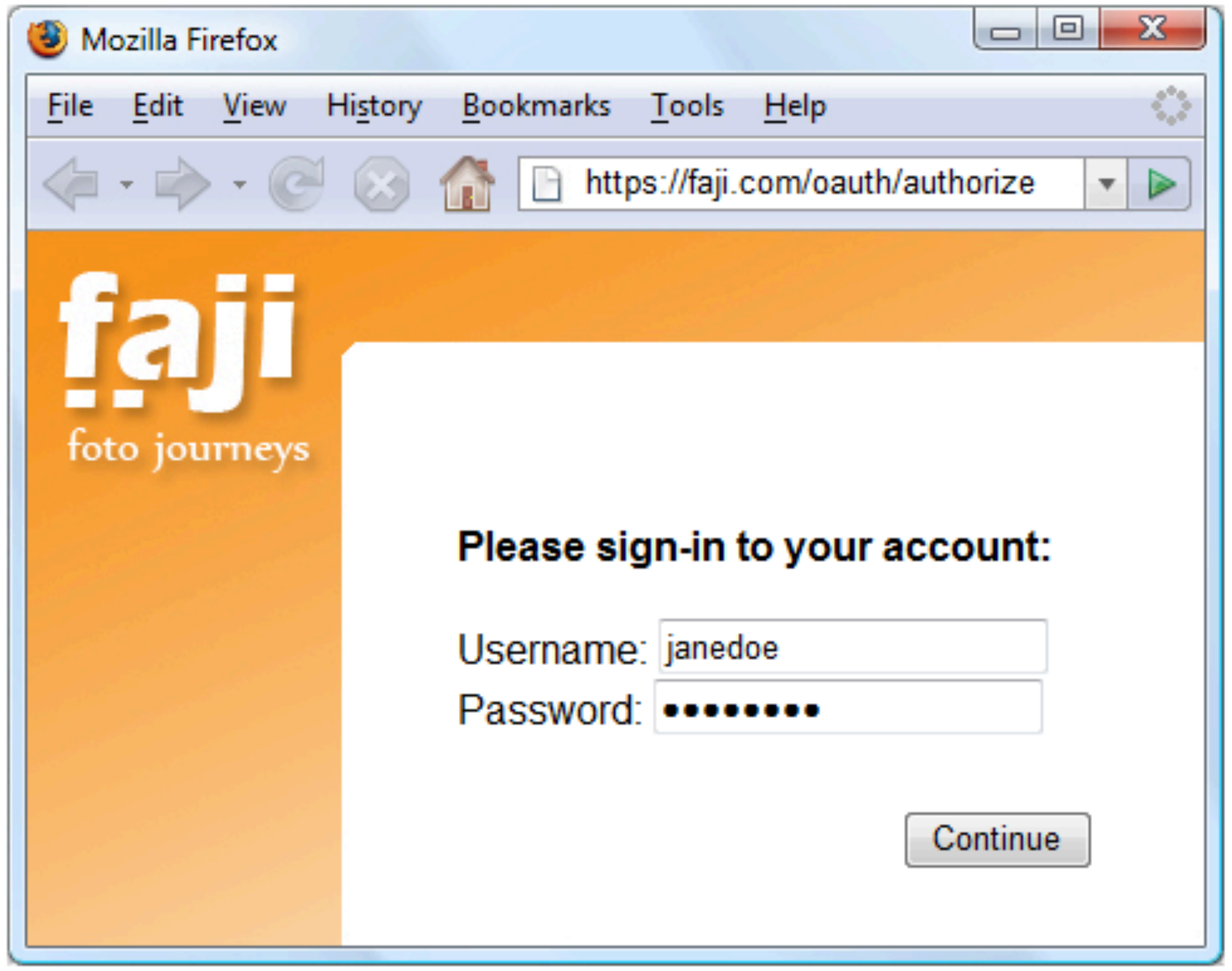
http://beppa.com

Where are your photos located?

○ Flickr
○ Fotolog
● **Faji**

What OAuth looks like: Protocol workflow



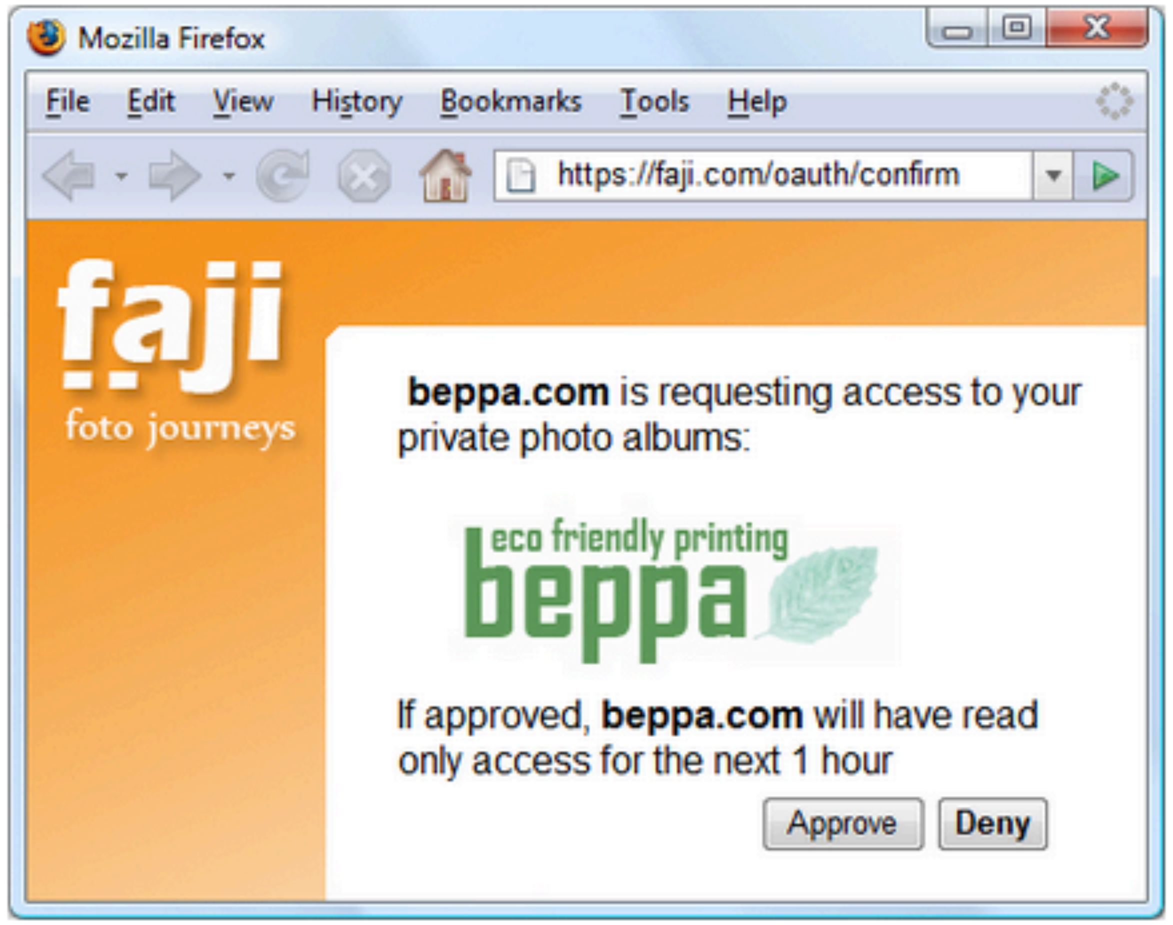

Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://faji.com/oauth/authorize
faji
foto journeys

Please sign-in to your account:

Username: janedoe

Password: •••••••••

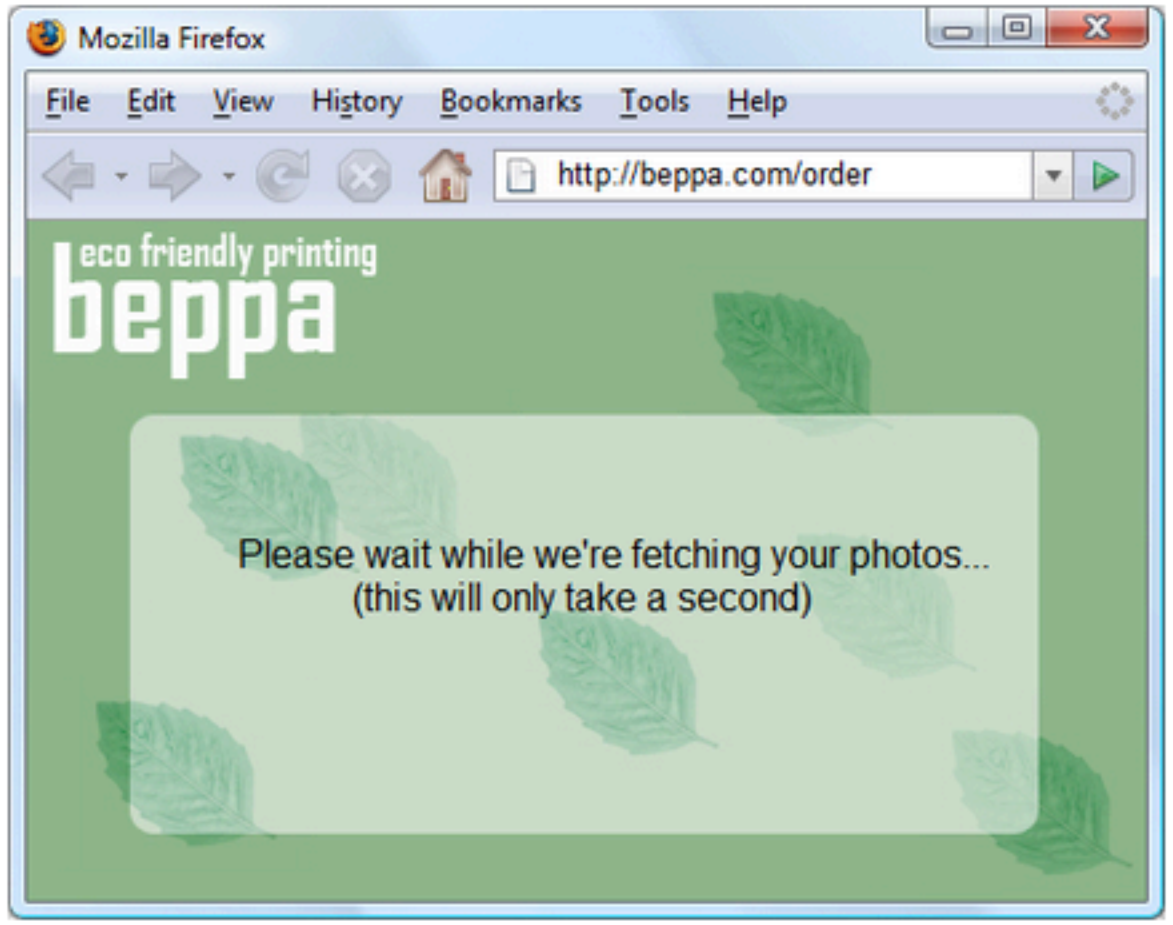
What OAuth looks like: Protocol workflow



https://faji.com/oauth/confirm

beppa.com is requesting access to your private photo albums:

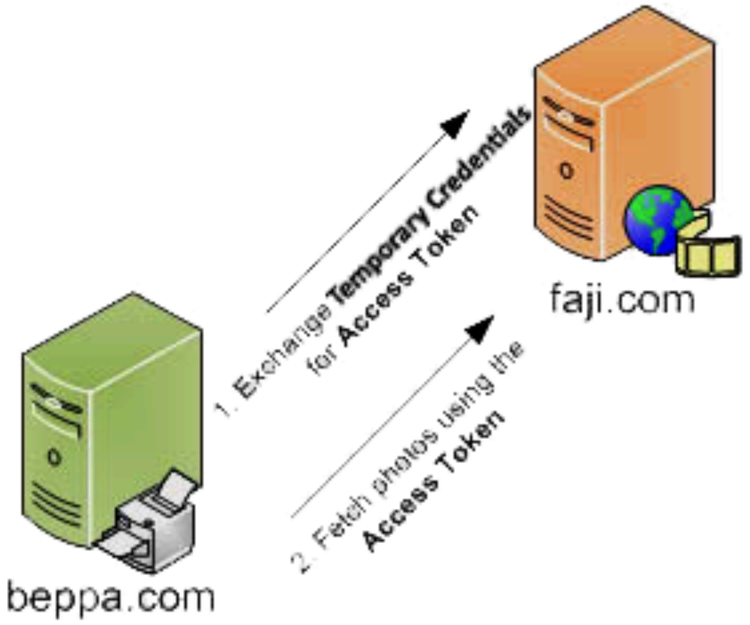
If approved, **beppa.com** will have read only access for the next 1 hour



http://beppa.com/order

Please wait while we're fetching your photos...
(this will only take a second)

What OAuth looks like: Protocol workflow

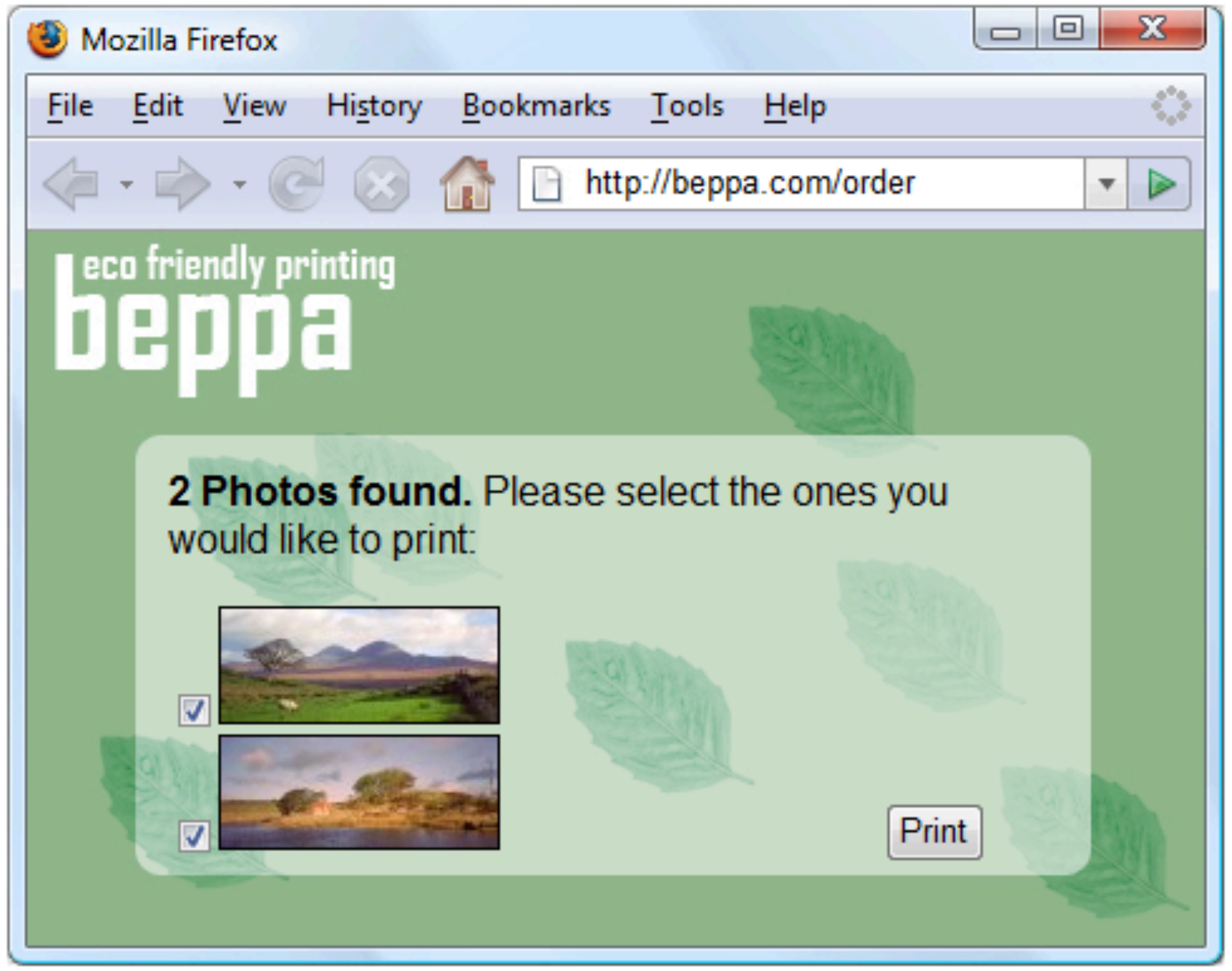


faji.com

1. Exchange **Temporary Credentials** for **Access Token**

2. Fetch photos using the **Access Token**

beppa.com



2 Photos found. Please select the ones you would like to print:

☑

☑

Technical pieces

Terminology

- Consumer: client
- Service Provider: server
- User: resource owner
- Consumer Key and Secret: client credentials
- Request Token and Secret: temporary credentials
- Access Token and Secret: token credentials

URL pattern(s)

(Related to protocol workflow)

- https://provider.example.net/{initiate,request_token} (Temporary Credential Request)
- https://provider.example.net/authorize (Resource Owner Authorization URI)
- https://provider.example.net/{token,access_token} (Token Request UR)
- http://consumer.example.com/{oauth_redirect,ready,...}

(Ref: URL patterns for Twitter, AllPlayers.com)

Demo Time

Refs

- http://tools.ietf.org/html/rfc1945#section-10.16 / http://en.wikipedia.org/wiki/Basic_access_authentication
- http://tools.ietf.org/html/rfc6265 / http://en.wikipedia.org/wiki/HTTP_cookie
- http://tools.ietf.org/html/rfc5849 / http://en.wikipedia.org/wiki/OAuth
- OAuth Checklist
- Build out and scratch pad notes
- Public Key Cryptography: Diffie-Hellman Key Exchange