

OAuth 2.0 in Depth

By Rohit Ghatol

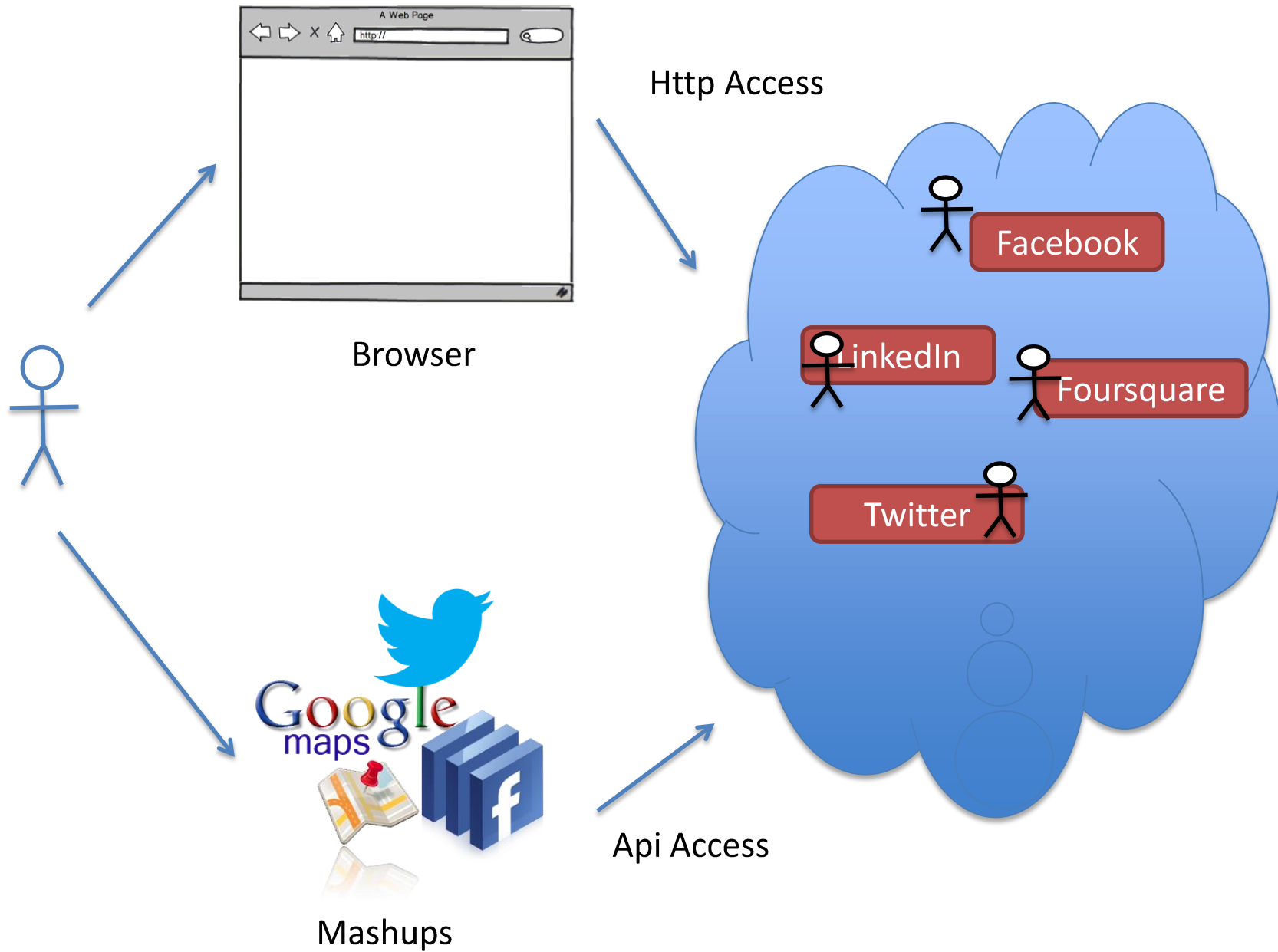
<http://www.slideshare.net/rohitsghatol/oauth-20-in-depth>

<http://tutorials.jenkov.com/oauth2/index.html>

Why study about OAuth?

Do you care about these or
Similar Sites?





7155 APIs listed on
<http://ProgrammableWeb.com>

← → ↻ 🏠 www.programmableweb.com ☆ 🎧 🗑

📌 Register / Login Find APIs, mashups, code and developers 🔍

programmableweb

Hot APIs » Twitter YouTube Facebook Google Maps Flickr LinkedIn More » Latest news Intelligent Learning With CCKF's Realizeit API

Home ▾ API News ▾ API Directory ▾ Mashups ▾ Community ▾ How-to ▾ Subscribe: 📡 📧 📱 📺

Keeping you up to date with APIs, mashups and the Web as platform. [Learn more »](#)


🔍

Popular searches: [photo](#) [google](#) [flash](#) [mapping](#) [enterprise](#) [sms](#)

New APIs

- ▶ LocalWiki
- ▶ WhyGo
- ▶ GoMobileIQ Headlight
- ▶ AppNowGo!
- ▶ FiftyOne
- ▶ Totango
- ▶ [See more APIs](#)


Mashup of the Day



▶ [See previous winners](#)

New Mashups

- ▶ Twups
- ▶ Erfahrungen.com
- ▶ Zip Code Catcher
- ▶ Furkot - free online road trip planner
- ▶ PhoneDuty
- ▶ Youplaylist.com
- ▶ [See more mashups](#)



390 APIs on <http://ProgrammableWeb.com>
support OAuth

www.programmableweb.com/apis/directory/1?auth=OAuth

Home API News API Directory Mashups Community How-to Subscribe: RSS Email Twitter Facebook

Web Services Directory

Subscribe to get the latest APIs

Sort by: Name Date Popularity Category

Hide Filters

Keywords:

Category:

Company:

Protocols / Styles:

Data Format:

Date: All

Managed By:

[Filter This List](#)

Viewing 1 to 390 of 390 APIs

« Previous 1 Next »

| API | Description | Category | Updated |
|---------------------------|---|--------------------|------------|
| #blue | Text messaging storage service | Messaging | 2011-04-23 |
| 11870 | Spanish bookmarking and directory service | Search | 2011-12-09 |
| 1DayLater | Business expense tracking tool | Enterprise | 2010-02-07 |
| 500px | Online community for photographers | Photos | 2011-10-18 |
| 7digital | Music downloads store | Music | 2010-08-13 |
| 88 Miles | Project time tracking services | Project Management | 2008-08-14 |

MASHERY
The Premier API Management Solution

inMOBI NEW MOBILE AD SDK
GET 100% REVENUE SHARE ▶

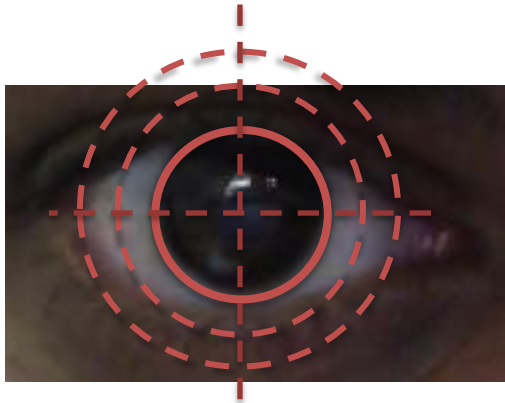
Our API's & your software system just go together!
[Click here for a free trial!](#)

Clickatell
Mobile Touch. Multiplied.

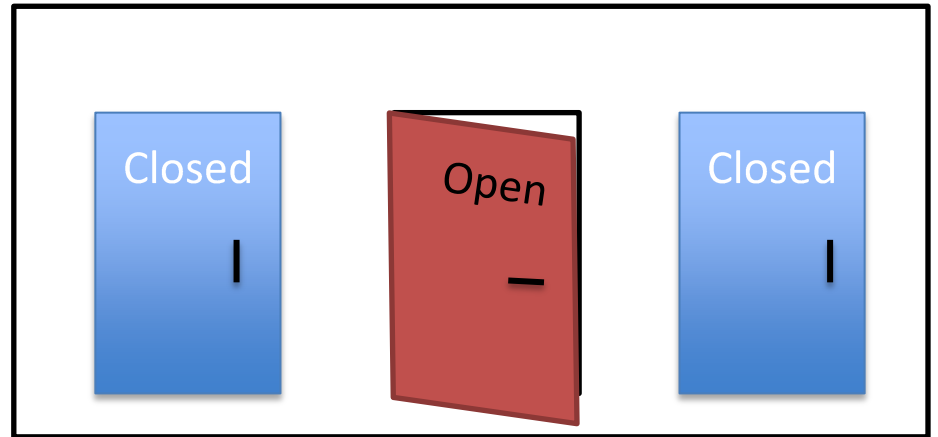
3scale
Infrastructure for the programmable web
API Management
FREE Solution
Up to 50,000 Hits per Day

txtNation
Mobile Billing & SMS Messaging APIs

Security



Authentication



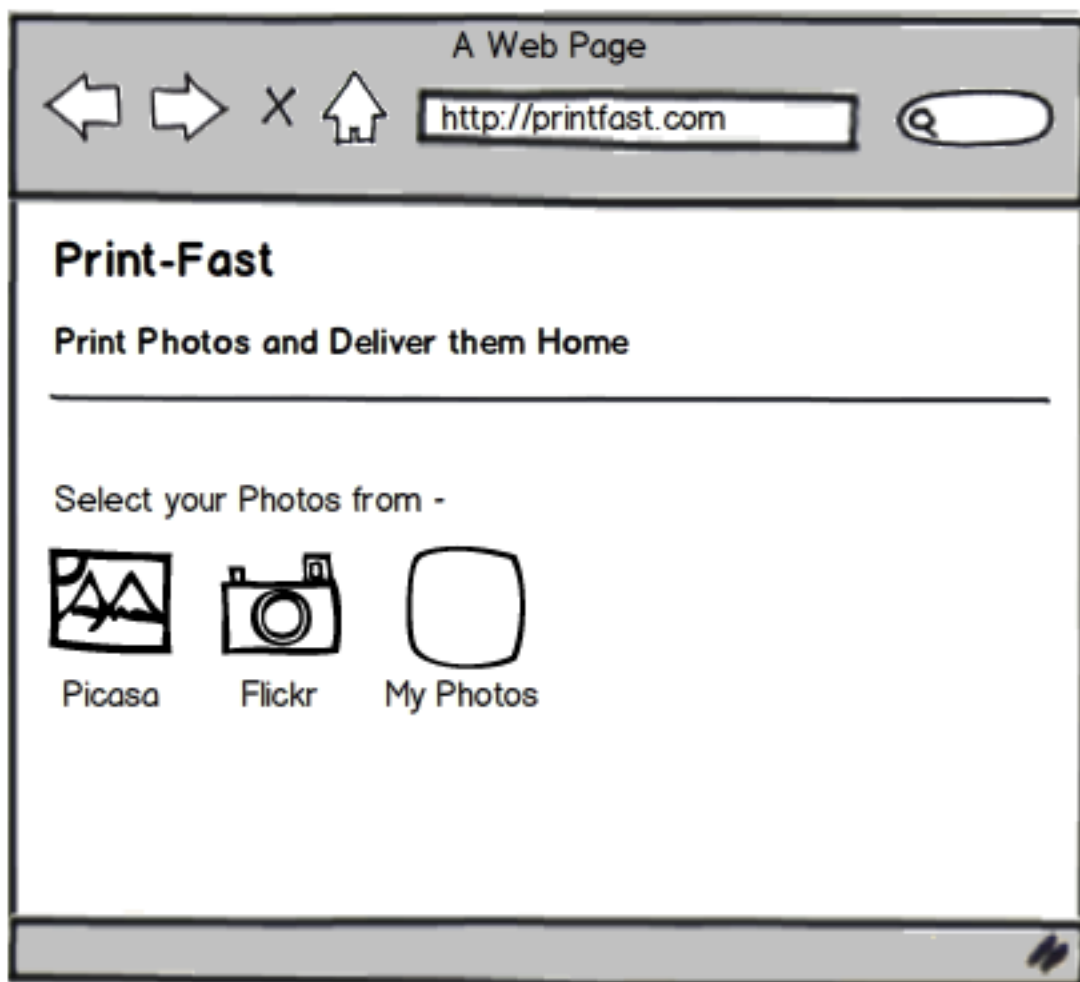
Authorization

OAuth Practical Example

Disclaimer before you read ahead:

All product names and people names used in the following slides are not entirely accurate. They are only placeholders to explain the concept. None of that information should be assumed to be correct or incorrect.

Without OAuth



Without OAuth

Se conosci
Username e
password puoi
fare quello che
vuoi !!!

A Web Page

http://printfast.com

Print-Fast

Print Photos and Deliver them Home

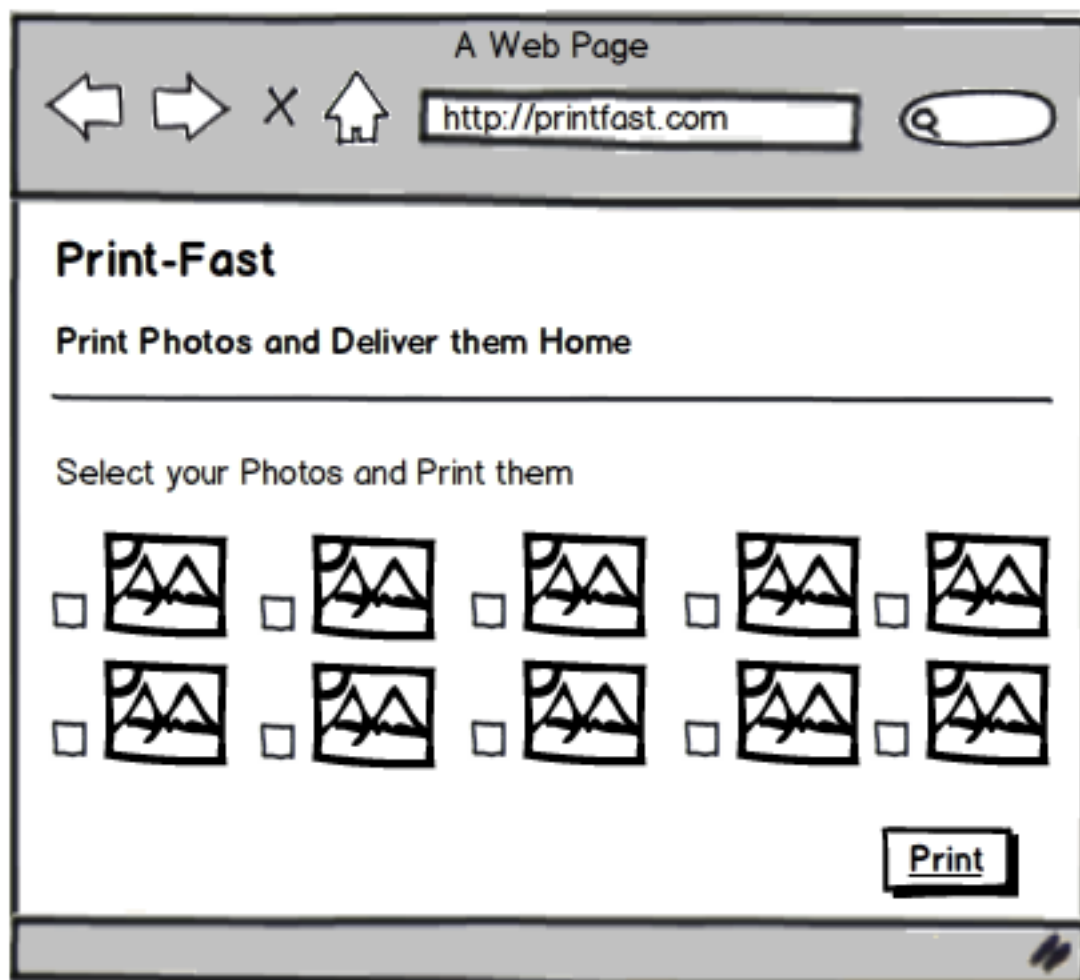
Login to Picasa

UserName

Password

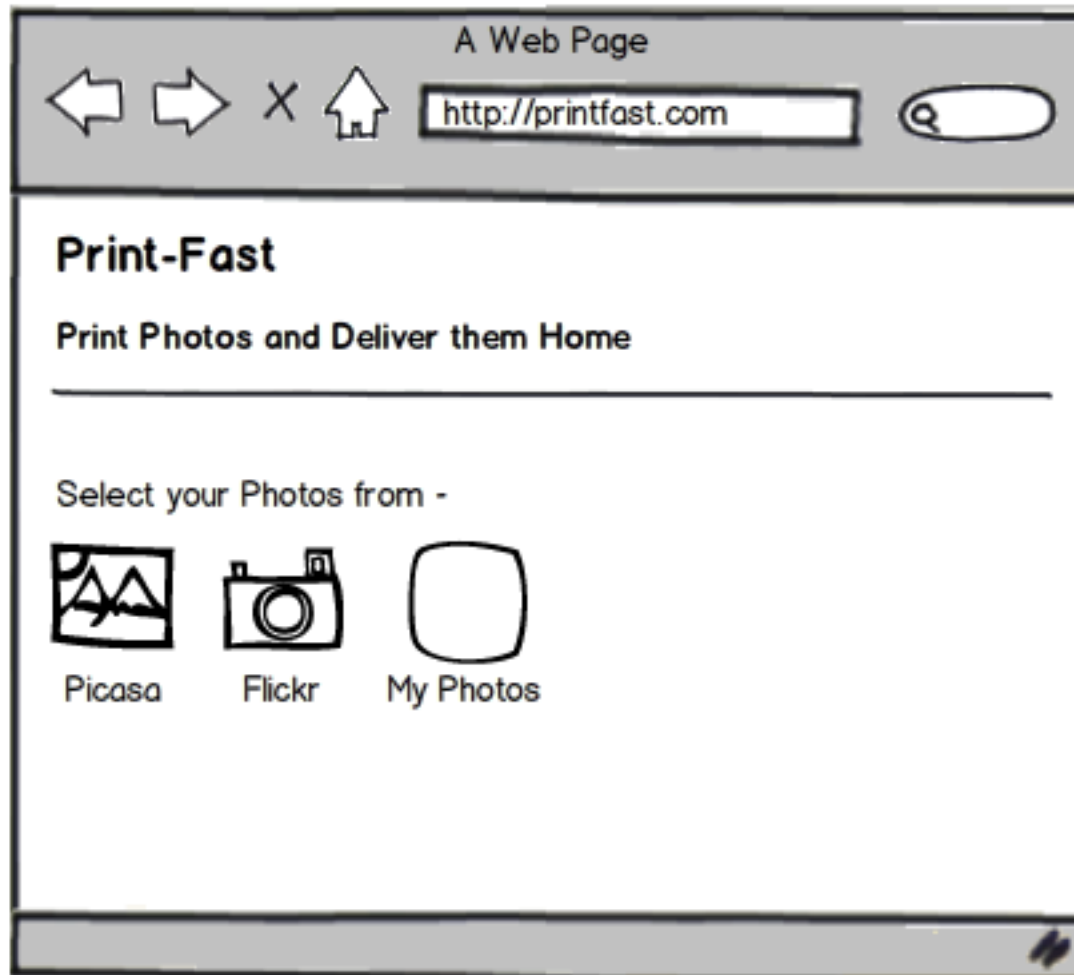
We swear we will not leak your picasa login name and password

Without OAuth



Lets Start Again

With OAuth



With OAuth

URL changed to
<http://picasa.com>

A Web Page

← → × 🏠 🔍

Picasa

Login to Picasa

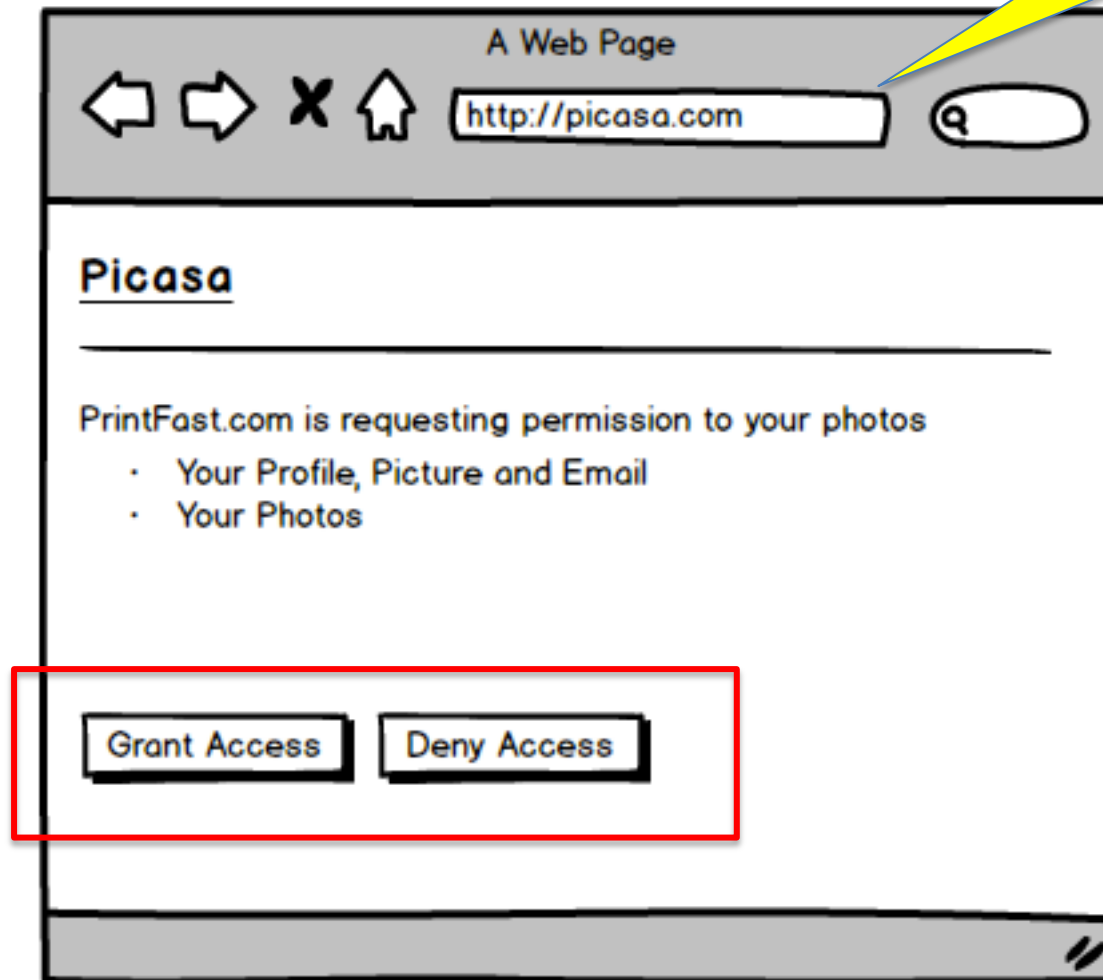
UserName

Password

Username e
password sono
forniti solo al
sito che li
detiene

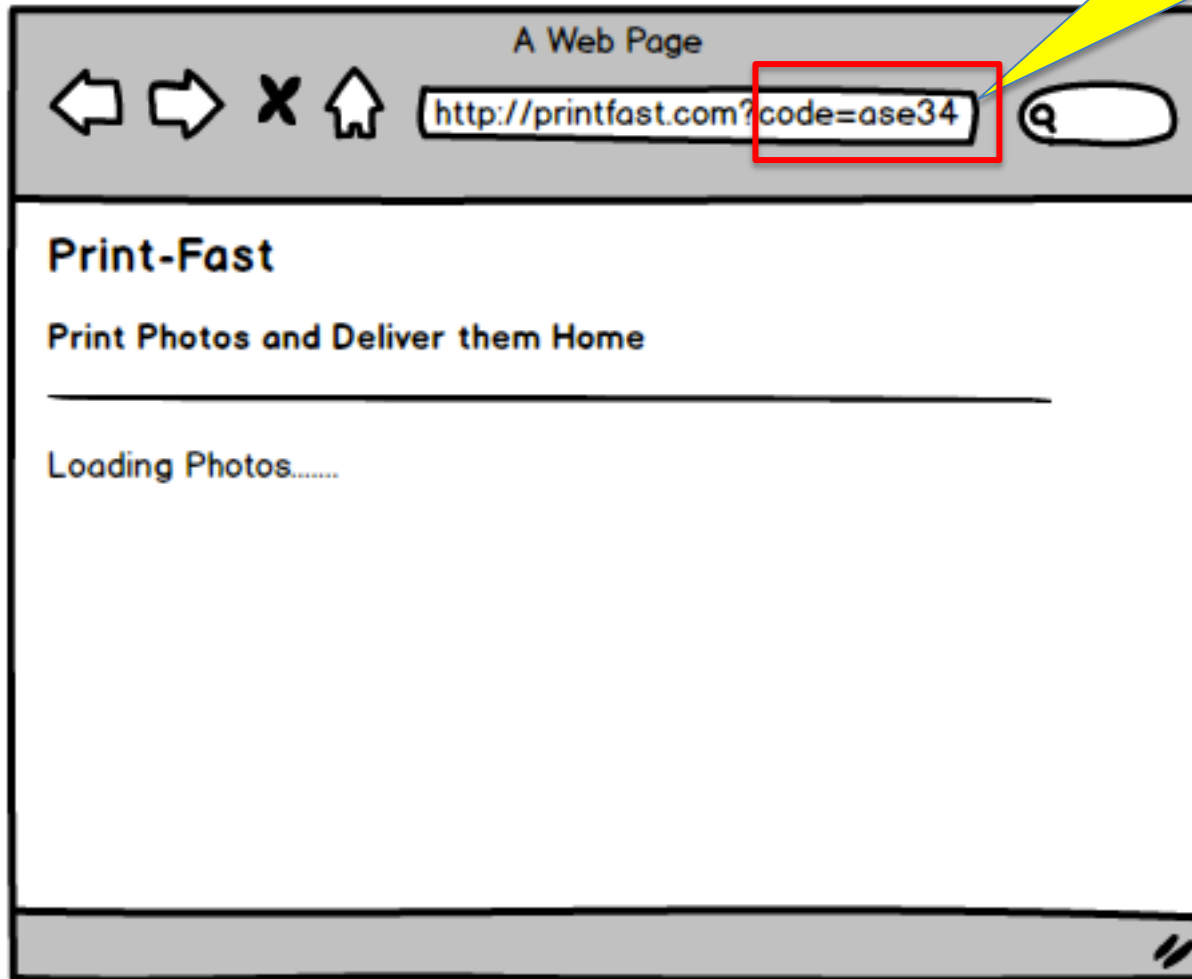
With OAuth

URL is
<http://picasa.com>

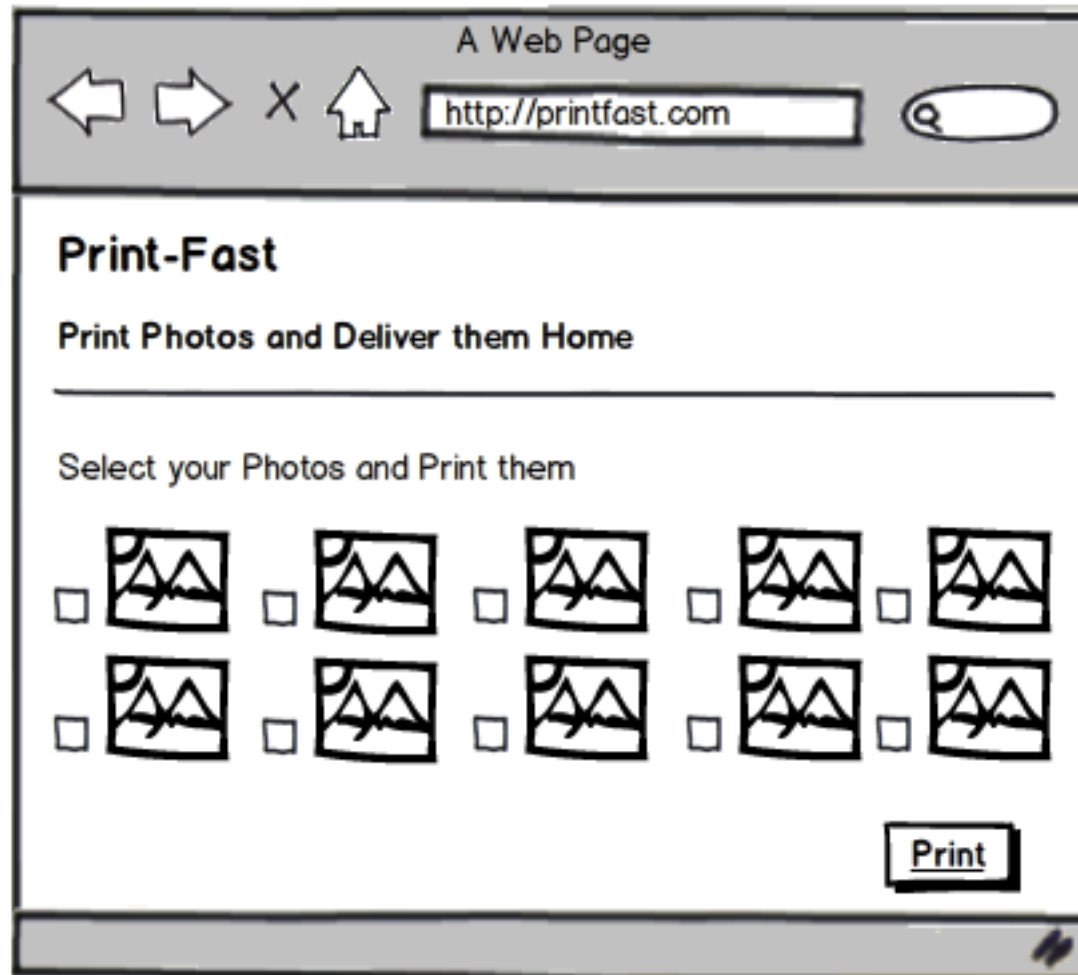


With OAuth

Codice d'accesso per
picasa

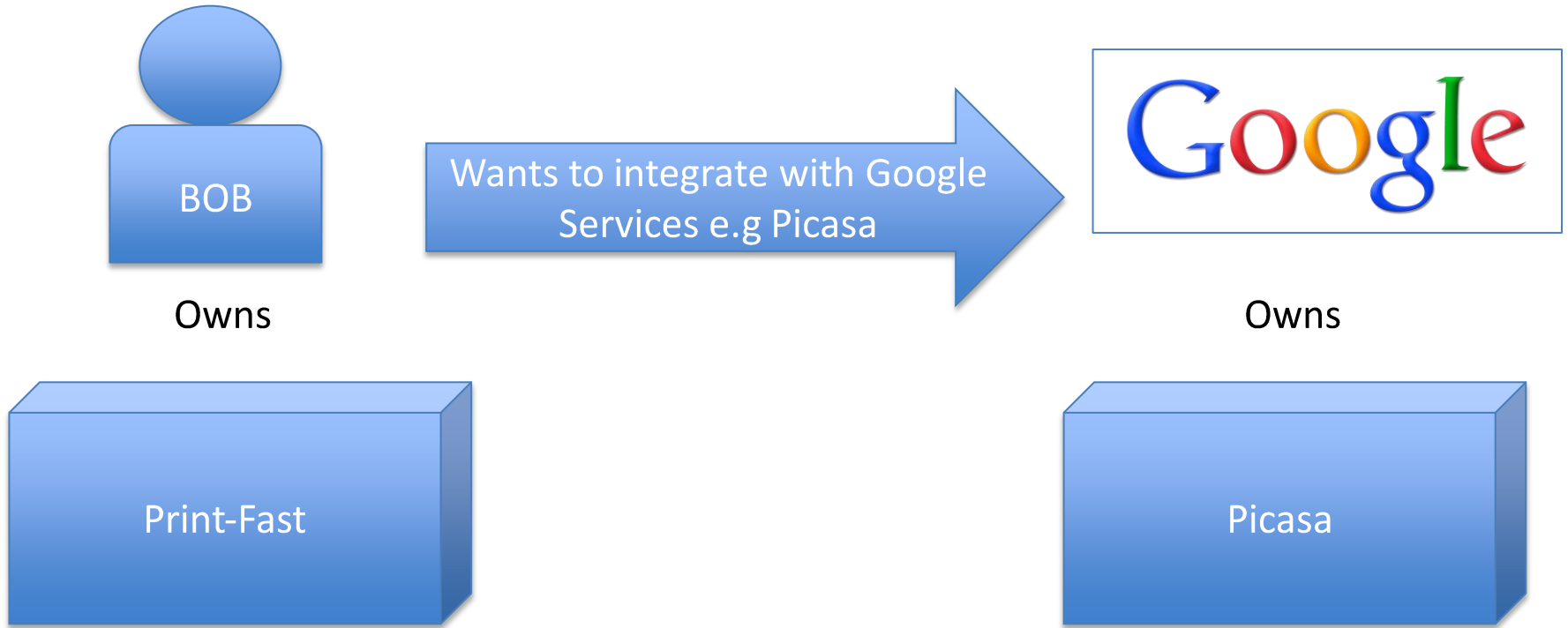


With OAuth

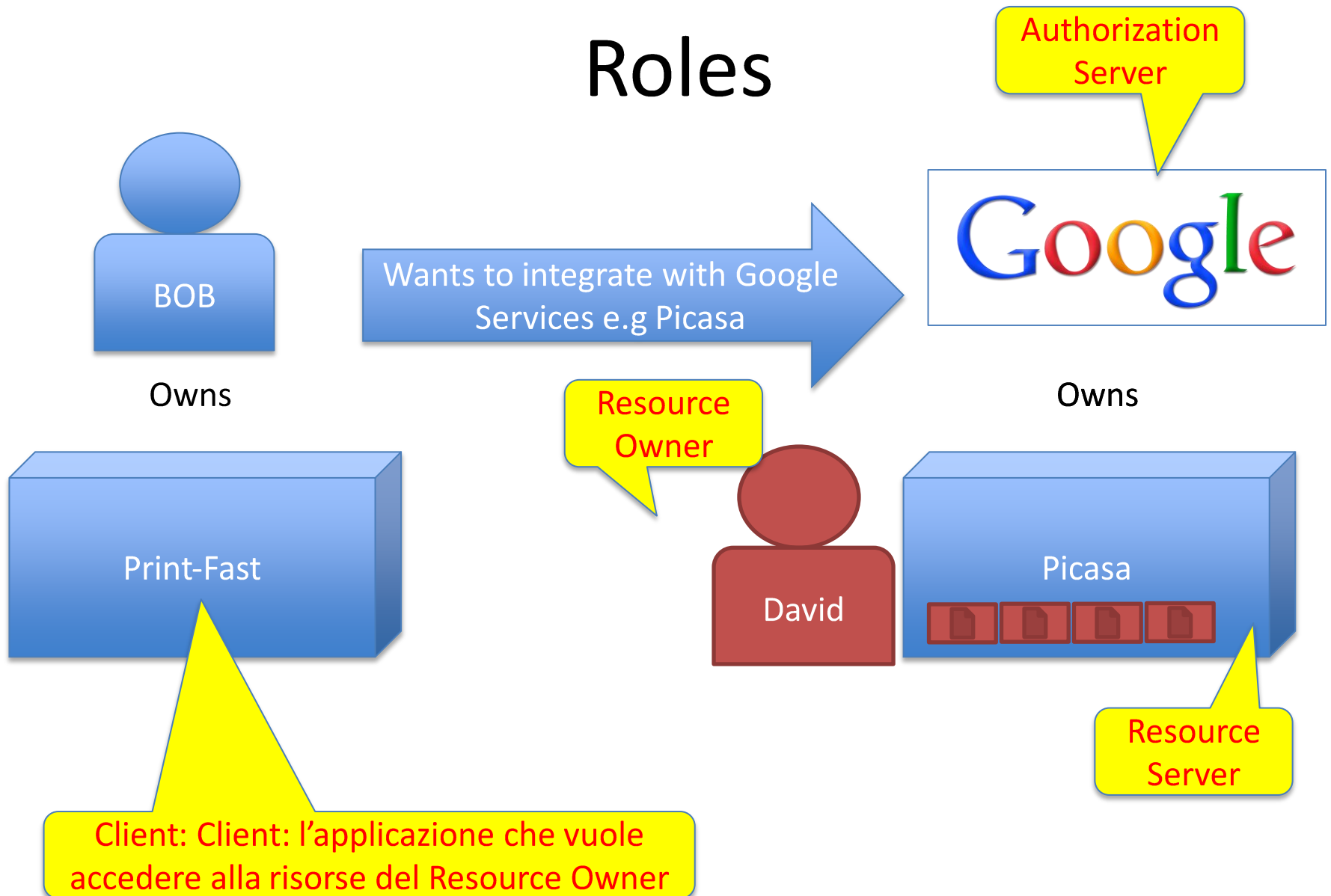


OAuth 2.0 Flow in Depth

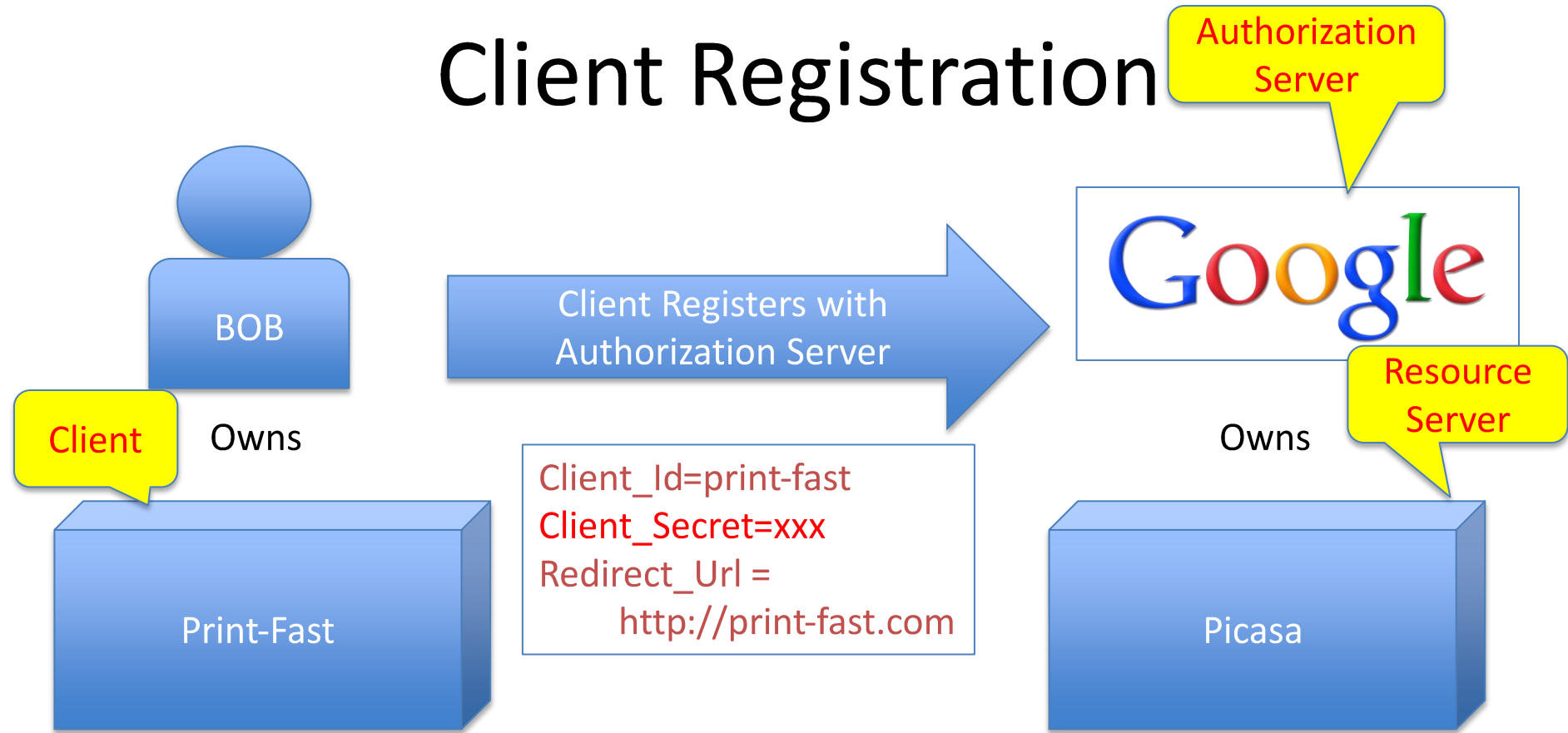
Scenario



Roles



Client Registration



- The Client register to the authorization server before accessing and gets a **secret**
- The registration remains valid unless is revoked
- When a resource owner has successfully authorized the client application via the authorization server, the resource owner is redirected back to the client application, to the redirect URI.

Client Secret

- OAuth2, uses the client secret mechanism as a means of authorizing a client, the software requesting an access token. You might think of it as a secret passphrase that proves to the authentication server that the client app is authorized to make a request on behalf of the user.
- You shouldn't confuse authorization with authentication. Users are authenticated (proven that they are whom they say they are), while apps are authorized (the app is allowed to use or access the resources)

<http://salesforce.stackexchange.com/questions/14009/whats-the-benefit-of-the-client-secret-in-oauth2>

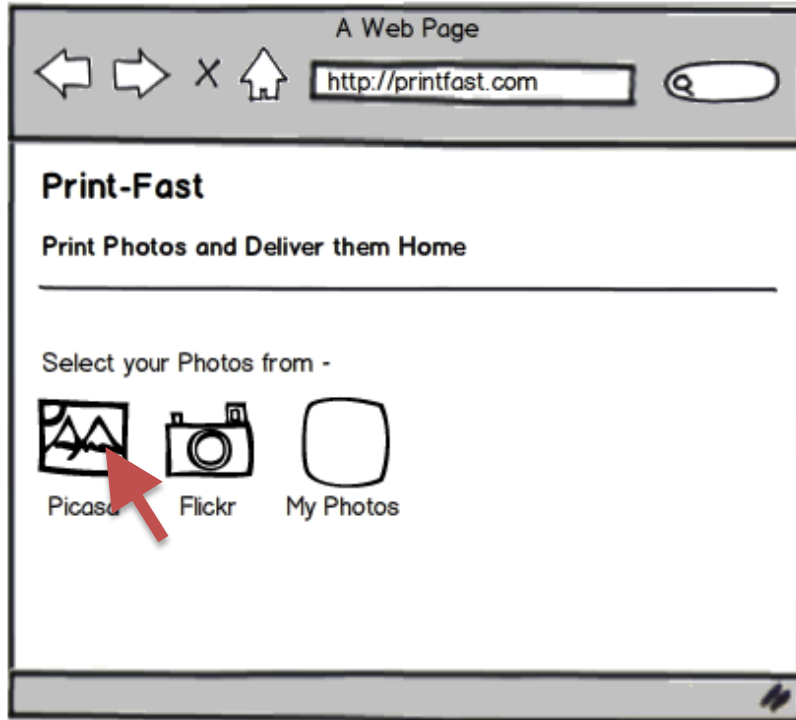
OAuth Flows/Grant Types

- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant

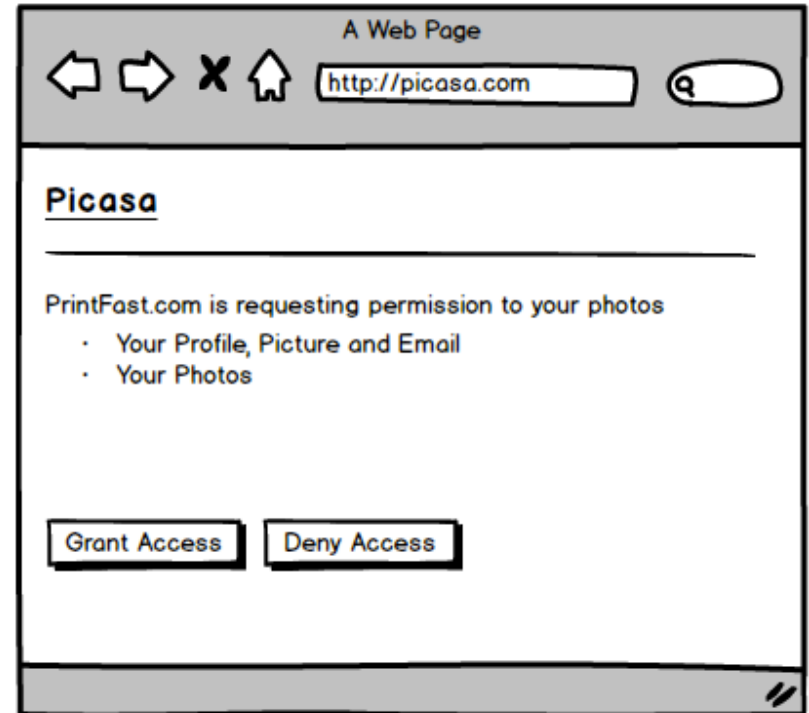
<http://stackoverflow.com/questions/31637852/how-to-get-a-jwt/31768524#31768524>

Step 1 – Get Authorization Grant

Authorization Request



Authorization Grant

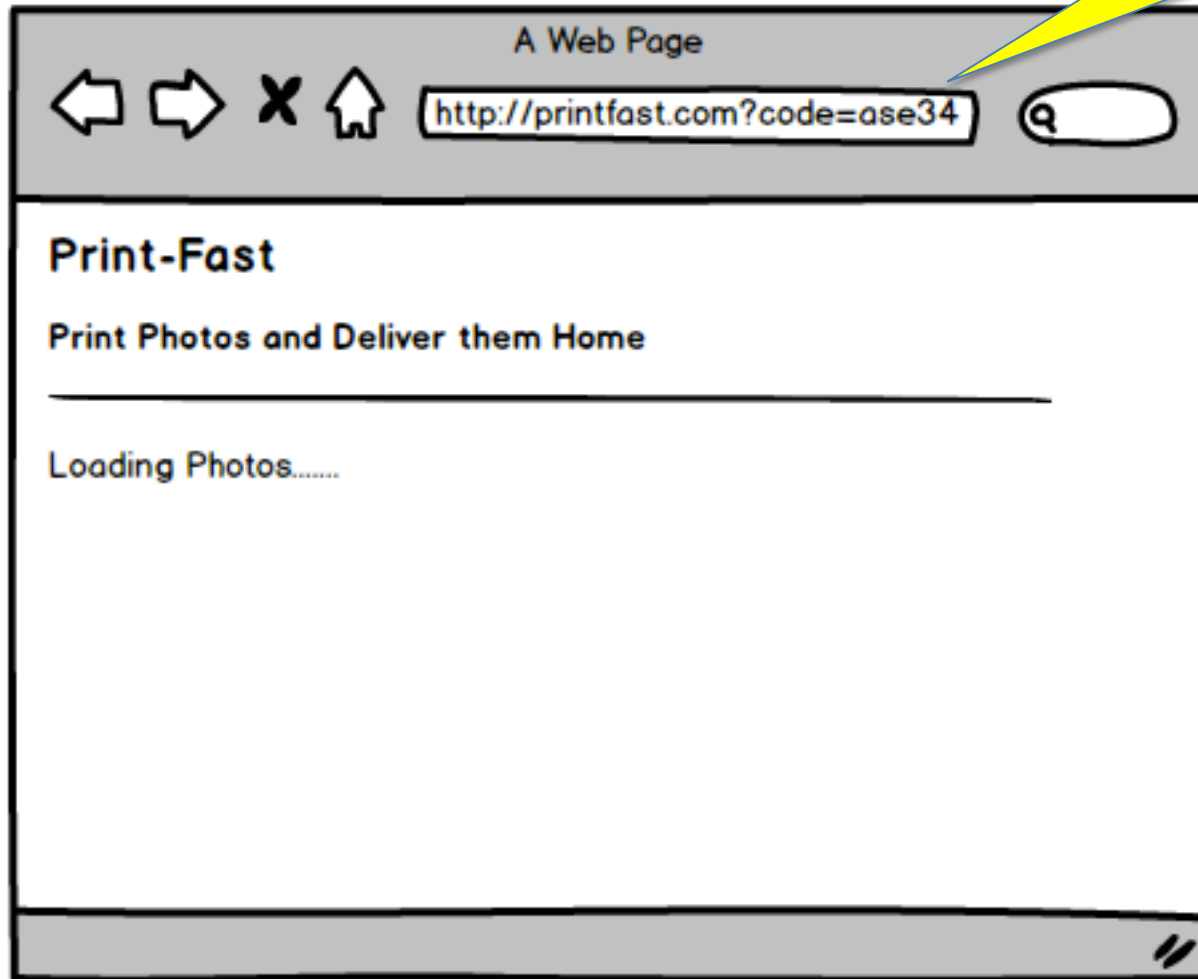


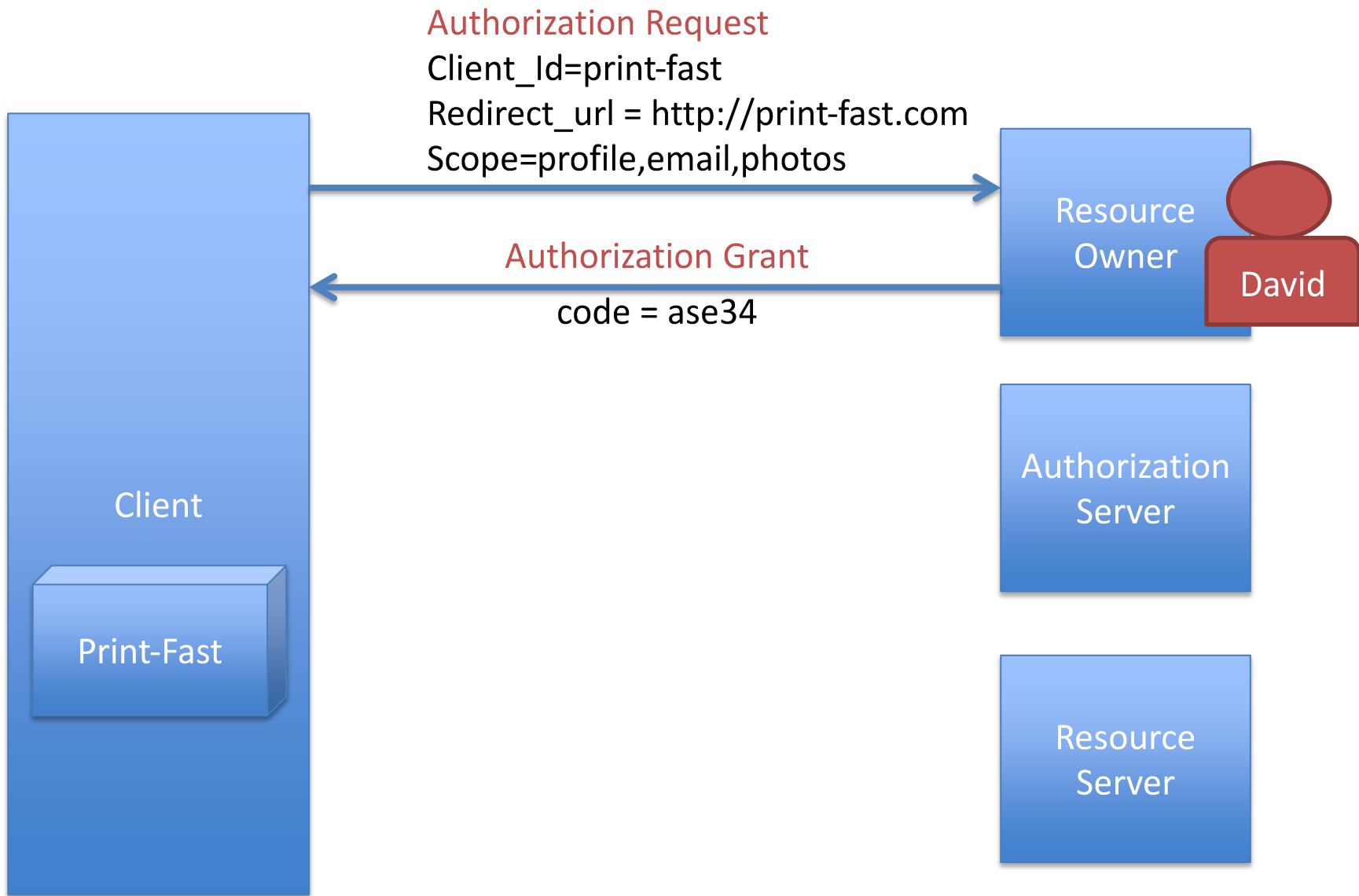
URL used is

`http://picasa.com/?client_id=photo-fast &scope=profile,email,photos
&redirect_uri=http://print-fast.com&response_type=code`

Authorization Grant

Authorization Grant
Code = ase34

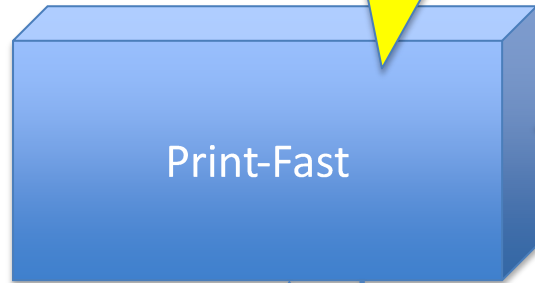




Protocol Flow

Step 2 – Exchange for Access Token

Client



Print-Fast

Code = ase34
Client_Id=print-fast
Client_Secret=xxx

Authorization
Server



access_token = x3e4

code = ase34

access_token = x3e4

A Web Page

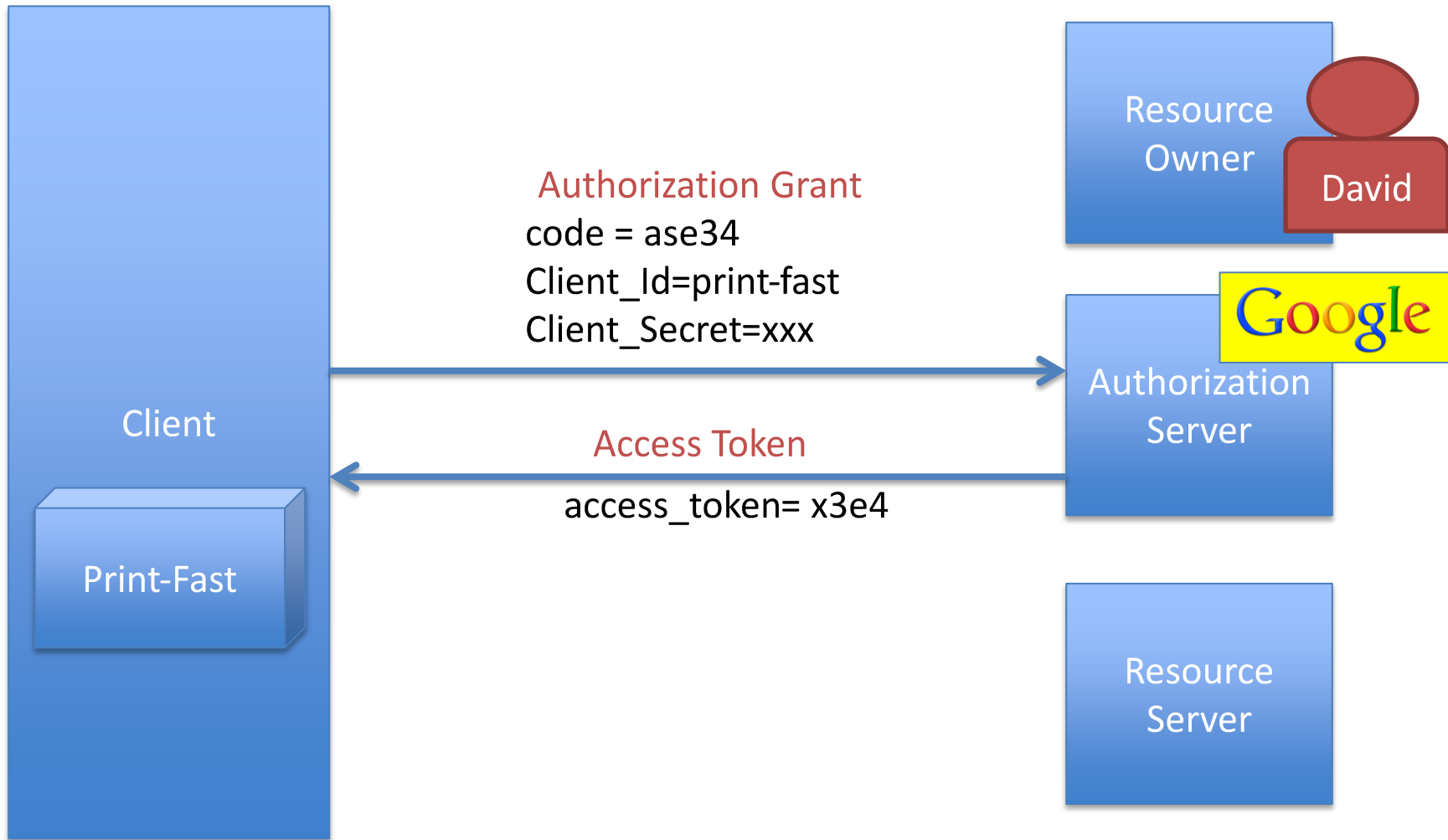


http://printfast.com?code=ase34

Print-Fast

Print Photos and Deliver them Home

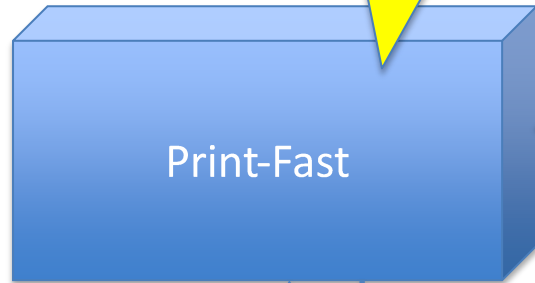
Loading Photos.....



Protocol Flow

Step 3 – Access Protected Resources

Client



Print-Fast

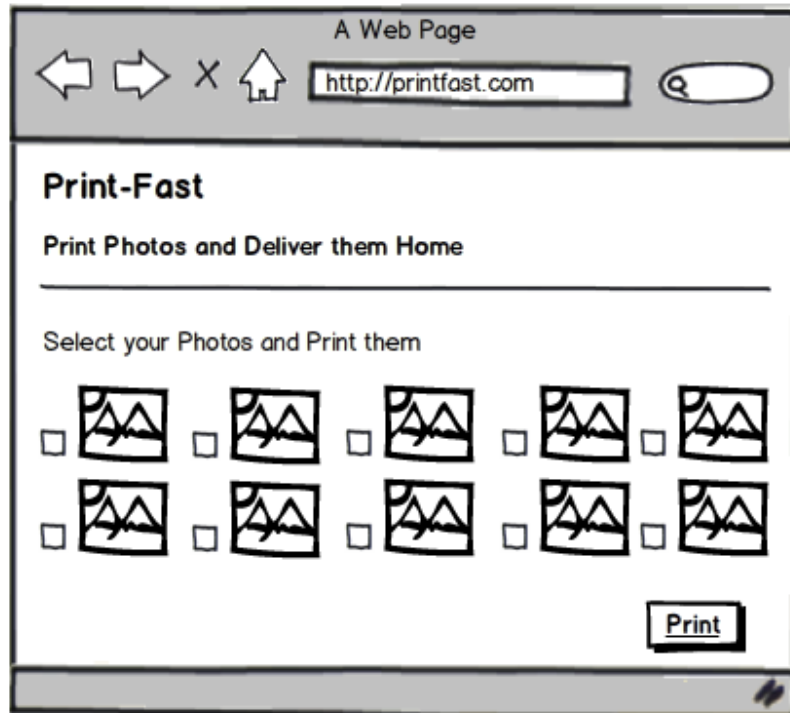
Authorization
Server



Code = ase34
Client_Id=print-fast
Client_Secret=xxx

access_token = x3e4

code = ase34



[http://picasa.com/
.../usr133/photos](http://picasa.com/.../usr133/photos)

access_token = x3e4

[
"http://.../DSC34.jpg",
"http://.../DSC44.jpg",
"http://.../DSC56.jpg",
"http://.../DSC98.jpg"
]

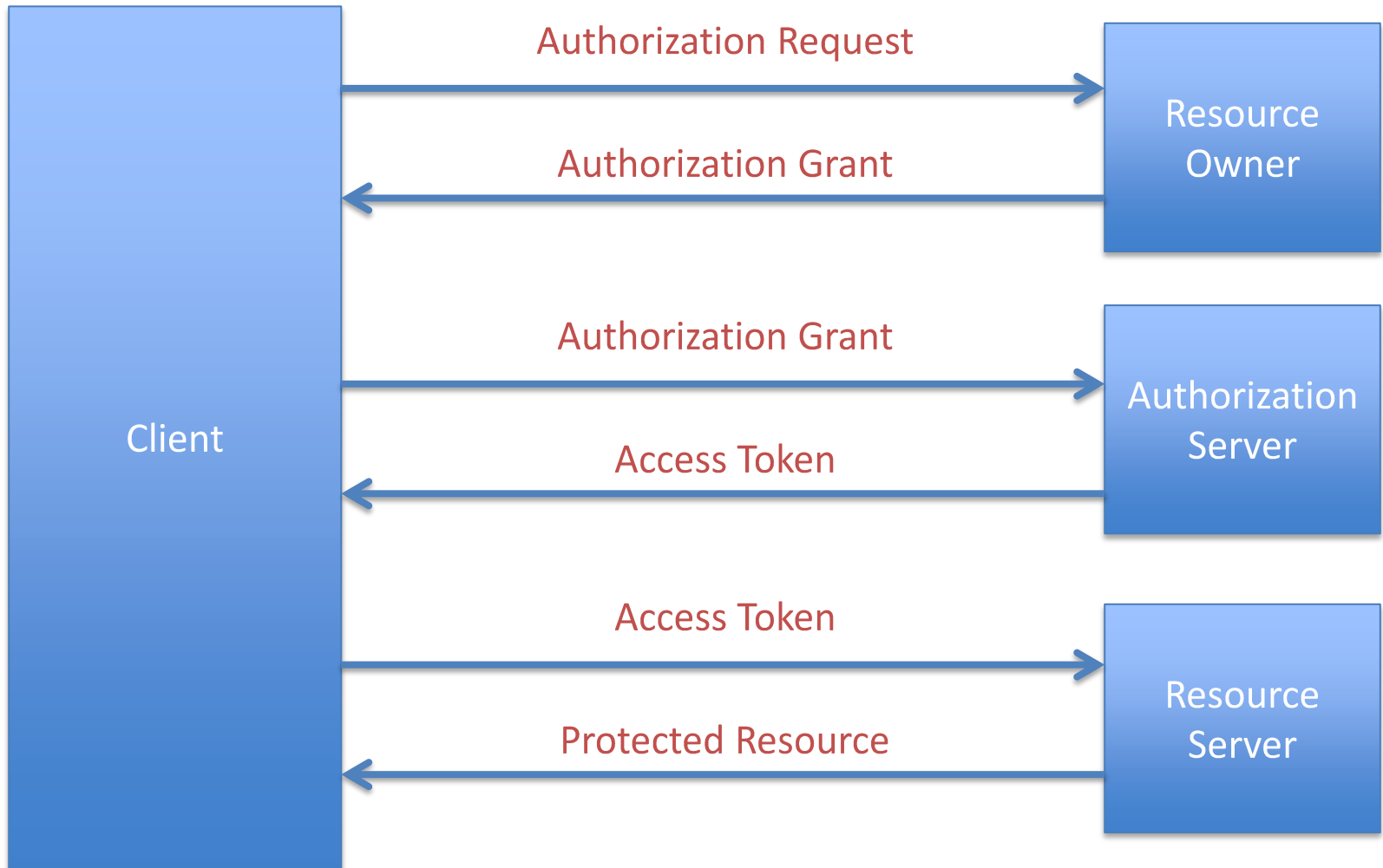
Picasa



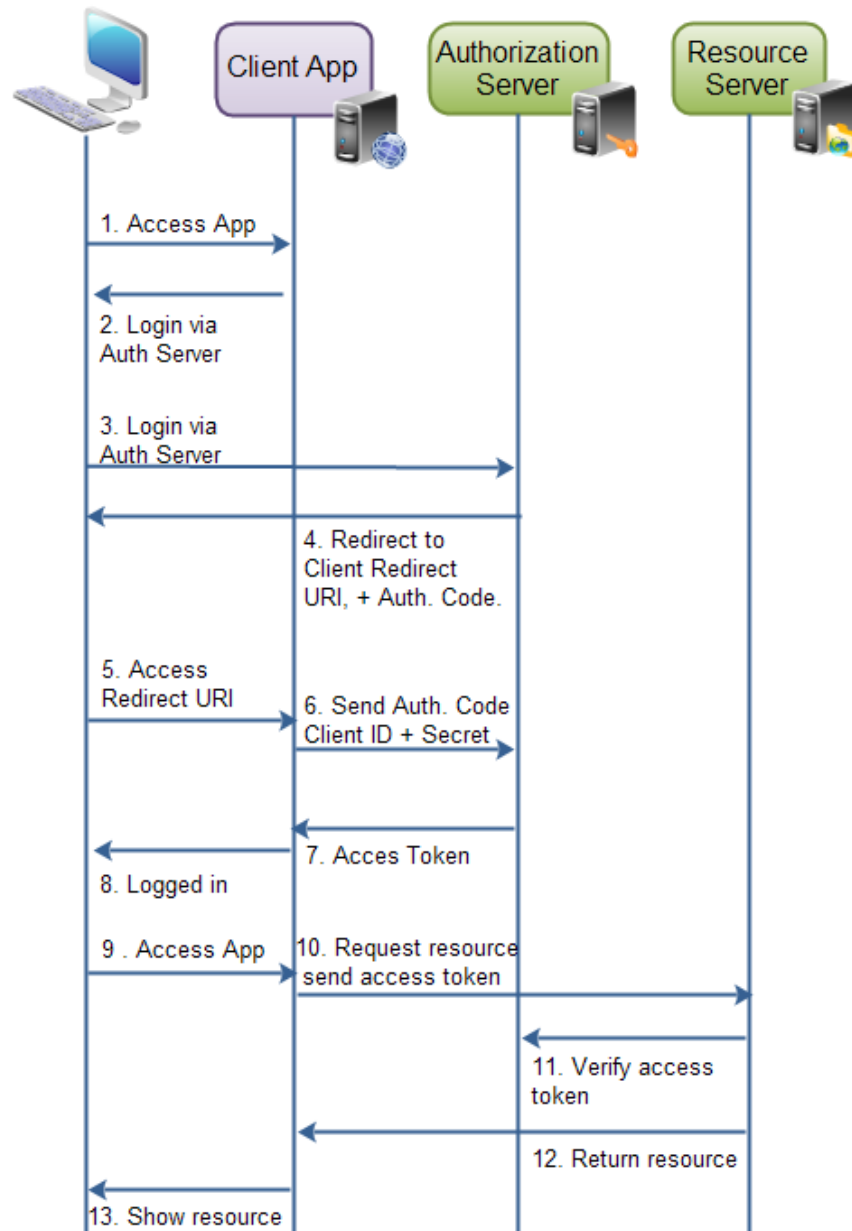


Protocol Flow

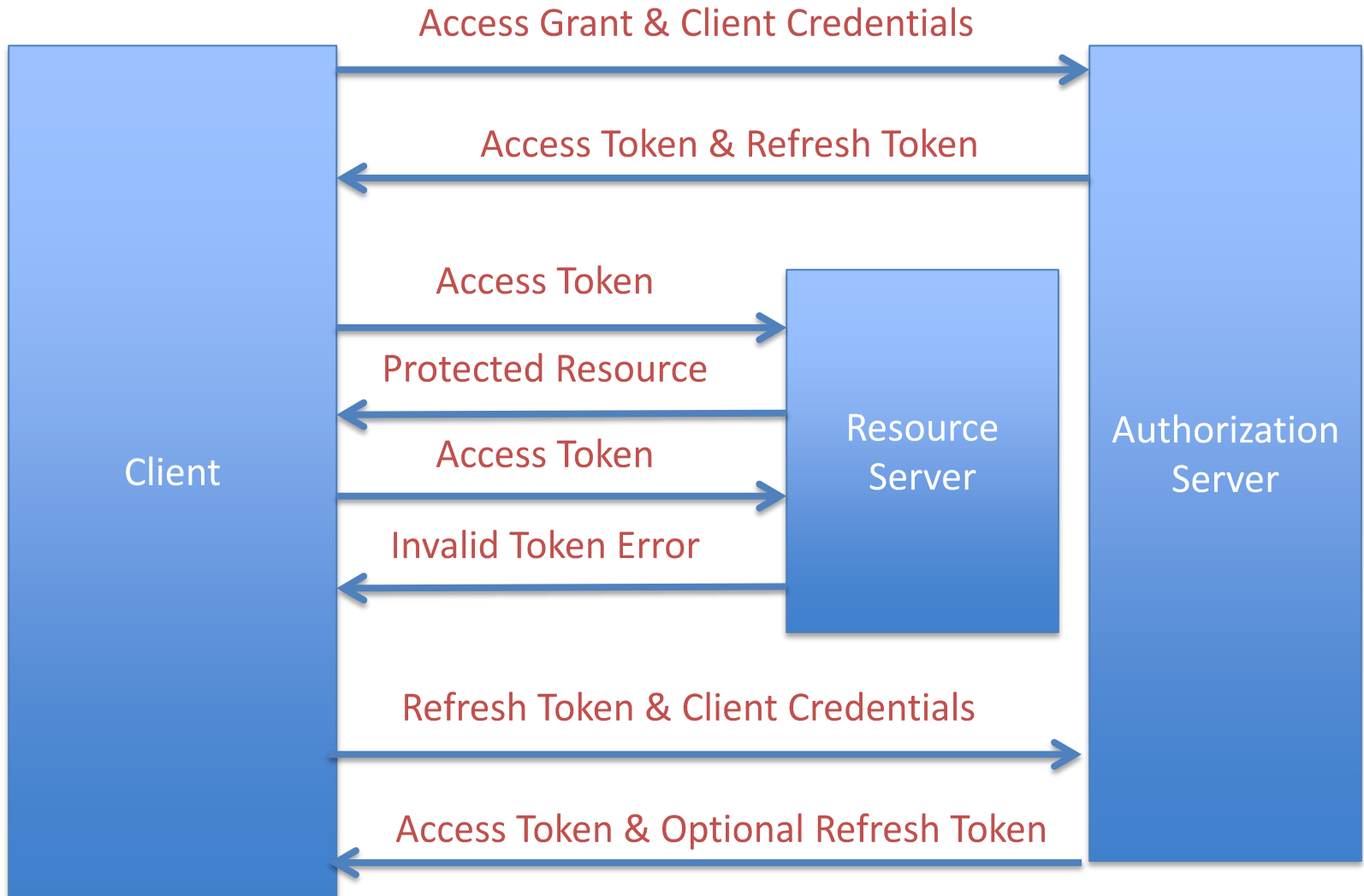
Complete Flow at Once



Protocol Flow



With Refresh Token



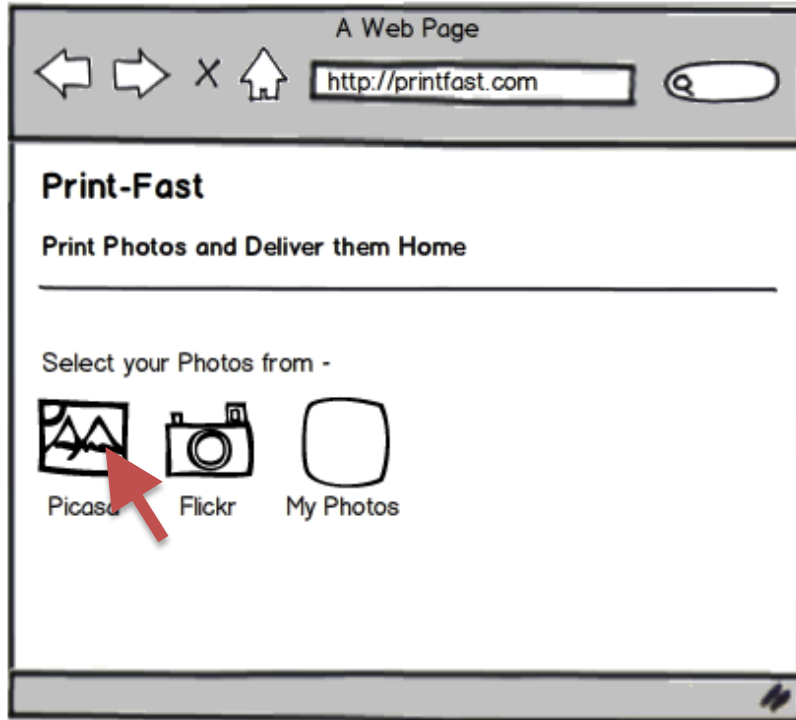
Protocol Flow

OAuth Flows/Grant Types

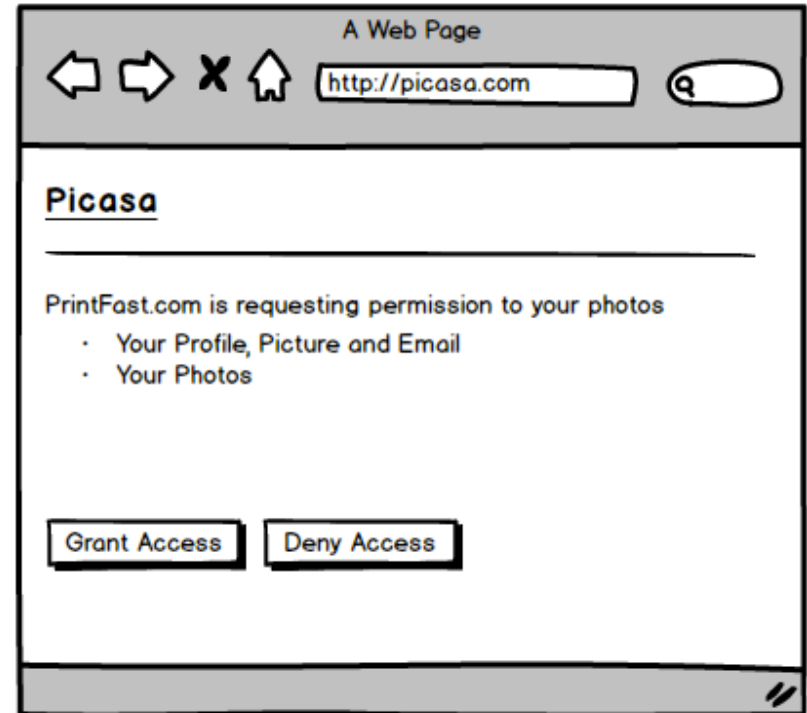
- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant

Step 1 – Get Access Token

Implicit Grant Request



Implicit Grant

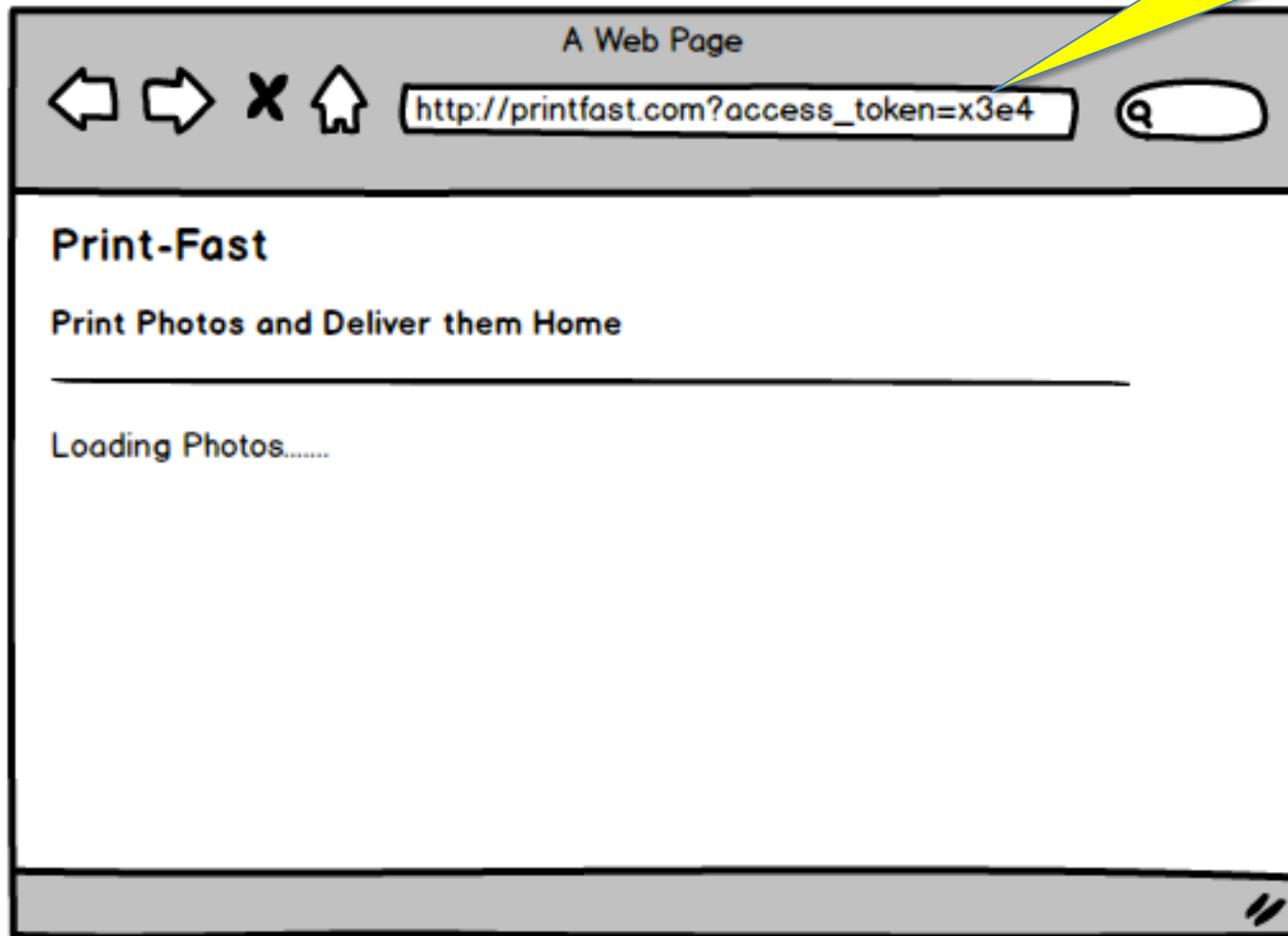


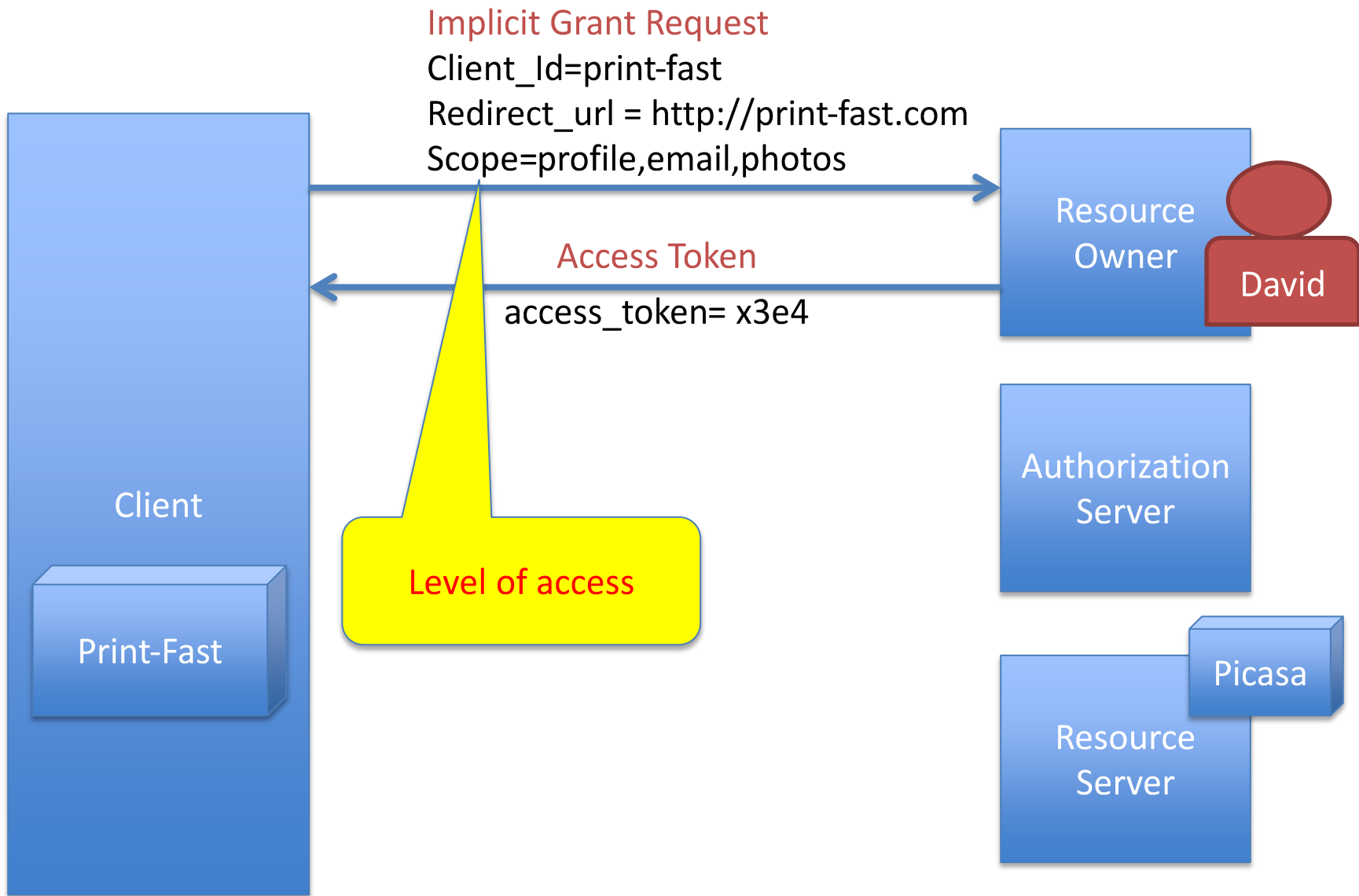
URL used is

http://picasa.com/?client_id=photo-fast &scope=profile,email,photos &redirect_uri=http://print-fast.com&response_type=token

Implicit Grant

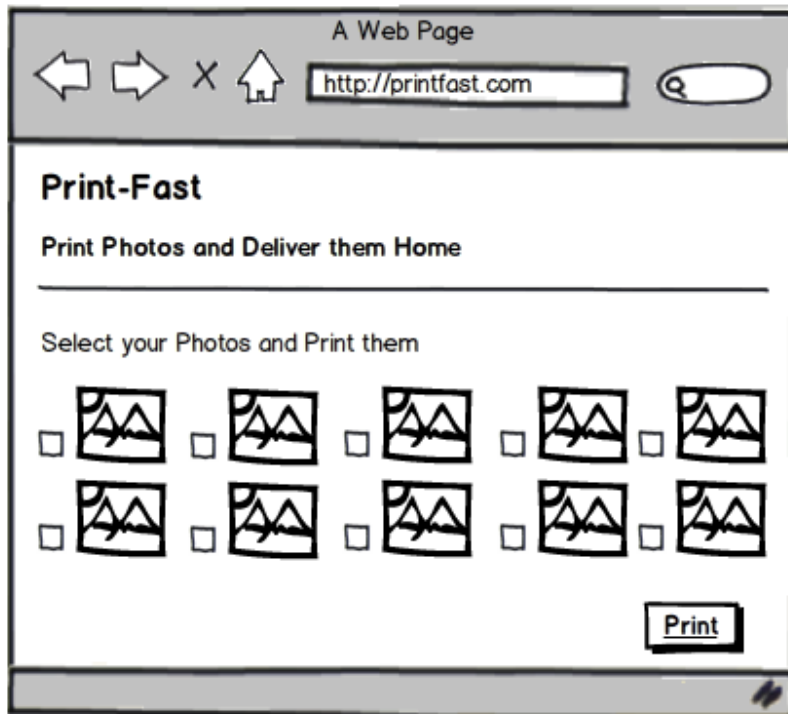
Access token = x3e4





Protocol Flow

Step 2 – Access Protected Resources



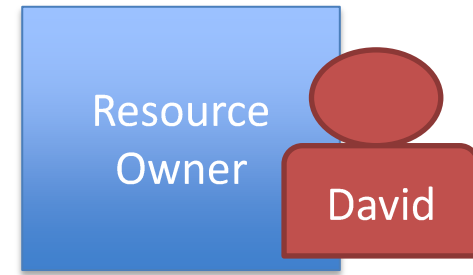
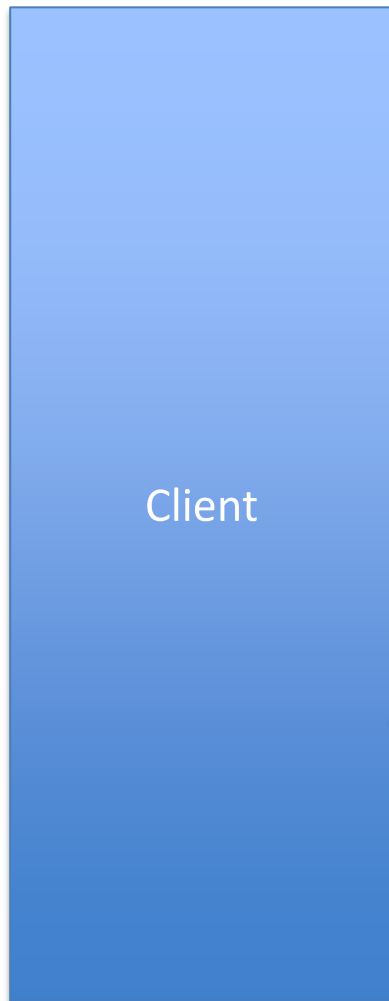
[http://picasa.com/
.../usr133/photos](http://picasa.com/.../usr133/photos)

access_token = x3e4

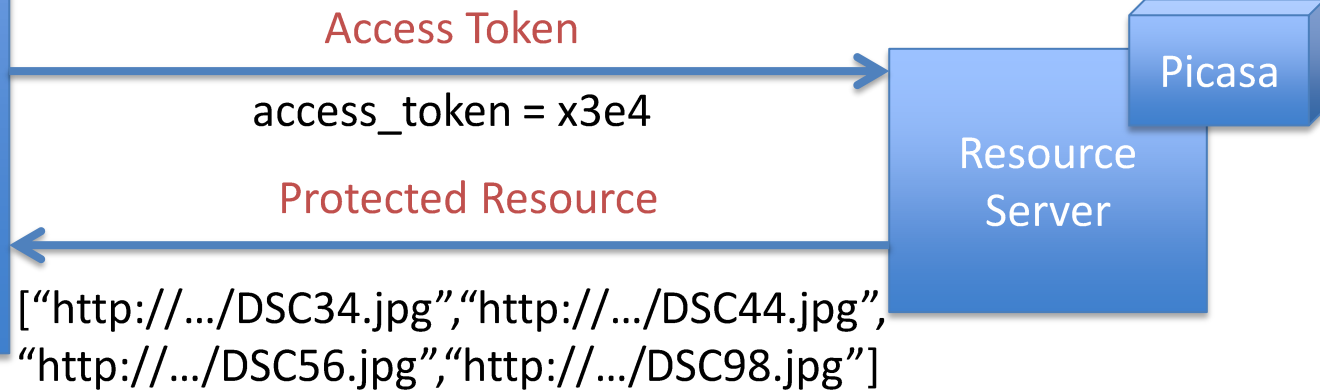


[
 "http://.../DSC34.jpg",
 "http://.../DSC44.jpg",
 "http://.../DSC56.jpg",
 "http://.../DSC98.jpg"
]



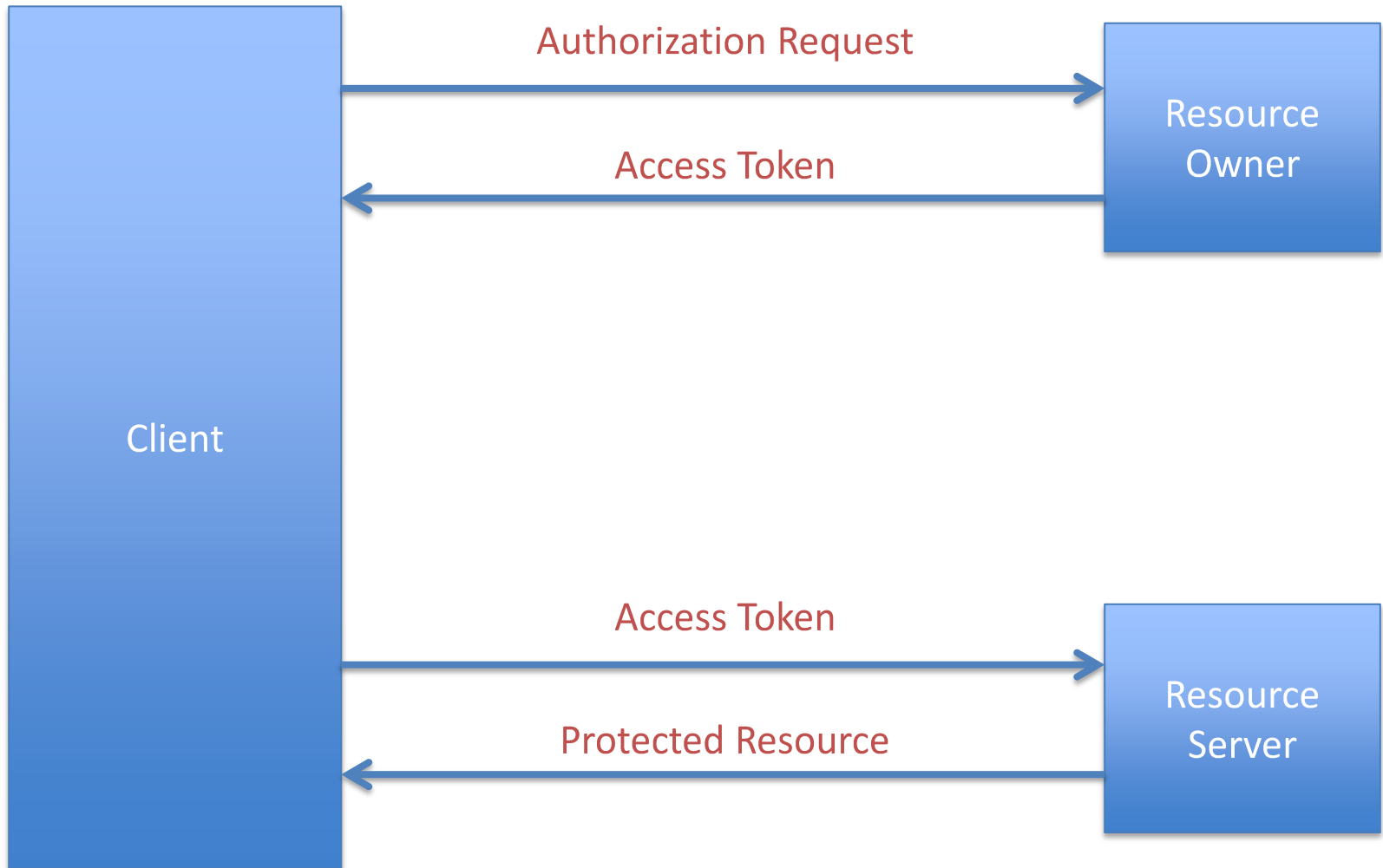


Meant for Pure Browser based Applications



Protocol Flow

Complete Flow at Once



Protocol Flow

OAuth Flows/Grant Types

- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant

<https://developers.google.com/identity/protocols/OAuth2WebServer?hl=en>

Reference

- Book – [Getting Started with OAuth 2.0](#)
- [Facebook Documentation](#)
- [Google Documentation](#)
- [Brian David Campbell's Presentation](#)