

OAuth2 Flows

Dominick Baier

<http://leastprivilege.com>

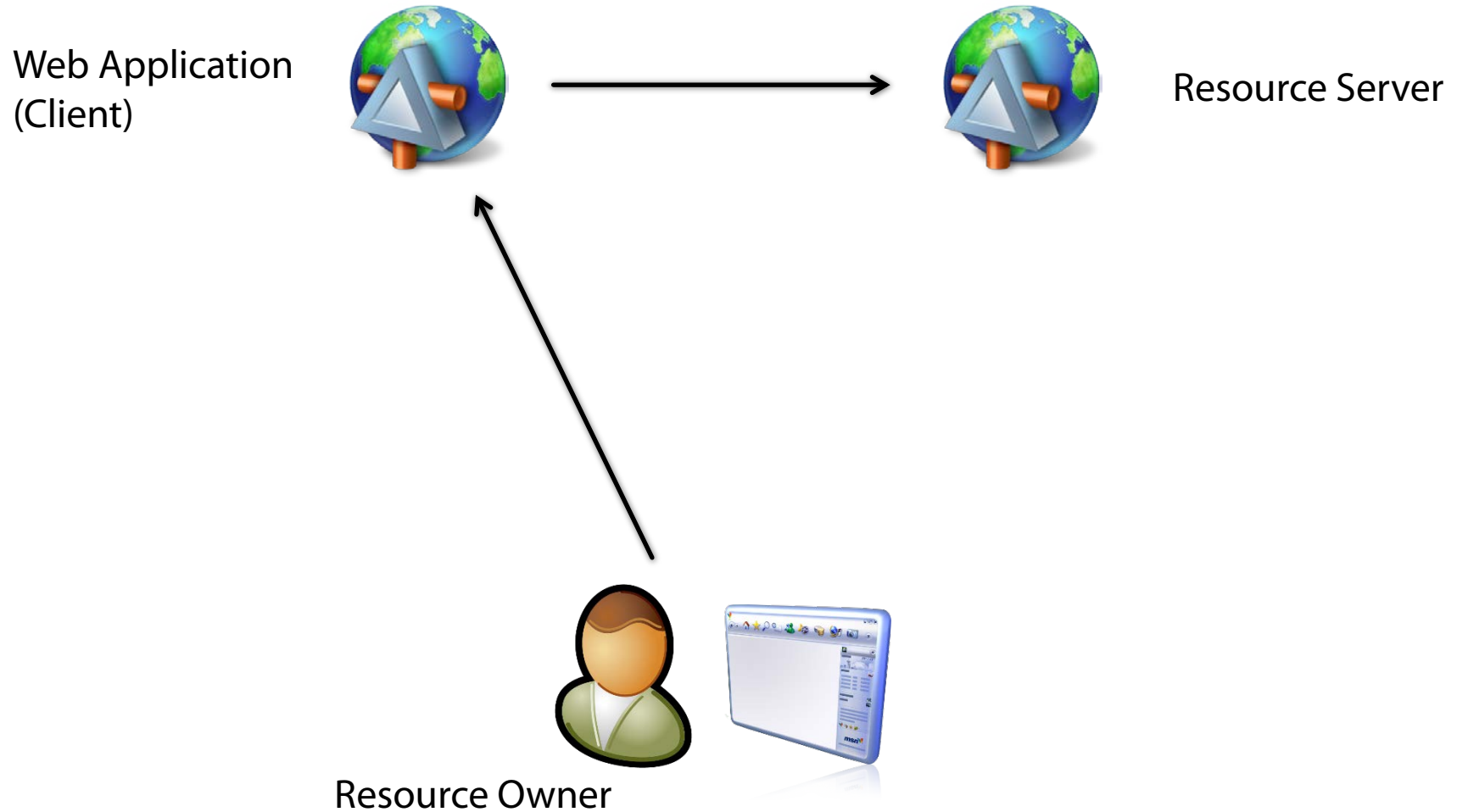
@leastprivilege



Outline

- **Authorization Code Flow**
- **Implicit Flow**
- **Resource Owner Credential Flow**
- **Client Credential Flow**

Authorization Code Flow (Web Application Clients)



Step 1a: Authorization Request

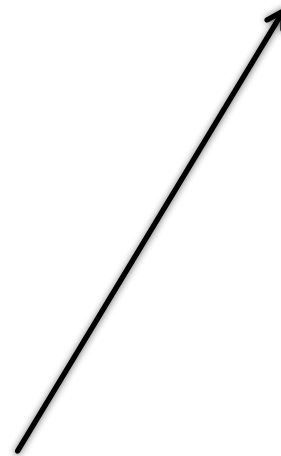
Web Application
(Client)



```
GET /authorize?  
  client_id=webapp&  
  scope=resource&  
  redirect_uri=https://webapp/cb&  
  response_type=code&  
  state=123
```



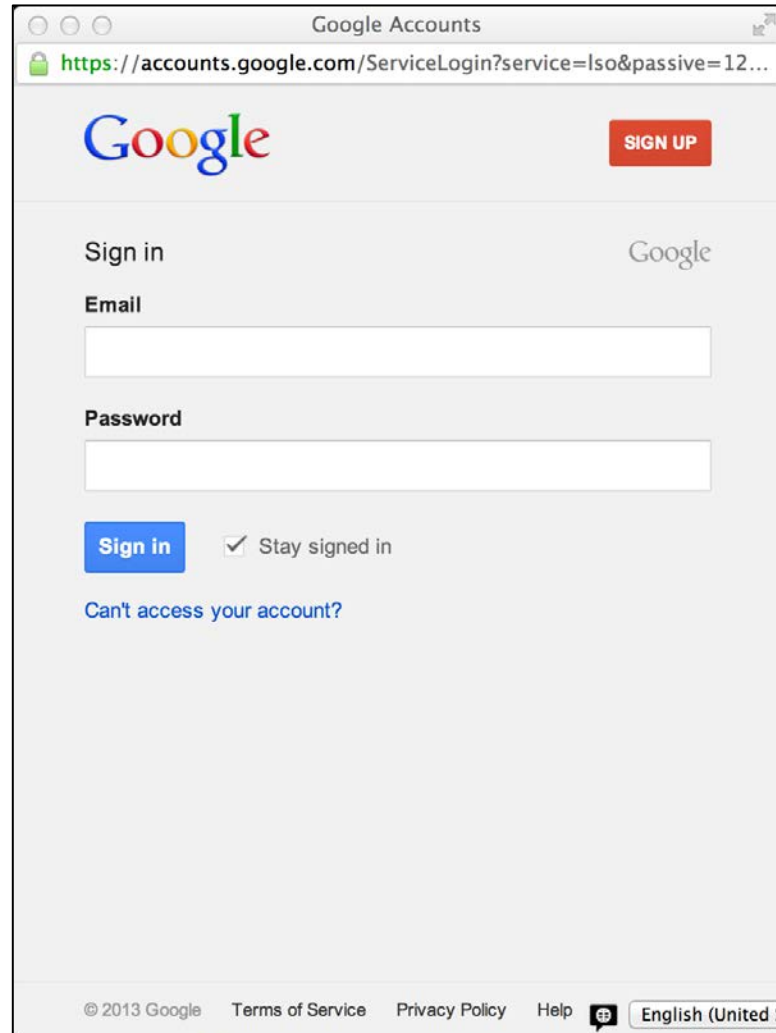
Authorization Server



Resource Owner



Step 1b: Authentication



A screenshot of a web browser window titled "Google Accounts". The address bar shows the URL <https://accounts.google.com/ServiceLogin?service=Iso&passive=12...>. The page features the Google logo at the top left and a red "SIGN UP" button at the top right. Below the logo, the text "Sign in" is displayed, followed by a "Google" logo. The form includes an "Email" label and a text input field, a "Password" label and a text input field, a blue "Sign in" button, and a checkbox labeled "Stay signed in" which is checked. A link "Can't access your account?" is located below the sign-in button. The footer contains copyright information "© 2013 Google", links for "Terms of Service", "Privacy Policy", and "Help", along with a language selector set to "English (United S)".

Google Accounts

<https://accounts.google.com/ServiceLogin?service=Iso&passive=12...>

Google

SIGN UP

Sign in

Google

Email

Password

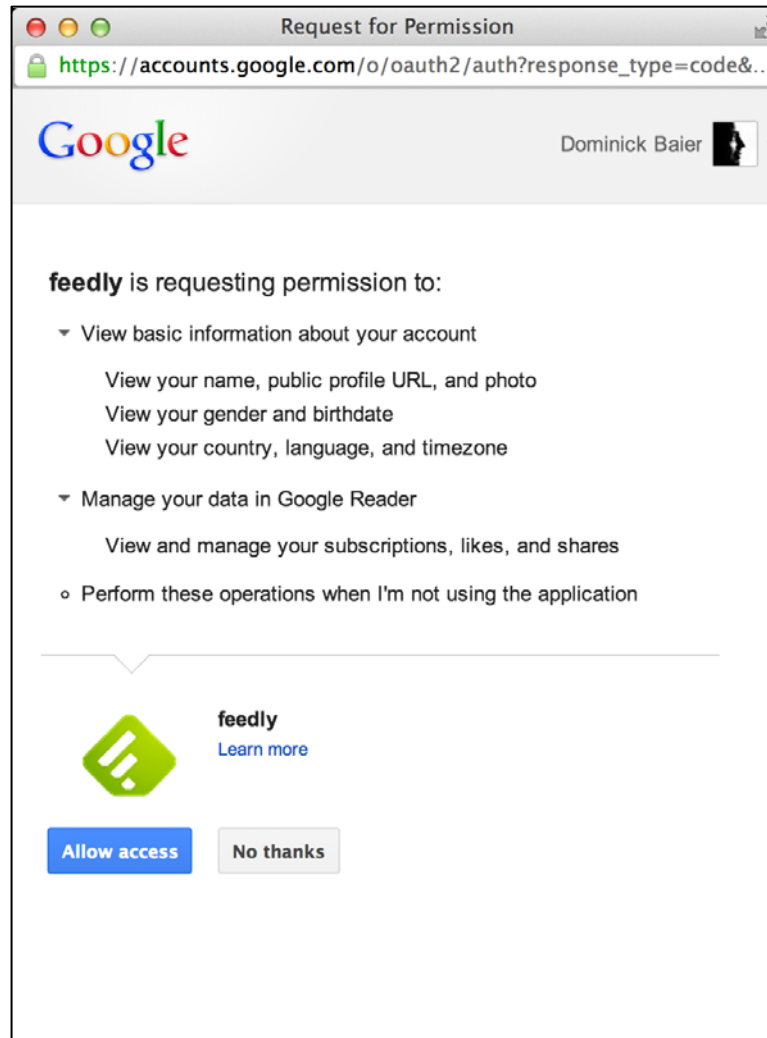
Sign in

☒ Stay signed in

[Can't access your account?](#)

© 2013 Google Terms of Service Privacy Policy Help English (United S)

Step 1c: Consent



Twitter Consent

Authorize Twitter for Windows to use your account?

This application **will be able to:**

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.
- Access your direct messages.

Username or email

Password

☐ Remember me · [Forgot password?](#)

This application **will not be able to:**

- See your Twitter password.

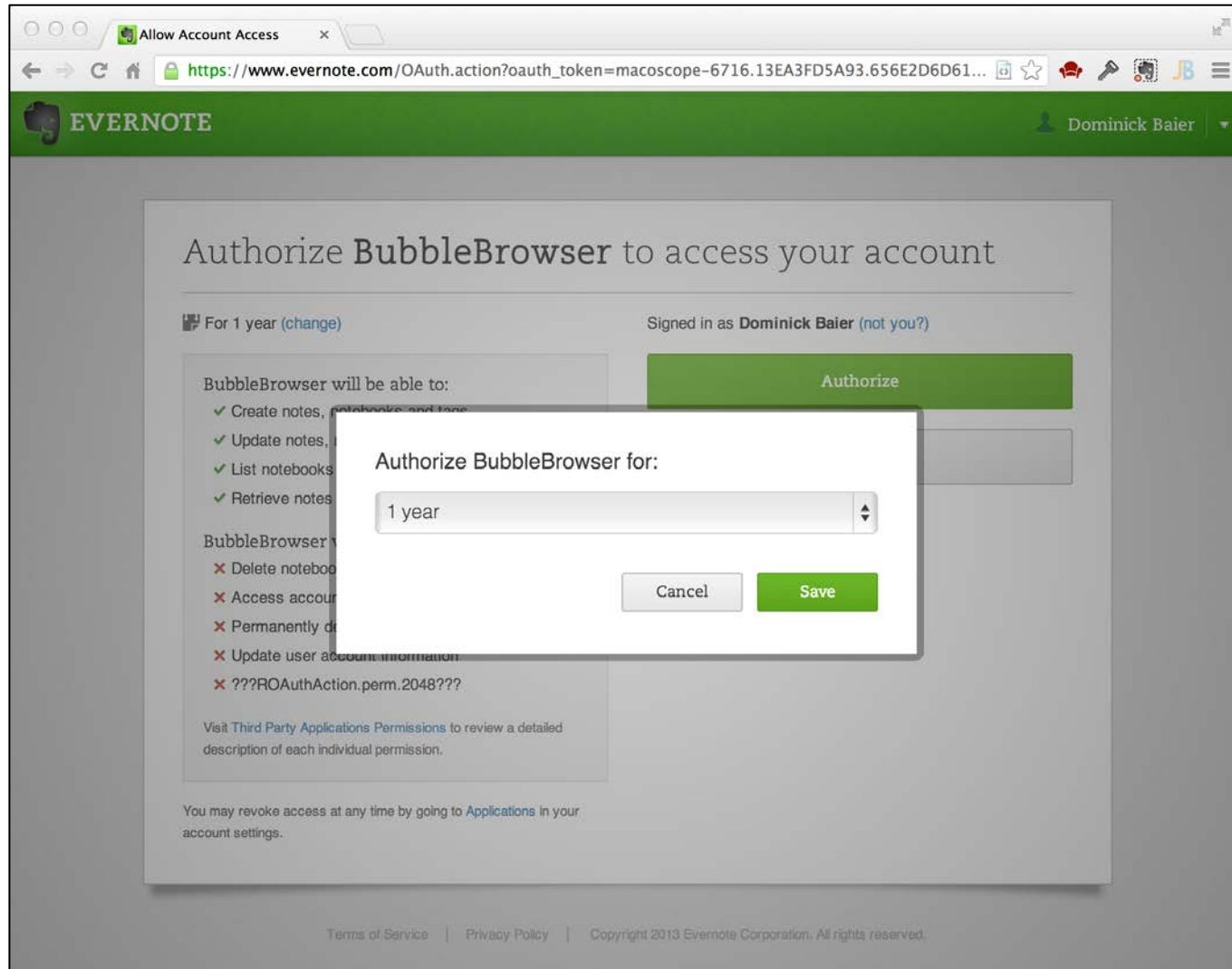


Twitter for Windows

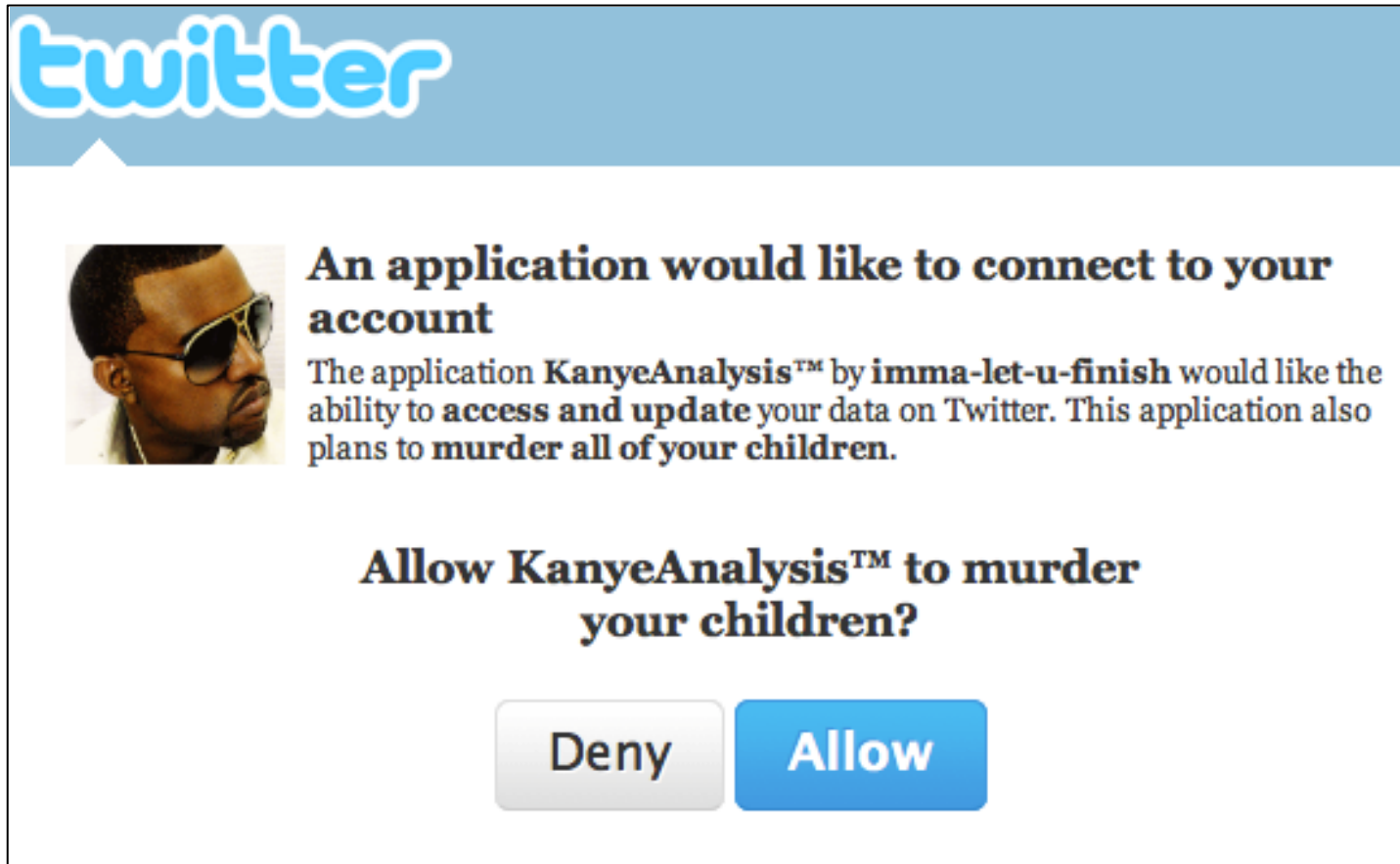
www.twitter.com

Official Twitter for Windows application.

Evernote Consent



The Consent Screen is important!



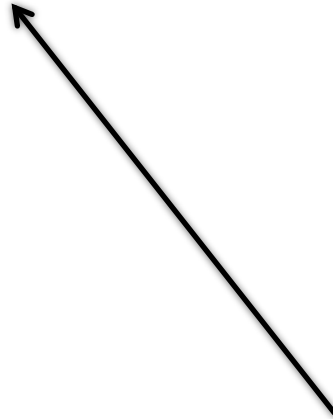
Step 1d: Authorization Response

Web Application
(Client)



Authorization Server

GET /cb?
code=xyz&
state=123



Resource Owner



Step 2a: Token Request

Web Application
(Client)



Authorization Server

POST /token

Authorization: Basic (client_id:secret)

**grant_type=authorization_code&
authorization_code=xyz&
redirect_uri=https://webapp/cb**



Resource Owner

Step 2b: Token Response

Web Application
(Client)



Authorization Server

```
{  
  "access_token" : "abc",  
  "expires_in" : "3600",  
  "token_type" : "Bearer",  
  "refresh_token" : "xyz"  
}
```



Resource Owner

Step 3: Resource Access

Web Application
(Client)



Resource Server

GET /resource

Authorization: Bearer access_token



Resource Owner

Access Token

- **The resource server will authorize the client & resource owner based on the contents of the access token**
 - after validation of issuer, signature and expiration
- **Typical claims for an access token are**
 - resource owner identifier
 - client identifier
 - granted scopes
 - ...anything additional that makes sense for your application

(Step 4: Refreshing the Token)

Web Application
(Client)



Authorization Server

POST /token

Authorization: Basic (client_id:secret)

**grant_type=refresh_token&
refresh_token=xyz**



Resource Owner

Client Management (Flickr)



leastprivilege

[Apps By You](#)

[Apps You're Using](#)

[Your Favorite Apps](#)

Below is a list of applications that you've given permission to interact with your Flickr account. It doesn't include apps that only use public photos and don't need to be authorized.




If you want to stop using one of these apps, click its "Remove permission" link.

Application	Permissions	
Adobe Photoshop Lightroom http://www.adobe.com/products/photoshoplightroom/	delete	Remove permission?
Flickr for Windows Phone 7 http://social.zune.net/redirect?type=phoneApp&id=2e49fb07-592b-e011-854c-00237de2db9e	delete	Remove permission?
Photorank.me	read	Remove permission?
Microsoft http://aka.ms/flickr	write	Remove permission?

Client Management (Dropbox)

My apps

You have given these apps access to your Dropbox account.

App name	Publisher	Access type	
 1Password	AgileBits	Full Dropbox	×
 1Password for Android	AgileWebSolutions Inc	Full Dropbox	×
 Dropbox Windows 8	Dropbox Windows 8	Official app	×

Client Management (Microsoft Live)

Microsoft account

Overview

Notifications

Permissions

Linked accounts

Kids' accounts

Add accounts

Manage accounts

Apps and Services

Billing

Apps and services you've given access

These apps and services can access some of your info. Choose one to view or edit the details.



WordPress.com

You last used WordPress.com on 6/6/2012.

[Edit](#)

WLID Test

You last used WLID Test on 5/11/2012.

[Edit](#)

Microsoft Minesweeper

You last used Microsoft Minesweeper on 9/26/2012.

Edit

idsrv

You last used idsrv on 2/20/2013.

[Edit](#)

Dominick's App

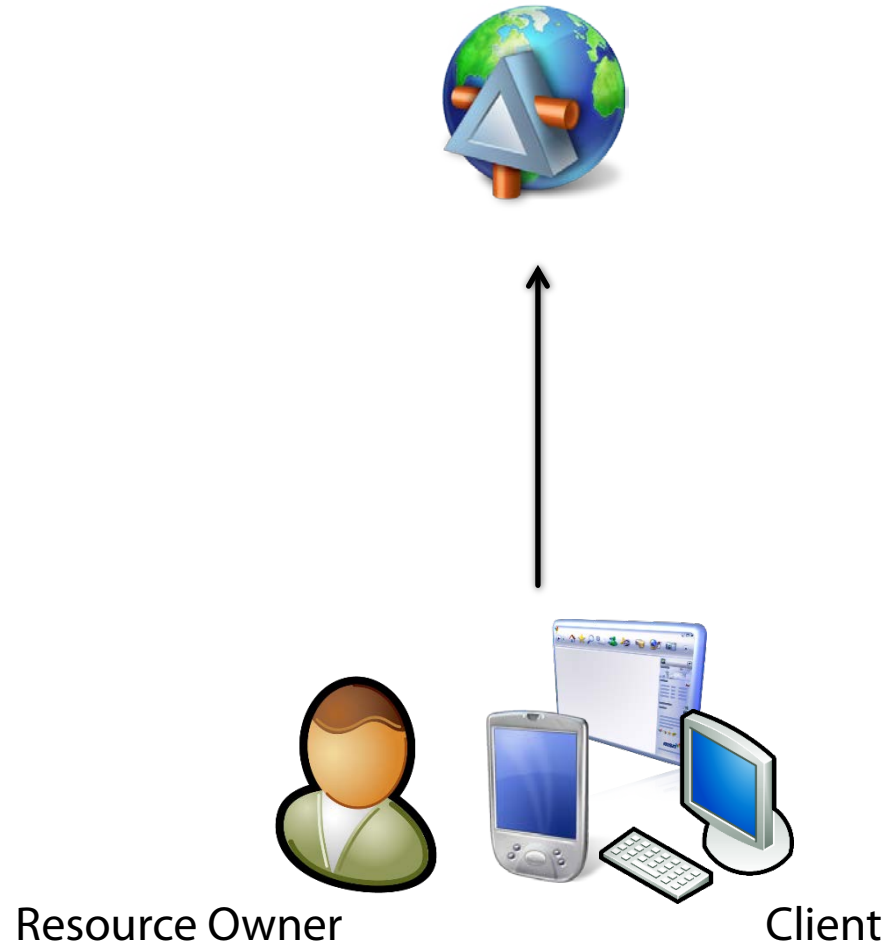
You last used Dominick's App on 2/27/2013.

[Edit](#)

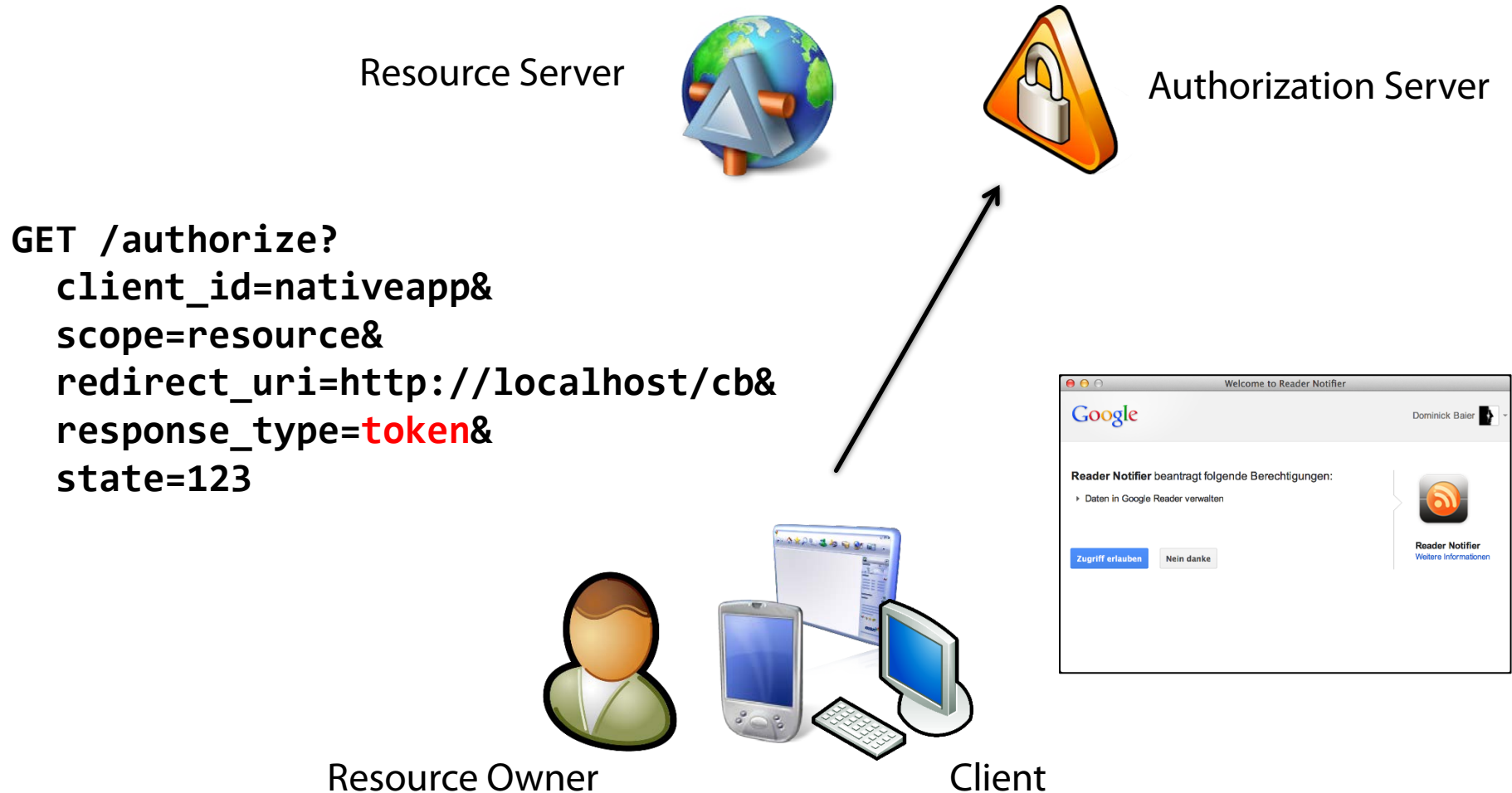
Summary – Code Flow

- **Designed for server-based applications**
 - Client can store secret securely on the server
- **Accountability is provided**
 - access token never leaked to the browser
- **Long-lived access can be implemented**

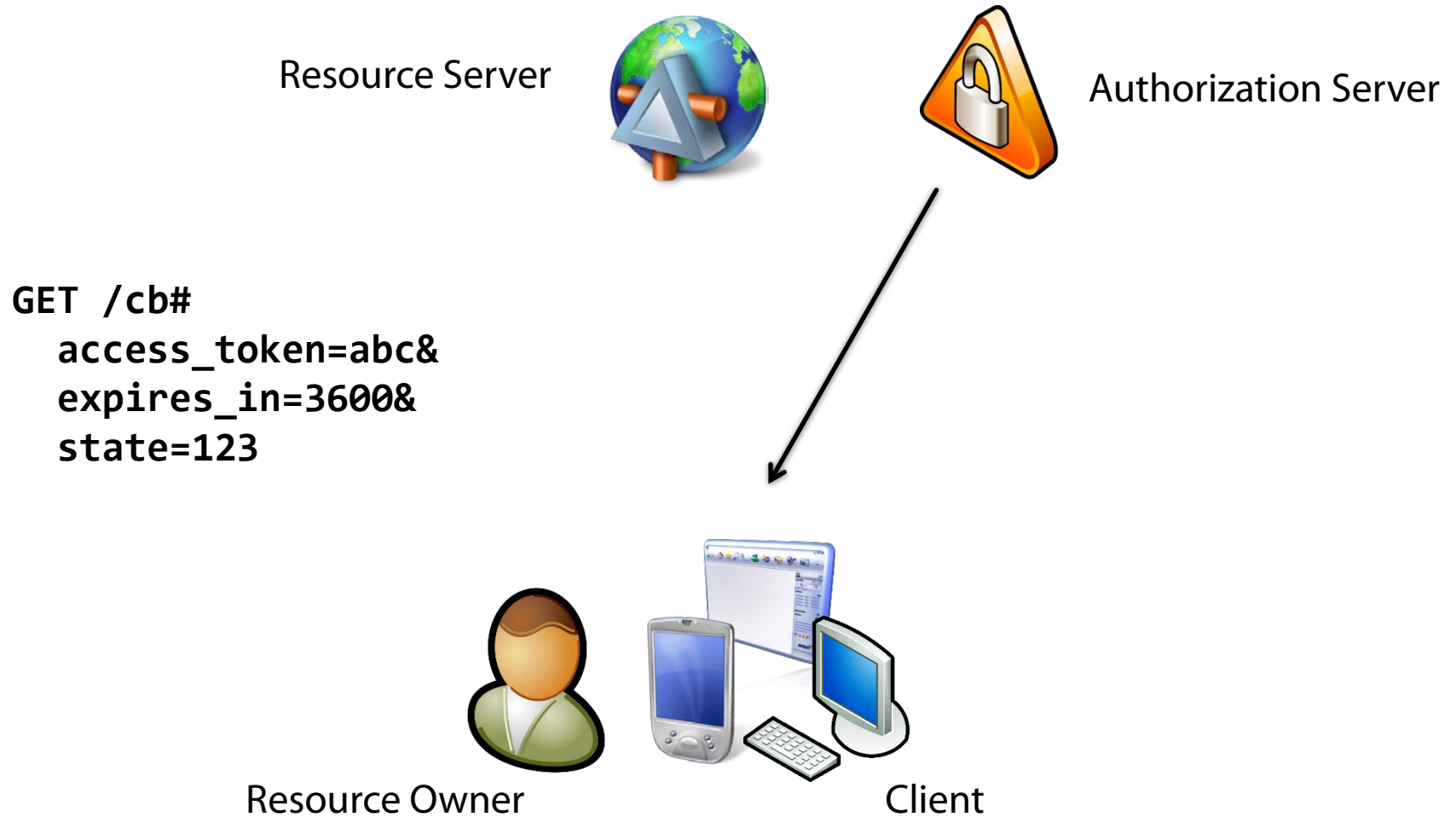
Implicit Flow (Native / Local Clients)



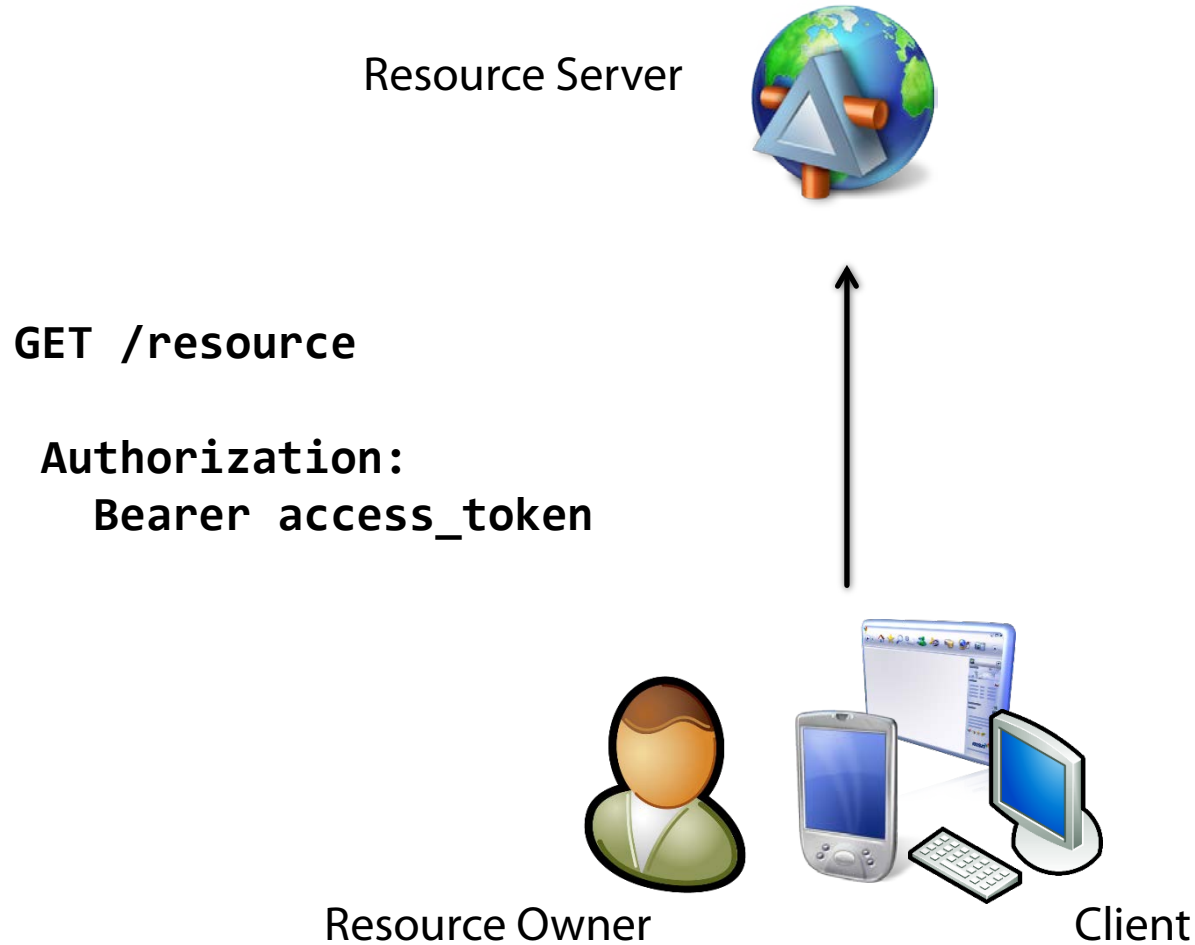
Step 1a: Authorization Request



Step 1b: Token Response



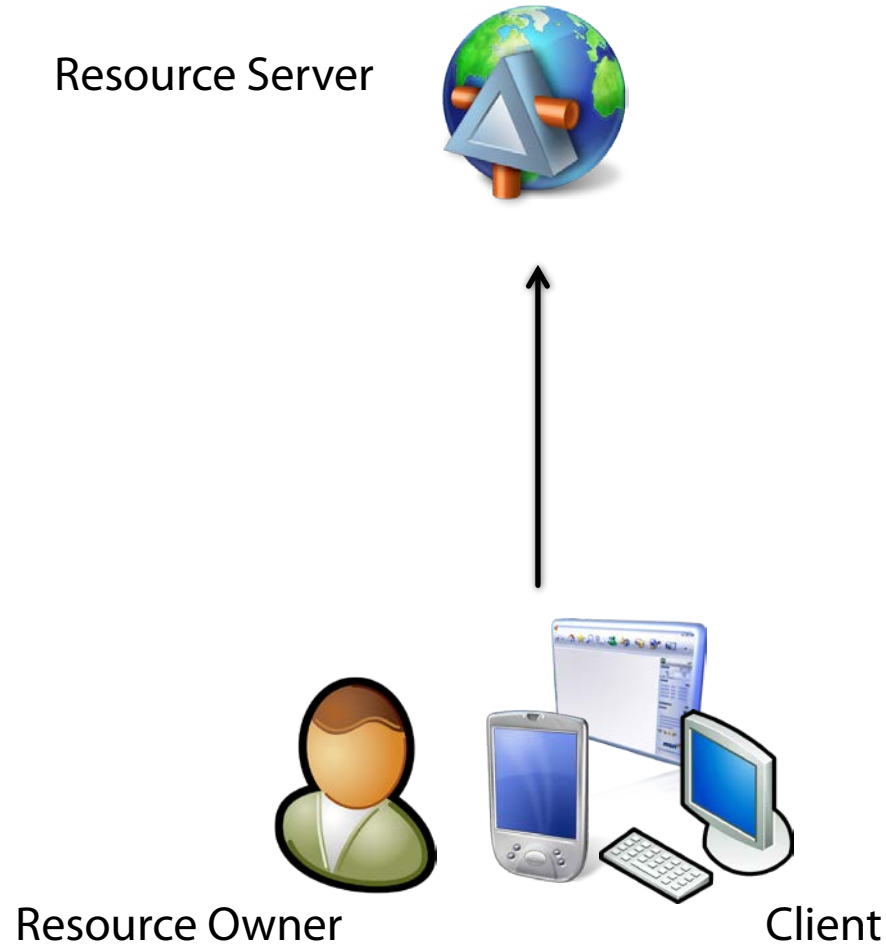
Step 2: Resource Access



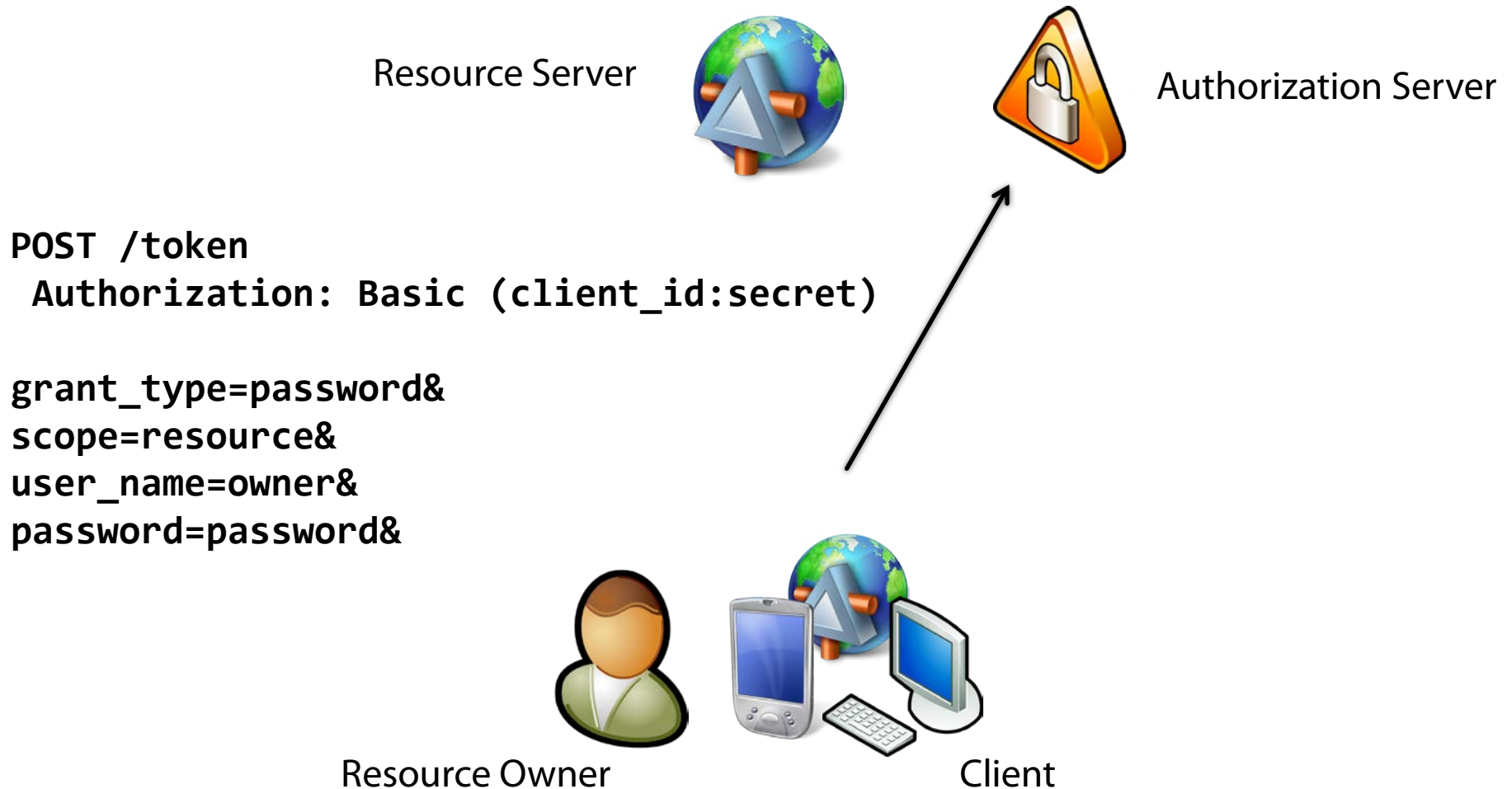
Summary – Implicit Flow

- **Simplified handshake**
 - no authorization code
- **Token is exposed to browser / local OS**
- **No client authentication**
 - no refresh tokens
- **Heavily debated and many "non-standard" variations**

Resource Owner Password Credential Flow (Trusted Application)



Step 1a: Token Request



Step 1b: Token Response

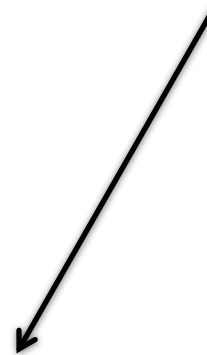
Resource Server



Authorization Server



```
{  
  "access_token" : "abc",  
  "expires_in" : "360",  
  "token_type" : "Bearer",  
  "refresh_token" : "xyz"  
}
```



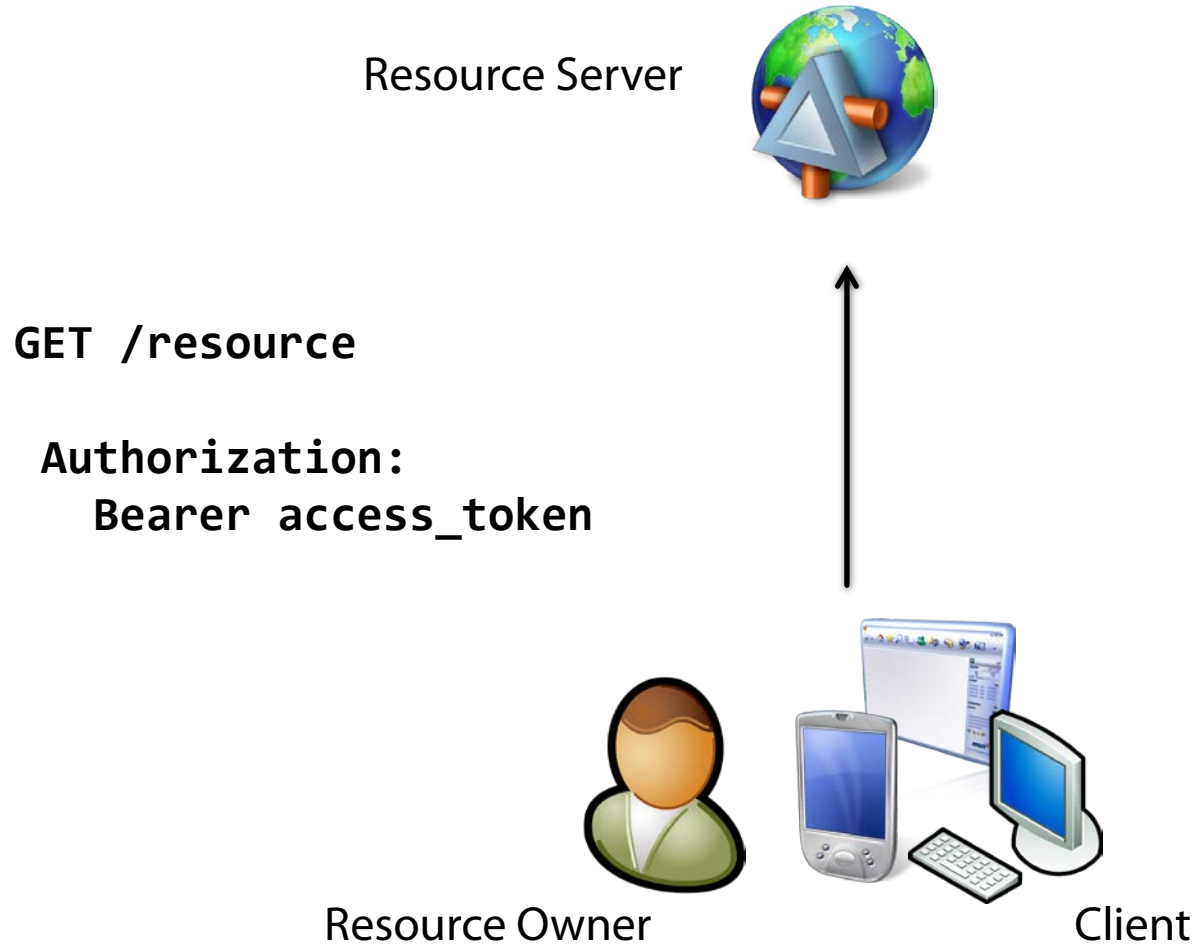
Resource Owner



Client



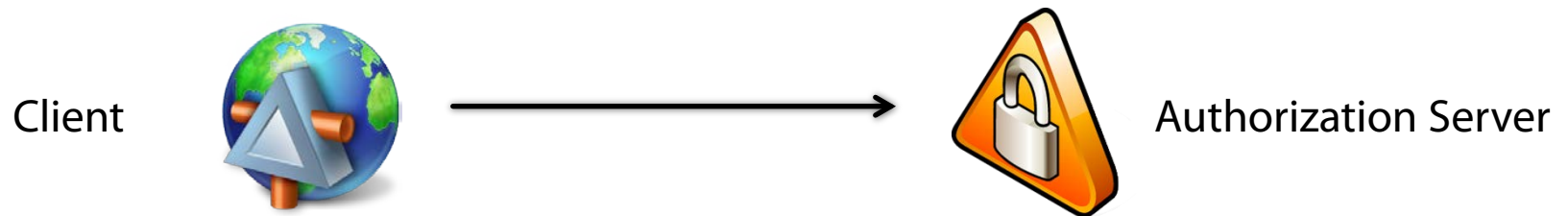
Step 2: Resource Access



Summary – Resource Owner Credential Flow

- **Resource owner credentials are exposed to client**
 - users should not become accustomed to that
- **Still better to store access/refresh token on device than password**
 - if the developer is using that feature

Client Credentials Flow – No human involved at all



POST /token

Authorization: Basic (client_id:secret)

**grant_type=client_credentials&
scope=resource**

Summary

- **The OAuth2 flows describe the various options for**
 - request authorization
 - request tokens
- **A separate spec (RFC 6750) describes how to transmit bearer access tokens to the resource server**