OAuth 2.0 in Depth

By Rohit Ghatol

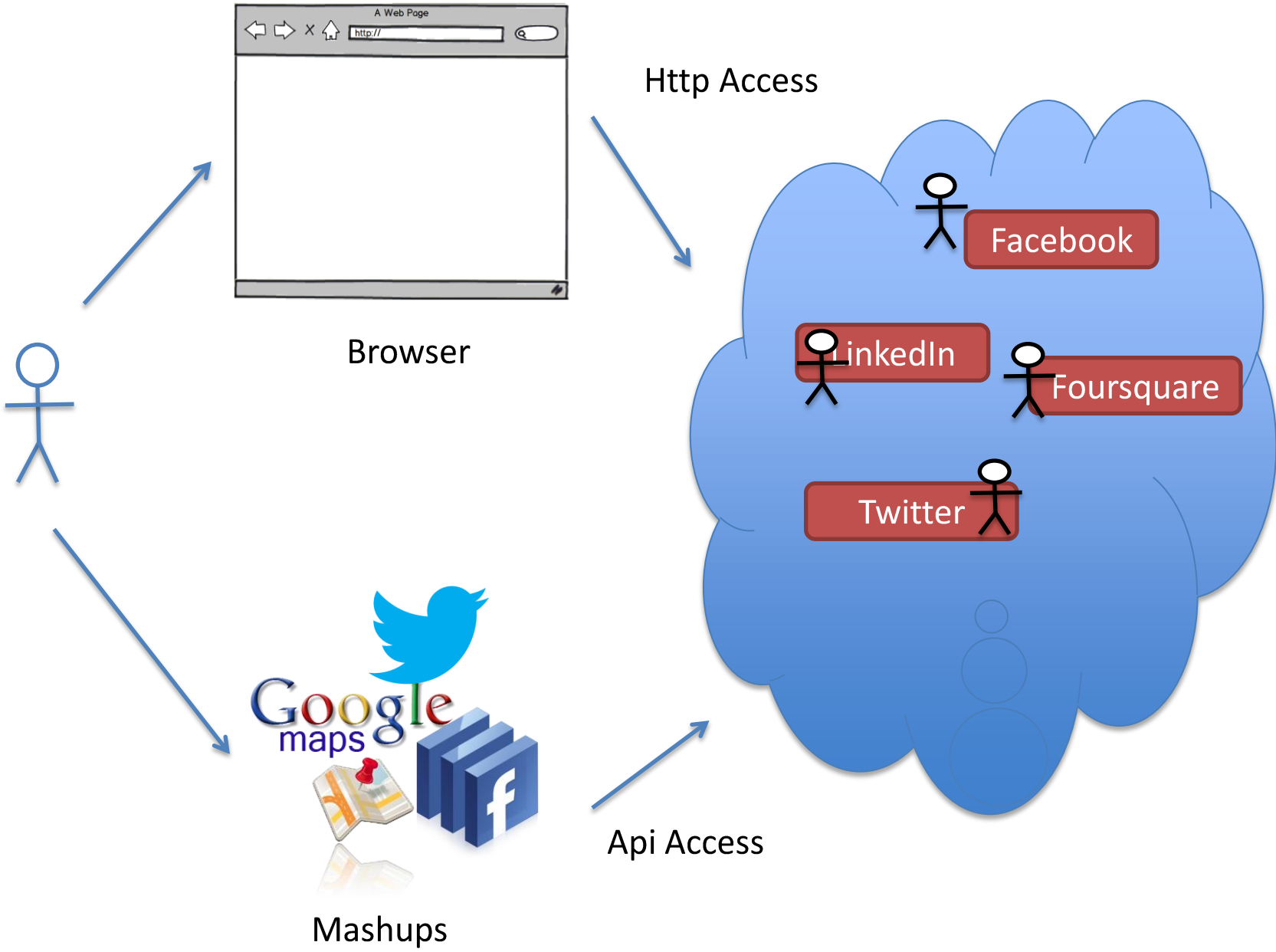
http://www.slideshare.net/rohitsghatol/oauth-20-in-depth

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

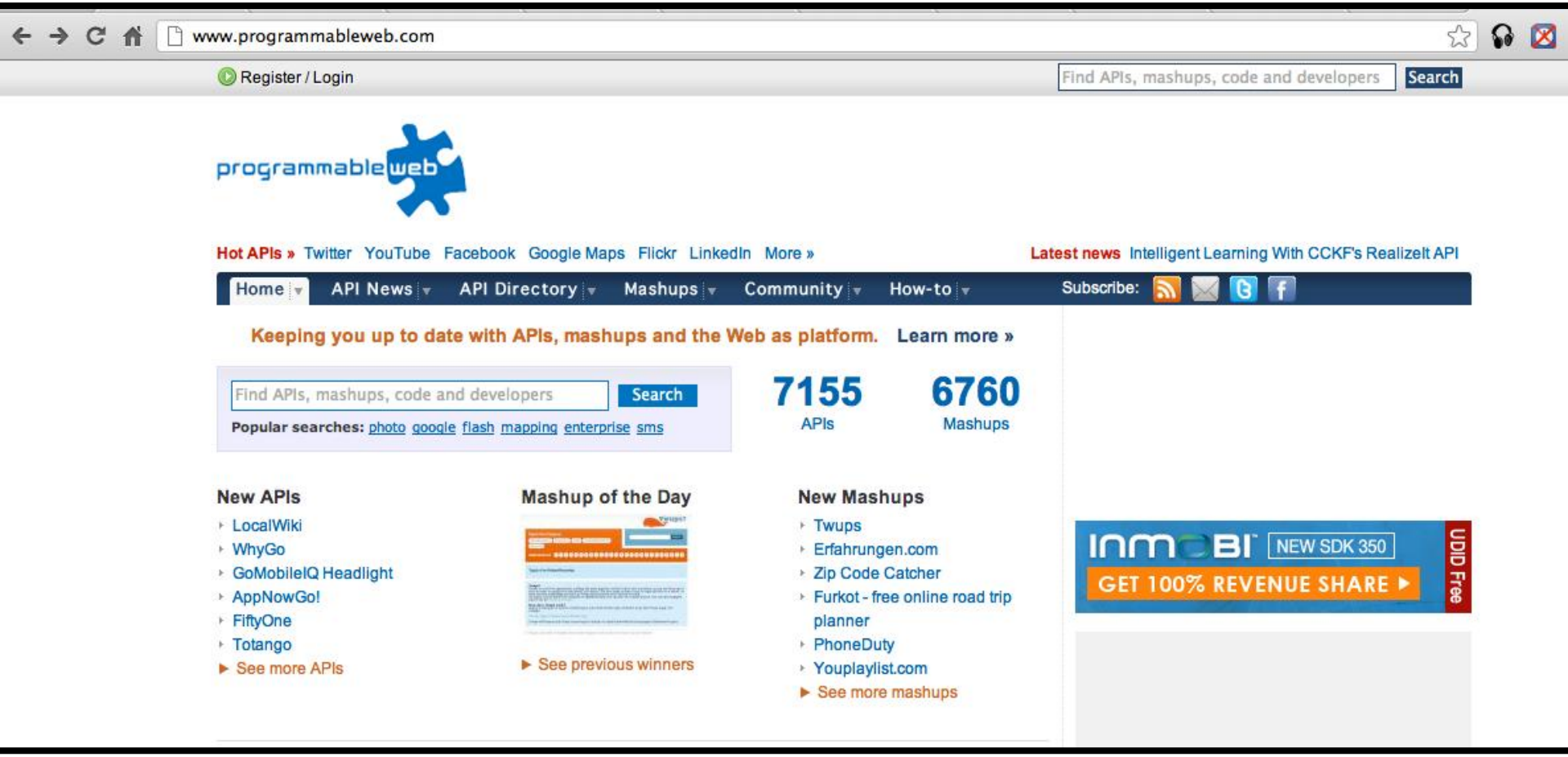
Why study about OAuth?

Do you care about these or Similar Sites?

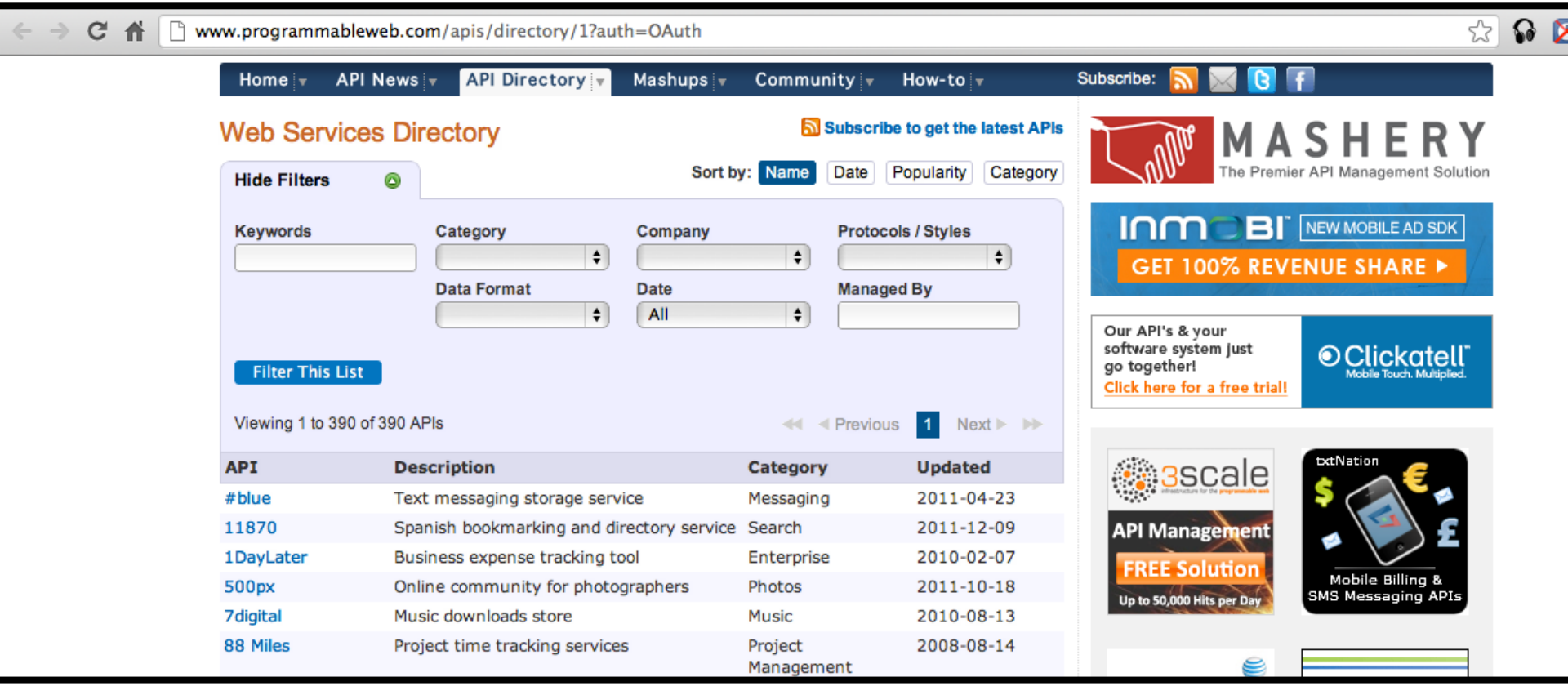
Reference - http://rainbowseo.com/wp-content/uploads/2012/06/smm.png


A Web Page
http://
Http Access
Browser
Facebook
LinkedIn
Foursquare
Twitter
Google maps
Api Access
Mashups

7155 APIs listed on
http://ProgrammableWeb.com

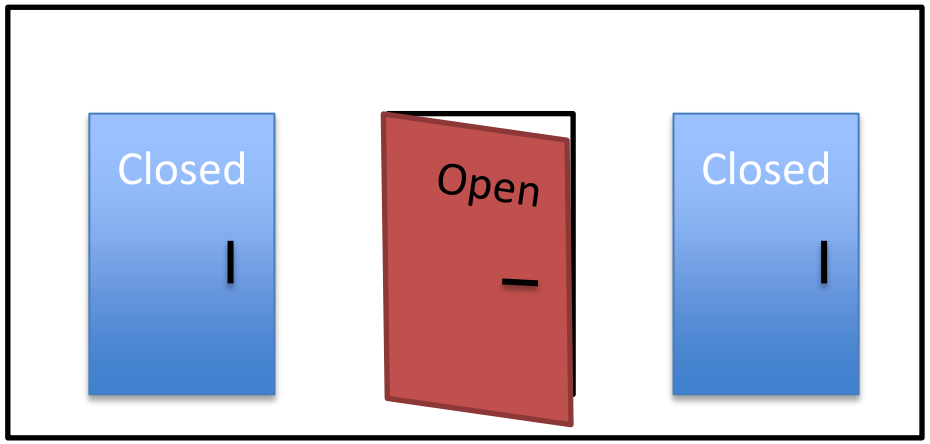


390 APIs on http://ProgrammableWeb.com
support OAuth



Security

Authentication



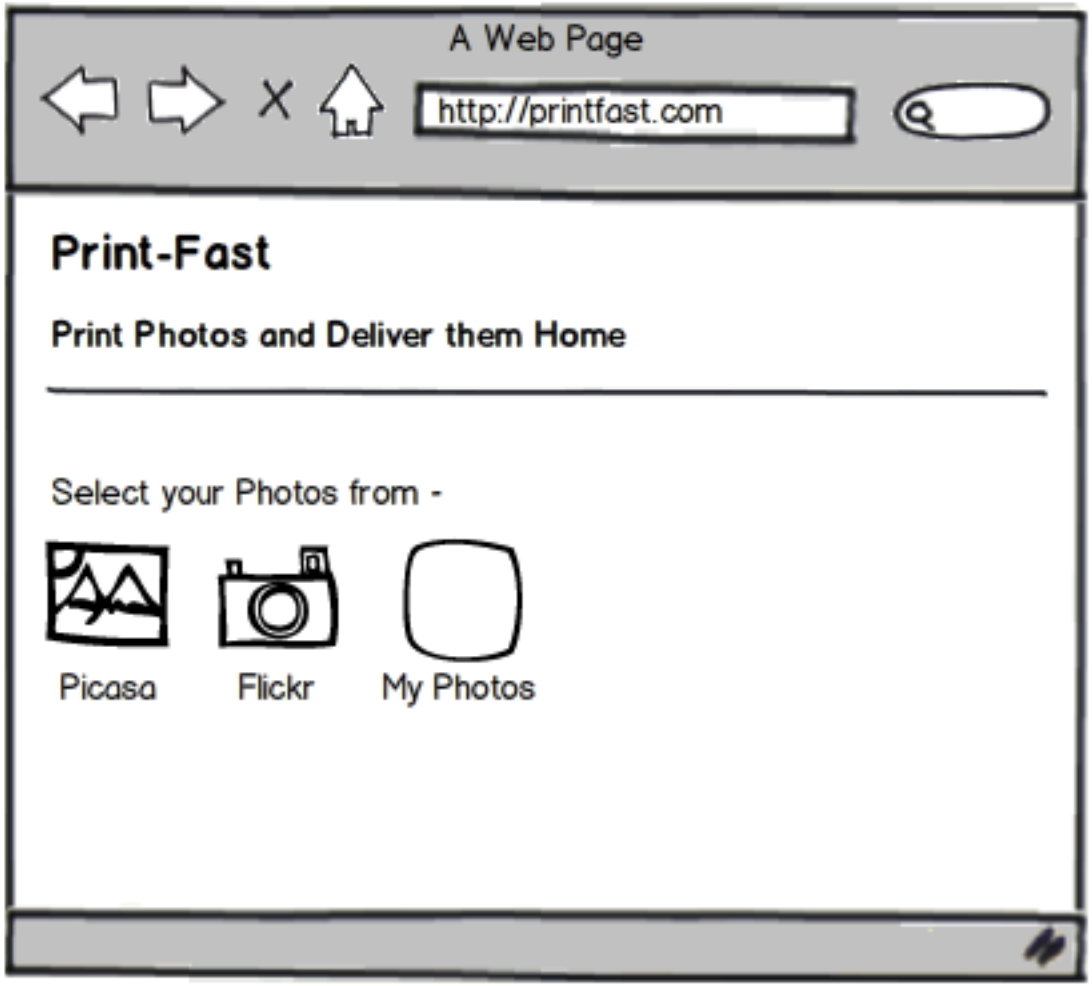
Authorization

OAuth Practical Example

Disclaimer before you read ahead:

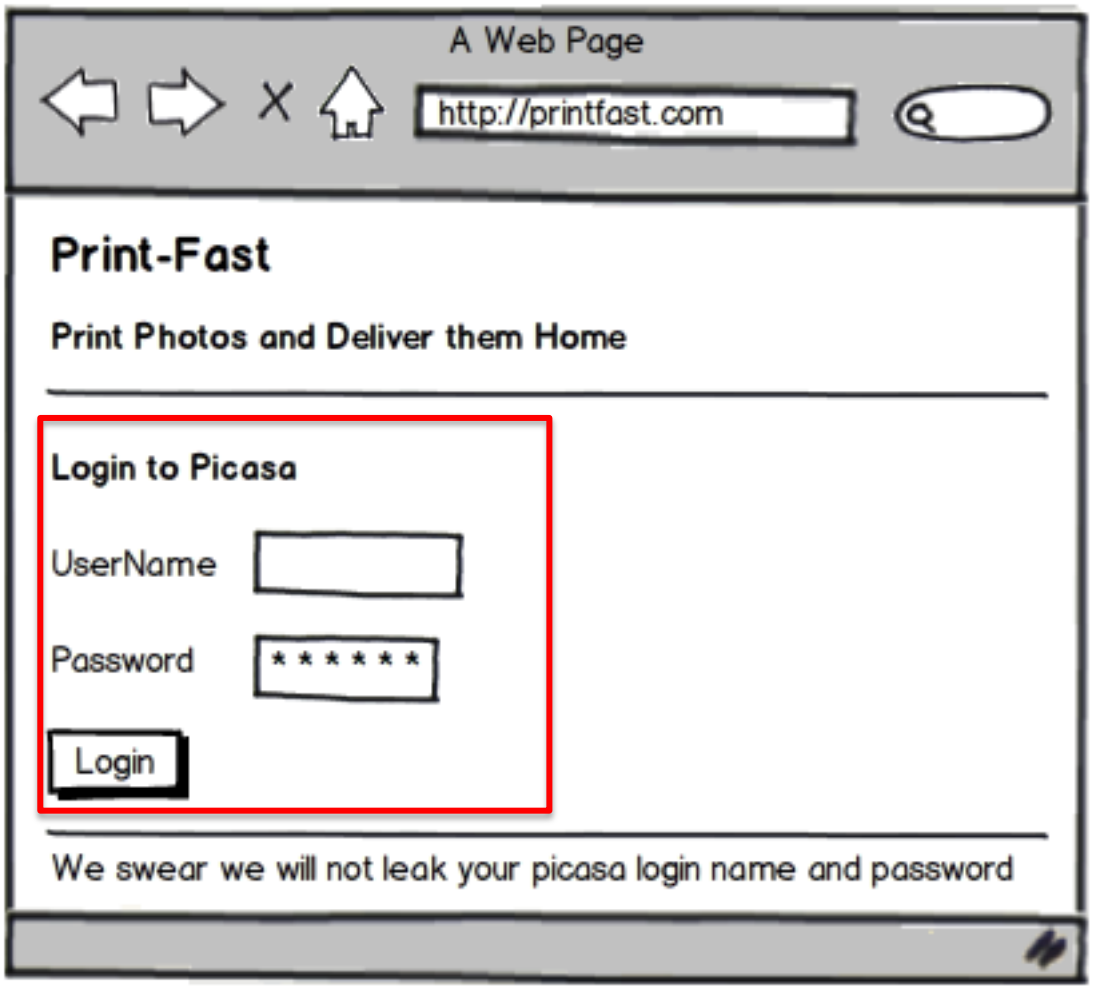
All product names and people names used in the following slides are not entirely accurate. They are only placeholders to explain the concept. None of that information should assumed to be correct or incorrect.

Without OAuth

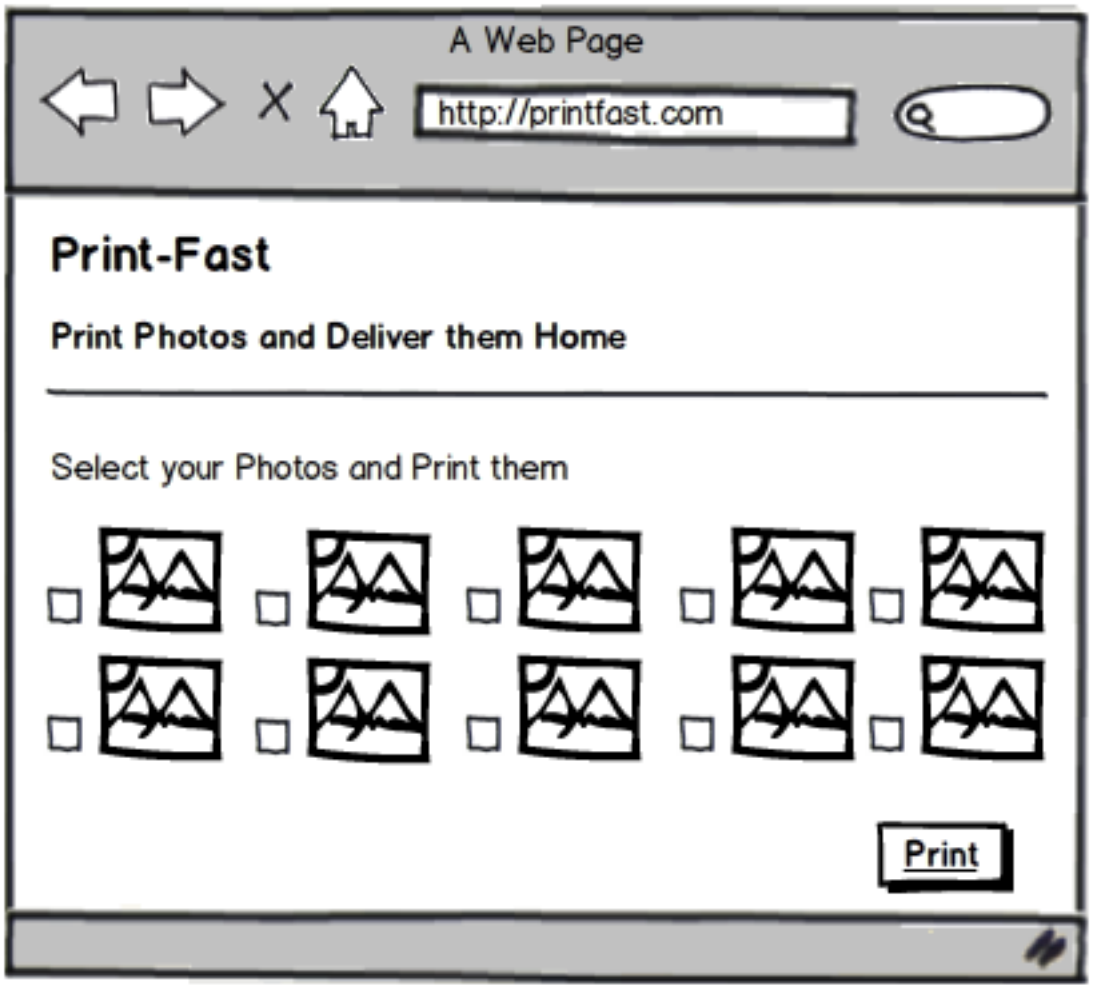


Without OAuth

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

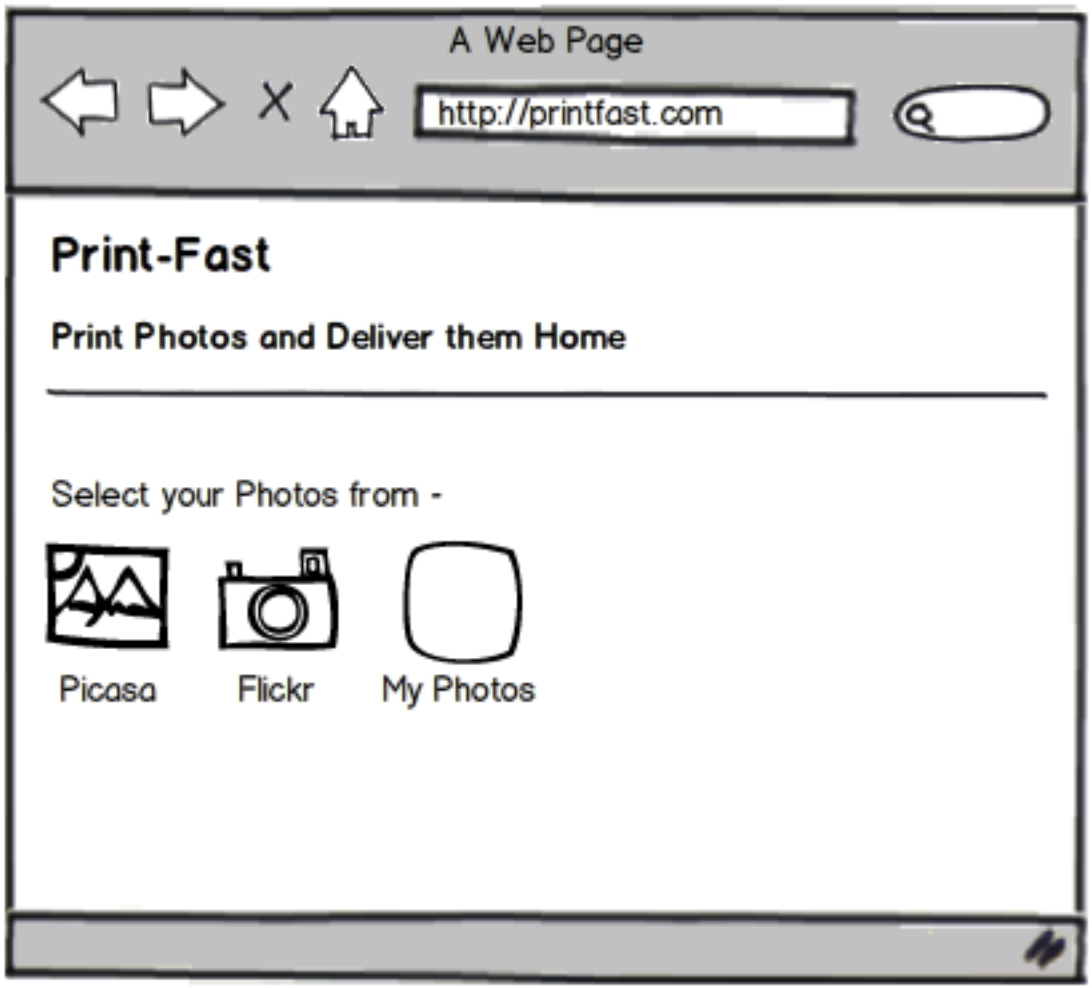


Without OAuth

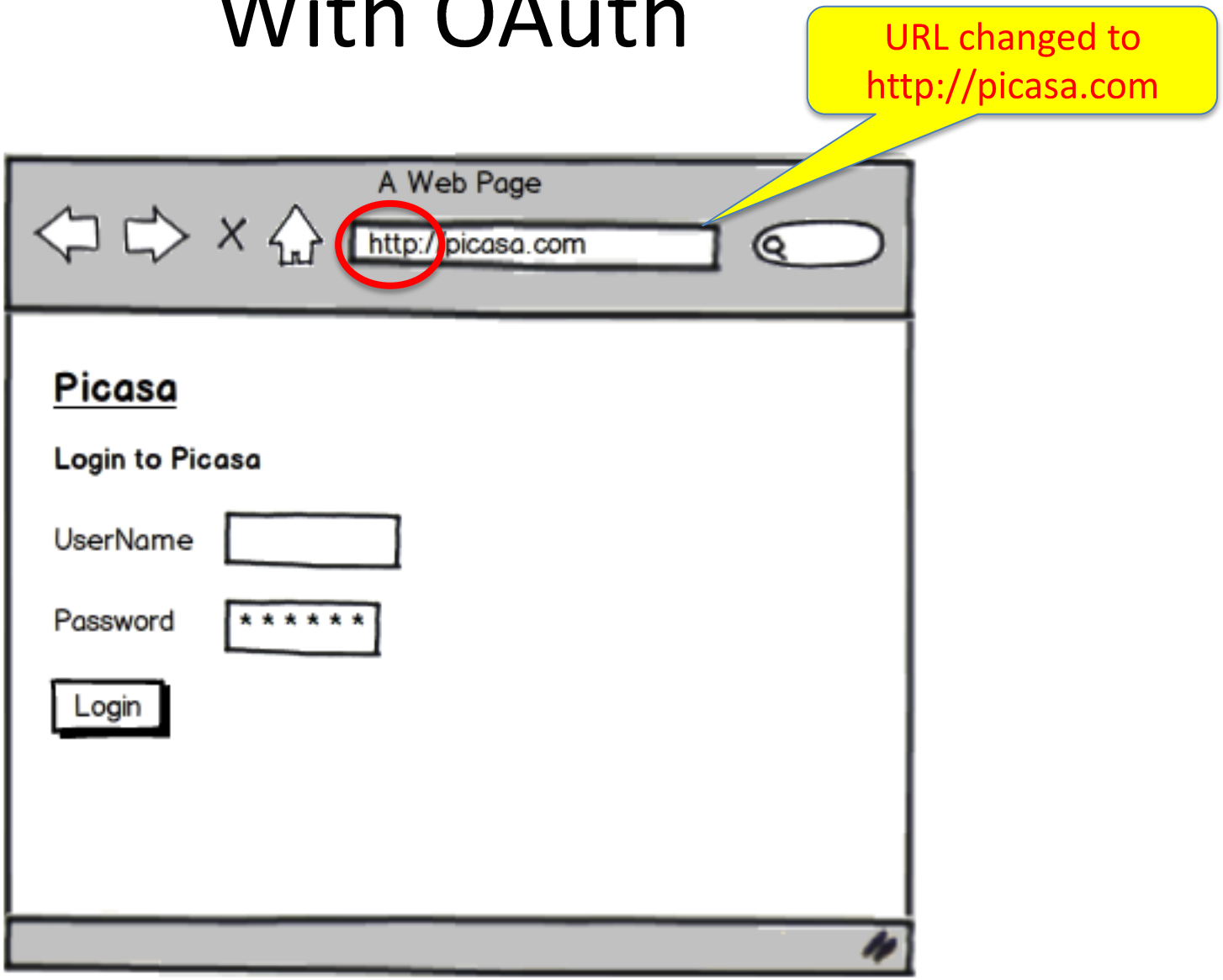


Lets Start Again

With OAuth

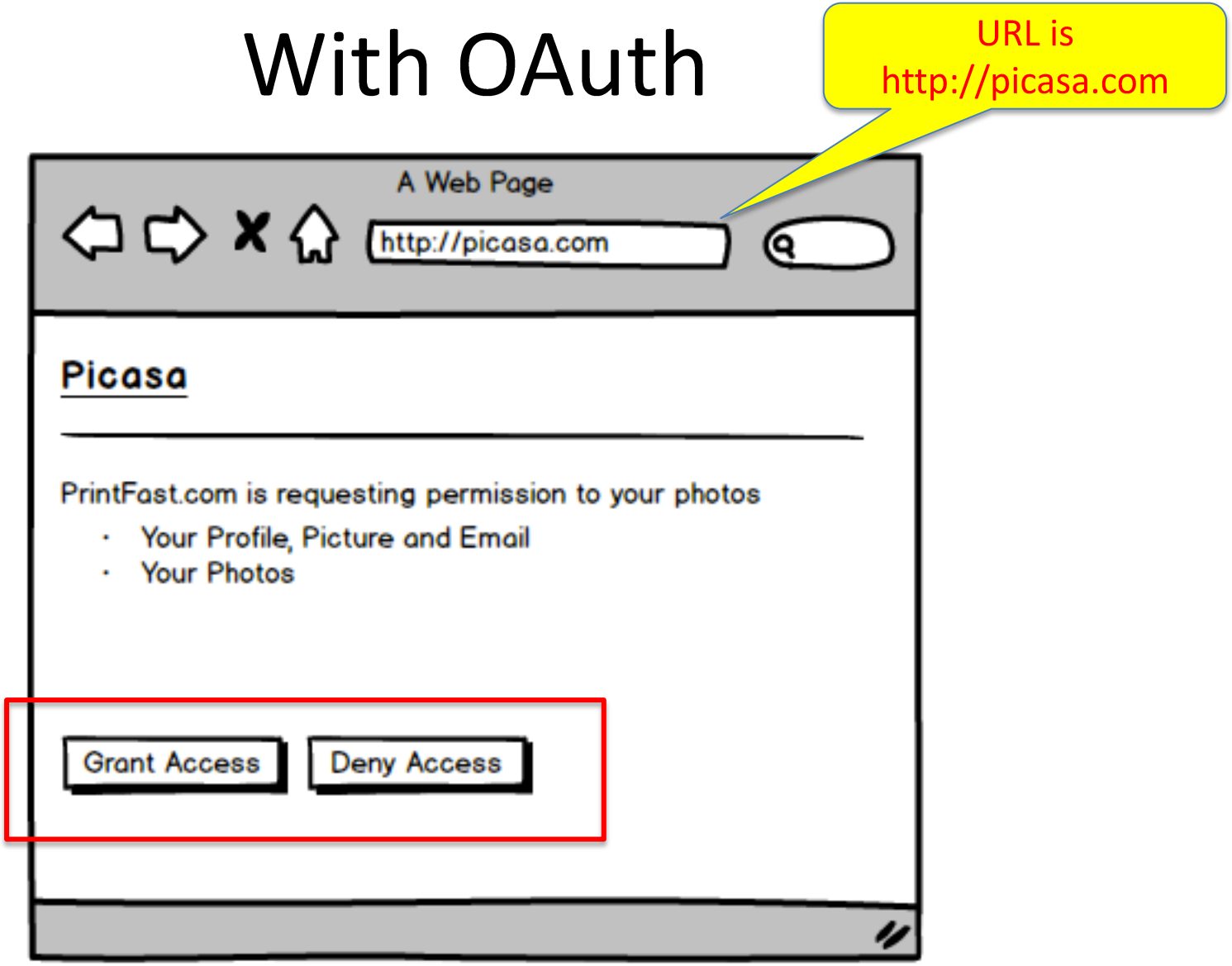

A Web Page
http://printfast.com
Print-Fast
Print Photos and Deliver them Home
Select your Photos from -
Picasa
Flickr
My Photos

With OAuth

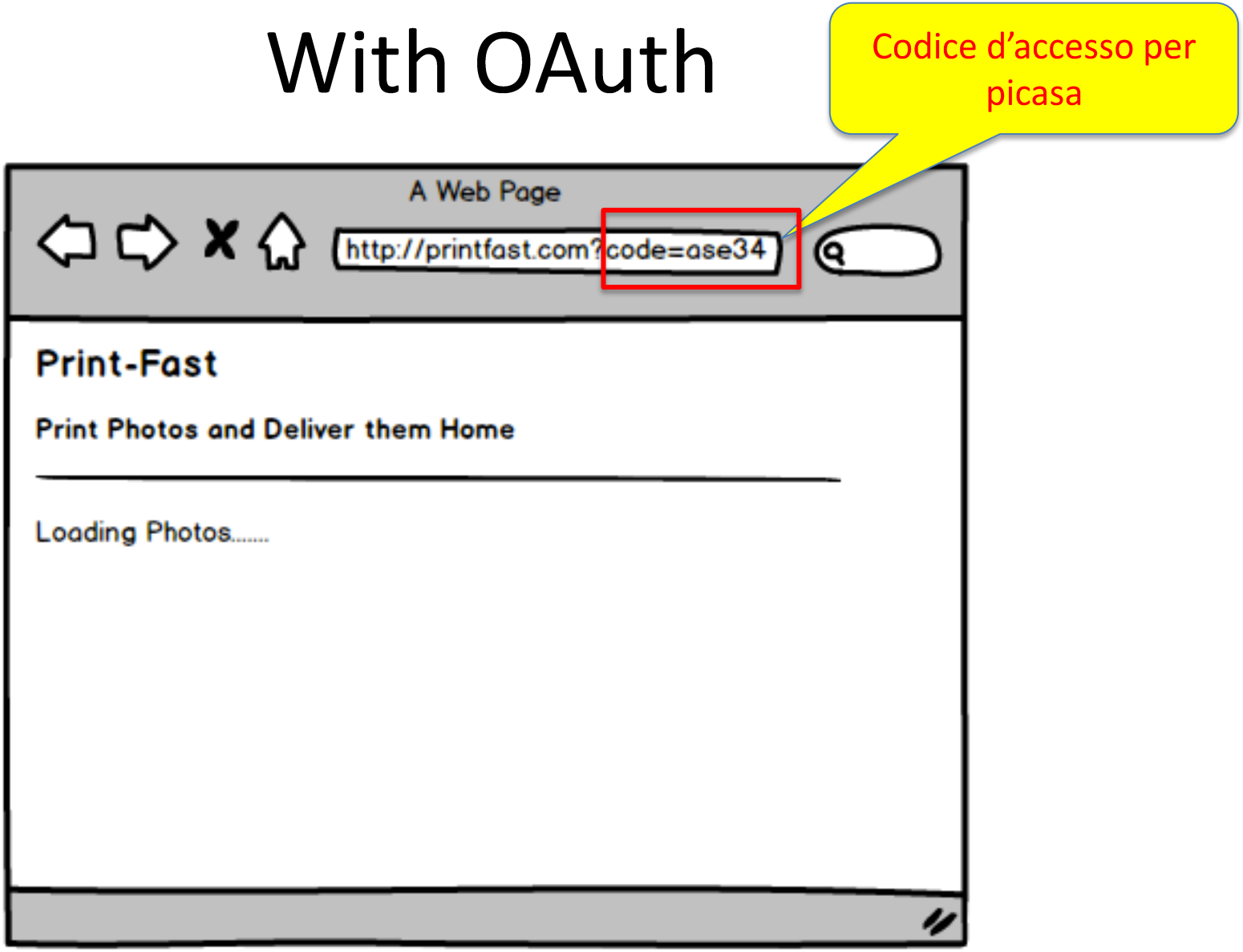


Username e password sono forniti solo al sito che li detiene

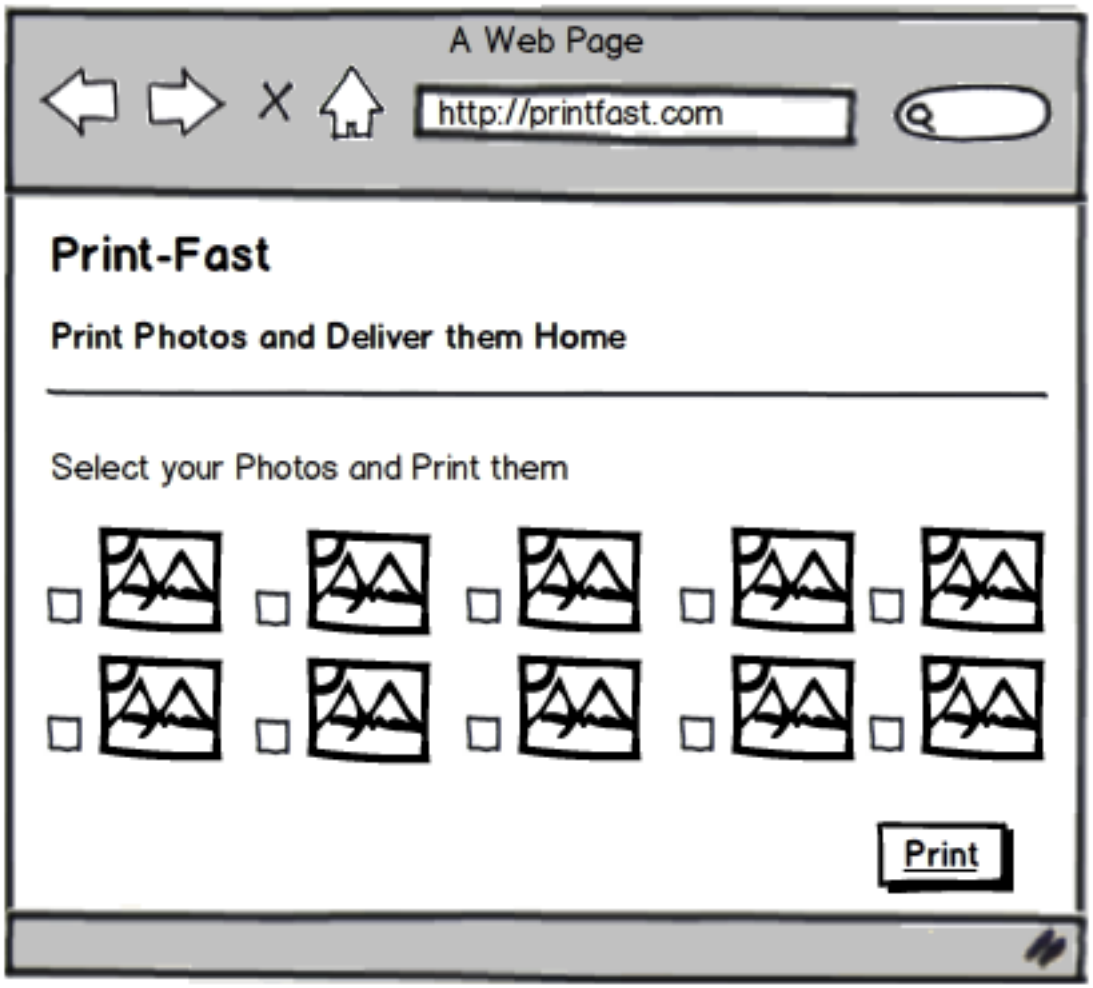
With OAuth


URL is
http://picasa.com
A Web Page
http://picasa.com
Picasa
PrintFast.com is requesting permission to your photos
Your Profile, Picture and Email
Your Photos
Grant Access
Deny Access

With OAuth

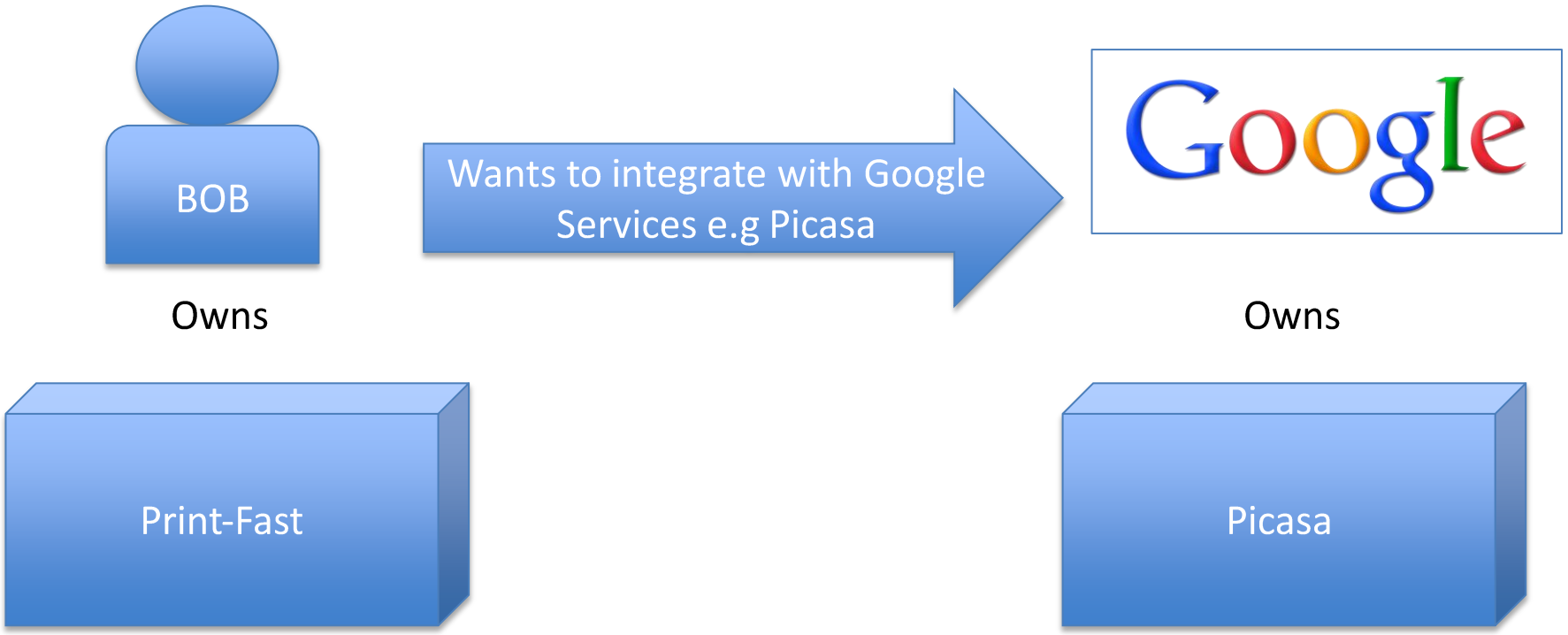

Codice d'accesso per picasa
A Web Page
http://printfast.com?code=ase34
Print-Fast
Print Photos and Deliver them Home
Loading Photos.....

With OAuth

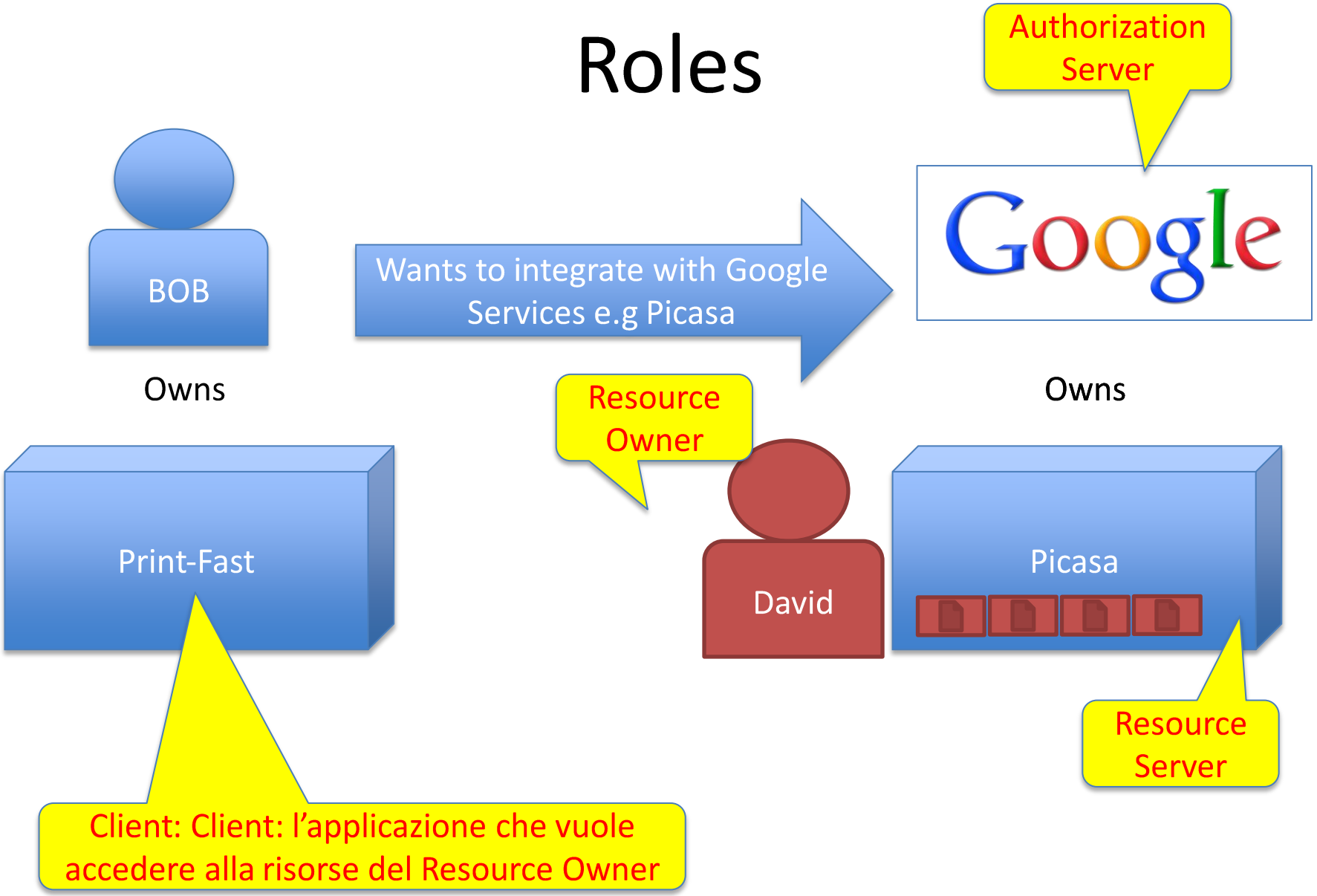

A Web Page
http://printfast.com
Print-Fast
Print Photos and Deliver them Home
Select your Photos and Print them
Print

OAuth 2.0 Flow in Depth

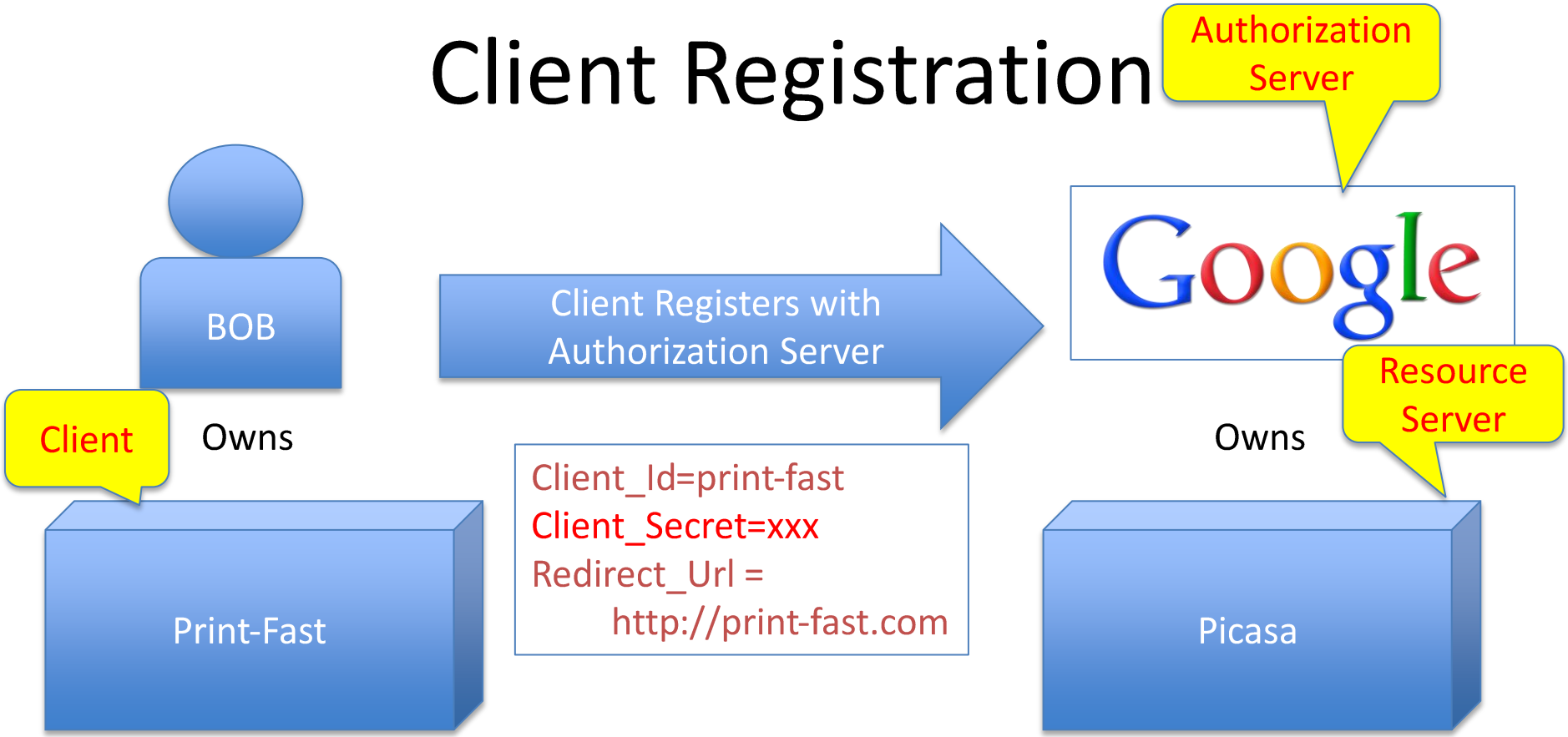
Scenario


BOB
Wants to integrate with Google Services e.g Picasa
Google
Owns
Owns
Print-Fast
Picasa

Roles


Authorization Server
BOB
Wants to integrate with Google Services e.g Picasa
Google
Owns
Resource Owner
Owns
Print-Fast
David
Picasa
Resource Server
Client: Client: l'applicazione che vuole accedere alla risorse del Resource Owner

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

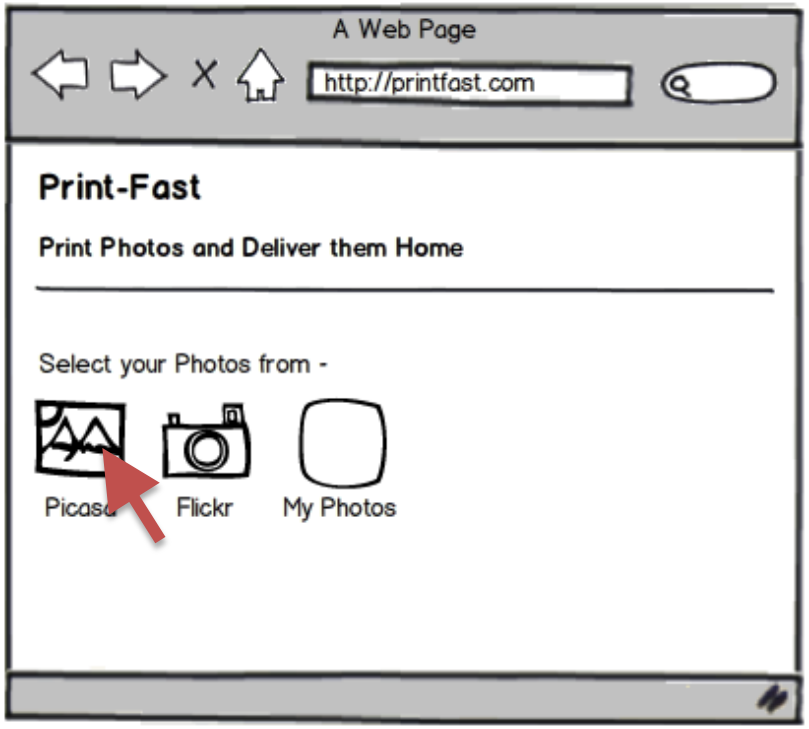
OAuth Flows/Grant Types

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

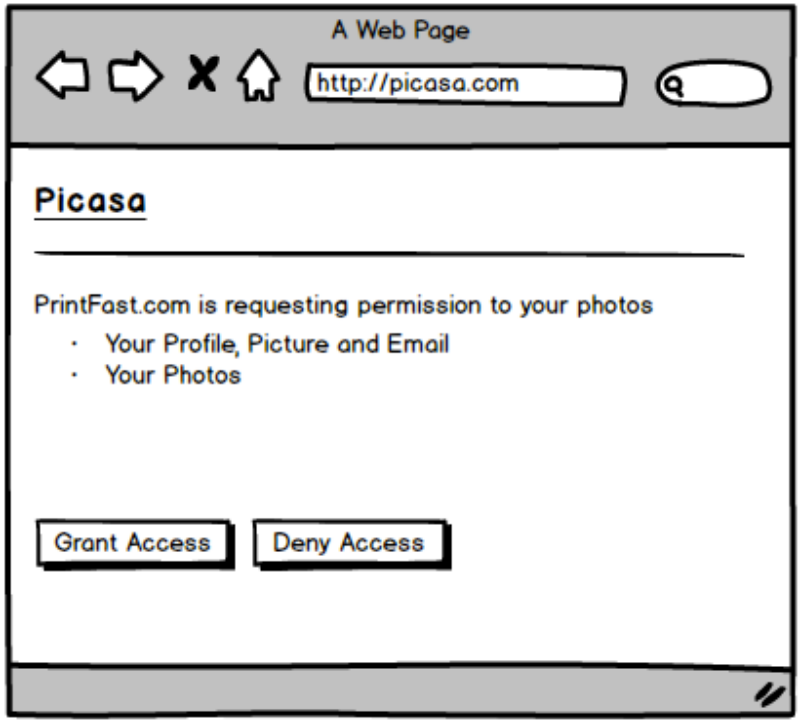
http://stackoverflow.com/questions/31637852/how-to-get-a-jwt/31768524#31768524

Step 1 – Get Authorization Grant

Authorization Request

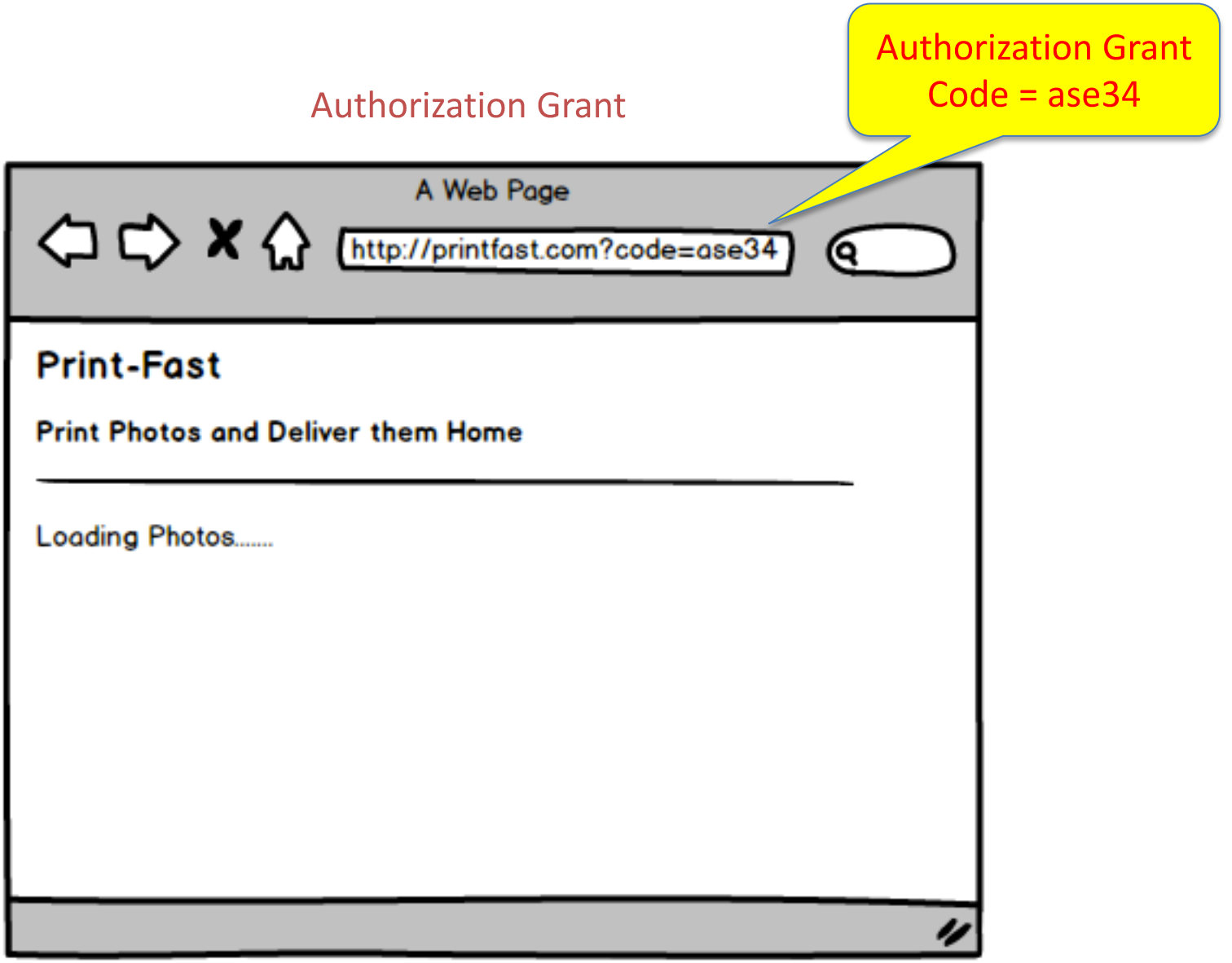


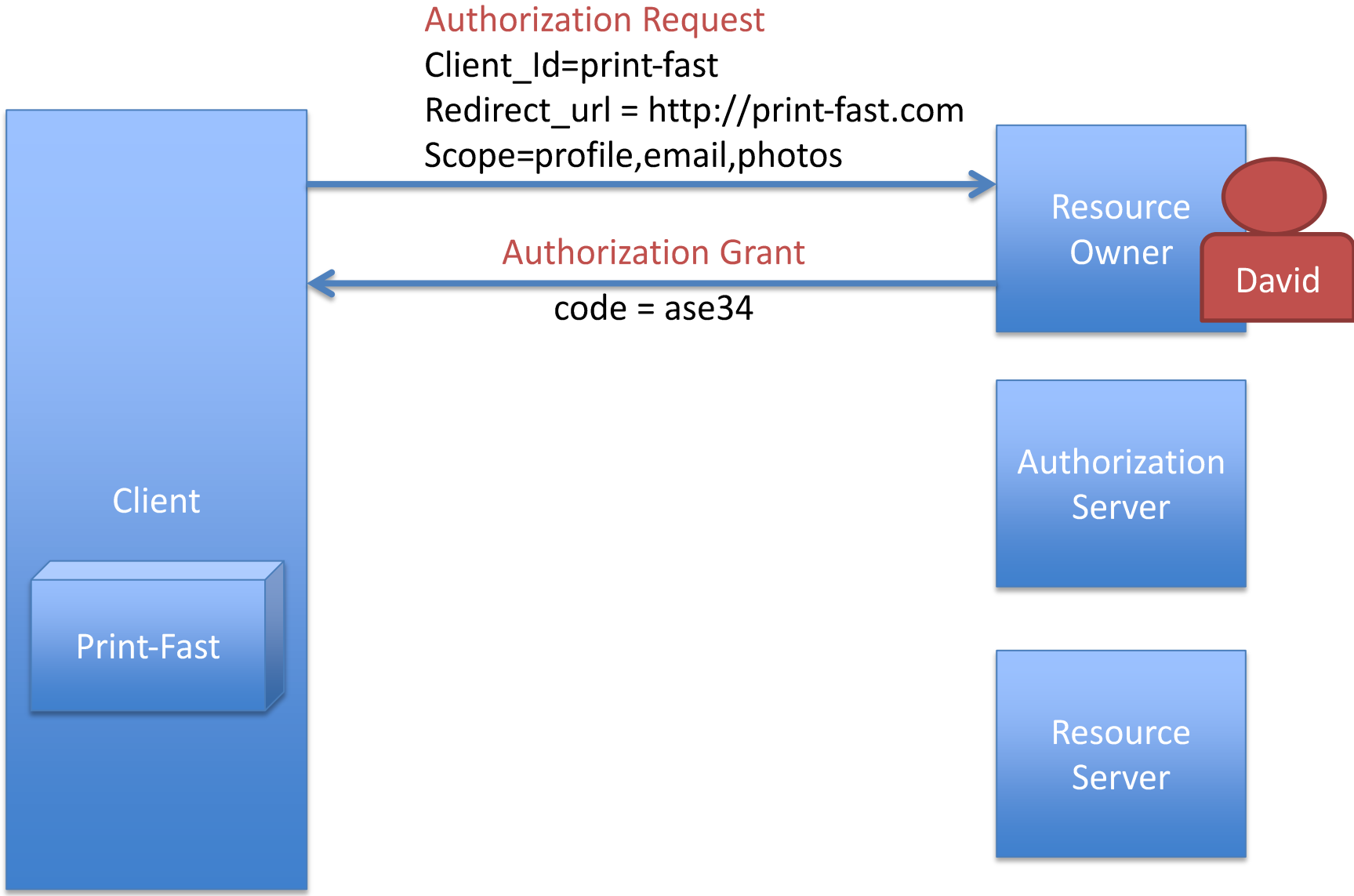
Authorization Grant



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

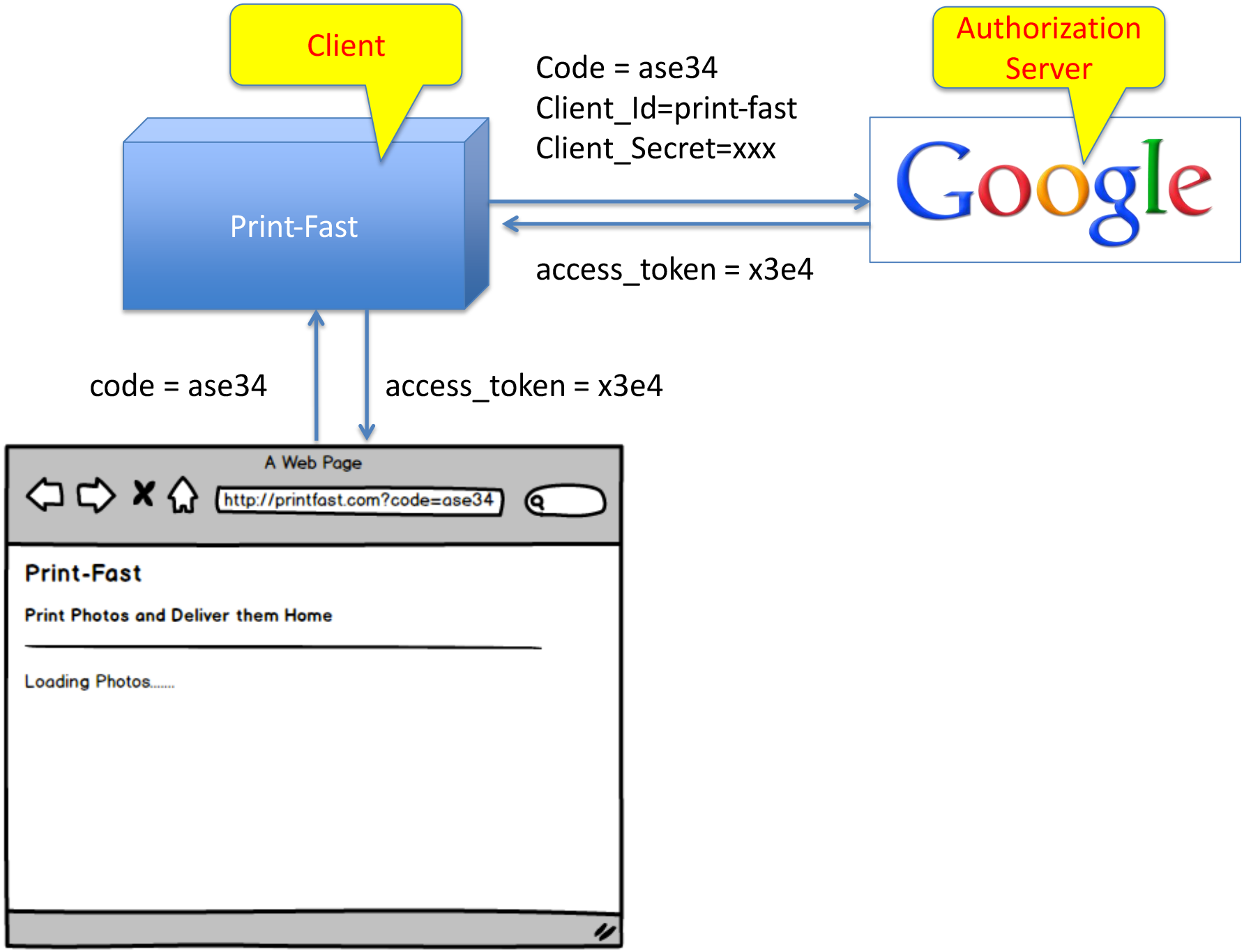
Authorization Grant

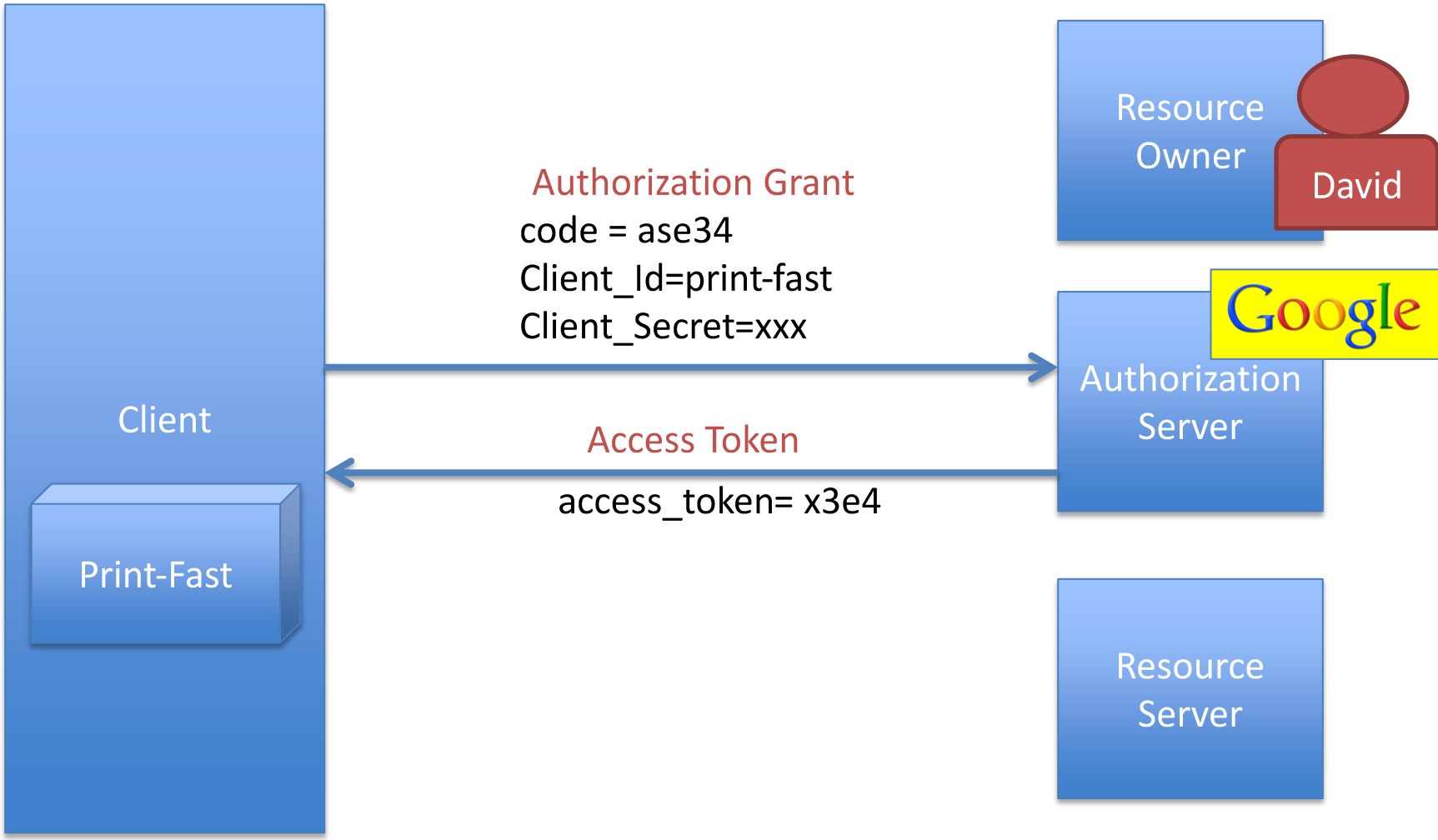




Protocol Flow

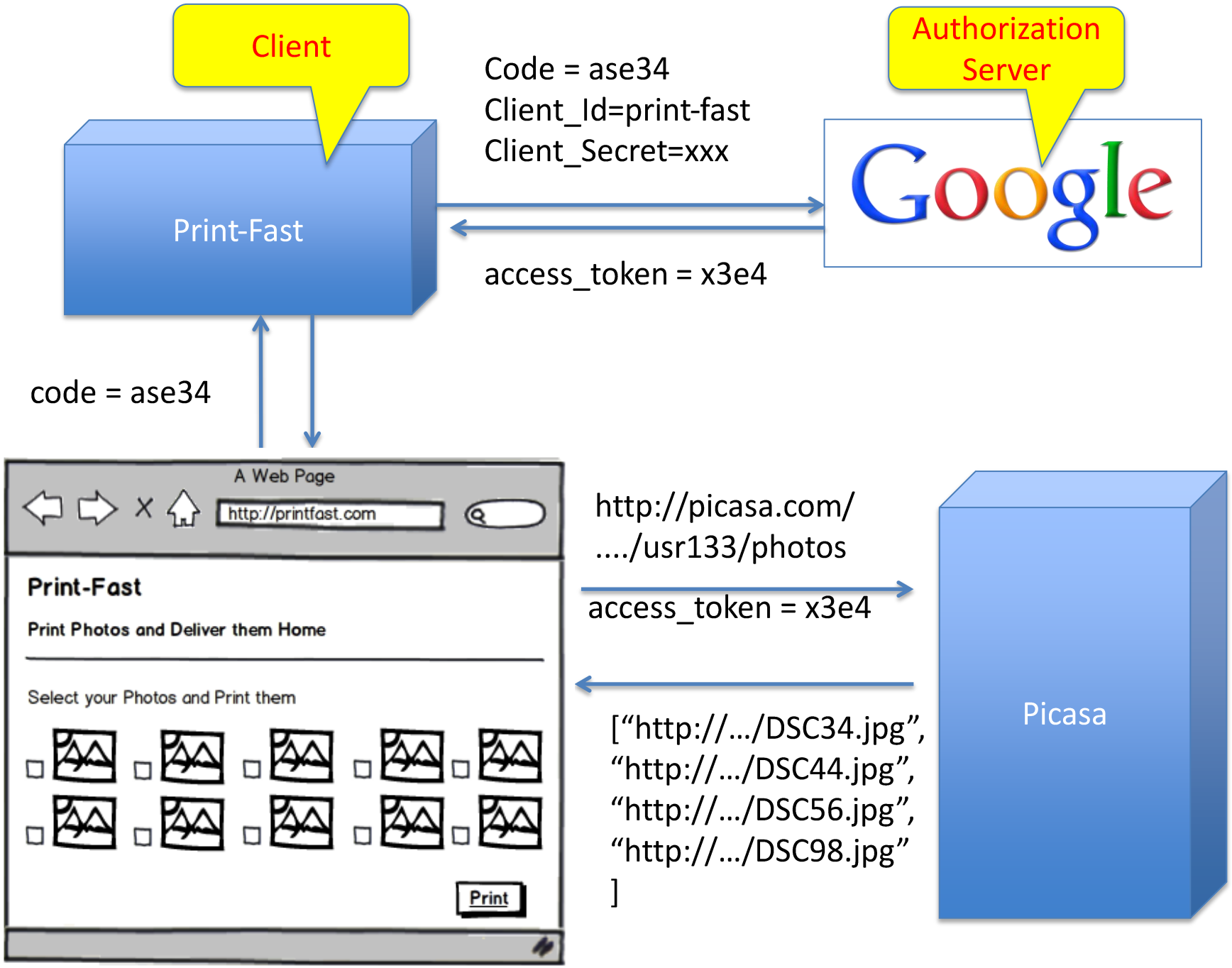
Step 2 – Exchange for Access Token

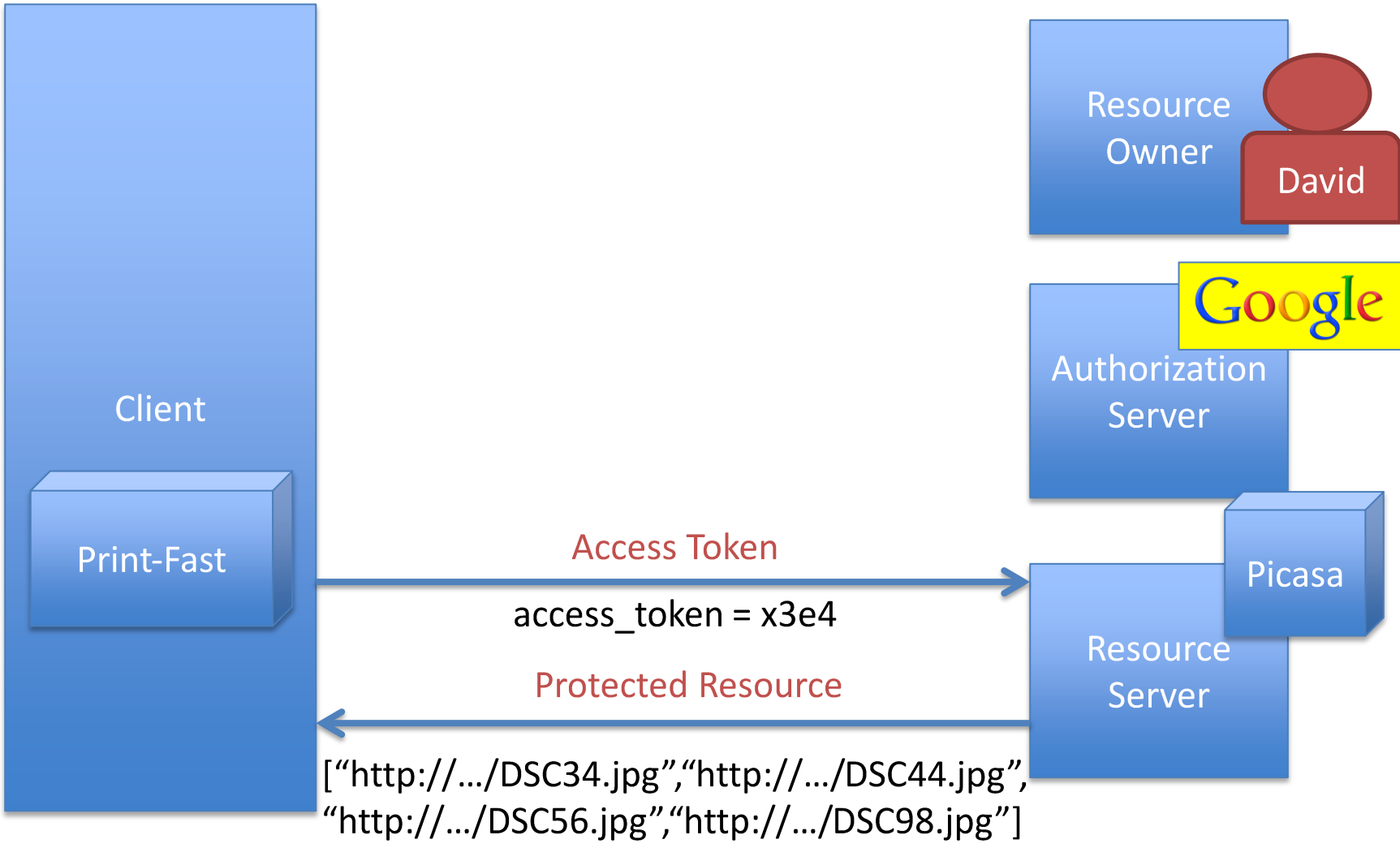

Client
Print-Fast
Code = ase34
Client_Id=print-fast
Client_Secret=xxx
Authorization Server
Google
access_token = x3e4
code = ase34
access_token = x3e4
A Web Page
http://printfast.com?code=ase34
Print-Fast
Print Photos and Deliver them Home
Loading Photos.....



Protocol Flow

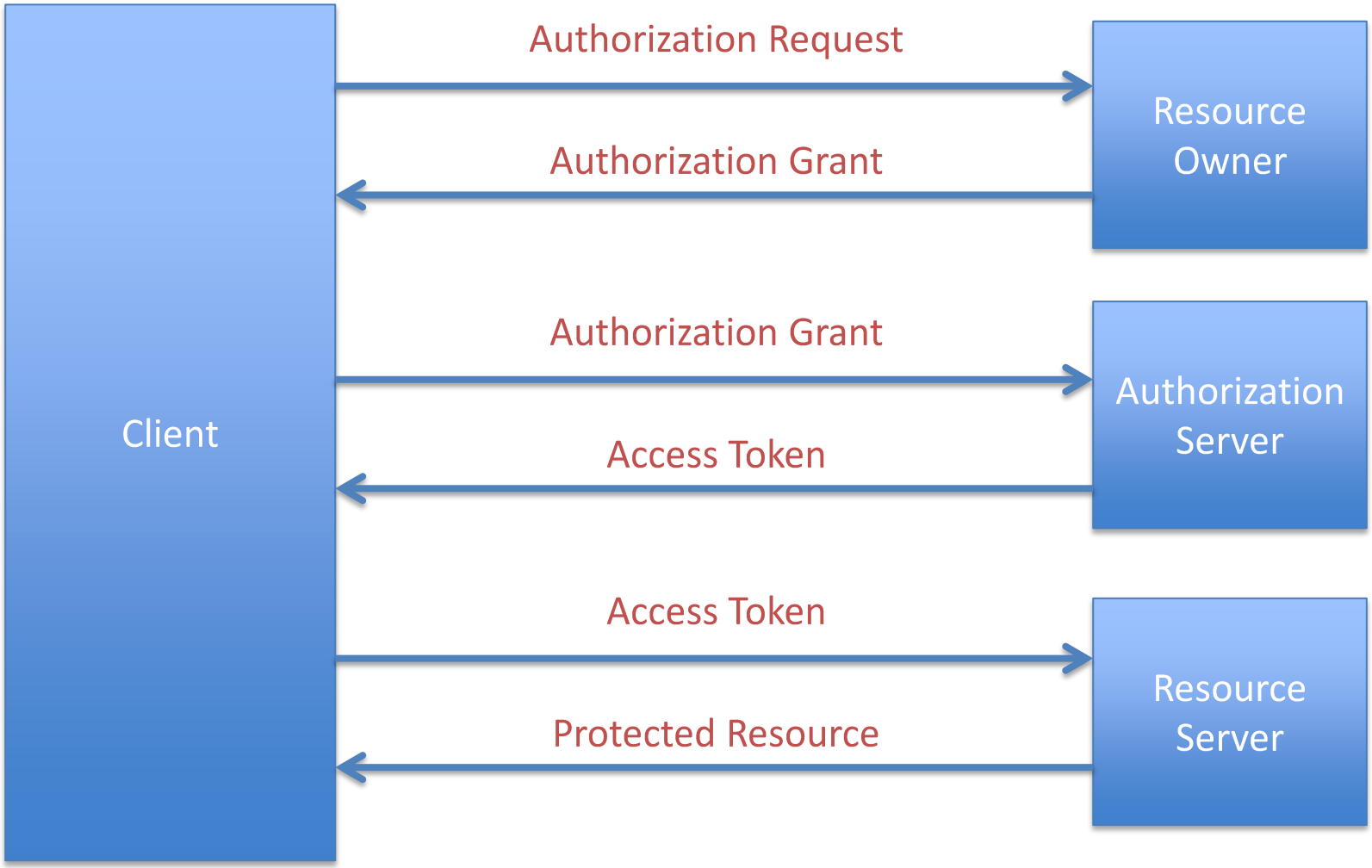
Step 3 – Access Protected Resources


Client
Print-Fast
Code = ase34
Client_Id=print-fast
Client_Secret=xxx
Authorization Server
Google
access_token = x3e4
code = ase34
A Web Page
http://printfast.com
Print-Fast
Print Photos and Deliver them Home
Select your Photos and Print them
Print
http://picasa.com/
..../usr133/photos
access_token = x3e4
["http://.../DSC34.jpg",
"http://.../DSC44.jpg",
"http://.../DSC56.jpg",
"http://.../DSC98.jpg"
]
Picasa

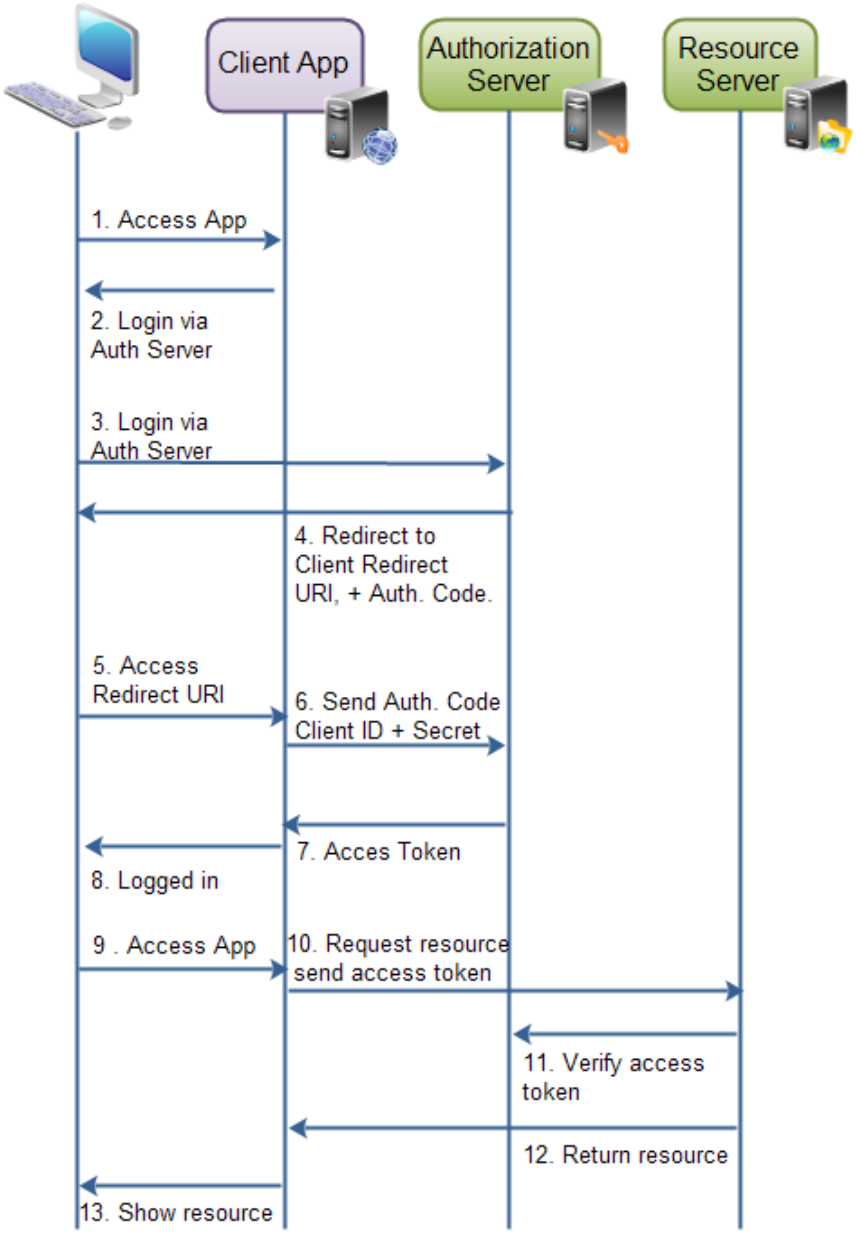


Protocol Flow

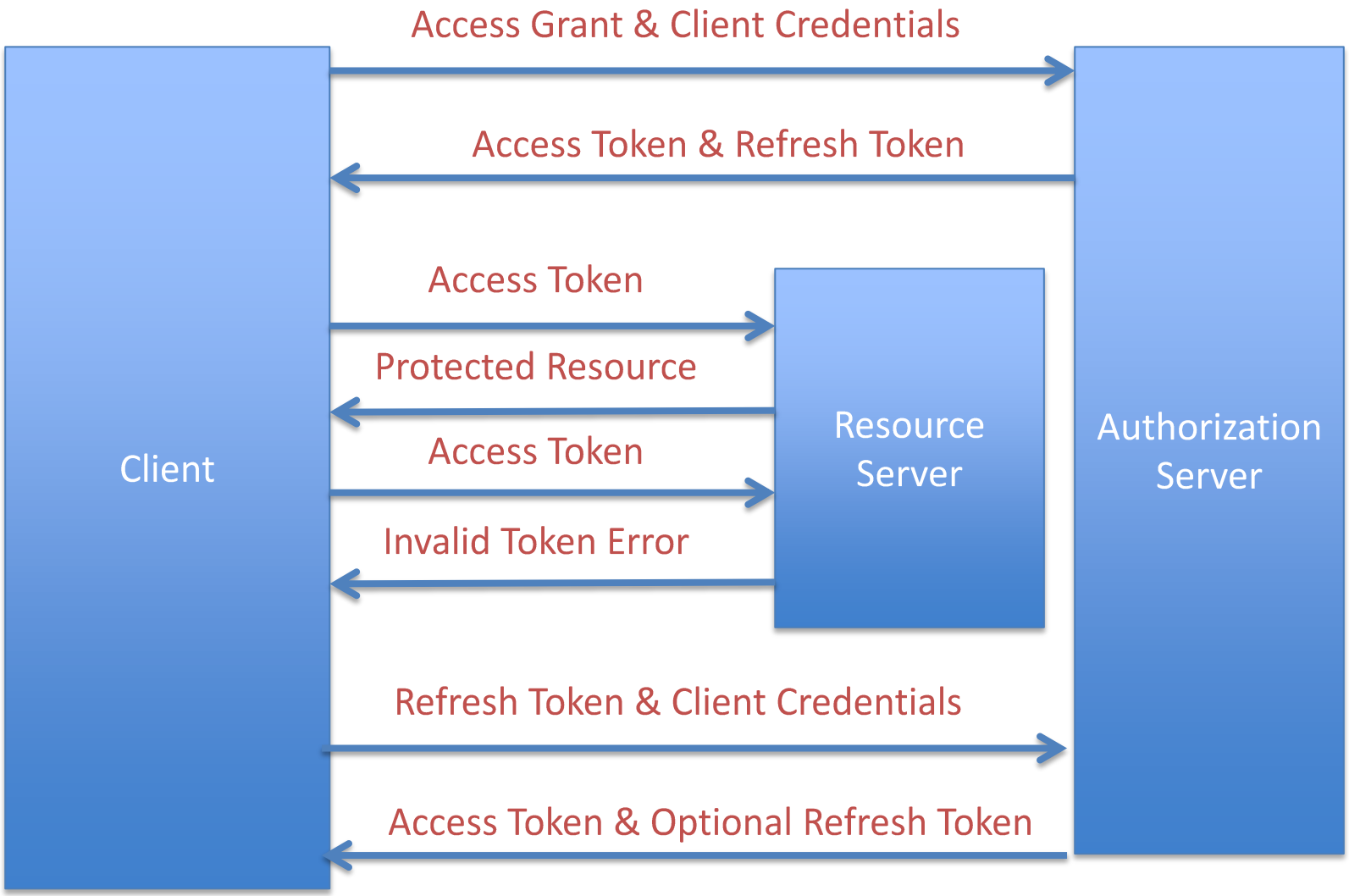
Complete Flow at Once



Protocol Flow


Client App
Authorization Server
Resource Server
1. Access App
2. Login via Auth Server
3. Login via Auth Server
4. Redirect to Client Redirect URI, + Auth. Code.
5. Access Redirect URI
6. Send Auth. Code Client ID + Secret
7. Acces Token
8. Logged in
9 . Access App
10. Request resource send access token
11. Verify access token
12. Return resource
13. Show resource

With Refresh Token



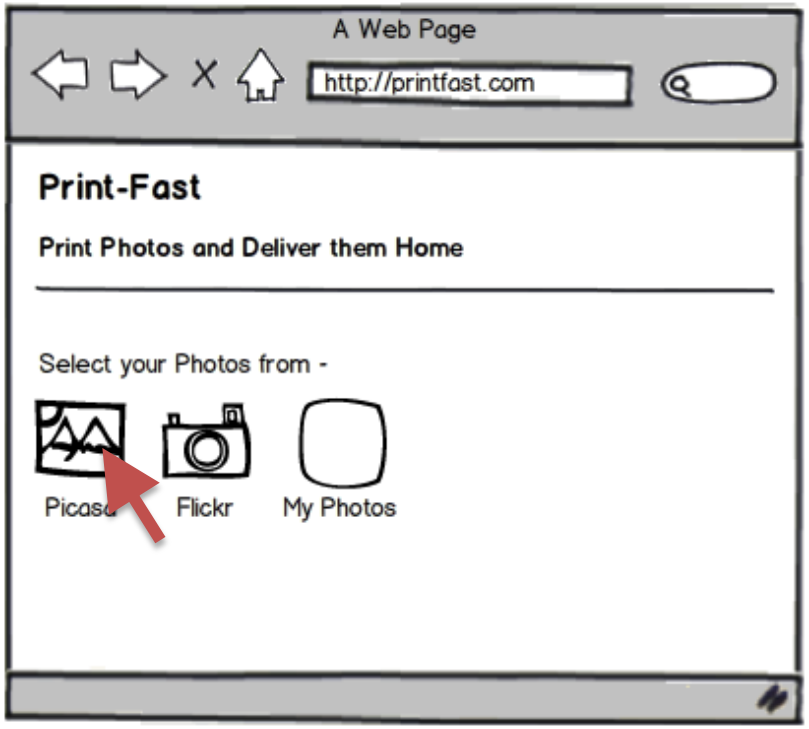
Protocol Flow

OAuth Flows/Grant Types

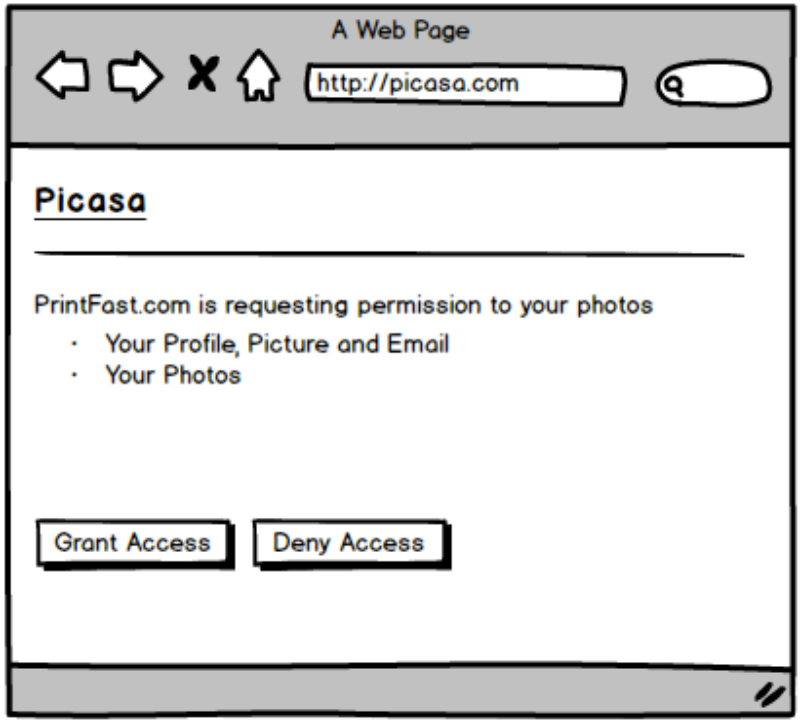
- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant

Step 1 – Get Access Token

Implicit Grant Request

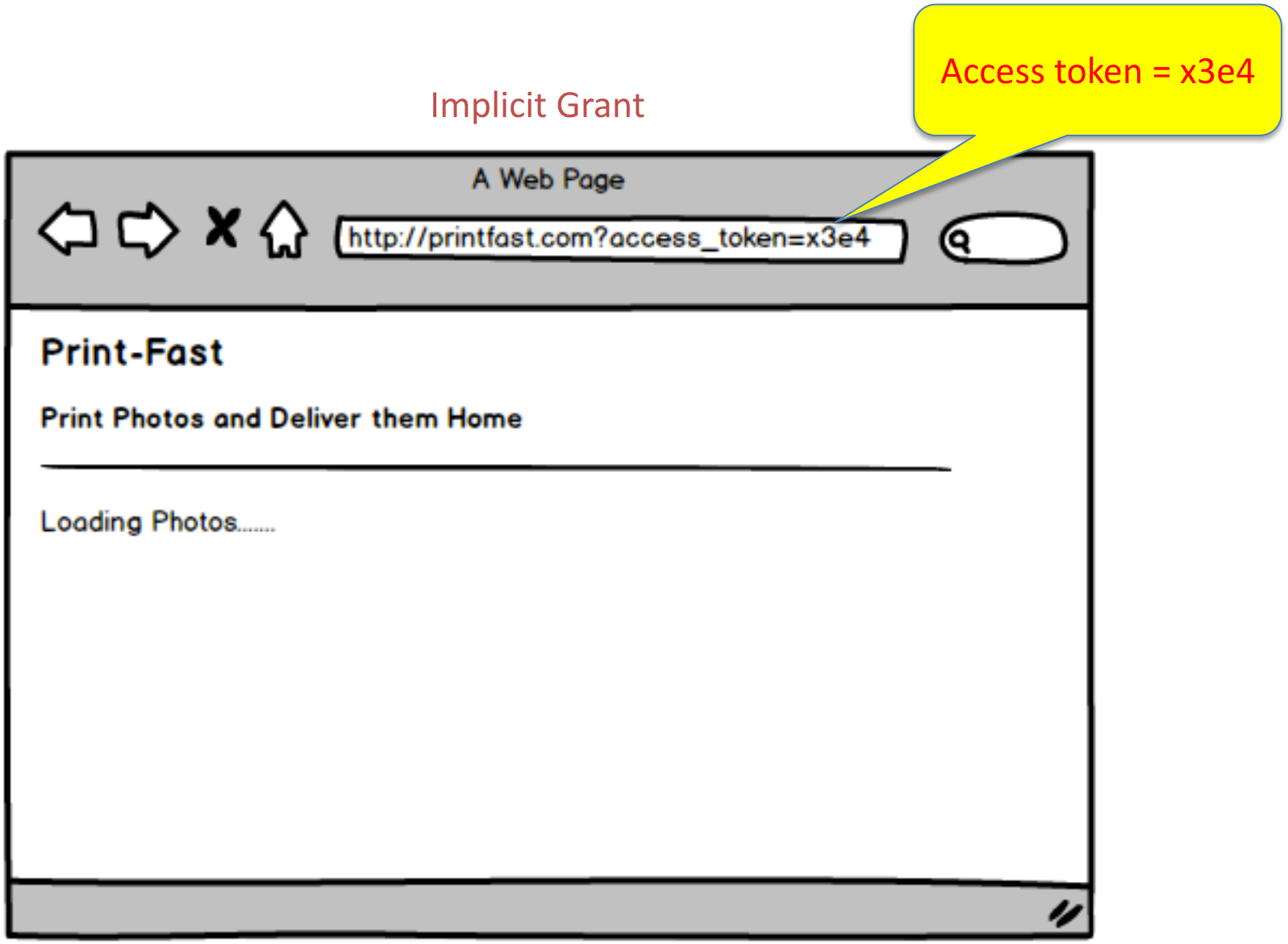


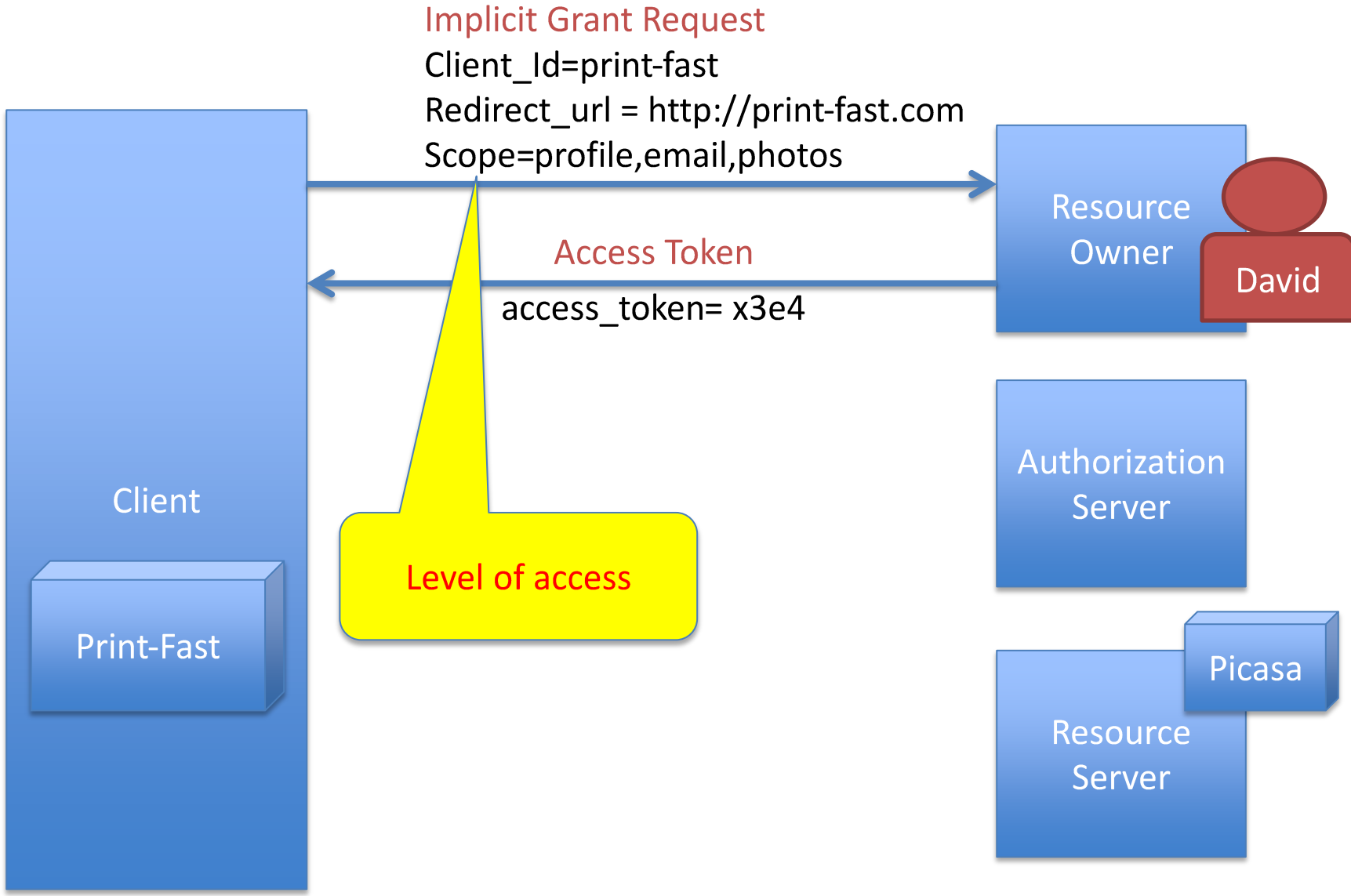
Implicit Grant



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

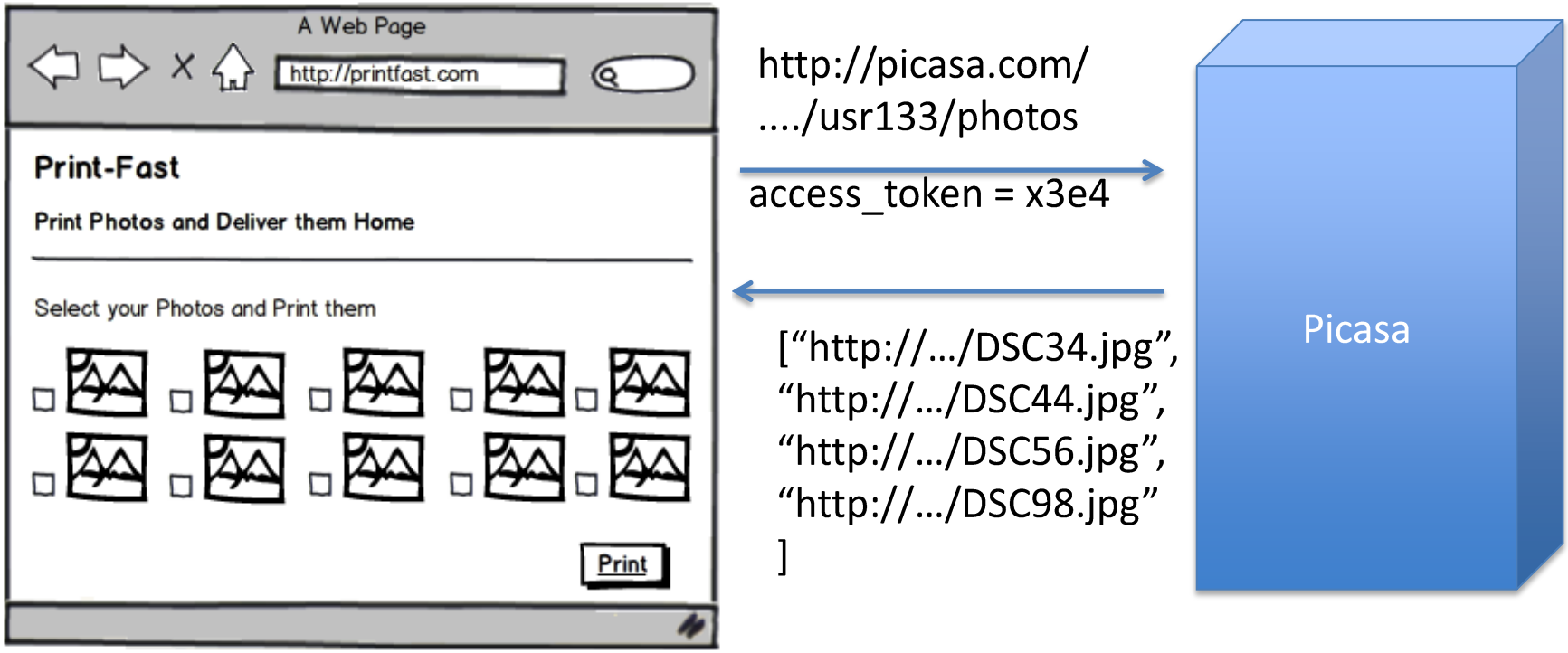
Implicit Grant

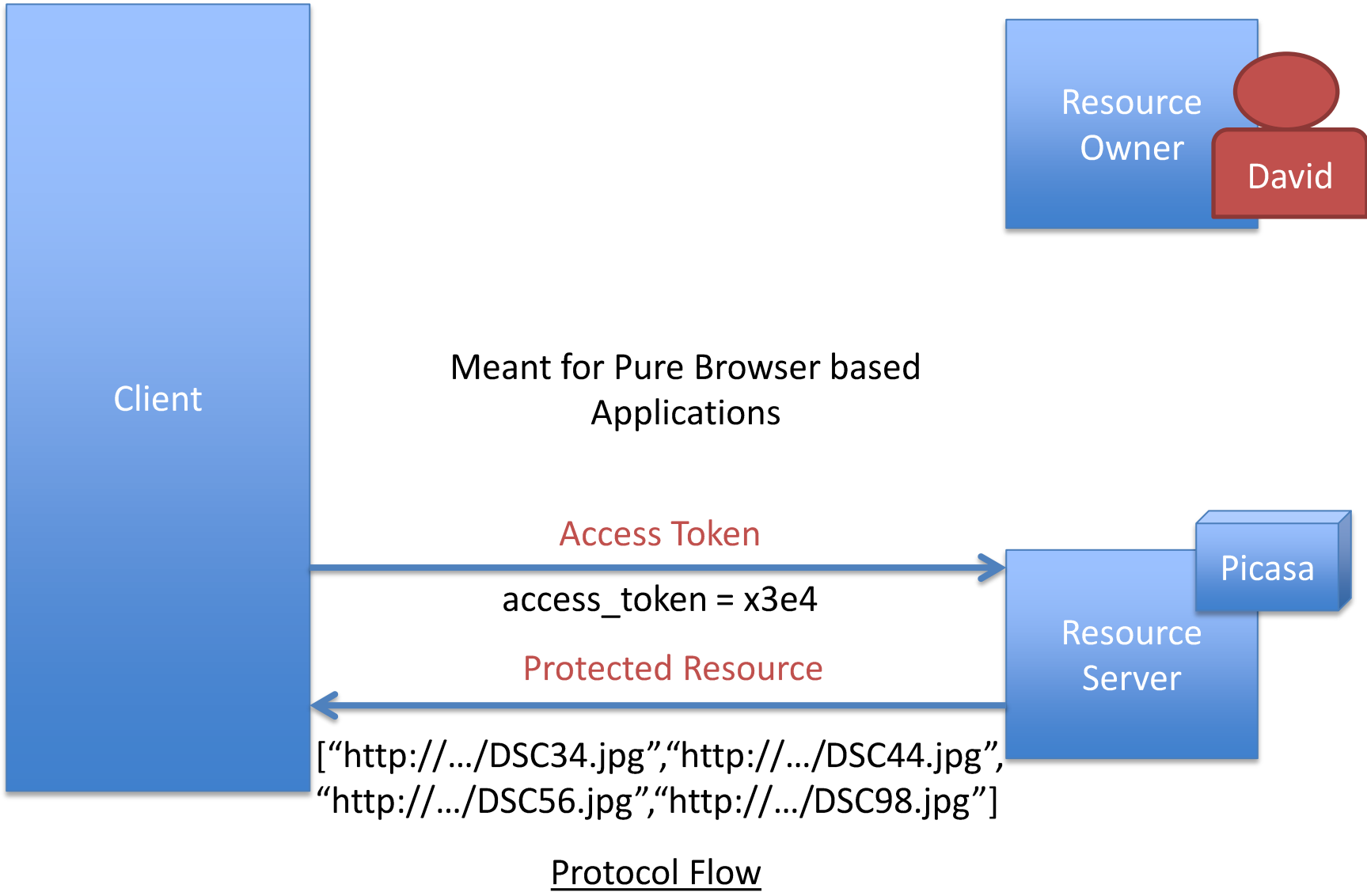




Protocol Flow

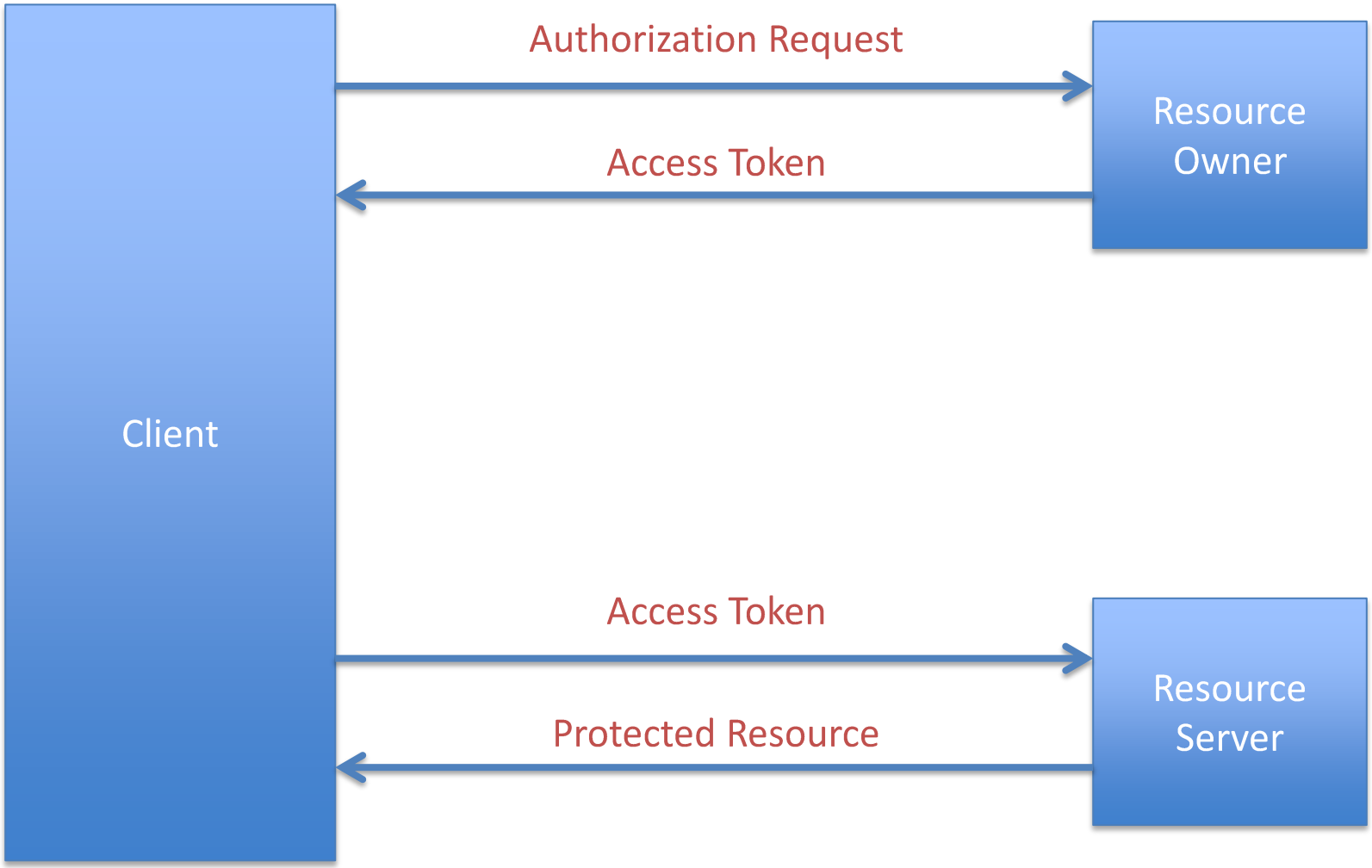
Step 2 – Access Protected Resources


A Web Page
http://printfast.com
Print-Fast
Print Photos and Deliver them Home
Select your Photos and Print them
Print
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

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