MASHERY

Authorization with OAuth

Rob Richards

October 22, 2009

cdatazone.org

http://xri.net/=rob.richards

Authentication

- HTTP Authentication
  - Basic
  - Digest
  - TLS/SSL
- WS-Security
- Developer Keys
- 3rd Party Authentication
  - Yahoo BBAuth
  - AOL OpenAuth

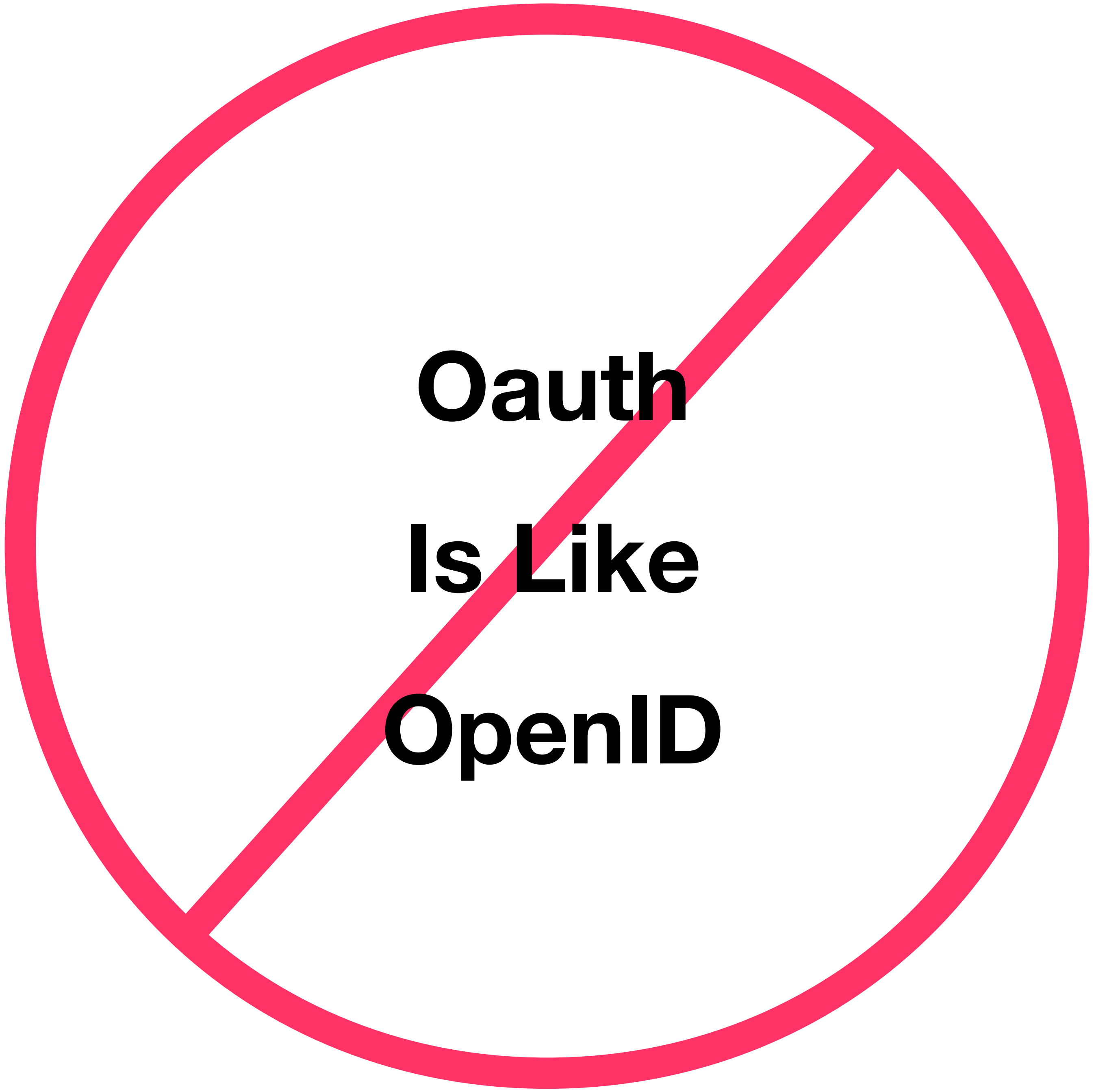
OAuth

An Open Protocol

to allow

Secure API Authorization

Oauth is not OpenID

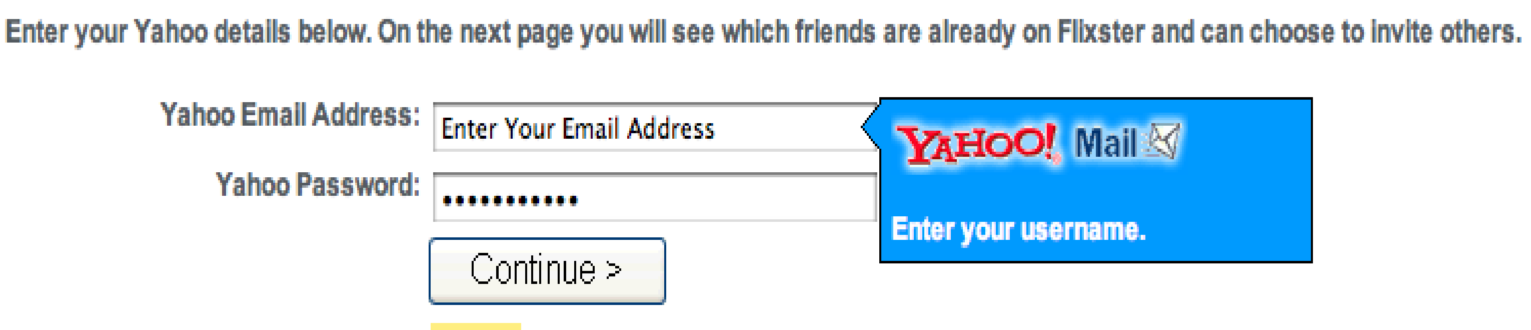


Oauth

Is Like

OpenID

Data Authorization



Enter your Yahoo details below. On the next page you will see which friends are already on Flixster and can choose to invite others.

Yahoo Email Address: Enter Your Email Address

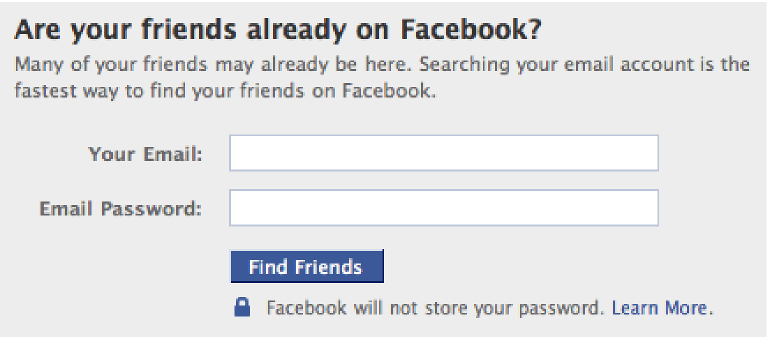
Yahoo Password: ••••••••••••

Continue >

YAHOO! Mail

Enter your username.

Or use: Hotmail | Yahoo | Gmail | AOL



Are your friends already on Facebook?

Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

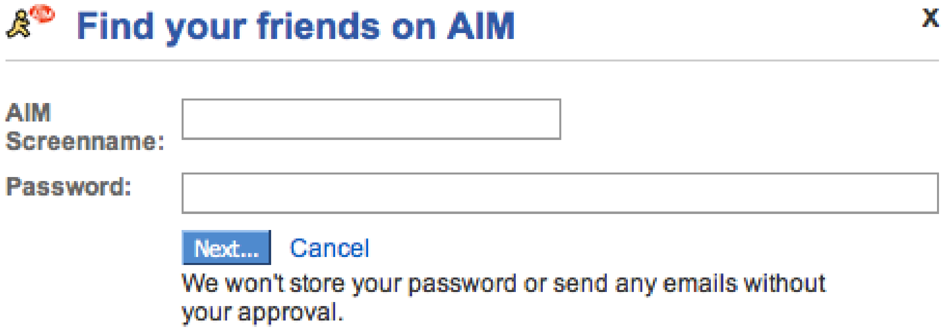
Your Email:

Email Password:

Find Friends

Facebook will not store your password. Learn More.

Plaxo



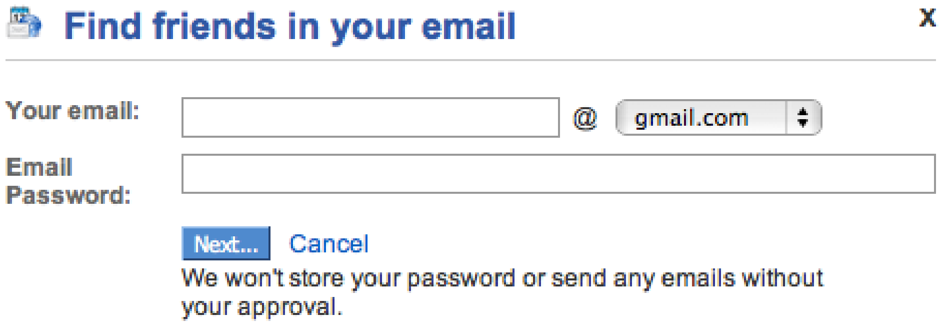
Find your friends on AIM x

AIM Screenname:

Password:

Next... Cancel

We won't store your password or send any emails without your approval.



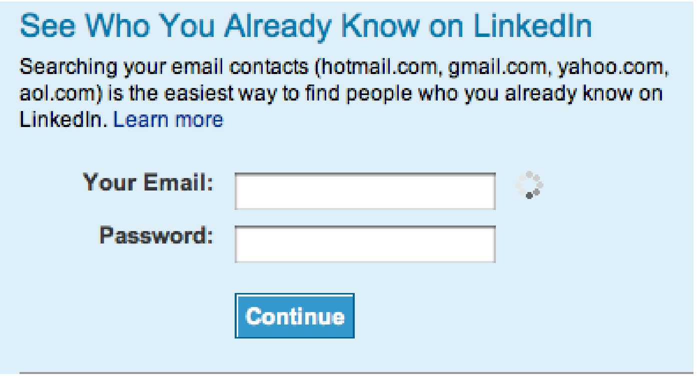
Find friends in your email x

Your email: @ gmail.com

Email Password:

Next... Cancel

We won't store your password or send any emails without your approval.



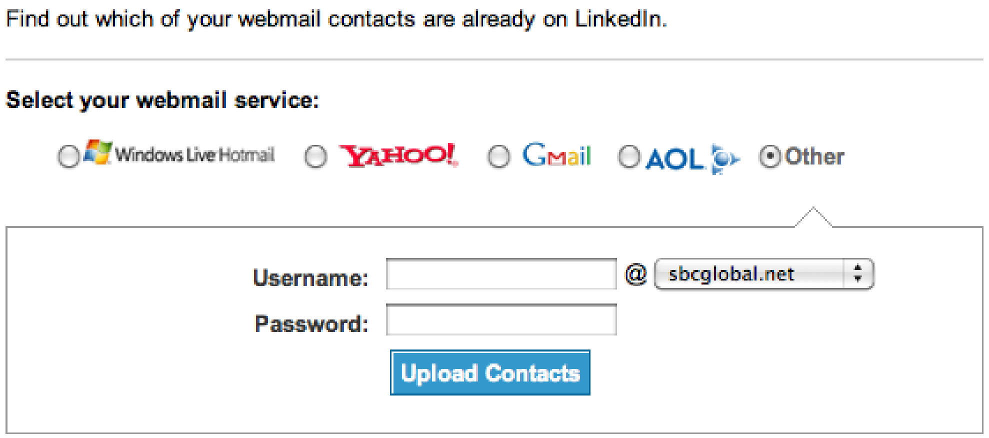
See Who You Already Know on LinkedIn

Searching your email contacts (hotmail.com, gmail.com, yahoo.com, aol.com) is the easiest way to find people who you already know on LinkedIn. Learn more

Your Email:

Password:

Continue



Find out which of your webmail contacts are already on LinkedIn.

Select your webmail service:

○ Windows Live Hotmail ○ YAHOO! ○ GMail ○ AOL ● Other

Username: @ sbcglobal.net

Password:

Upload Contacts

OAuth

OAuth

is like a

Valet Key

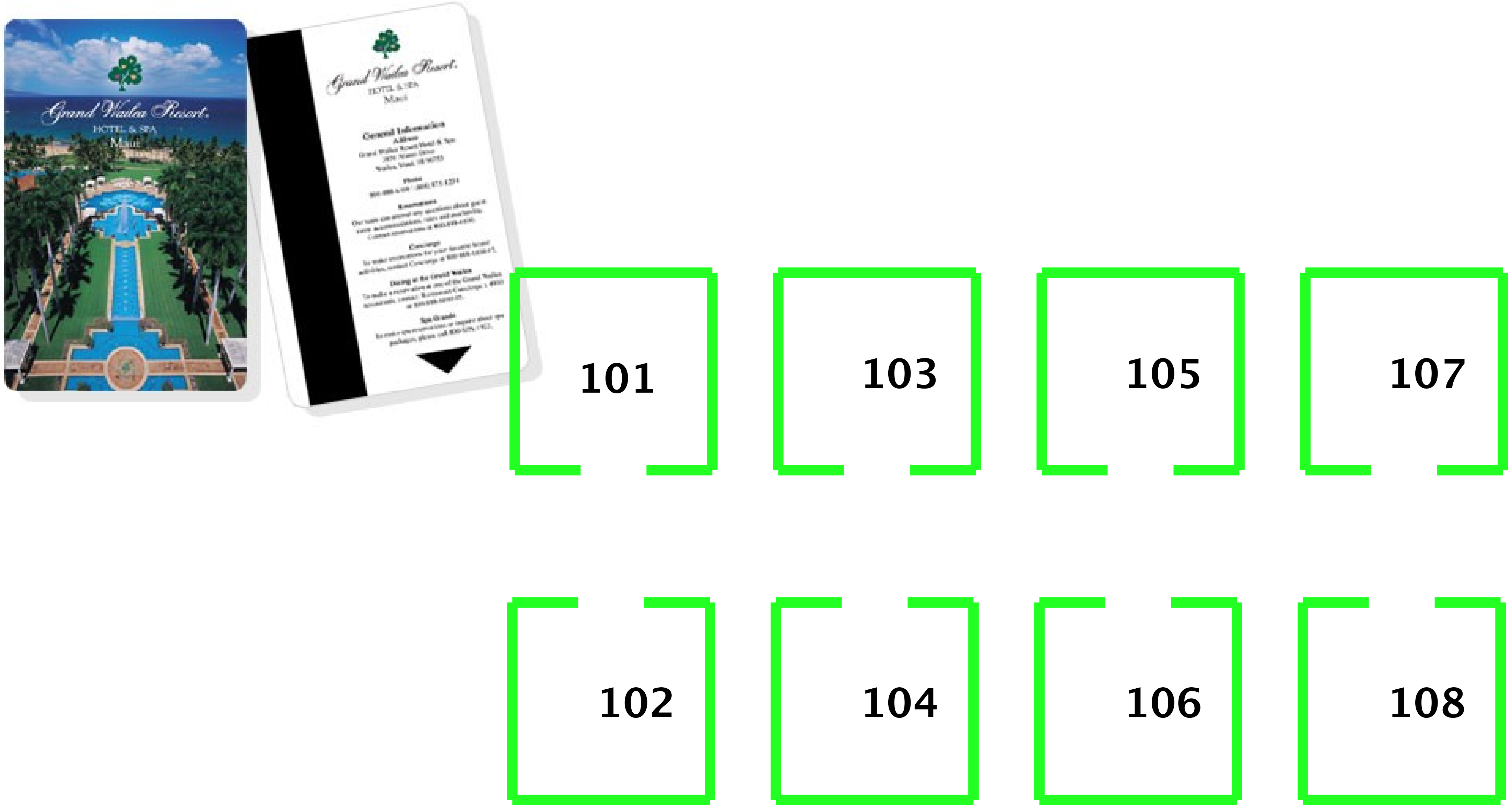
OAuth

OAuth

is like a

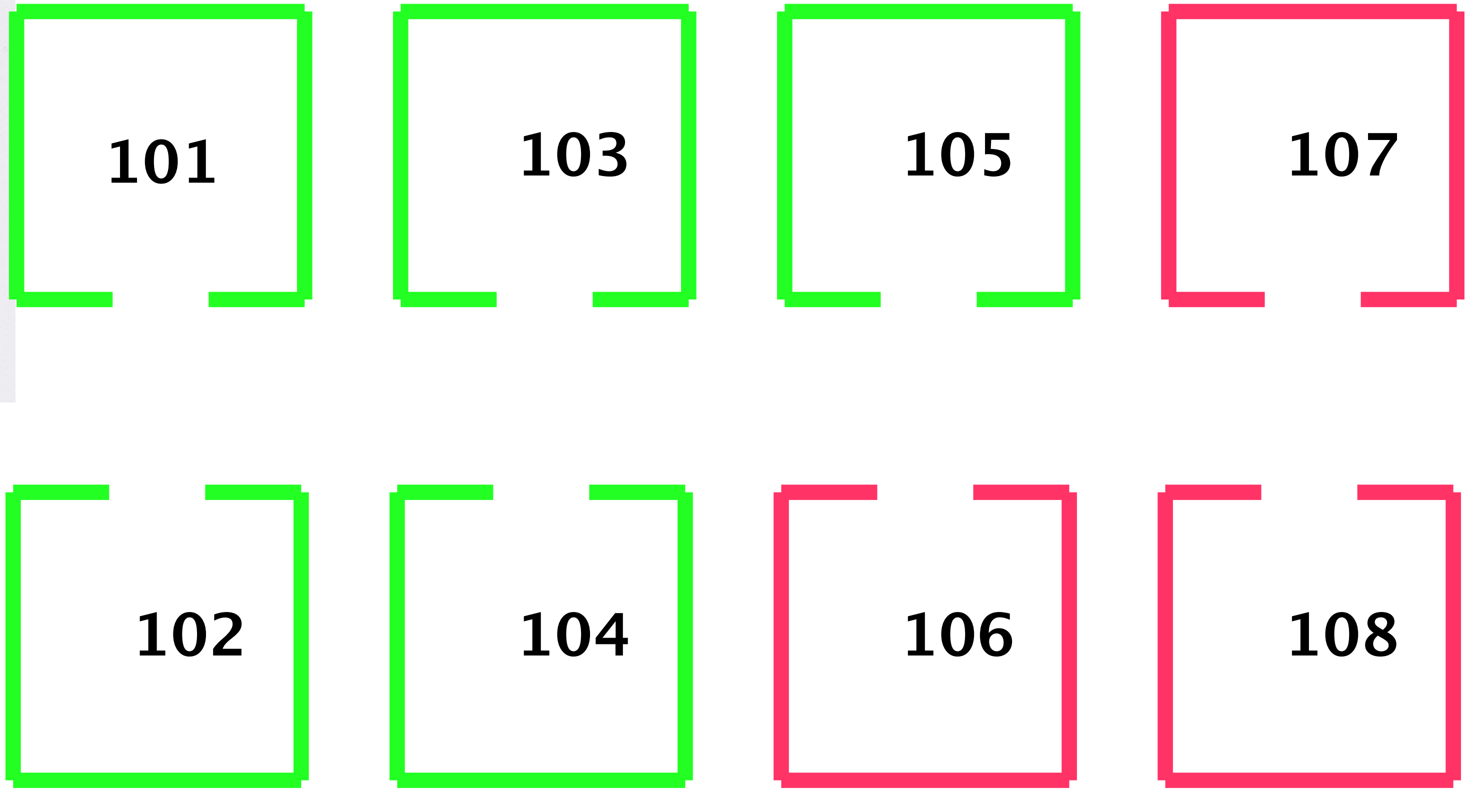
Hotel Keycard

Master Key


Grand Wailea Resort
HOTEL & SPA
Maui
101
103
105
107
102
104
106
108

Guest Key: Granting Access

KEY CARD
THE LEAFY HOTEL
An alternative way to stay
I am an environmentally-friendly card made from recycled PVC.
Hotel Keycard
I am a card made from plastic. I've already bee
www.eco-card.co.uk 0845 643 5125
PVC

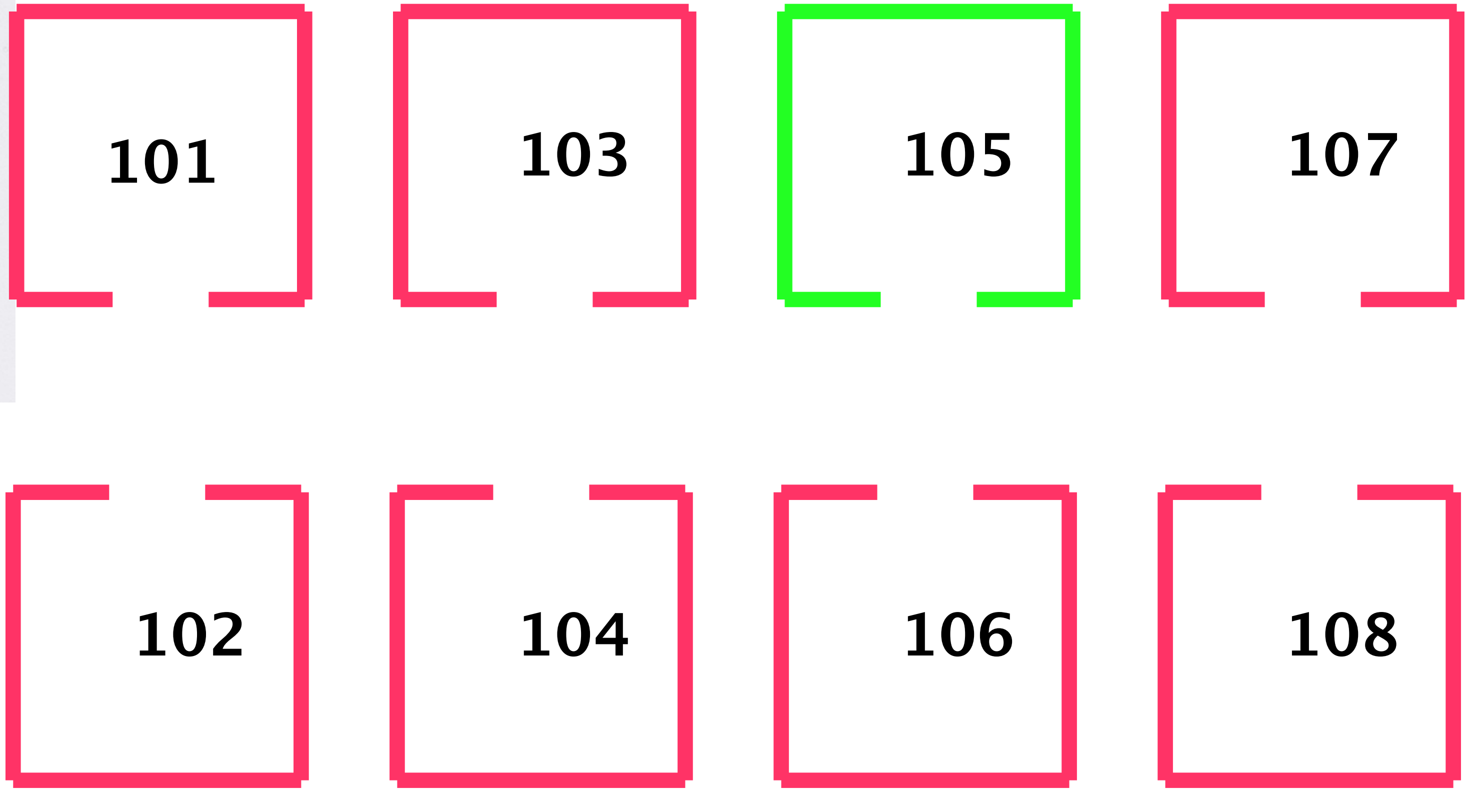


101 103 105 107

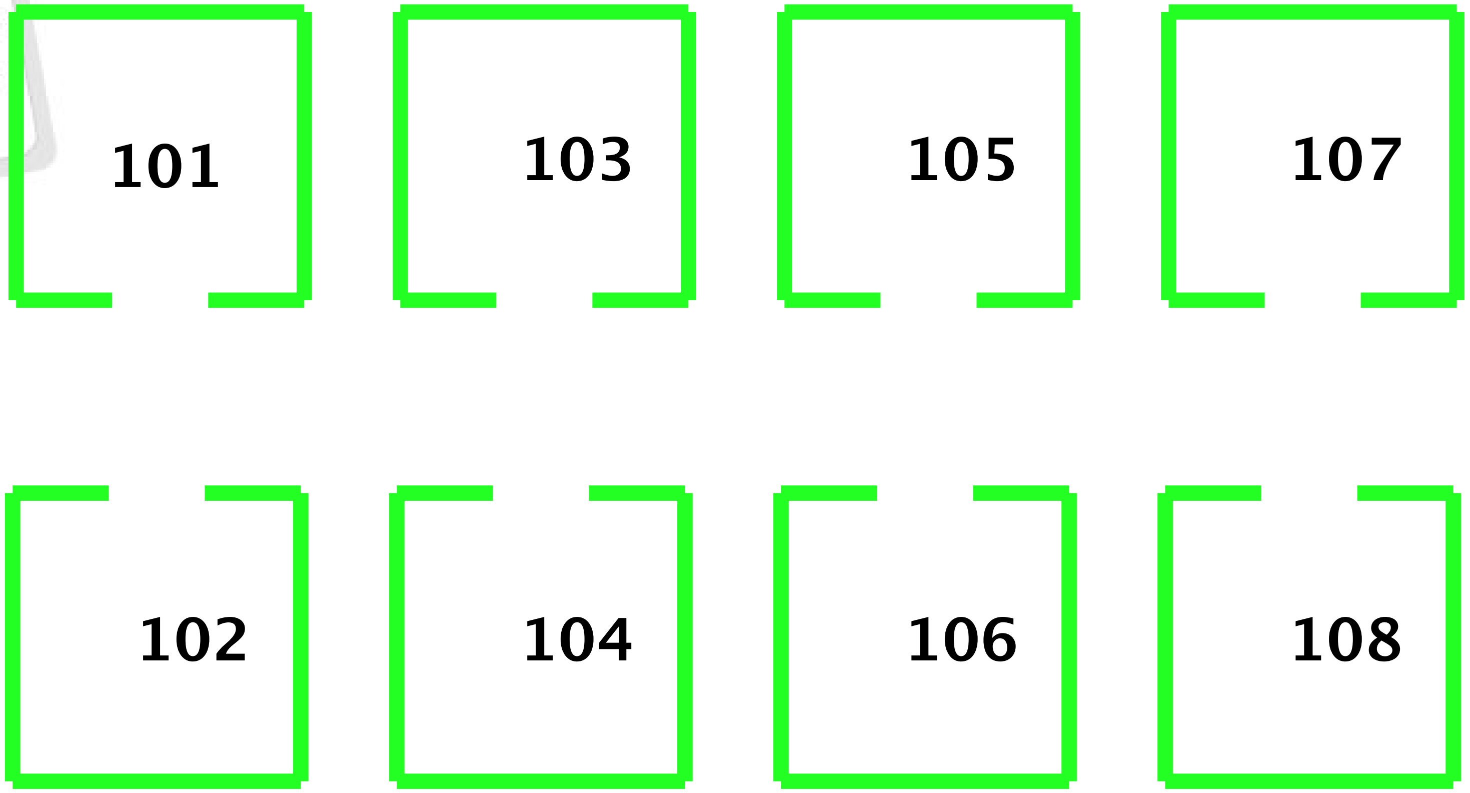
102 104 106 108

Guest Key: Revoking Access

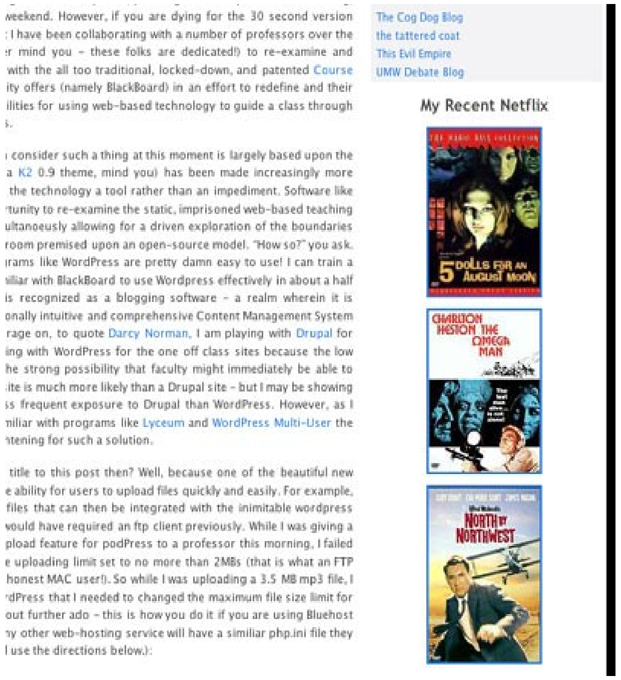
KEY CARD
THE LEAFY HOTEL
An alternative way to stay
I am an environmentally-friendly card made from recycled PVC.
Hotel Keycard
I am a card made from plastic. I've already bee
www.eco-card.co.uk 0845 643 5125
PVC



Master Key Maintains Full Access


101
103
105
107
102
104
106
108

Oauth Clients



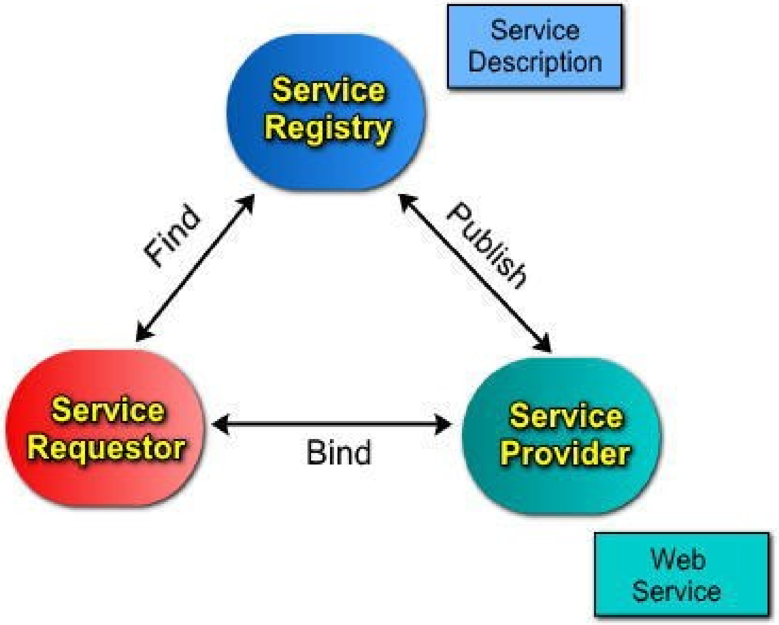
weekend. However, if you are dying for the 30 second version
: I have been collaborating with a number of professors over the
r mind you – these folks are dedicated!) to re-examine and
with the all too traditional, locked-down, and patented Course
ity offers (namely BlackBoard) in an effort to redefine and their
ilities for using web-based technology to guide a class through
s.

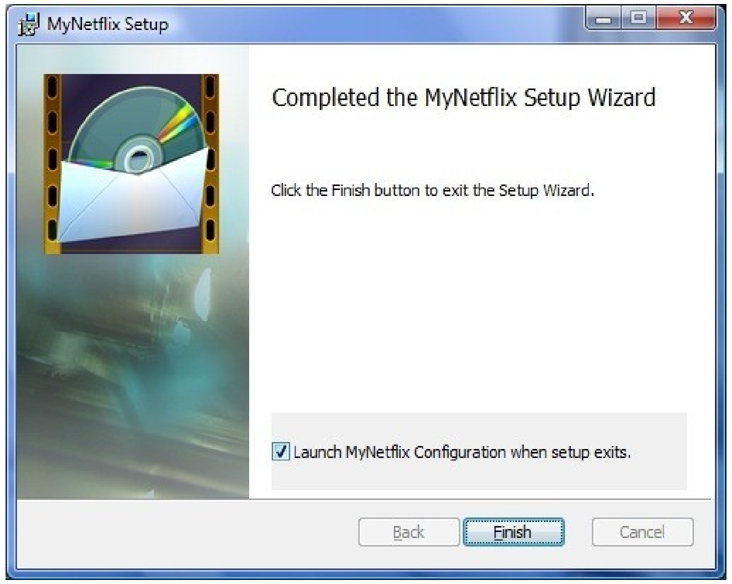
consider such a thing at this moment is largely based upon the
a K2 0.9 theme, mind you) has been made increasingly more
the technology a tool rather than an impediment. Software like
rtunity to re-examine the static, imprisoned web-based teaching
ultanoeusly allowing for a driven exploration of the boundaries
room premised upon an open-source model. "How so?" you ask.
rams like WordPress are pretty damn easy to use! I can train a
iliar with BlackBoard to use Wordpress effectively in about a half
is recognized as a blogging software – a realm wherein it is
onally intuitive and comprehensive Content Management System
rage on, to quote Darcy Norman, I am playing with Drupal for
ing with WordPress for the one off class sites because the low
he strong possibility that faculty might immediately be able to
ite is much more likely than a Drupal site – but I may be showing
s frequent exposure to Drupal than WordPress. However, as I
miliar with programs like Lyceum and WordPress Multi-User the
ntening for such a solution.

title to this post then? Well, because one of the beautiful new
e ability for users to upload files quickly and easily. For example,
files that can then be integrated with the inimitable wordpress
would have required an ftp client previously. While I was giving a
pload feature for podPress to a professor this morning, I failed
e uploading limit set to no more than 2MBs (that is what an FTP
honest MAC user!). So while I was uploading a 3.5 MB mp3 file, I
rdPress that I needed to changed the maximum file size limit for
out further ado – this is how you do it if you are using Bluehost
ny other web-hosting service will have a similiar php.ini file they
l use the directions below.):

The Cog Dog Blog
the tattered coat
This Evil Empire
UMW Debate Blog

My Recent Netflix





MyNetflix Setup

Completed the MyNetflix Setup Wizard

Click the Finish button to exit the Setup Wizard.

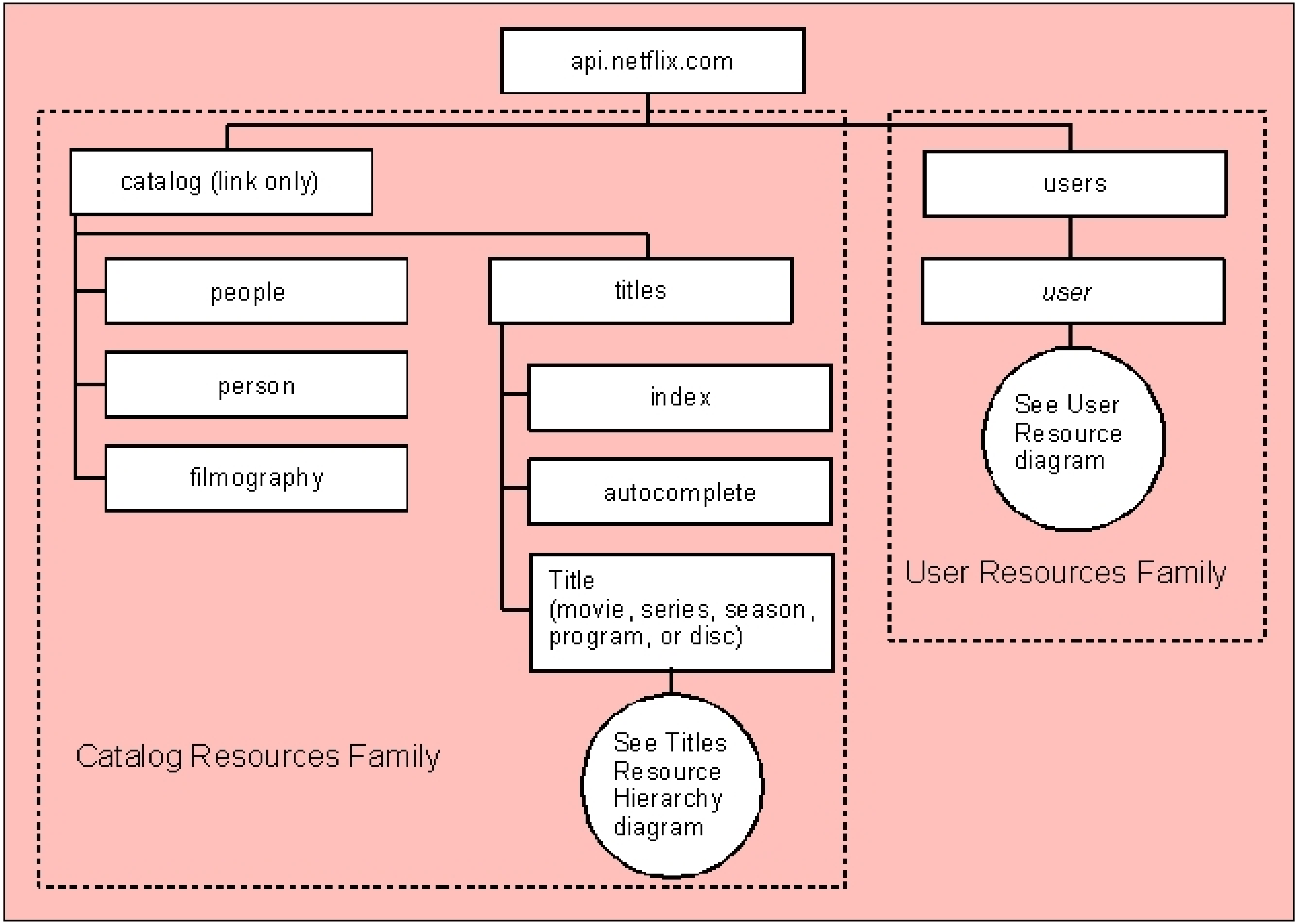
☑ Launch MyNetflix Configuration when setup exits.

MASHERY

OAuth and Netflix

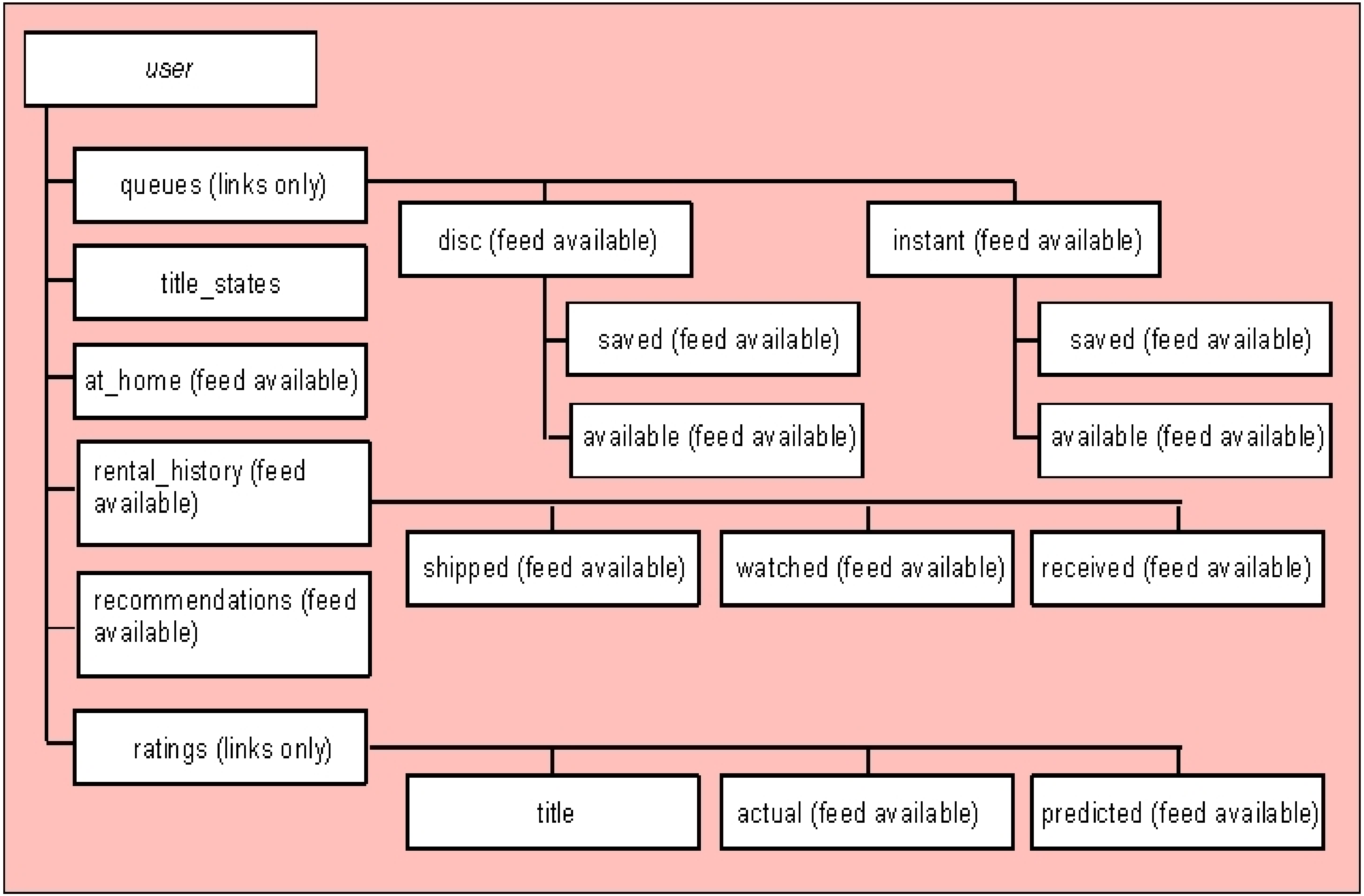
developer.netflix.com

Netf ix API



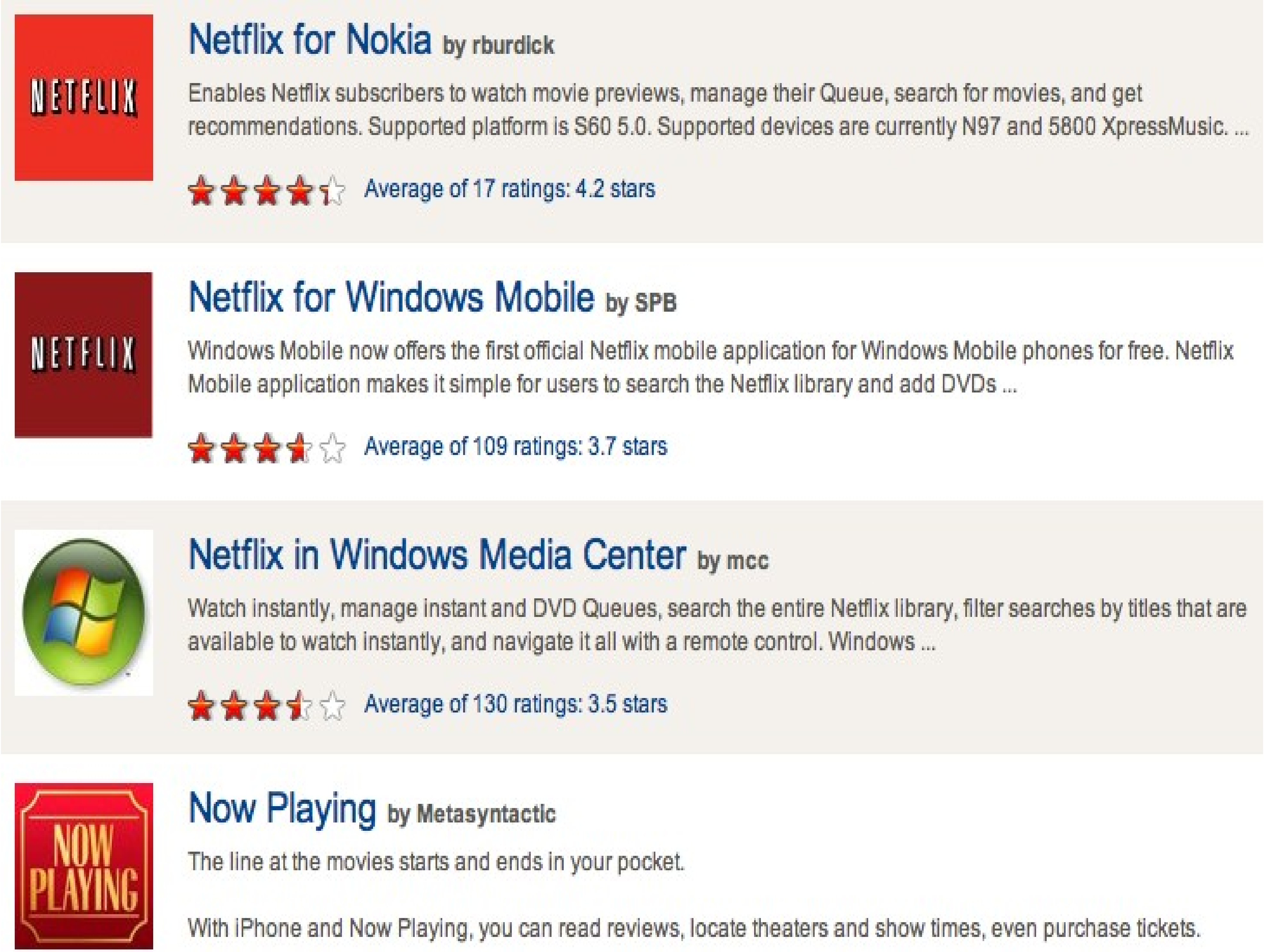
MASHERY

Netflix API: User Resources



MASHERY

Netflix Applications… and many more



Netflix for Nokia by rburdick

Enables Netflix subscribers to watch movie previews, manage their Queue, search for movies, and get recommendations. Supported platform is S60 5.0. Supported devices are currently N97 and 5800 XpressMusic. ...

Average of 17 ratings: 4.2 stars

Netflix for Windows Mobile by SPB

Windows Mobile now offers the first official Netflix mobile application for Windows Mobile phones for free. Netflix Mobile application makes it simple for users to search the Netflix library and add DVDs ...

Average of 109 ratings: 3.7 stars

Netflix in Windows Media Center by mcc

Watch instantly, manage instant and DVD Queues, search the entire Netflix library, filter searches by titles that are available to watch instantly, and navigate it all with a remote control. Windows ...

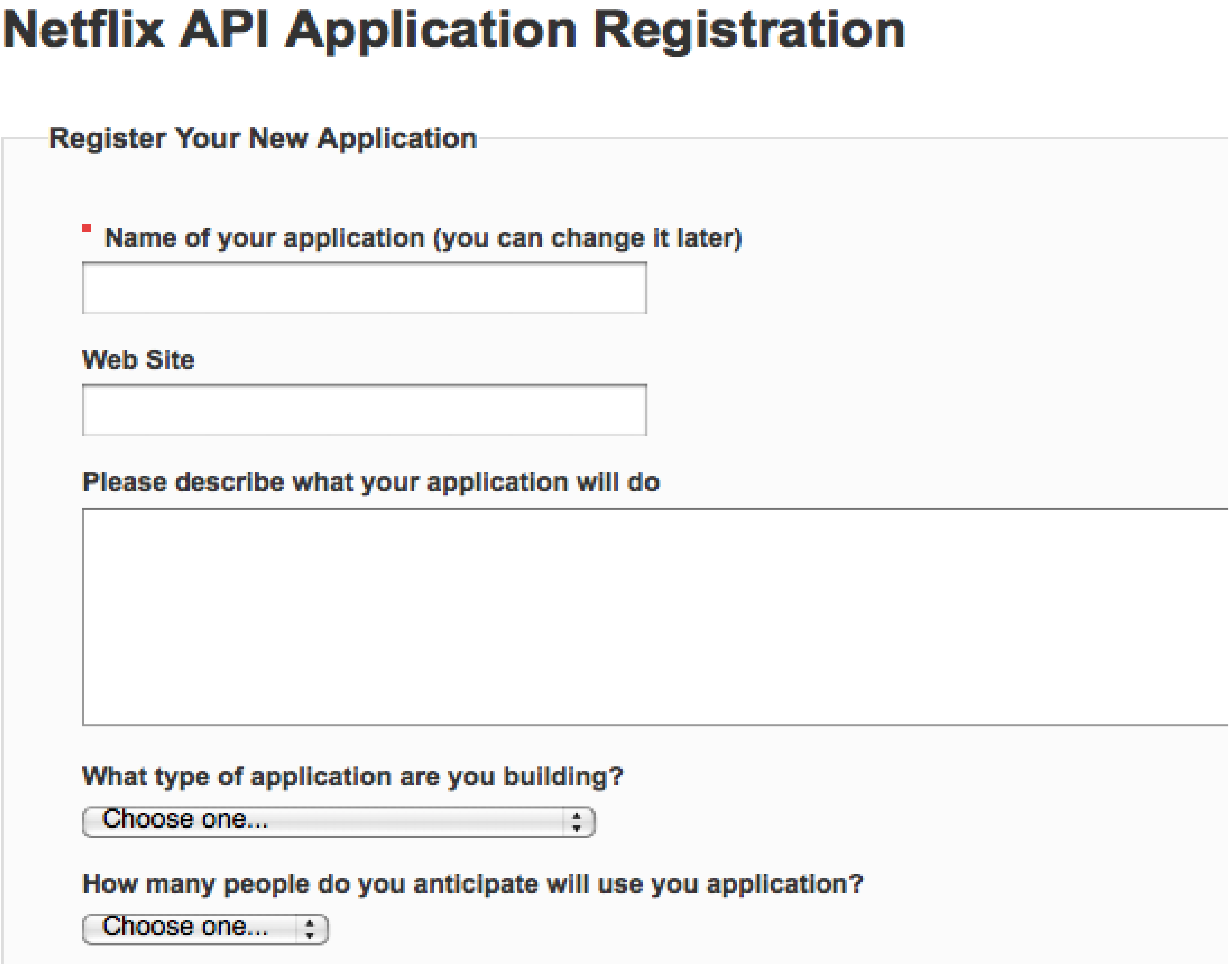
Average of 130 ratings: 3.5 stars

Now Playing by Metasyntactic

The line at the movies starts and ends in your pocket.

With iPhone and Now Playing, you can read reviews, locate theaters and show times, even purchase tickets.

Obtaining a Consumer Key / Secret



Netflix API Application Registration

Register Your New Application

Name of your application (you can change it later)

Web Site

Please describe what your application will do

What type of application are you building?

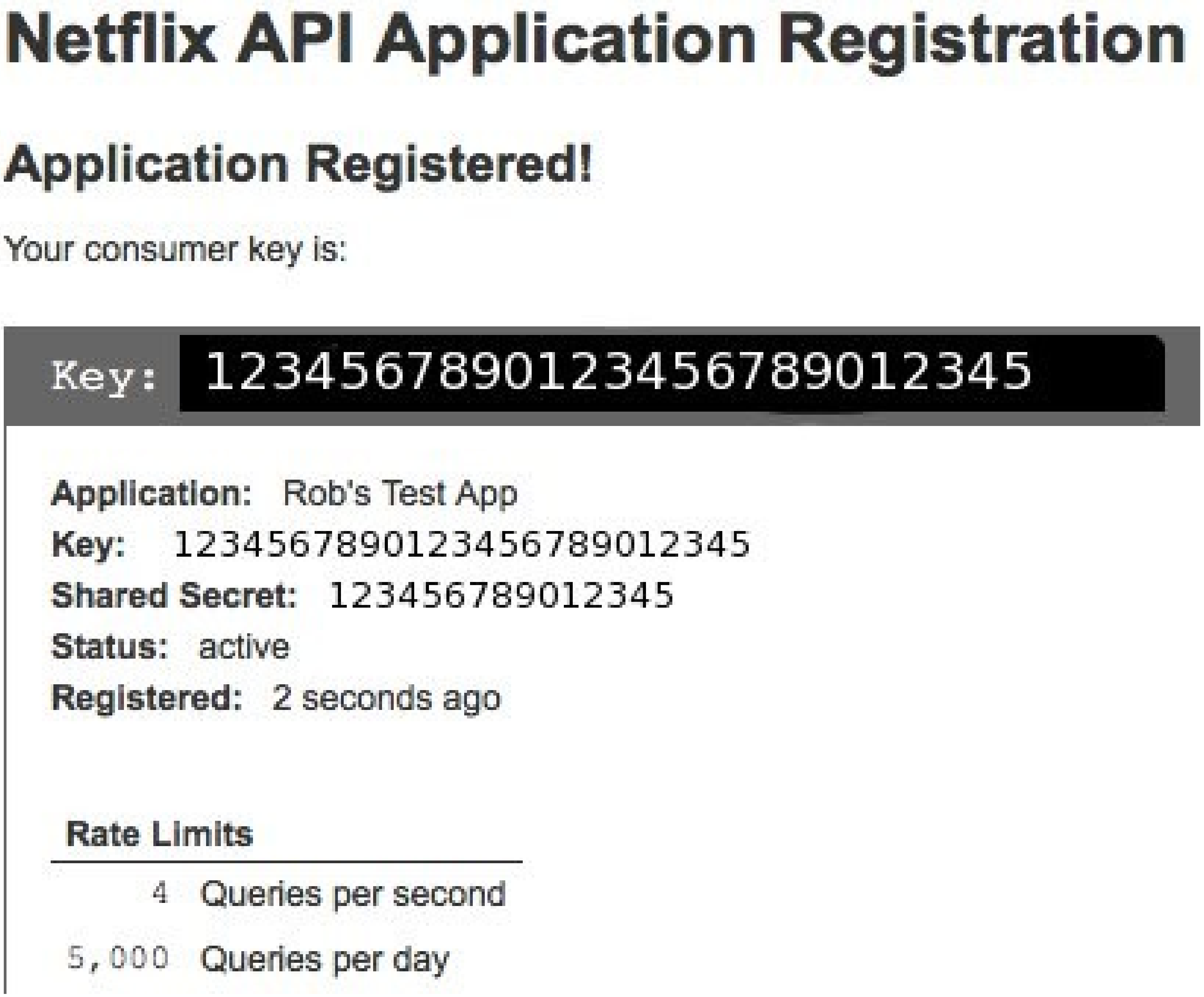
Choose one...

How many people do you anticipate will use you application?

Choose one...

MASHERY

Obtaining a Consumer Key / Secret



Netflix API Application Registration

Application Registered!

Your consumer key is:

Key: 1234567890123456789012345

Application: Rob's Test App

Key: 1234567890123456789012345

Shared Secret: 123456789012345

Status: active

Registered: 2 seconds ago

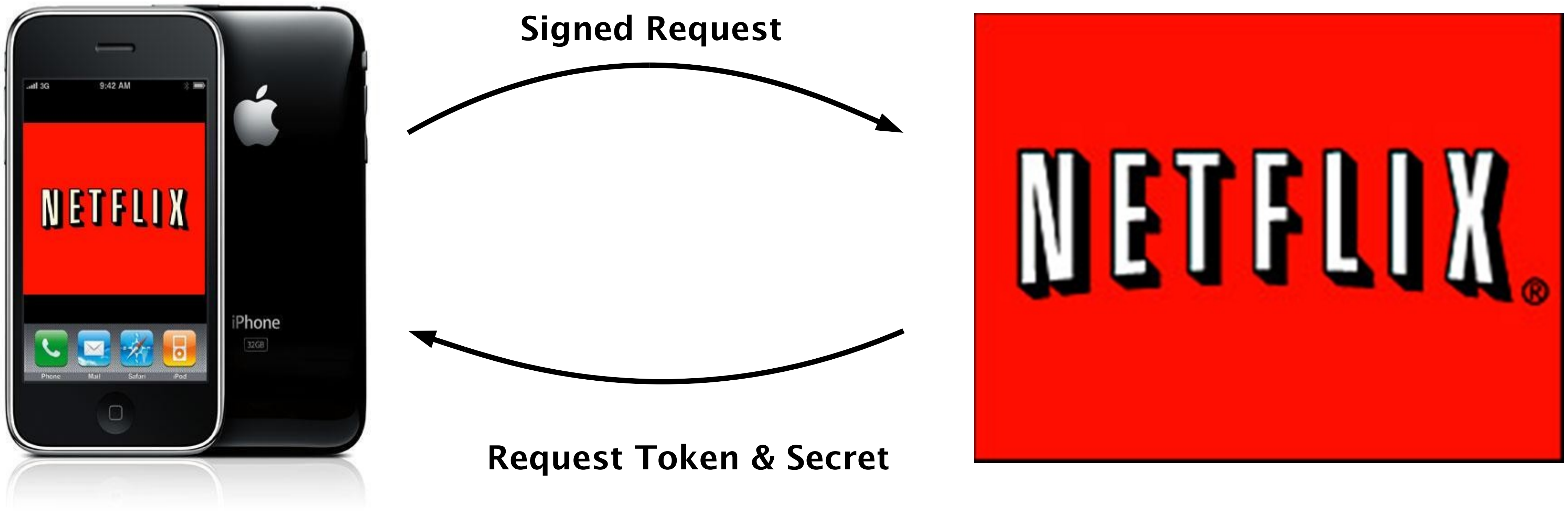
Rate Limits	
4	Queries per second
5,000	Queries per day

MASHERY

3-Legged OAuth
“The OAuth Dance”

Step 1: Obtaining a Request Token

http://api.netflix.com/oauth/request_token



Signed Request

Request Token & Secret

Step 1: Obtaining a Request Token

```
http://api.netflix.com/oauth/request_token?
oauth_callback=http%3A%2F%2Fwww.example.com%2Fcallback
&oauth_consumer_key=12345678901234567890123 45
&oauth_nonce=60a3f1c4a18c2a68d8cb216f46bceb4ad7dff32e
&oauth_signature=SB%2BjBrcHkQRgMP8XKVyps3rw6Xo%3D
&oauth_signature_method=HMAC-SHA1
&oauth_timestamp=1255631744
&oauth_version=1.0
```

Calculating The Signature

Calculate Base String

<HTTP method>&<canonicalized URL path>&<parameters>

GET&http%3A%2F%2Fapi.netflix.com%2Foauth%2Frequest_token&oauth_callback%3Dhttp%253A%252F%252Fwww.example.com%252Fcallback%26oauth_consumer_key%3D1234567890123456789012345%26oauth_nonce%3D3eb496472d2a46ceb71d65fc1b7341ae359f932c%26oauth_signature_method%3DHMAC-SHA1%26oauth_timestamp%3D1255631744%26oauth_version%3D1.0

Calculating The Signature

- Parameters are collected, sorted and concatenated into a normalized string
  - Parameters in the OAuth HTTP Authorization header excluding the realm parameter.
  - Parameters in the HTTP POST request body (with a content-type of application/x-www-form-urlencoded).
  - HTTP GET parameters added to the URLs in the query part (as defined by [RFC3986] section 3)
- The oauth_signature parameter MUST be excluded
- Parameters are sorted by name, using lexicographical byte value ordering

Calculating The Signature (Authorization Header)

```
GET /oauth/request_token HTTP/1.1

User-Agent: PECL::HTTP/1.6.4 (PHP/5.2.10)

Host: api.netflix.com

Accept: */*

Authorization: OAuth oauth_callback="http%3A%2F
  %2Fwww.example.com%2Fcallback",
  oauth_consumer_key="1234567890123456789012345",
  oauth_nonce="60a3f1c4a18c2a68d8cb216f46bceb4ad7dff32e",
  oauth_signature="SB%2BjBrcHkQRgMP8XKVyps3rw6Xo%3D",
  oauth_signature_method="HMAC-SHA1",
  oauth_timestamp="1255631744", oauth_version="1.0"
```

Calculating The Signature

Create Secret

<consumer secret>&<token secret>

12345678901234567890012345&

Sign Base String using algorithm specified

HMAC(12345678901234567890012345&,<Base String>)

Base64 encode then URL encode result:

oauth_signature=SB%2BjBrcHkQRgMP8XKVyps3rw6Xo%3D

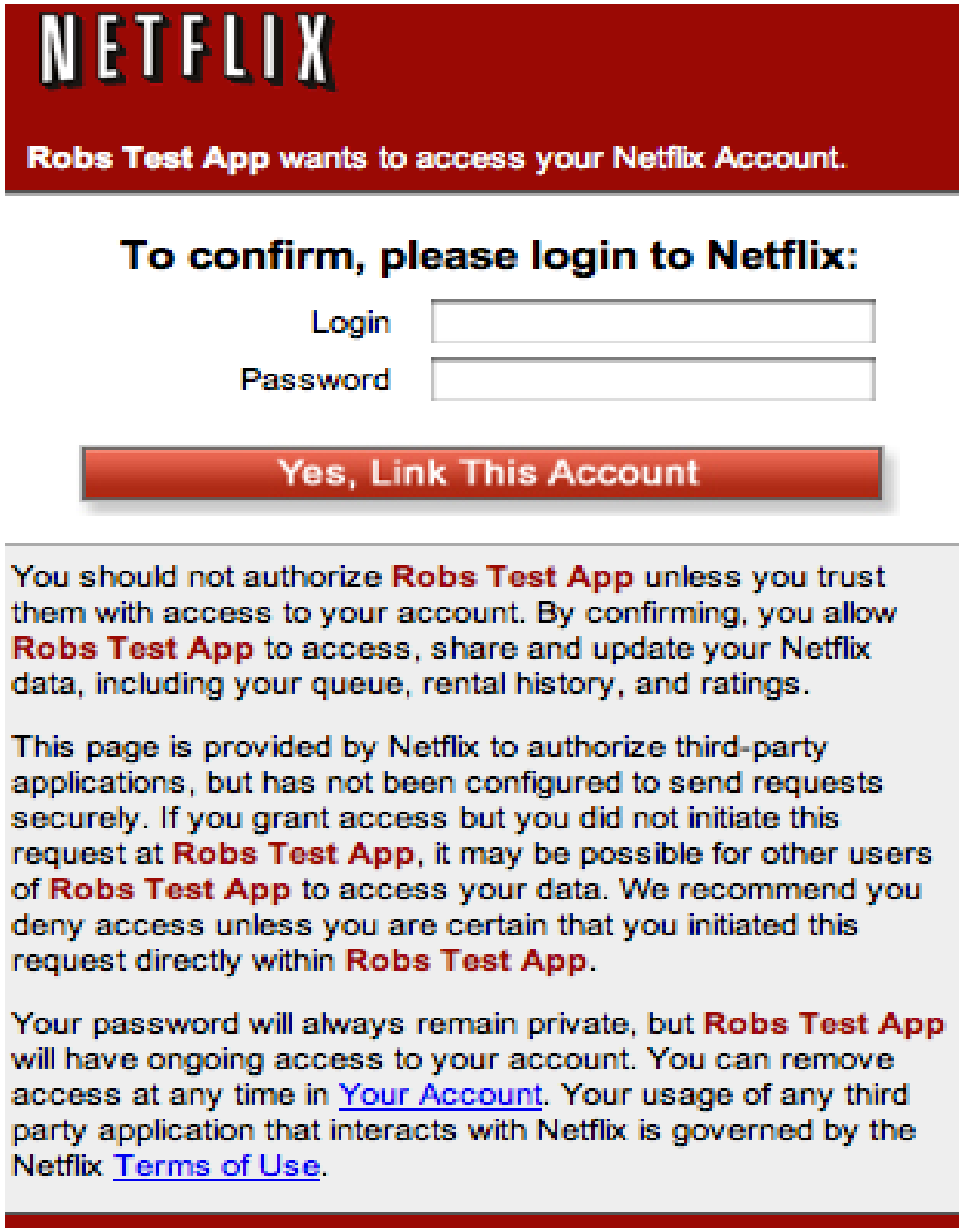
Step 1: Obtaining a Request Token (Response)

```
oauth_token=bqba9rku48yacfatjxjw3fkc
&oauth_token_secret=EZ2mBk6rC2vZ
&oauth_callback_confirmed=true
&login_url=https%3A%2F%2Fapi-user.netflix.com%2Foauth%2Flogin
```

Step 2: User Authentication

Determined by needs of Service Provider

https://api-user.netflix.com/oauth/login?oauth_token=bqba9rku48yacfatjxjw3fkc



Robs Test App wants to access your Netflix Account.

To confirm, please login to Netflix:

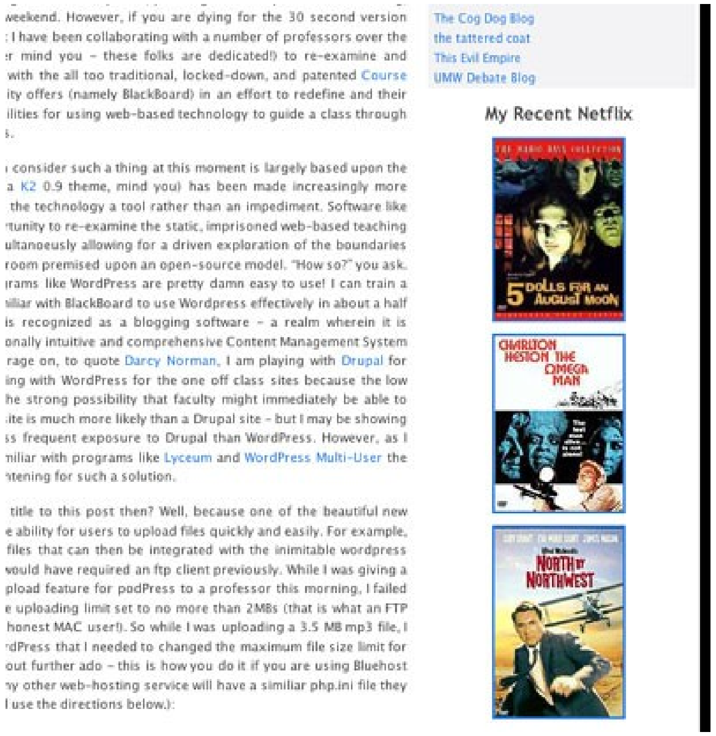
You should not authorize **Robs Test App** unless you trust them with access to your account. By confirming, you allow **Robs Test App** to access, share and update your Netflix data, including your queue, rental history, and ratings.

This page is provided by Netflix to authorize third-party applications, but has not been configured to send requests securely. If you grant access but you did not initiate this request at **Robs Test App**, it may be possible for other users of **Robs Test App** to access your data. We recommend you deny access unless you are certain that you initiated this request directly within **Robs Test App**.

Your password will always remain private, but **Robs Test App** will have ongoing access to your account. You can remove access at any time in Your Account. Your usage of any third party application that interacts with Netflix is governed by the Netflix Terms of Use.

Step 2: User Authentication

Determined by needs of Service Provider



weekend. However, if you are dying for the 30 second version
: I have been collaborating with a number of professors over the
r mind you – these folks are dedicated!) to re-examine and
with the all too traditional, locked-down, and patented Course
ity offers (namely BlackBoard) in an effort to redefine and their
ilities for using web-based technology to guide a class through
s.

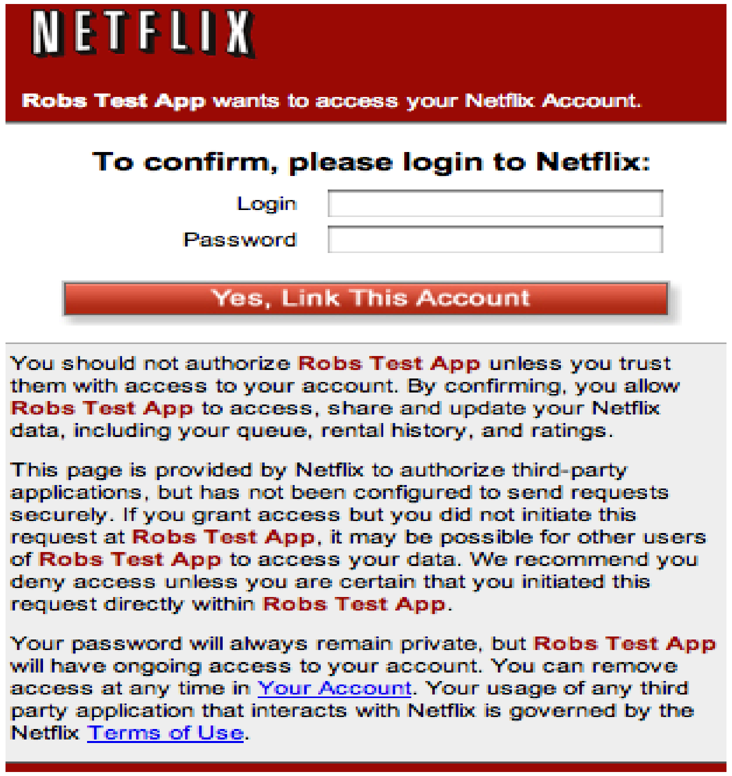
consider such a thing at this moment is largely based upon the
a K2 0.9 theme, mind you) has been made increasingly more
the technology a tool rather than an impediment. Software like
rtunity to re-examine the static, imprisoned web-based teaching
ultanoeusly allowing for a driven exploration of the boundaries
room premised upon an open-source model. "How so?" you ask.
grams like WordPress are pretty damn easy to use! I can train a
illiar with BlackBoard to use Wordpress effectively in about a half
is recognized as a blogging software – a realm wherein it is
onally intuitive and comprehensive Content Management System
rage on, to quote Darcy Norman, I am playing with Drupal for
ing with WordPress for the one off class sites because the low
he strong possibility that faculty might immediately be able to
ite is much more likely than a Drupal site – but I may be showing
ss frequent exposure to Drupal than WordPress. However, as I
niliar with programs like Lyceum and WordPress Multi-User the
ntening for such a solution.

title to this post then? Well, because one of the beautiful new
e ability for users to upload files quickly and easily. For example,
files that can then be integrated with the inimitable wordpress
would have required an ftp client previously. While I was giving a
pload feature for podPress to a professor this morning, I failed
e uploading limit set to no more than 2MBs (that is what an FTP
honest MAC user!). So while I was uploading a 3.5 MB mp3 file, I
rdPress that I needed to changed the maximum file size limit for
out further ado – this is how you do it if you are using Bluehost
ny other web-hosting service will have a similiar php.ini file they
I use the directions below.):

The Cog Dog Blog
the tattered coat
This Evil Empire
UMW Debate Blog

My Recent Netflix

Callback



Robs Test App wants to access your Netflix Account.

To confirm, please login to Netflix:

Login

Password

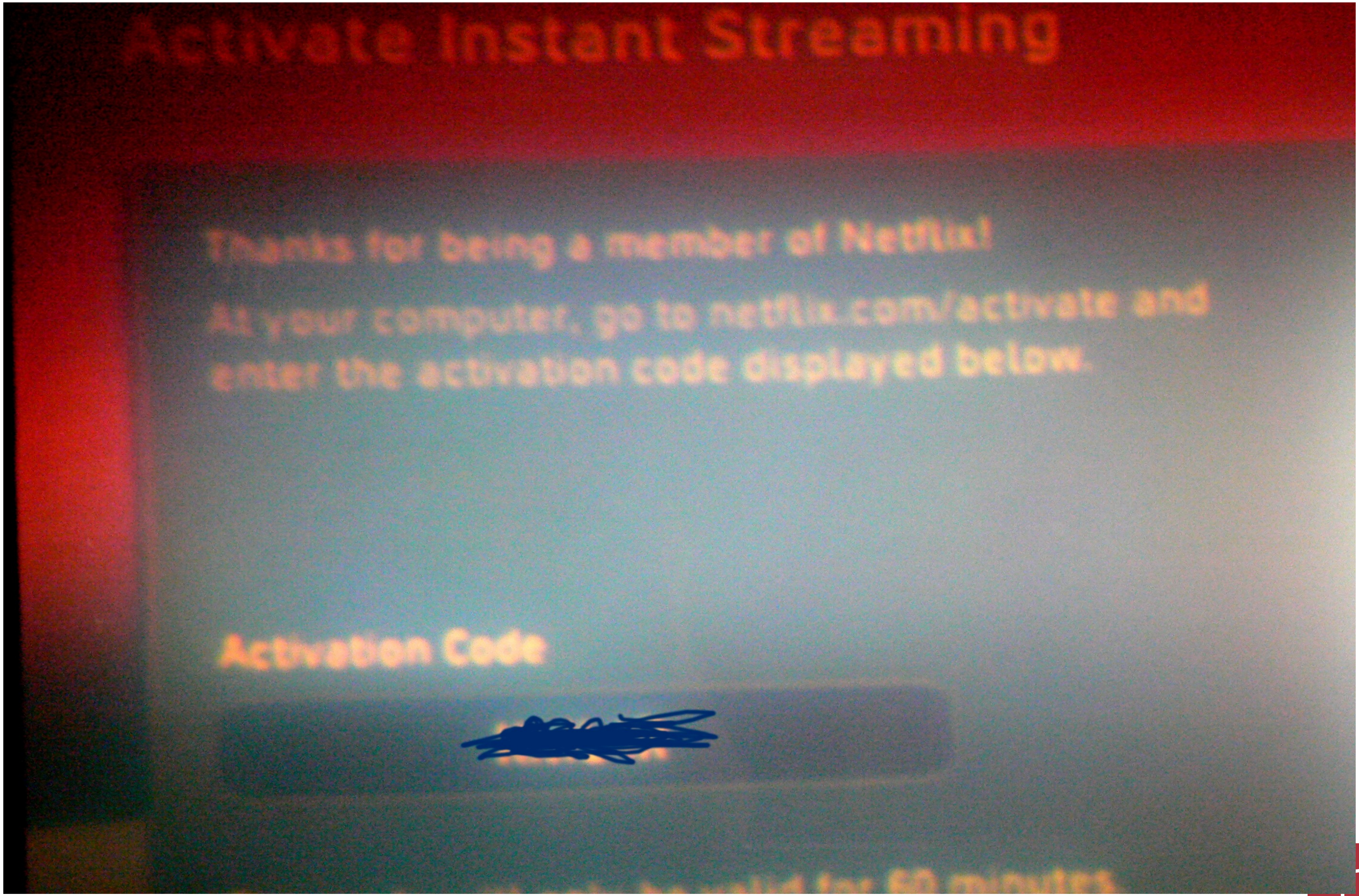
You should not authorize **Robs Test App** unless you trust them with access to your account. By confirming, you allow **Robs Test App** to access, share and update your Netflix data, including your queue, rental history, and ratings.

This page is provided by Netflix to authorize third-party applications, but has not been configured to send requests securely. If you grant access but you did not initiate this request at **Robs Test App**, it may be possible for other users of **Robs Test App** to access your data. We recommend you deny access unless you are certain that you initiated this request directly within **Robs Test App**.

Your password will always remain private, but **Robs Test App** will have ongoing access to your account. You can remove access at any time in Your Account. Your usage of any third party application that interacts with Netflix is governed by the Netflix Terms of Use.

oauth_token=bqba9rku48yacfatjxjw3fkc&oauth_verifier=abcdefg

Step 2: User Authentication



Activate Instant Streaming

Thanks for being a member of Netflix!

At your computer, go to netflix.com/activate and enter the activation code displayed below.

Activation Code

[redacted]

be valid for 60 minutes

Oauth Trust

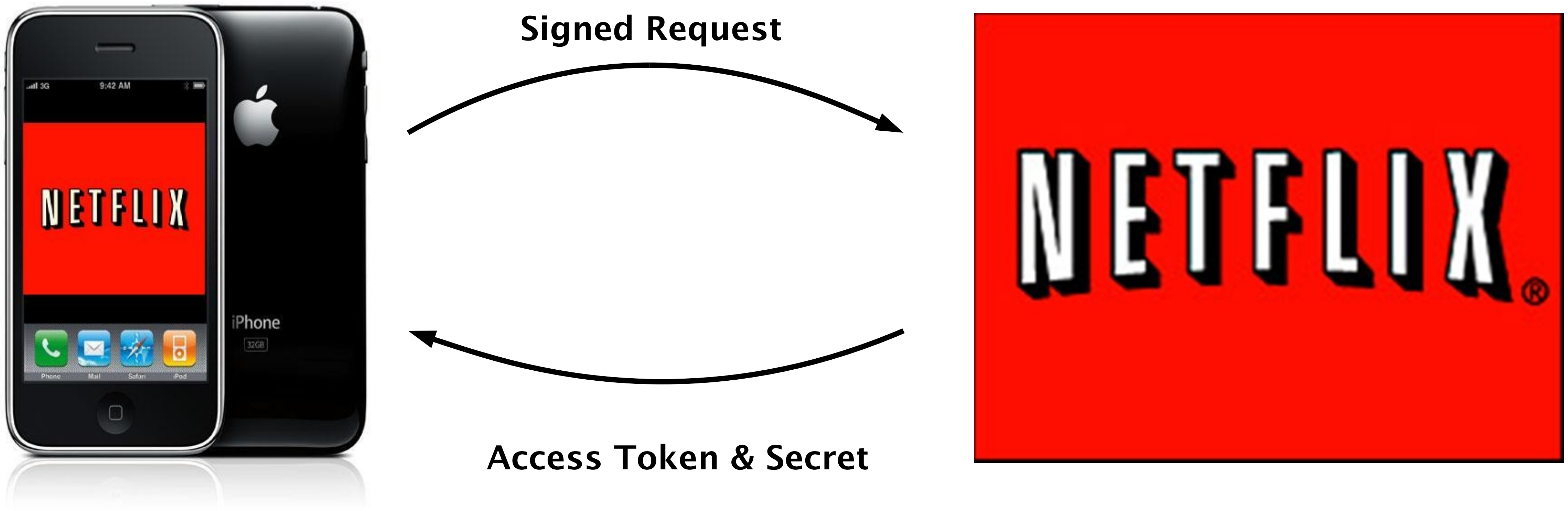
A Matter

Of

Trust

Step 3: Obtaining an Access Token

http://api.netflix.com/oauth/access_token



Signed Request

Access Token & Secret

Step 3: Obtaining an Access Token

http://api.netflix.com/oauth/access_token?

oauth_consumer_key=1234567890123456789012345

&oauth_nonce=0a5ebd08b88e3ec7d7e27c7fb8735c7aa9a7229a

&oauth_signature=FXDtkQtg6u42YYipJhBgCBvVXHI%3D

&oauth_signature_method=HMAC-SHA1

&oauth_timestamp=1255704433

&oauth_token=bqba9rku48yacfatjxjw3fkc

&oauth_verifier=abcdefg

&oauth_version=1.0

Calculating The Signature

Calculate Base String

<HTTP method>&<canonicalized URL path>&<parameters>

GET&http%3A%2F%2Fapi.netflix.com%2Foauth
%2Faccess_token&oauth_consumer_key
%3D123456789012345678901234%26oauth_nonce
%3D0a5ebd08b88e3ec7d7e27c7fb8735c7aa9a7229a
%26oauth_signature_method%3DHMAC-
SHA1%26oauth_timestamp%3D1255704433%26oauth_token
%3Dbqba9rku48yacfatjxjw3fkc%26oauth_verifier%3Dabcdefg
%26oauth_version%3D1.0

Calculating The Signature

Create Secret

<consumer secret>&<token secret>

1234567890123456789012345&EZ2mBk6rC2vZ

Sign Base String using algorithm specified

HMAC(1234567890123456789012345&EZ2mBk6rC2vZ,<Base String>)

Base64 encode then URL encode result:

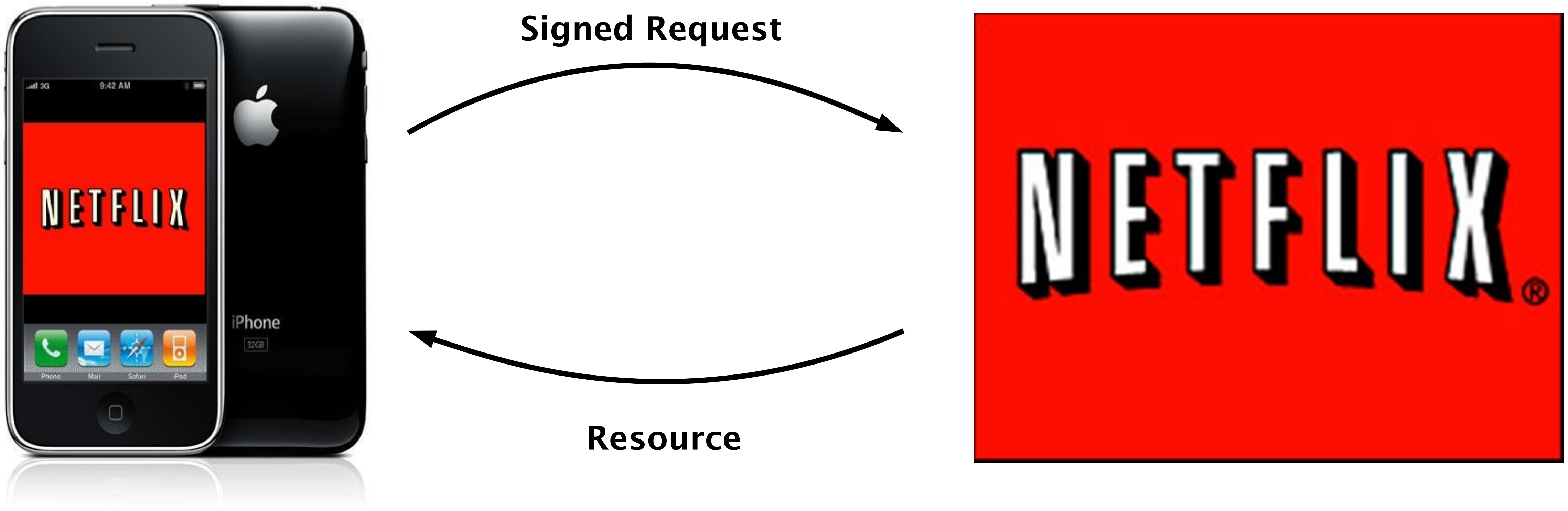
oauth_signature=eCLuRjEhSB%2BFImlN8sqrusPd9AE%3D

Step 3: Obtaining an Access Token (Response)

```
oauth_token=54321098765432109876543210987654321
&user_id=123myuserid456
&oauth_token_secret=543210987654321
```

Accessing Resources

http://api.netflix.com/<path to resource>



Signed Request

Resource

Accessing Resources

```
http://api.netflix.com/users/123myuserid456/queues?
oauth_consumer_key=1234567890123456789012345
&oauth_nonce=0c36fbefee5af0316687c6984a32c0184526e7b2
&oauth_signature=IXkzzAhF9hnsFleftxEdfG0nx1s%3D
&oauth_signature_method=HMAC-SHA1
&oauth_timestamp=1255712310
&oauth_token=5432109876543210987654321
&oauth_version=1.0
&v=1.5
```

MASHERY

Calculating The Signature

Create Secret

<consumer secret>&<token secret>

1234567890123456789012345&543210987654321

Sign Base String using algorithm specified

HMAC(1234567890123456789012345&543210987654321,<Base String>)

Base64 encode then URL encode result:

oauth_signature=IXkzzAhF9hnsFIeftxEdfG0nx1s%3D

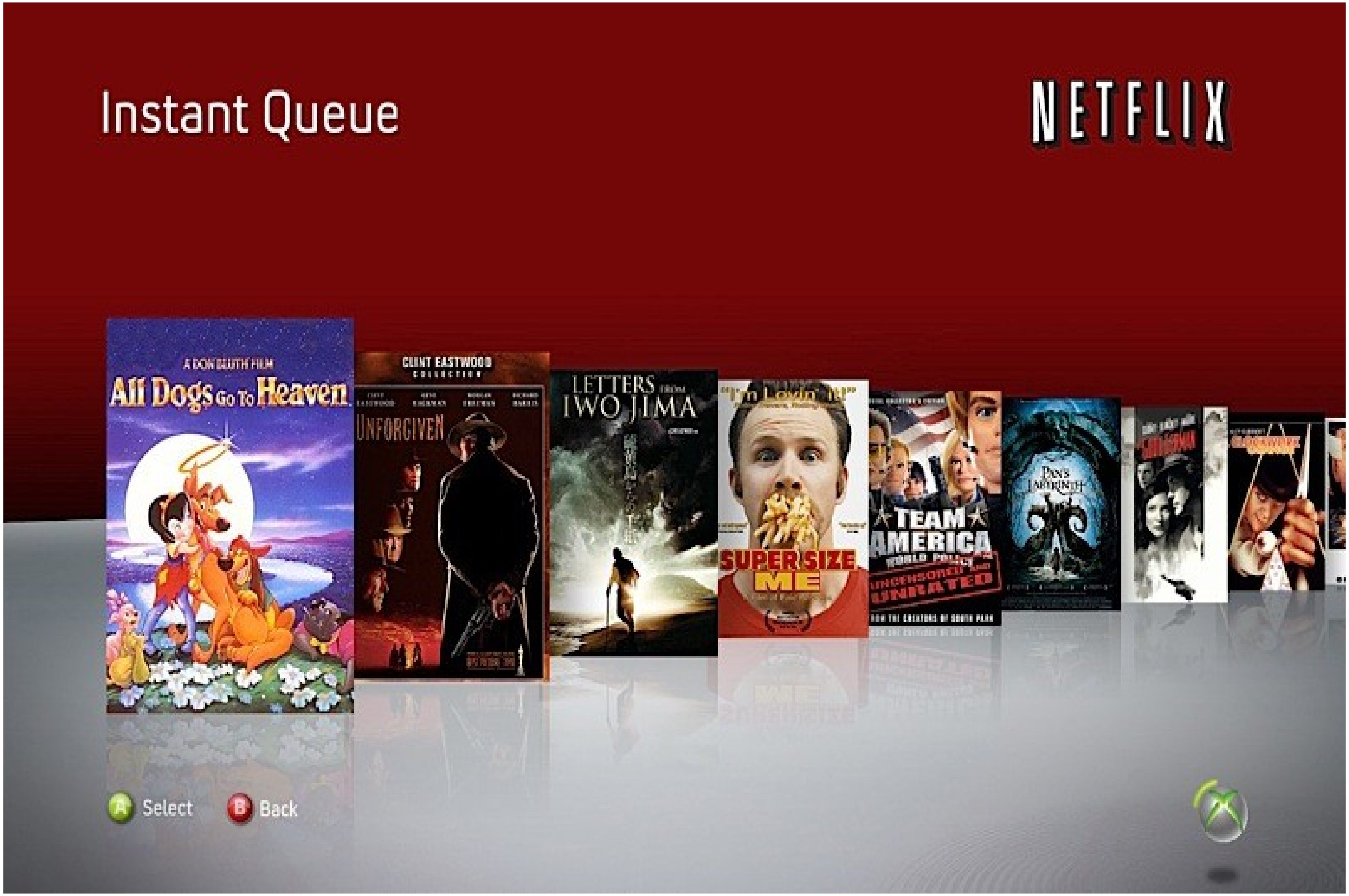
MASHERY

Accessing Resources (Response)

```
<?xml version="1.0" standalone="yes"?>
<resource>
  <link href="http://api.netflix.com/users/123myuserid456/queues/disc"
          rel="http://schemas.netflix.com/queues.disc" title="disc queue" />
  <link href="http://api.netflix.com/users/123myuserid456/queues/instant"
          rel="http://schemas.netflix.com/queues.instant"
          title="instant queue" />
</resource>
```

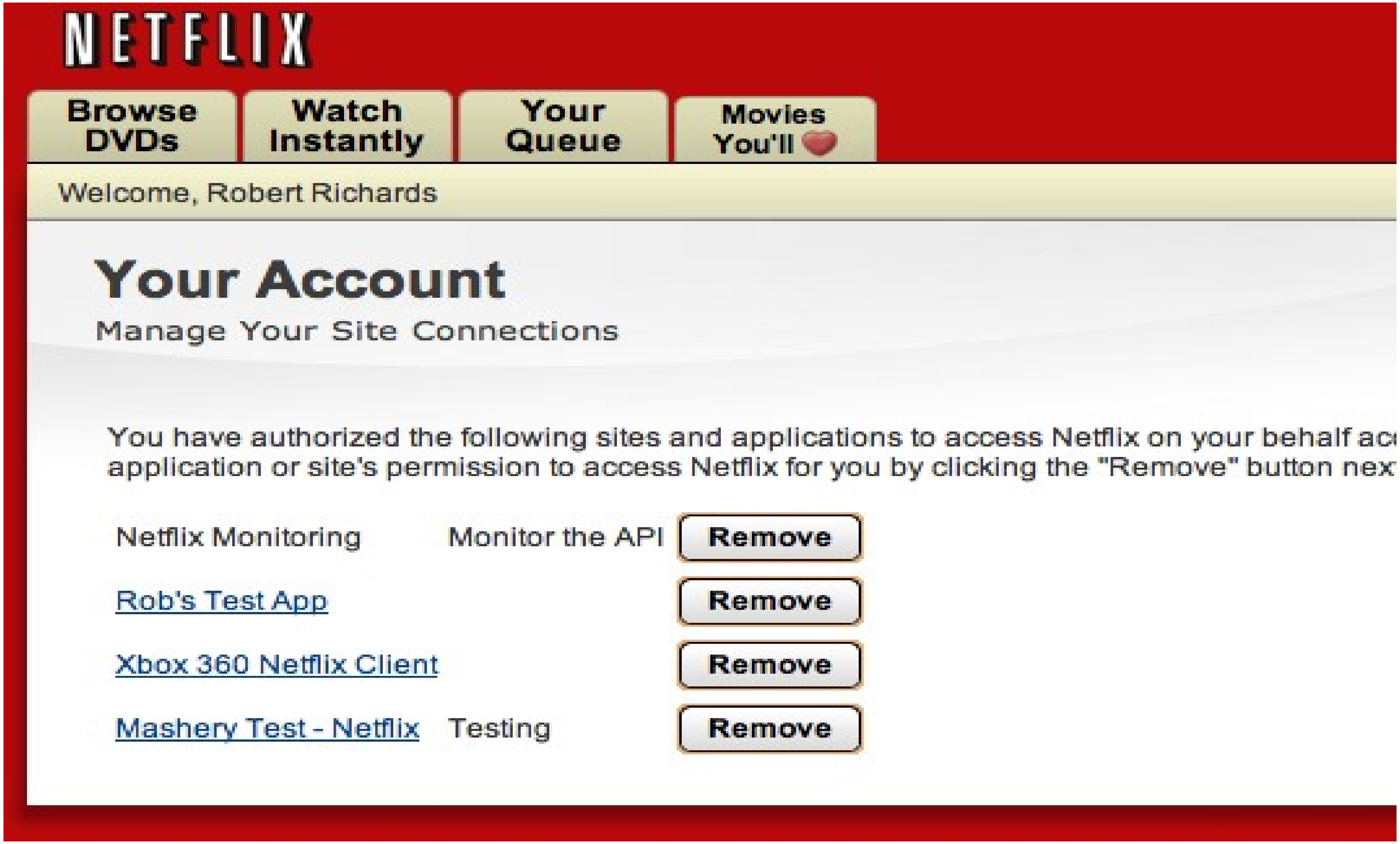
MASHERY

Accessing Resources (Response)



MASHERY

Managing Access Tokens



Welcome, Robert Richards

Your Account

Manage Your Site Connections

You have authorized the following sites and applications to access Netflix on your behalf ac
application or site's permission to access Netflix for you by clicking the "Remove" button nex

Netflix Monitoring	Monitor the API	Remove
Rob's Test App		Remove
Xbox 360 Netflix Client		Remove
Mashery Test - Netflix	Testing	Remove

2-Legged OAuth

- No Dance Required
- Only Consumer Key and Secret required
- Application making requests on its own behalf
- Direct Access / No Delegation
- Replacement for HTTP Basic Authentication
- Sign request just as if they were requests for Request Tokens

MASHERY

Questions?

MASHERY

Authorization with OAuth

Rob Richards

http://xri.net/=rob.richards
www.cdatazone.org