



Stephanie Chamblee Østephchamblee







brightlink

Stephanie Chamblee

Software Developer at BrightLink (we're hiring!) Auth0 Ambassador

stephaniechamblee.com

- schamblee@thebrightlink.com
 - Stephchamblee







CONTEXT Open Standards Brief History of Identity

FOUNDATION

Four roles in OAuth

Tokens

1

Authorization Flows

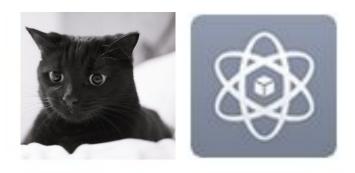
OAUTH & OIDC AUTHORIZATION CODE FLOW OAuth 2.0 & OpenID Connect (OIDC) Walkthrough





OAuth2





MyFirstApps will receive the following info: your public profile and email address.

Edit the info you provide

This does not let the app post to Facebook.



OpenID Connect Sign in with Google



Sign in with Google

Sign in with Google





Thanks

Stephanie Chamblee Østephchamblee



OPEN STANDARDS

Open Standards in Identity

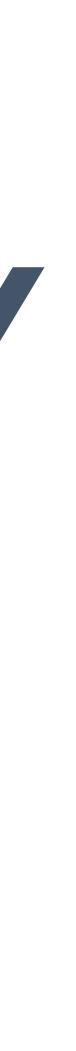


* OAuth2





HISTORY OF IDENTITY

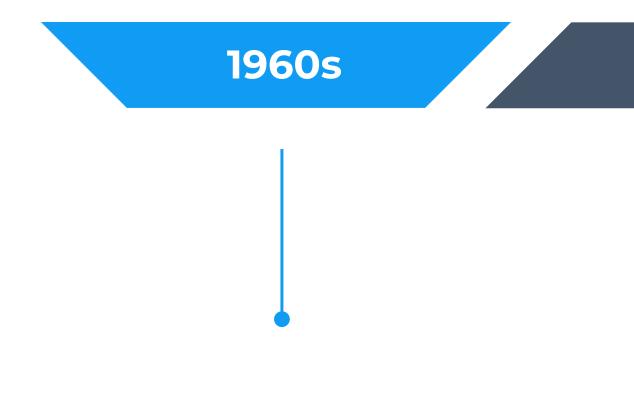












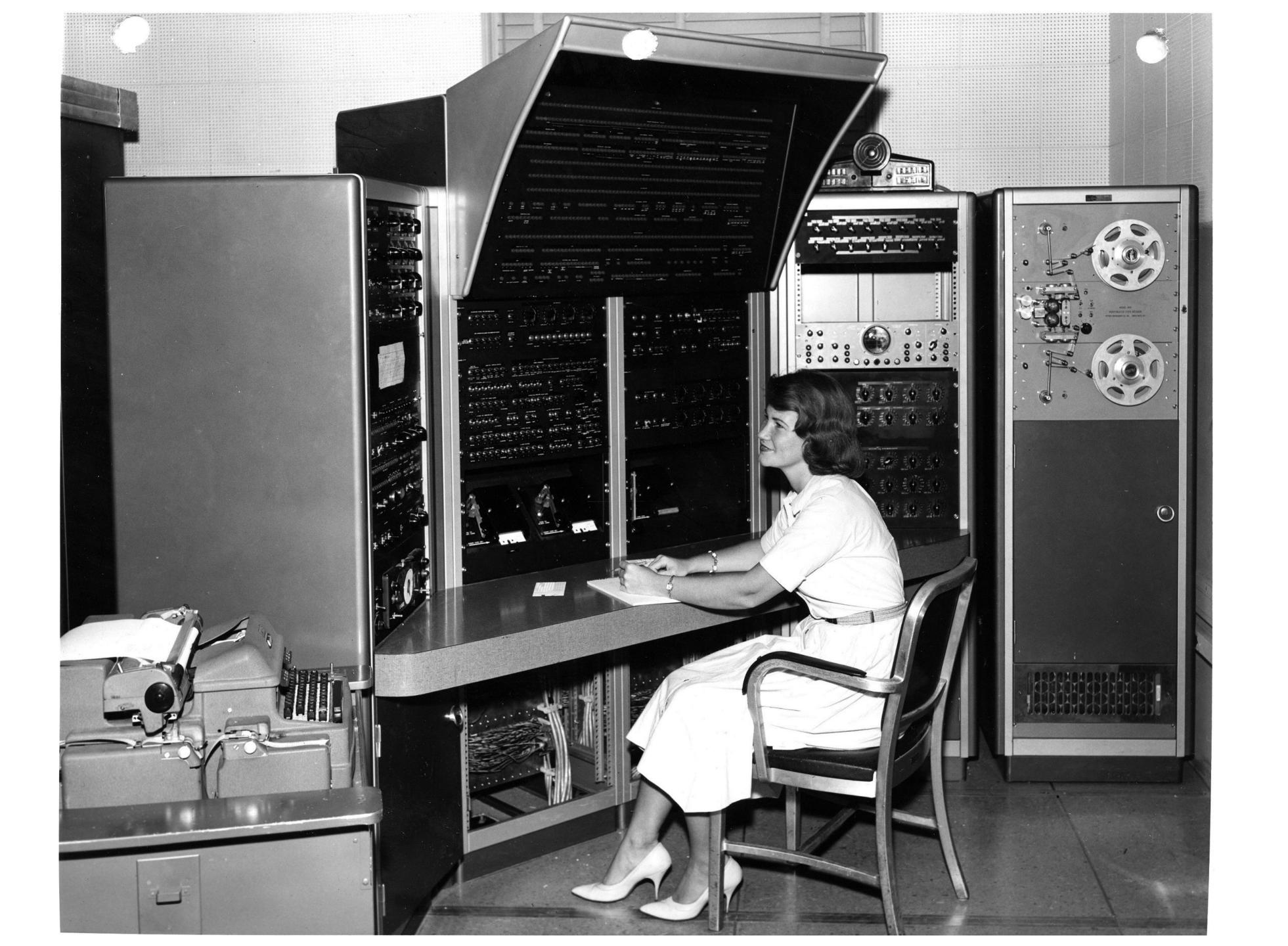
Passwords

HISTORY OF IDENTITY

2002

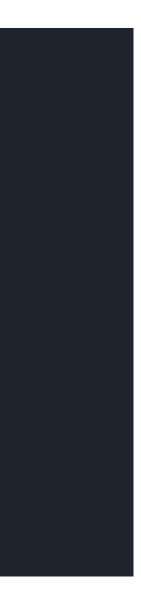
2010

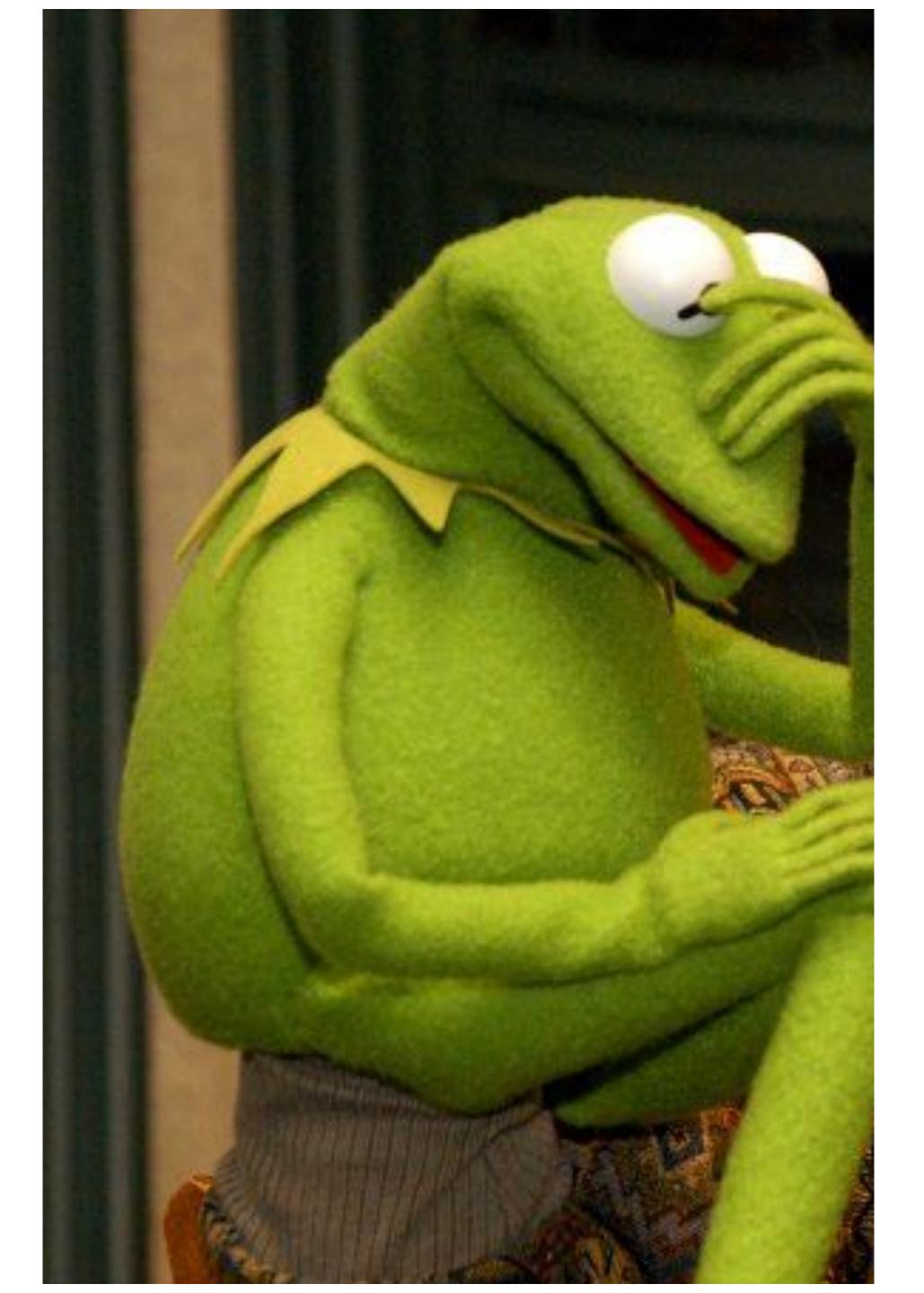
2014



schamblee@sjc-ThinkPad-P52s:~/steph\$ sudo vim cat_jokes.txt [sudo] password for schamblee:











Password



Computer









s here	Google search
DETRIC	
CALL CA	JAZ CAL
login:	to.neopets
ter your username & passwo	ord below.
to Neopets , you will be ab	le to enjoy classic neopets.
sername our password t's cAsE sEnSitIvE!):	
Log Into Neopets!	
ets Account?	
ow to create one! Creating a than a couple of minutes.	an account is easy and
Fign Up!	
	No. 111

Simple Login Security

* Password Strength Requirements

* Password Hashing

***** Two-Factor Authentication

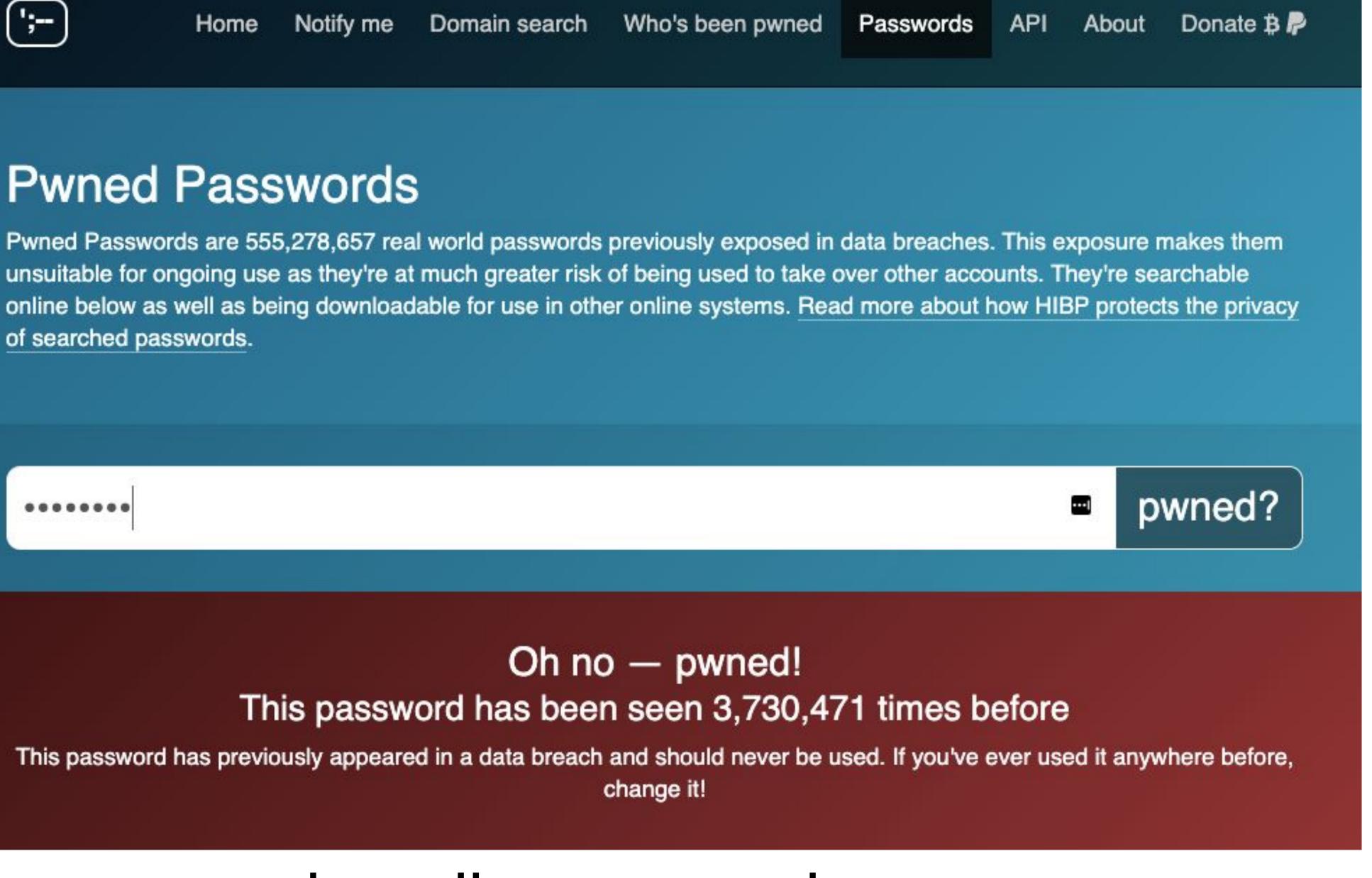


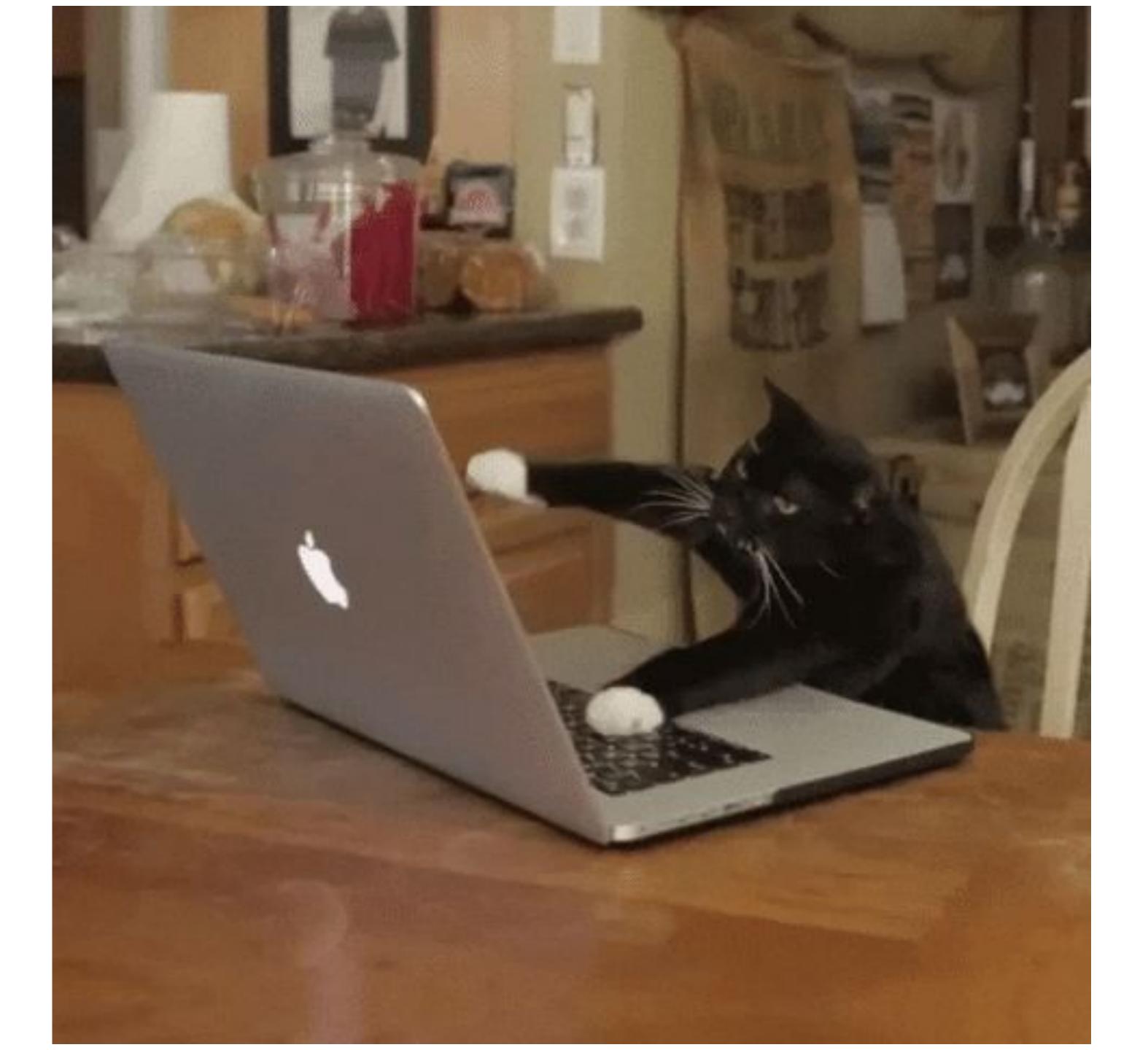
Pwned Passwords

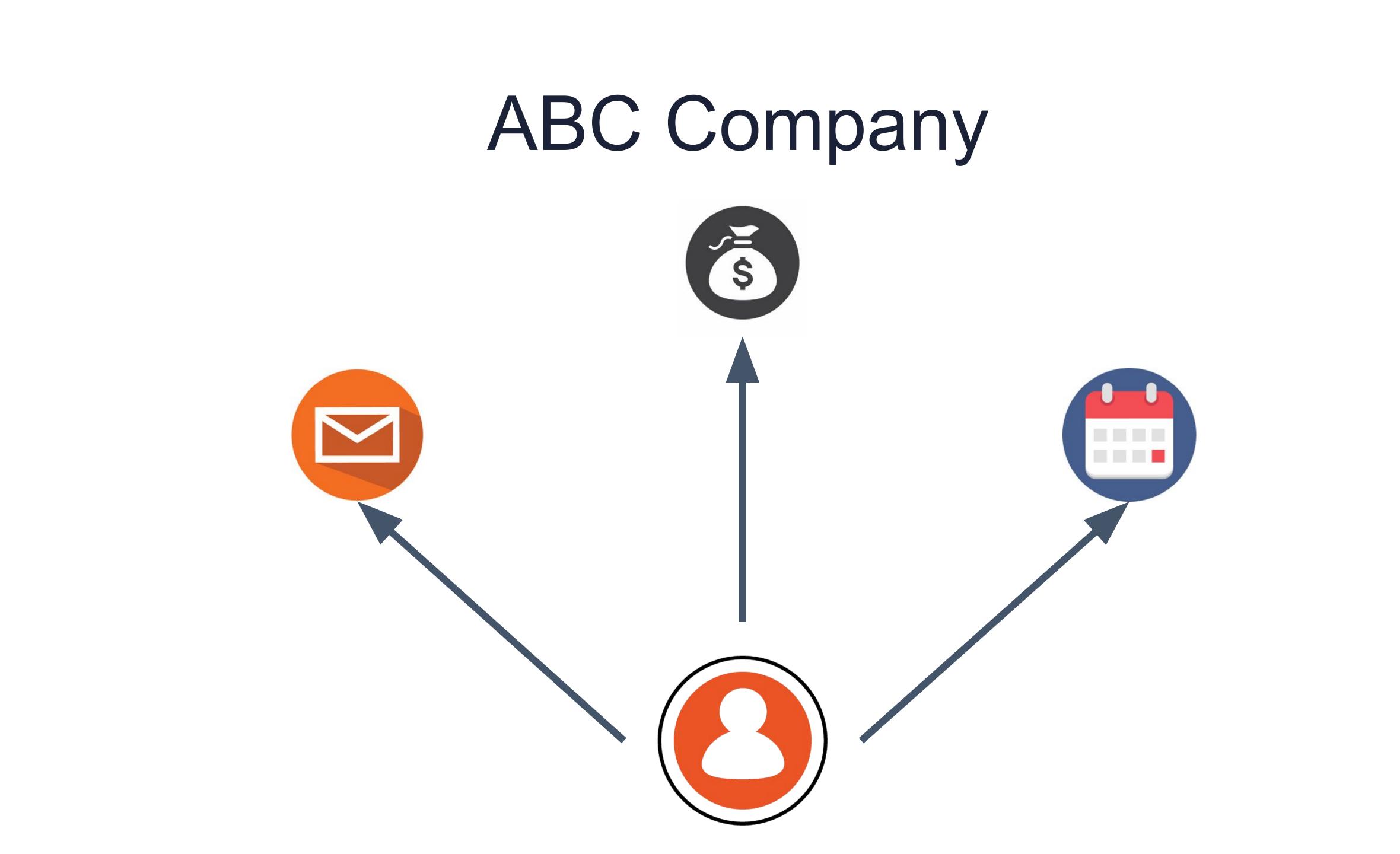
of searched passwords.



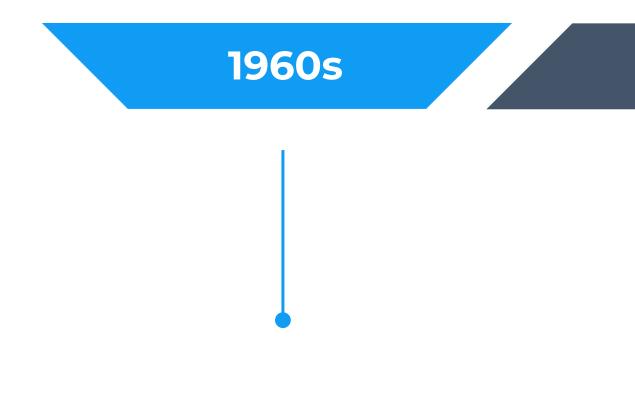
haveibeenpwned.com







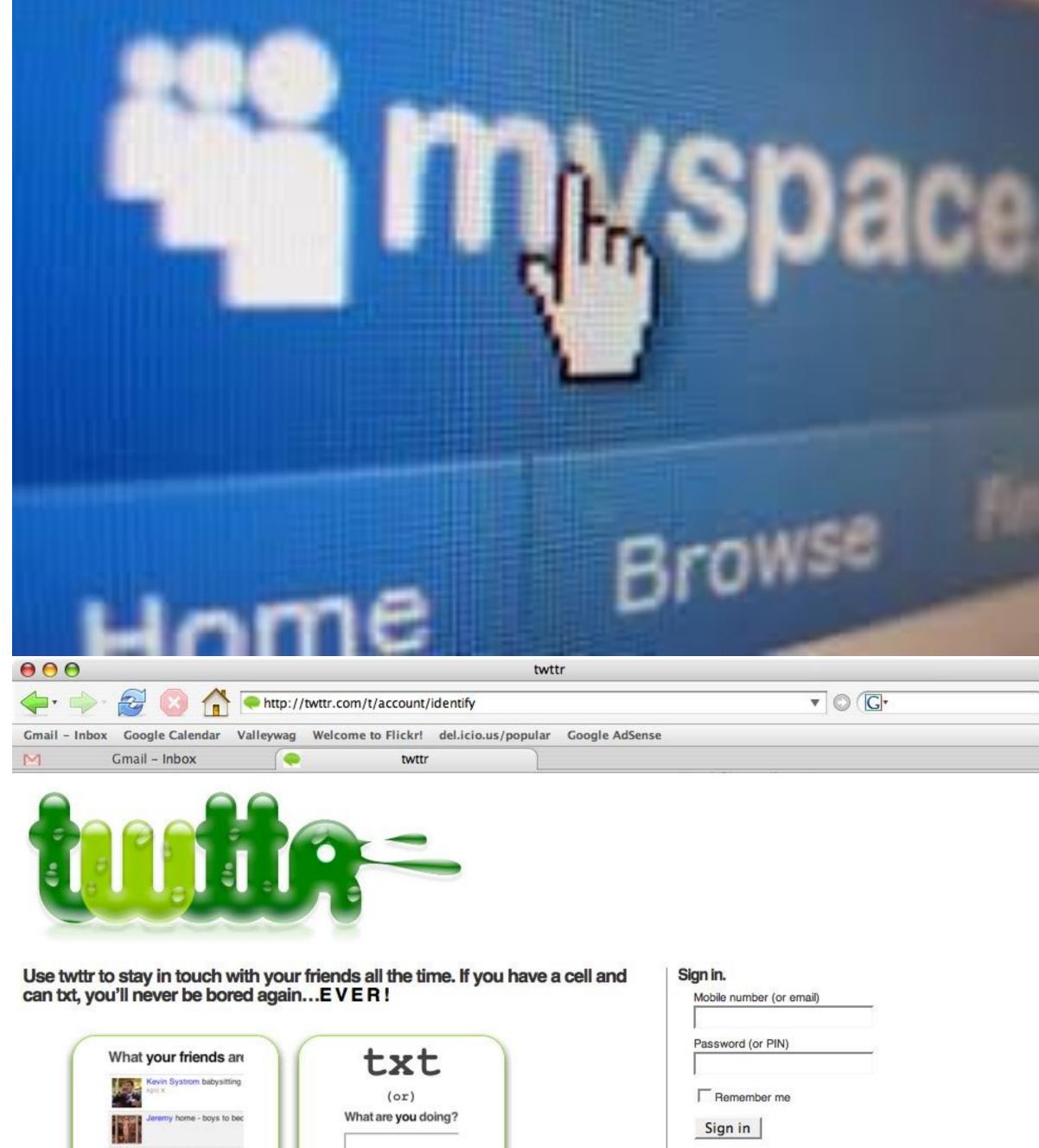




Passwords







Katie it's my birthday! (idea

.fimetine

Send

.what up?

New?	Sign	up!
------	------	-----

twttr works best when updated from your mobile phone. To verify you are you, we'll need your number.

Bad id: "stephOliciOus" (There is no flooble chatterbox with this id. It may have been deleted, or never existed. You can sign up for a new account if y

aviil 26, 2003 » song of the day « » BABy DONT CRy - TUPAc « emmx my head + eyes hurt a griPp xl.n' somy that ii didnt go to flute choir for those flute choir memberz u guys could do goot out with out me anyways erm *yawn* anyways ii started that new drama * neh een seng xP PARK GWANG HYUN hes foinne =] he looks like SOH J1 SUp =] rofiz a younger cuter version of him =] n' ii watched CHUN NYUN J1AE it was hella goot the japanese guy is frikkin hot his names like hujiouara taseu fooz hella foinne though >.< oh yesss n' ii found that kwon sang woo + kim min jung music video ii was looking for ii was looking for ii was tie * o_O *durooLx* * when ii saw the music video whOoO kwon sang wooz hella jal sseng guy usu so are my eyesx ii should go take another napP or something orng spring breakz almost over n' ii didnt do shit cept go out wid my ppgz oh well there goot enough mwoahahahahahahahahahaha ermmmm yeaPpP mak know why but ii wanted a new color xD mwoahahahahahahahaha ermmmm yeaPpP mak know why but ii wanted a new color YOUr HEAd UPp EVEn WHEN THE ROAd IS HARd , NEVEr G1Ve UPp* 8:35 PM - add eprops - add comments - email it	uji in the drar uh >.< aiigOh
» song of the day « » BABy DONT CRy - TUPAc « errr	uji in the drar uh >.< aiigOh
errrrx my head + eyes hurt a griPp x\n' somy that ii didnt go to flute choir for those flute choir memberz u guys could do goot out with out me anyways errr "yawn" anyways ii started that new drama " neh een seng xP PARK GWANG HYUN hes foinne =] he looks like SOH J1 SUp =] roftz a younger cuter version of him =] n' ii watched CHUN NYUN J1AE it was hella goot the japanese guy is frikkin hot his names like hujiouara taset fooz hella foinne though >.< oh yesss n' ii found that kwon sang woo + kim min jung music video ii was looking for ii was lie " o_O "durooLx"" when ii saw the music video whOoO kwon sang wooz hella jal sseng gyu sst so are my eyesx ii should go take another napP or something omg spring breakz almost over n' ii didnt do shit cept go out wid my ppgz oh well there goot enough mwoahahahahahahahahahahahaha ermmmm yeaPpP mak know why but ii wanted a new color xD mwoahahahahahahaw well im out	uji in the drar uh >.< aiigOl
xP PARK GWANG HYUN hes foinne =] he looks like SOH J1 SUp =] roftz a younger outer version of him =] n' ii watched CHÜN NYUN J1AE it was hella goot the japanese guy is frikkin hot his names like hujiouara taset fooz hella foinne though >.< oh yesss n' ii found that kwon sang woo + kim min jung music video ii was looking for ii was lie " o_O *durooLx* " when ii saw the music video whOoO kwon sang wooz hella jal sseng gyu set so are my eyesx ii should go take another napP or something orng spring breakz almost over n' ii didnt do shit cept go out wid my ppgz oh well there goot enough mwoahahahahahahahahahahae ermimmm yeaPpP mak know why but ii wanted a new color xD mwoahahahahahahawell im out " BABy DOnT CRy , HOPe YOu GOt YOUr HEAd UPp EVEn WHEn THE ROAd IS HARd , NEVEr G1Ve UPp"	uji in the dra uh >.< aiigO
know why but ii wanted a new color xD mwoahahah well im out " BABy DOnT CRy , HOPe YOu GOt YOUr HEAd UPp EVEn WHEn THe ROAd IS HARd , NEVEr G1Ve UPp "	ide my xang
8:35 PM - add eprops - add comments - email it	
n song of the day n as time goes by - T n	
aiiiyahhhx ANOThEr CRAPPy DAy x[argHsx errr yeaHh wenT tO regaLs met uPp w/ my faGgaT frienDs x] CHOPST1Ck omGx u dumbfuck xD we gOt fuckinGg kiCked out of regaLs cause of ur SK1NNy A/ was happy ^a see ray oh yea jun too ^^, ernnn anyways yeapP drank some wcz 8) mwoaahhahaa =D n' ii gotta pedicure cause ii was so pissed off at that regaLs bitchH guy omGg he was ONE SON OF A B1TCHHhl pedicure made uPp for it =] n' lets see oh yayee-!!! ii saw my lyl dee nelOx ii was happy too see him ^_ ii didnt get too see jason guhguh though x[ii miss him =D roftz ii never miss him btw xP hrmmm its cold "bRrRR	HhH- aroH
12:04 AM - add eprops - add comments - email it	
April 23, 2003	
a song of the day a do ii ever cr0ss ur mind ? - brian mcknight a	
ii havent touched this thing for a while =T err sony guyz ive been busy planning for my madness of a bestfriend/ppg =] JOY SHOY BOY TOY ^, * err yeahh my dayz have been shiz / hell =] but oh yes ii must take the crew there for me~ =] err yeahh today was fun like hell cause we had a suprise birthday for joy =] it turned out pretty goot n' joy was so happy n' she felt so special im glad HAPPY B1RTHDAY JOY~ YOU ARE SPEC LOVE U SO MUCHS N' ii HOPE OUR FR1ENDSH1P NEVER ENDS LOVE U LOTS BUBBLEZ x] errr yeahs ii cant write whateverz on my mind cause my cousin reads this once in a while n' all that cuhraps so yeaf B1RTHDAY JOY ii HOPE UR W1SH COMES TRUE	C1AL N' ALI
- days like this, ii miss u even more	
Tutus PM - add eprops - add comments - email it	
18, 2003	
AHHHHH ii SWEAR ii ALWAYS GET THIS FUCKING SHIT FOR NO REASON >=I ii hate this =[NAH UH DDUH KEH	
10:57 PM - 2 eprops - 1 comment - email it	
ril 15, 2002	
) im still lo
11:57 PM - add eprops - add comments - email it	
	Trees
	Ima
	10
	Pic
	aligabilityx ANOTHER CRAPPY DAy x[argHsx err., yeaHh wenT tO regals met uPp w/ my faGgaT frienDs x] CHOPST1Ck omGx u dumbfuck xD we gOt fuckinGg kiCked out of regals cause of ur SK1NNY A was happy "see ray of yea jun too "^_ ernnm anyways yeapP drank some wucz 8) mwoaahahaa = D n ii gota pedicure cause ii was so pissed off at that regals bithH guy omGg he was ONE SON OF A BITCHHH pedicure made uPp for it =] n' lets see oh yave-!!! ii saw my lyid ee nelOx ii was happy too see him ^_ ii didnt get too see jason gubguh though x] ii miss him =D roftz ii never miss him bbv xD hmmm its oold "bR/RR 'yaw" alisHHL ii dont wonnex LALALA ii gotta smile it off though :) >=! ima go nowz - stepho' - 12.04 AM - add eprops - add comments - email it April 23, 2003 a song of the day = do ii ever cr0ss ur mind ? - brian mcknight = ii havent touched this thing for a while =T err sorry guyz ive been busy planning for my madness of a bestfriend/ppg =] JOY SHOY BOY TOY ^* err yeahh my daya have been shiz / hell =] but oh yes ii must take the crew there for me - =] err yeahhtoday was fun like hell cause we had a suprise bithday for joy =] it turned out pretty goot n' joy was so happy n' she feit so special. im gladHAPPY BIRTHDAY JOY - VOU ARE SFEL LOVE U SO MUCHS N' ii HOPE OUR FRIENDSHIP NEVER ENDS LOVE U LOTS BUBBLEZ x] errr yeahs ii cant write whateverz on my mind cause my cousin reads this once in a while n' all that cubraps so yeal if the this , ii miss u even more 10:09 PM - add eprops - add comments - email it 12:09 PM - add eprops - add comments - email it 18: APRY BITHDAY SET THIS FUCKING SHIT FOR NO REASON >= ii hate this =[NAH UH DDUH KEH



 \odot

[thefacebook

home search global social net invite fag logout



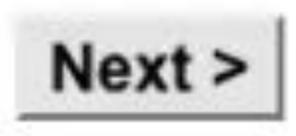
Information	
Account Info:	
Name:	
Member Snoe:	January 12, 2005
Last Update:	February 3, 2005
Basic Info:	
Enalt	
Statue:	Alumnus/Alumna
Sex	Male
Yeari	2004
Concentration:	Computing Sciences Mathematics
Phone:	
High School:	
Extended Info:	
Screenname:	
Looking For:	theraship



Find your friends on Tagged! Check your Gmail address book:

Gmail email address:

Gmail password:

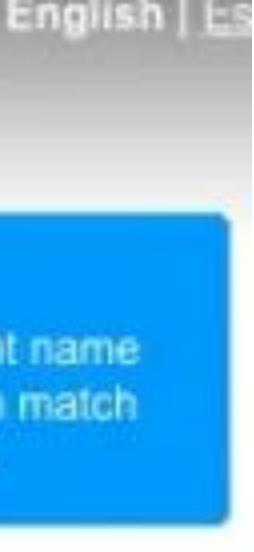




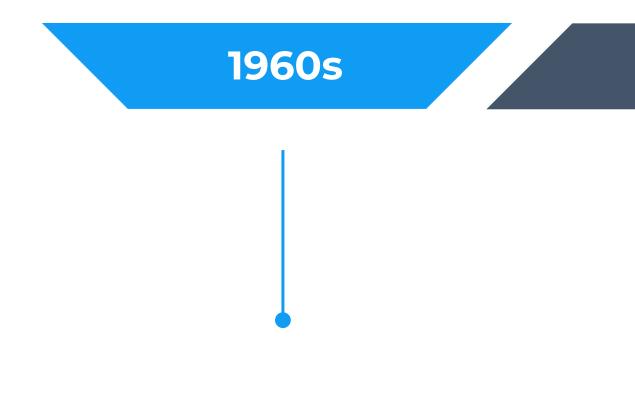
Gmail

Enter your Gmail account name and password so we can match you up with your friends.

@gmail.com

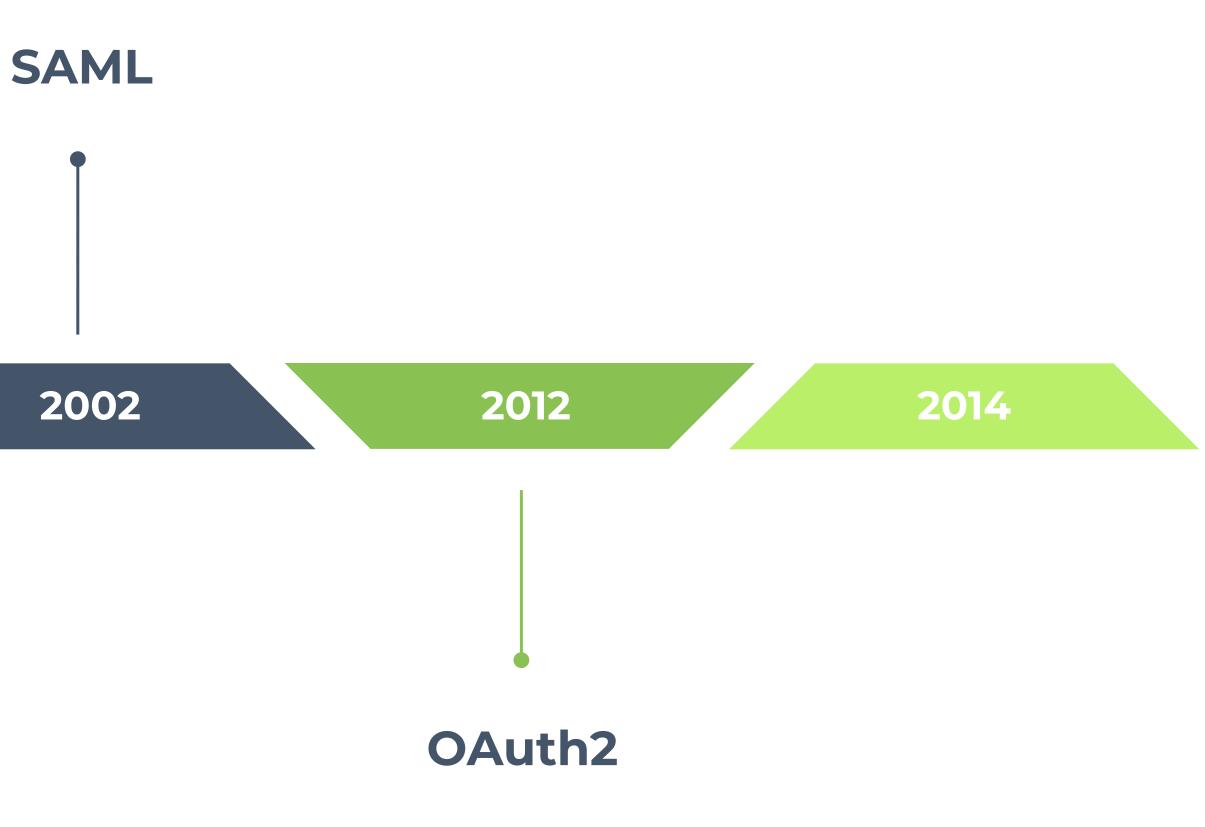






Passwords

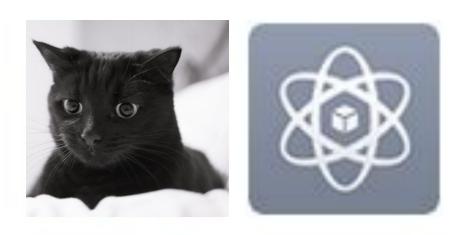




DELEGATED AUTHORIZATION

F Log in with Facebook - Google Chrome

Log in with Facebook \$



MyFirstApps will receive the following info: your public profile and email address.

Edit the info you provide

This does not let the app post to Facebook.



https://www.facebook.com/v2.0/dialog/oauth?scope=user_likes%2Cpub



Login to my account

If you have an account with us, please log in.

Password*			
Forgot your password?			
SIGN IN			
SIGN IN	OR		

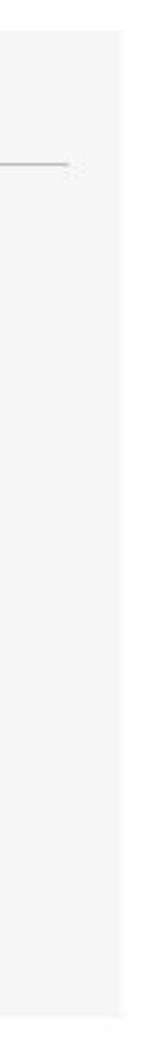
New user registration

tracyyan12345@gmail.com	
-------------------------	--

Please send me emails about special offers, exclusives and promotions monthly.

I agree to Rosewe.com Terms and Conditions.





VS.

Authorization Authentication





Authorization





Authentication



RUBY PRINCESS 01/24/16 to 01/31/16

Muster Station: D

3864

PRINCESS CRUISES

MR JOSEPH LASICA

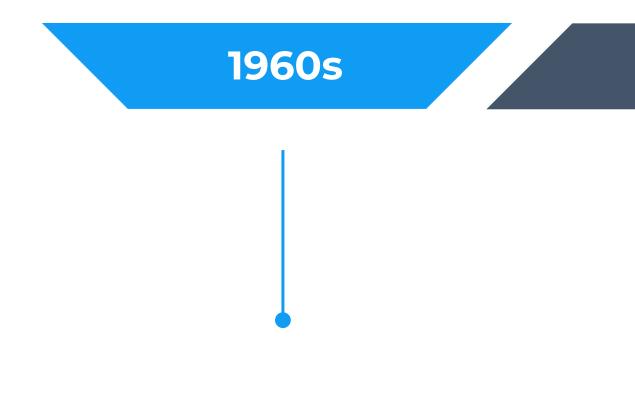
Dining Room: Anytime Dining Time: Anytime Table: Any





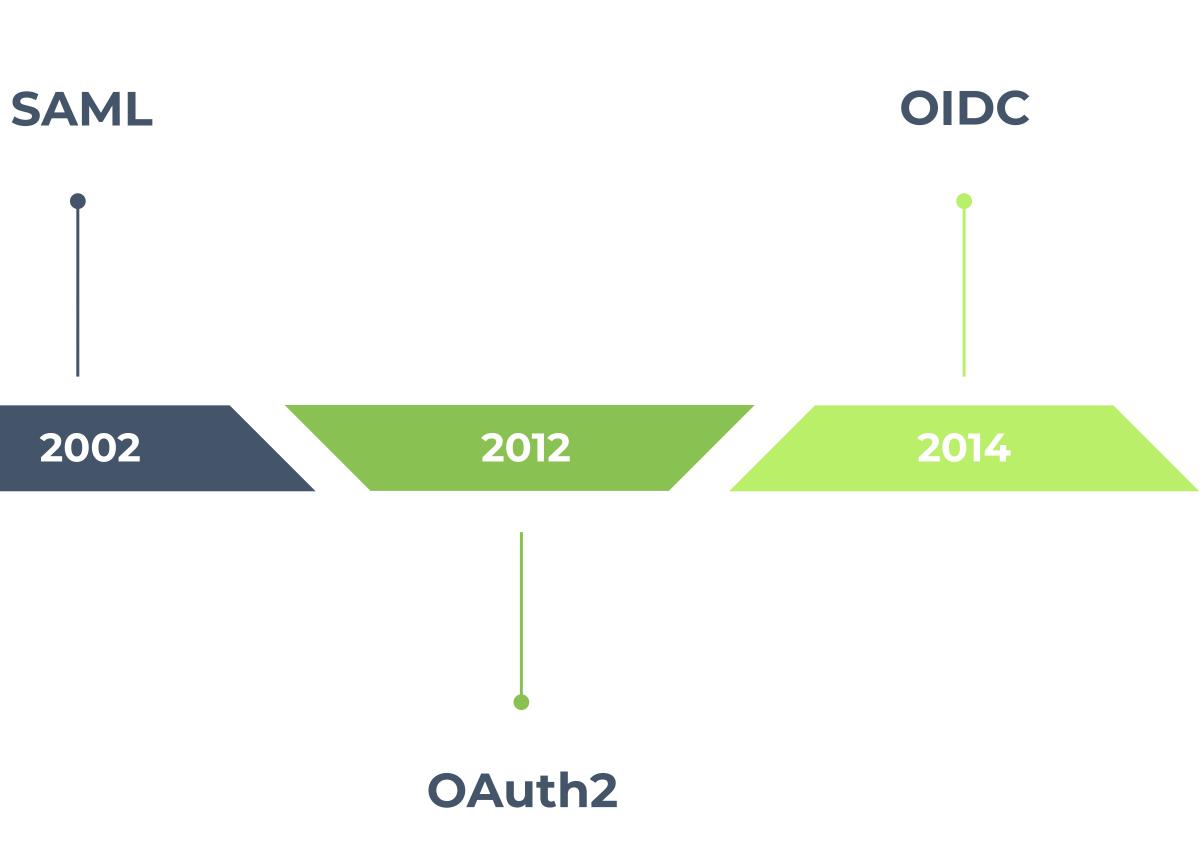






Passwords

HISTORY OF IDENTITY





RUBY PRINCESS 01/24/16 to 01/31/16 **MR JOSEPH LASICA**

Dining Room: Anytime Dining Time: Anytime Table: Any





TEXT SUMMARY





Four Roles Defined by OAuth2



End User who provides consent for scopes

Resource Owner (RO)



Resource Owner (RO)

end user scopes





End User who provides consent for scopes



API or Application controlling the data

Resource Server (RS)

Application Controlling the data

Google



LinkedIn would like to:



View your email address



View your basic profile info



Manage your contacts

By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Cancel







End User who provides consent for scopes



API or Application controlling the data Application handling delegated authorization decisions





End User who provides consent for scopes



API or Application controlling the data Application handling delegated authorization decisions

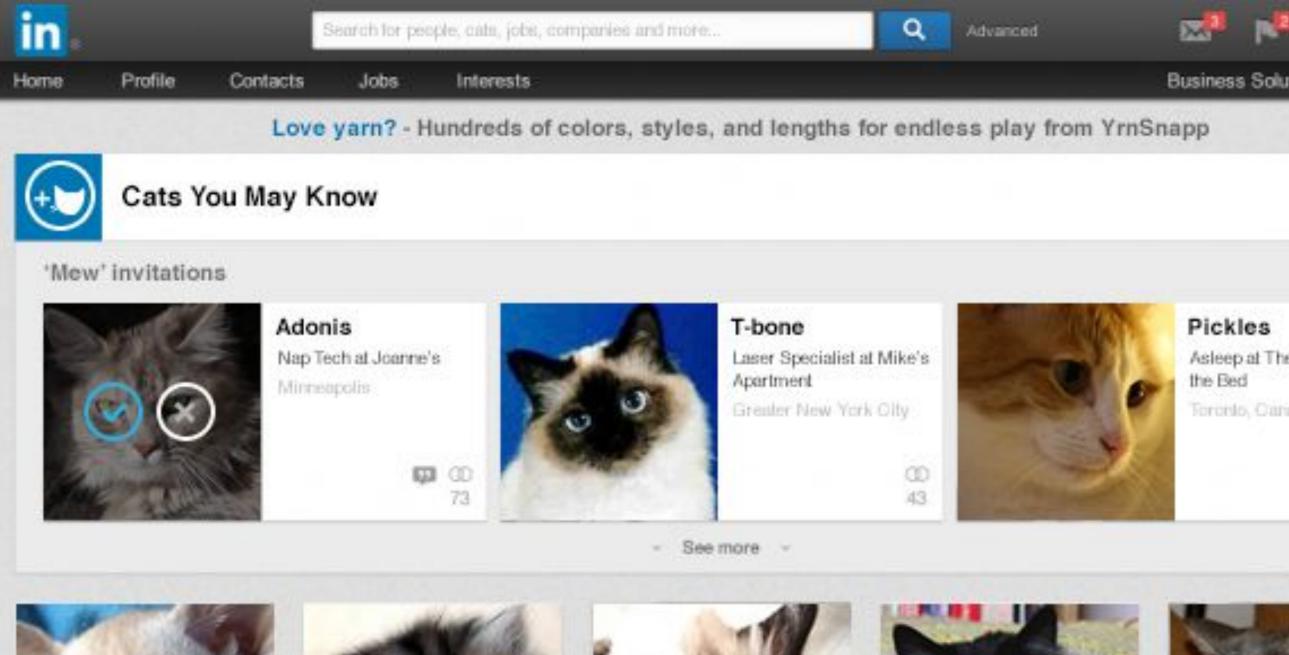


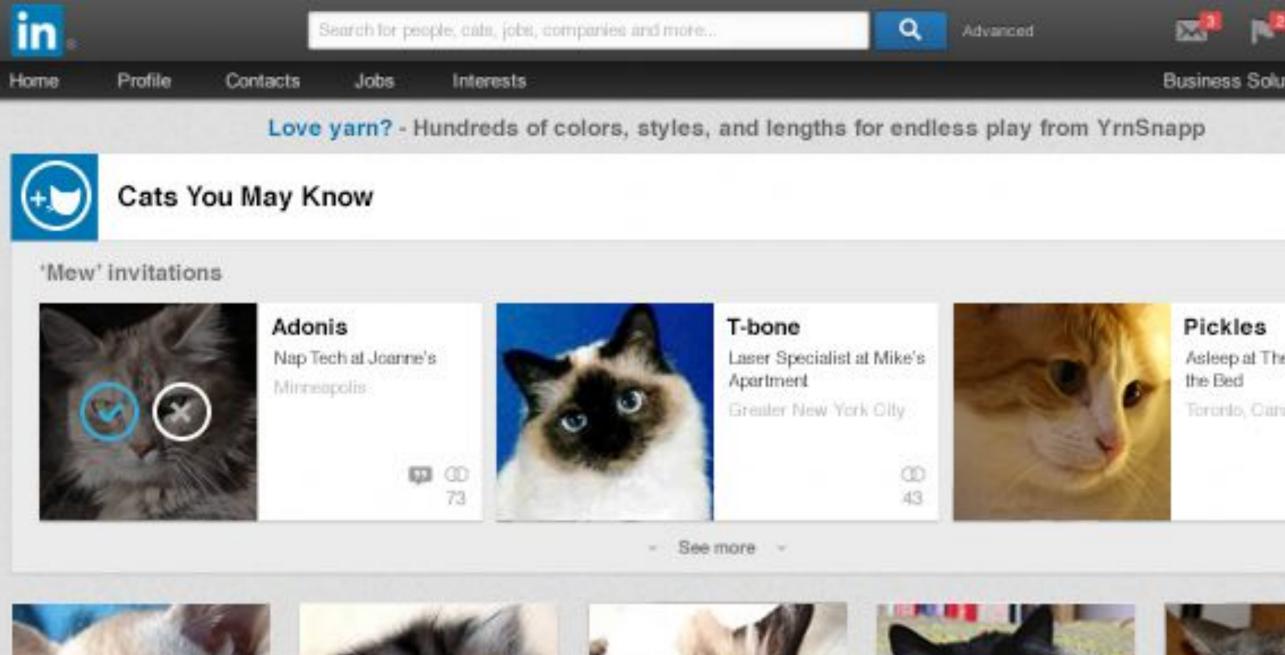
Application requesting the data

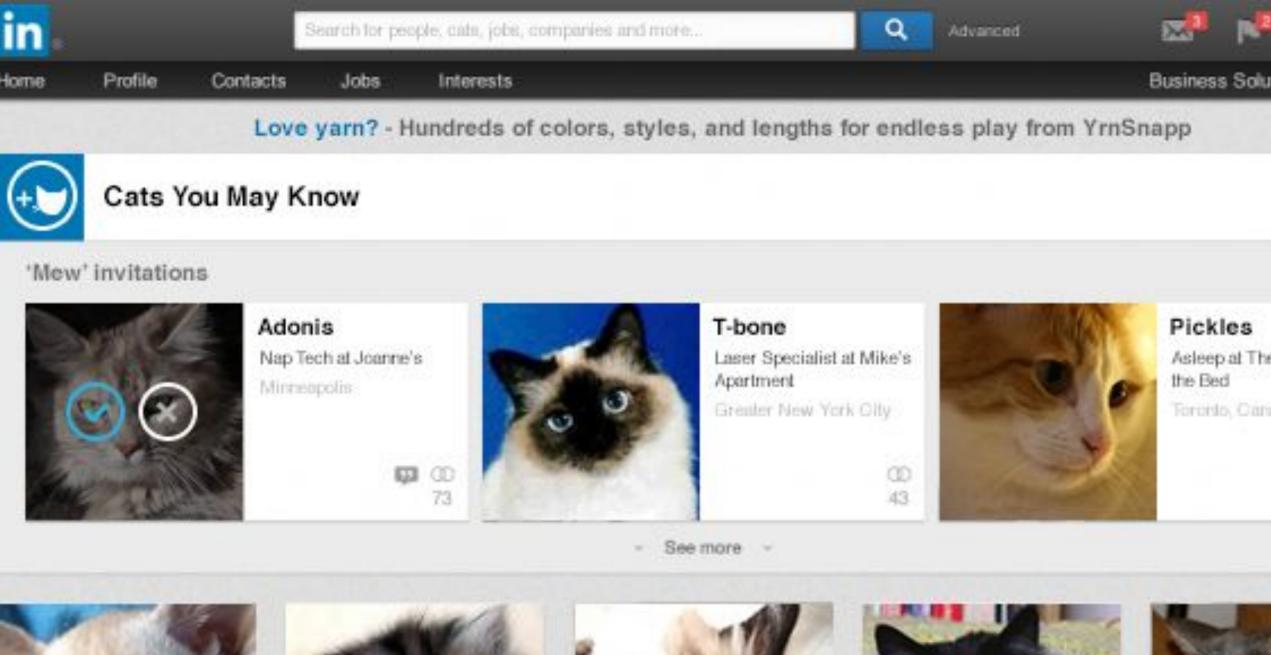
Client

Client

Application requesting the data















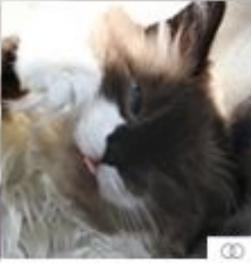
Mildred

57 Mouser at Stephen's Bachelor

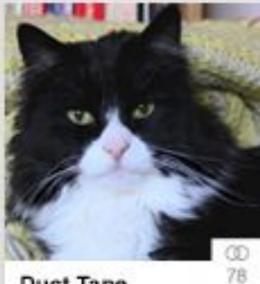
San Francisco Bay Area



Pooptart Feather Chaser at Kim's Place Sacramento, California



60 **Prissy Sissy** Hairball 'Hacker' at Nisha's Apartment Datias, Texas



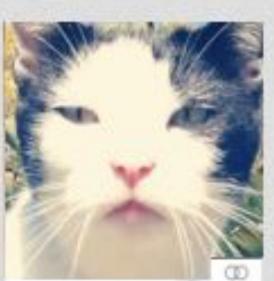
Duct Tape Purr Engineer at Dale's Trailer Park Etuceville, Indiana







13 Sir Meawington



Tuna

63



20



Humperdinck



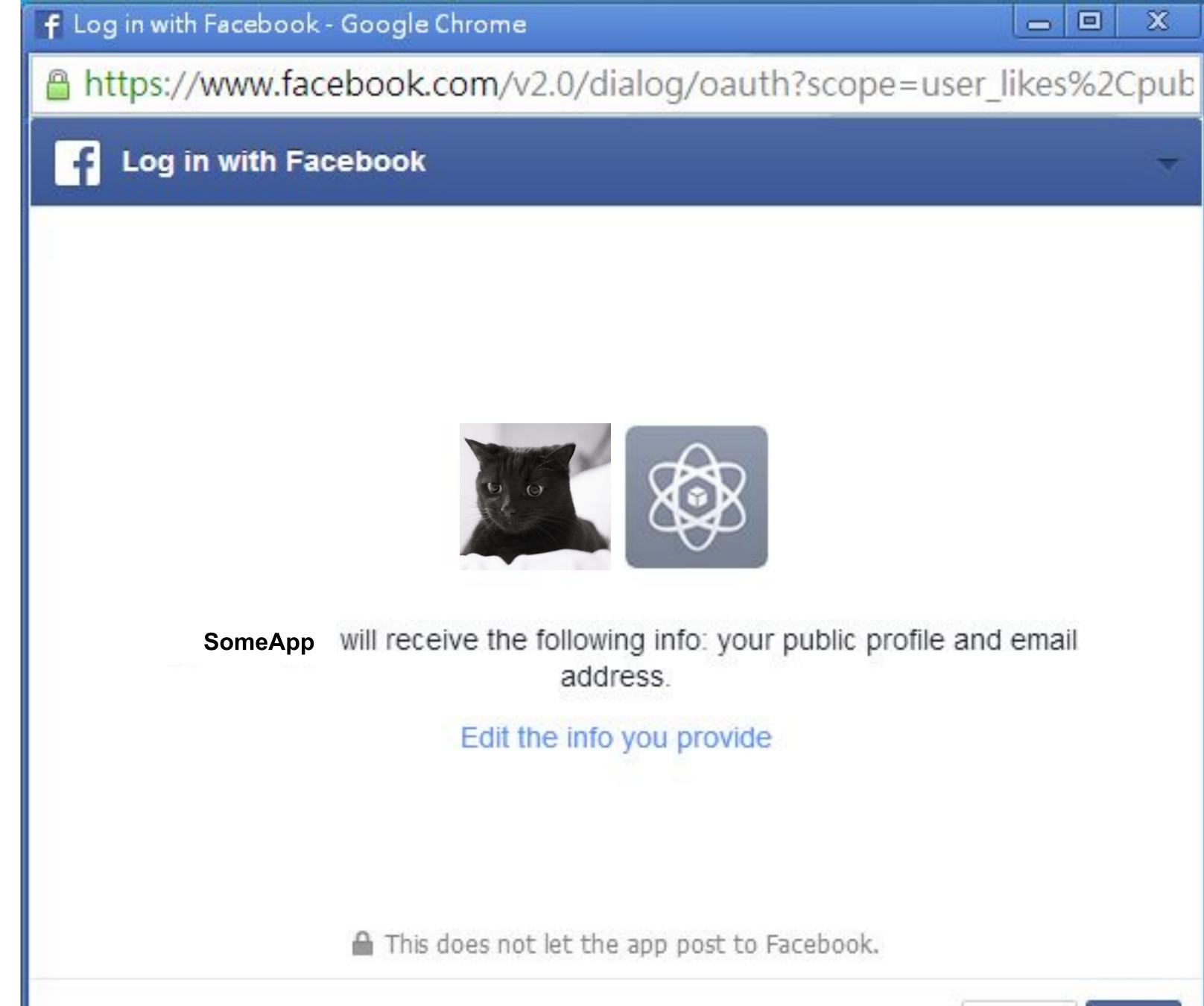
Admiral Wigglee

90



Let's review.





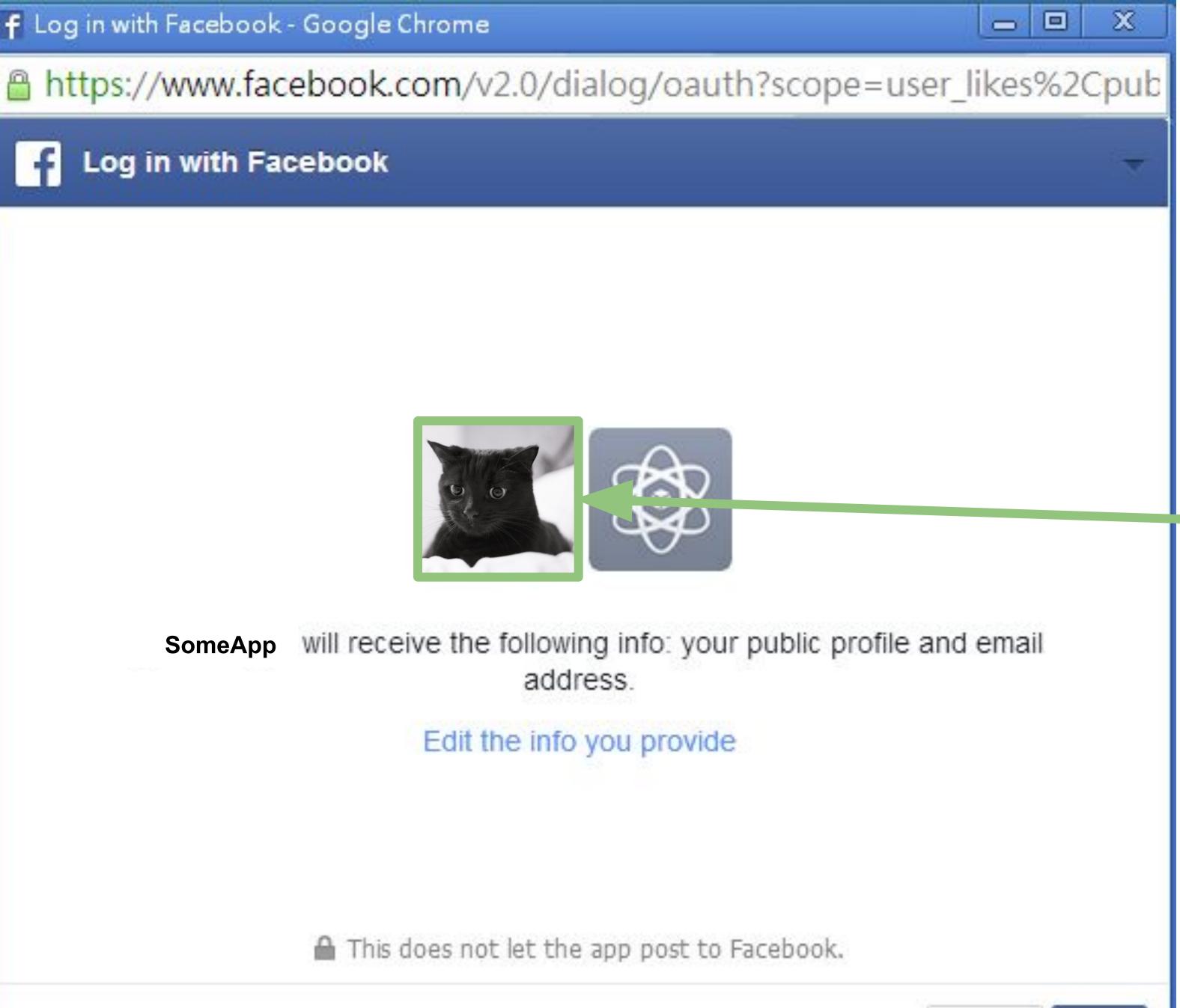


will receive the following info: your public profile and email





Log in with Facebook \$



Okay

Cancel

SomeApp



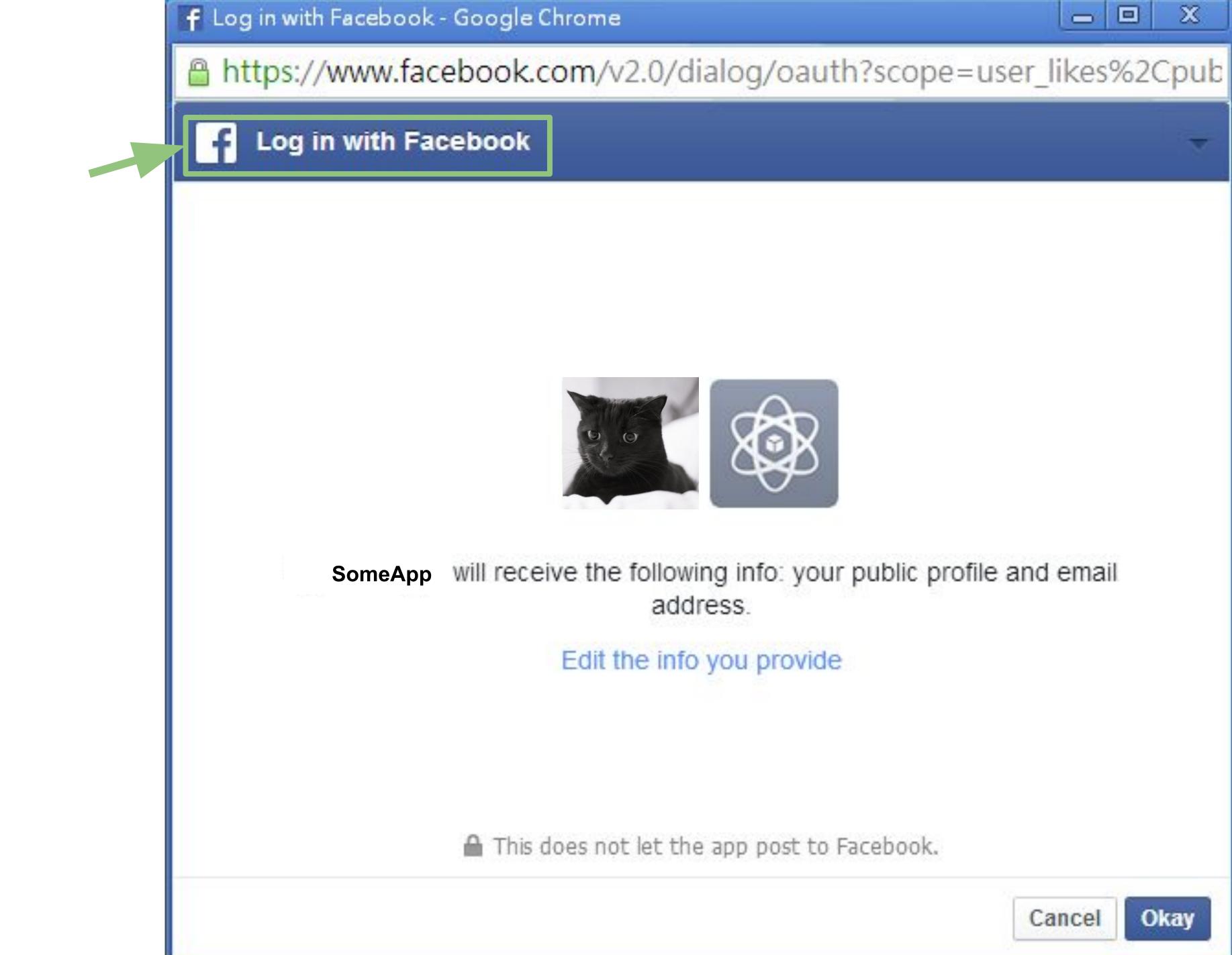
Log in with Facebook

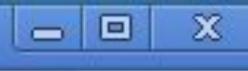


will receive the following info: your public profile and email SomeApp address. Edit the info you provide This does not let the app post to Facebook. Okay Cancel

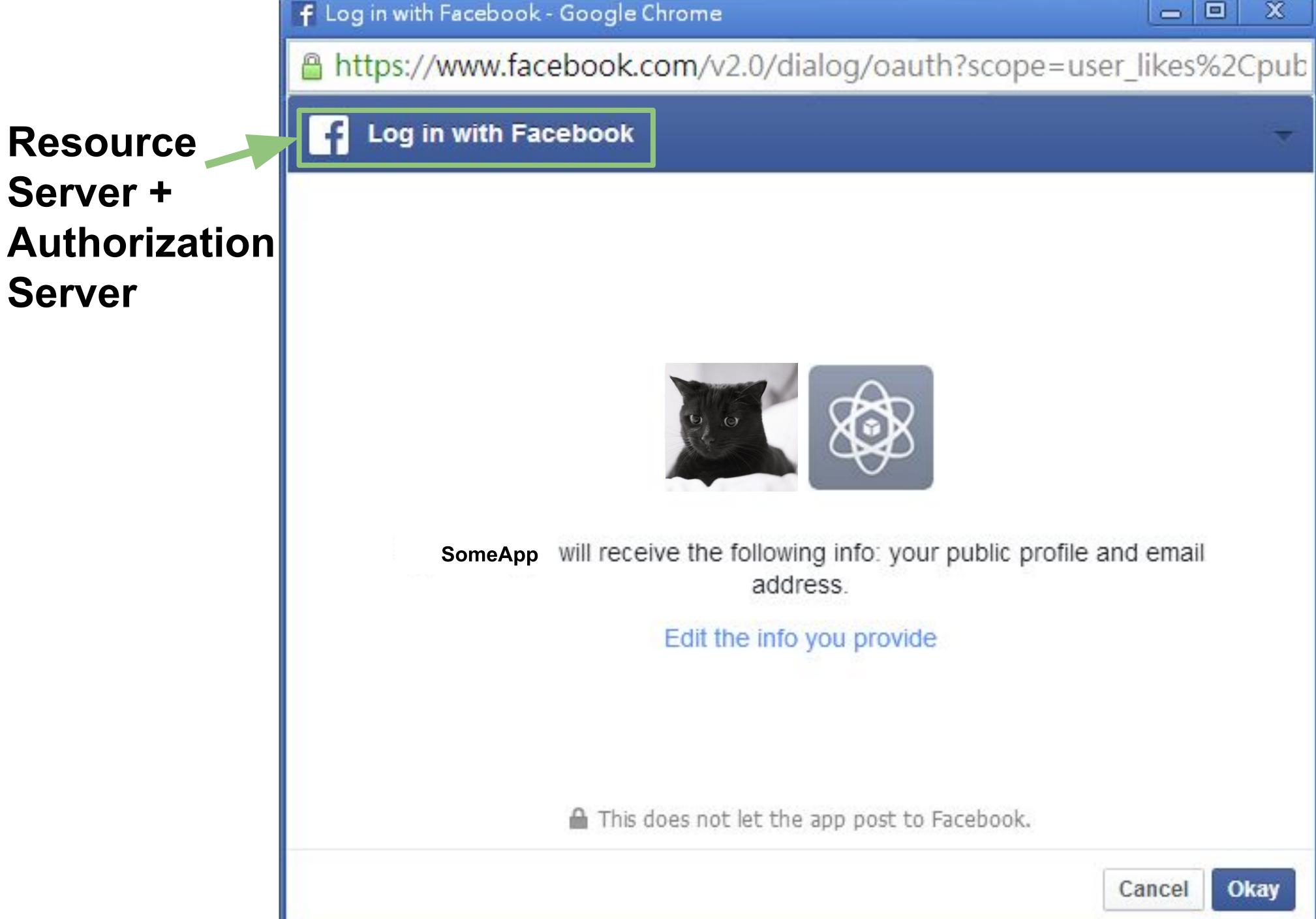
Resource **Owner**

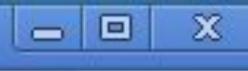




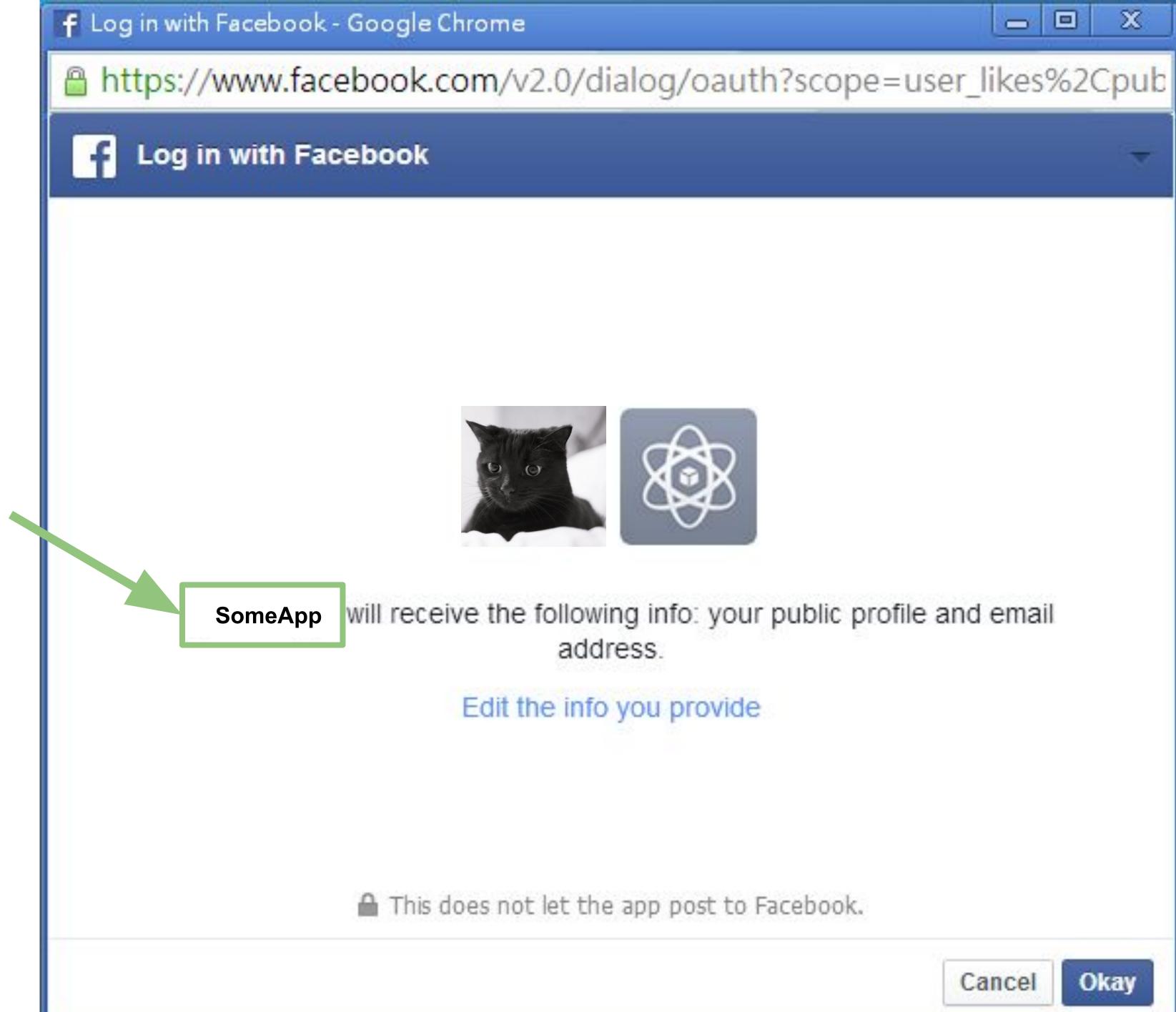








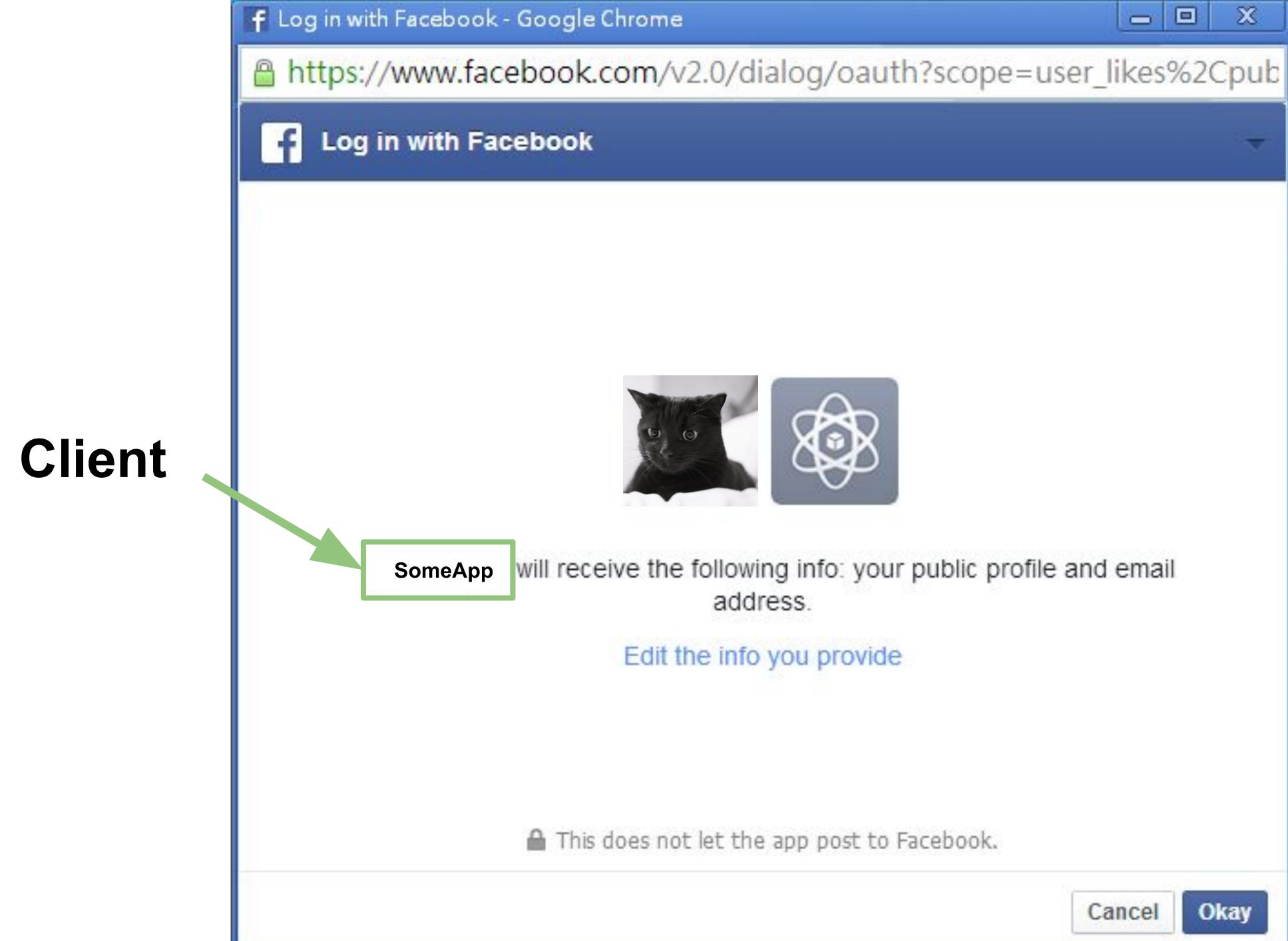






will receive the following info: your public profile and email

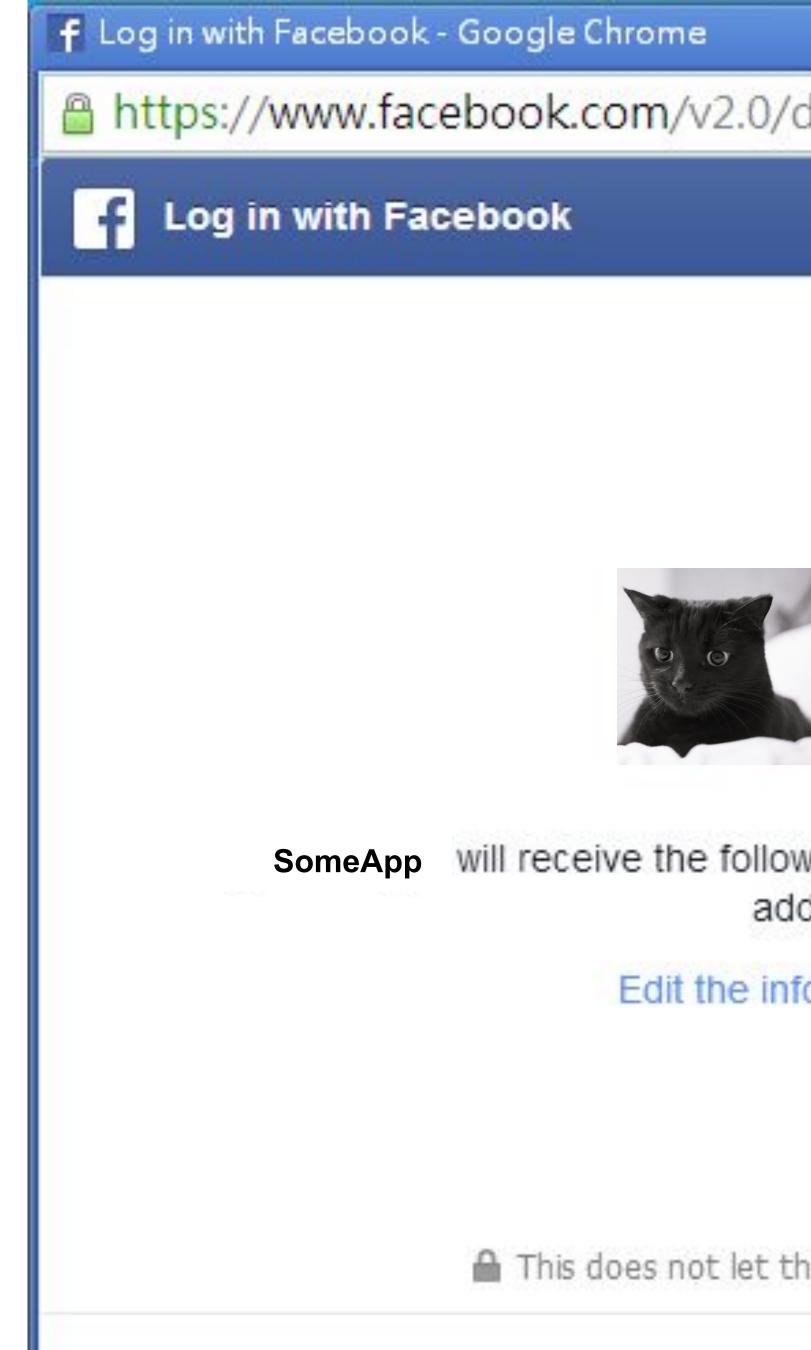




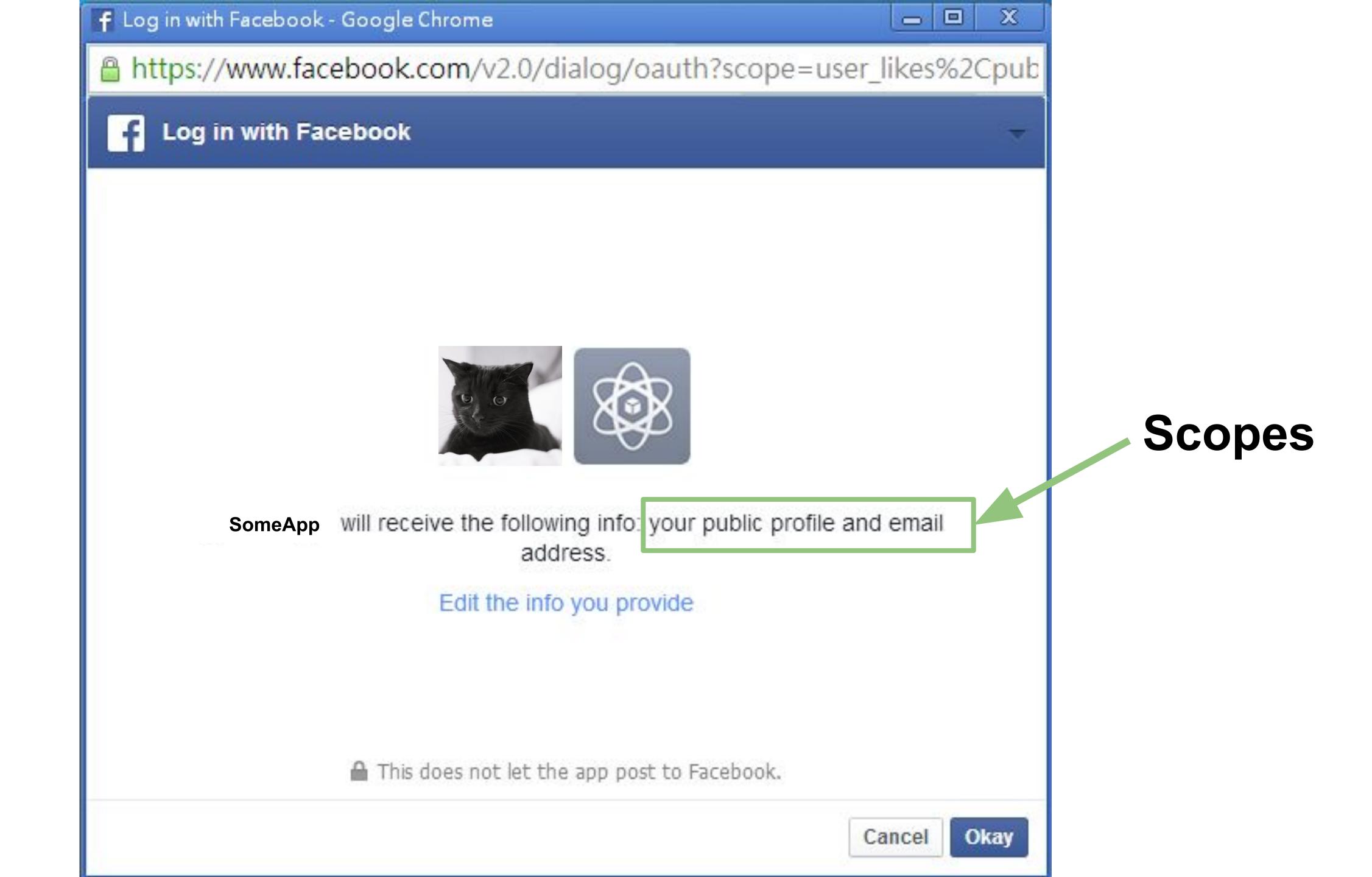


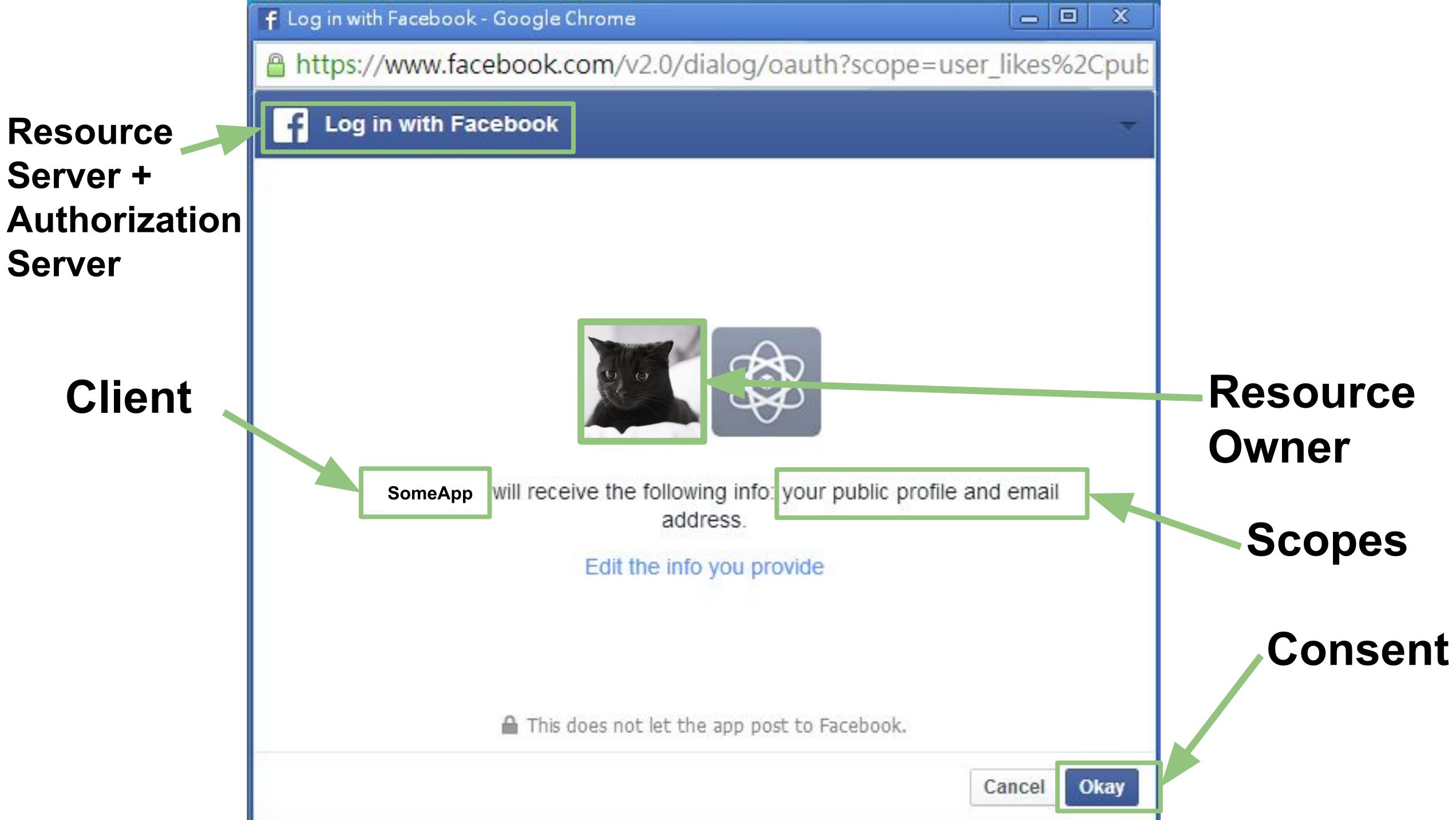
will receive the following info: your public profile and email





/dialog/oauth?scope=user_likes%2Cpub	
wing info: your public profile and email ddress. Info you provide	
Cancel Okay	









Tokens

Tokens Access Token Refresh Token ID Token





Access Token

Refresh Token

Membership Card

4297 4392 7156 8735





Sally Sample

SEX: F EYES: BL HT: 5-09 E: NONE

R: NONE



DRIVER LICENSE CLASS DM ID Number Document ISSUED: 07-18-05 EXPIRES: 07-18-13 Number 83145522



ID Number

Document Number

JSON Web Token (JWT)

Encoded Claims (user data) Stateless validation Signed for authenticity

3 parts of JWT Header Payload

Signature

3 parts of JWT

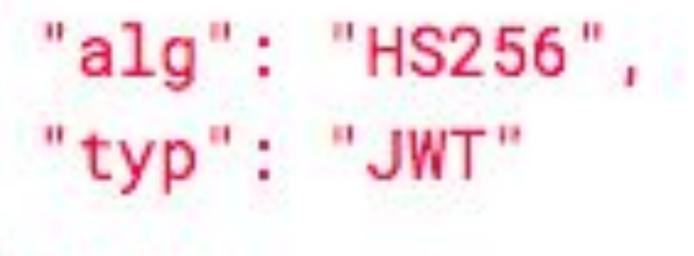
Header

Payload Signature

- hhhhhhhhh .pppppppppp .sssssssssssssss
- eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ zdWIiOiIxMjM0NTY30DkwIiwibmFtZSI6IlNwaWR lcm1hbiIsImlhdCI6MTUxNjIzOTAyMn0.rMAPKVY oWblhBAKQ1-qrZgMksb6FoS-ajM4b5p1bKUg

HEADER

"typ": "JWT"



PAYLOAD

"iss": "https://example.com", "sub": "123", "aud": "some-client-id", "exp": 1311281970, "iat": 1311280970

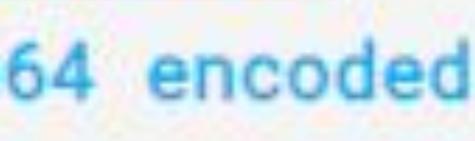


SIGNATURE

HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload),

your-256-bit-secret

secret base64 encoded





Parts of a JWT Summary Header - alg (algorithm) & type (JWT) Payload - claims (data about the user) Signature - uses payload, header and secret and specified algorithm verify that a token is authentic

Authorization Grants

Authorization Grants

methods for a client application to acquire an access token which represents a user's permission for the client to access their data

Authorization Grant Flows

***** Authorization Code

***** Authorization Code + PKCE

***** Client Credentials

Front-Channel Browser to API Not-so secure

Back-Channel Server to API Very Secure



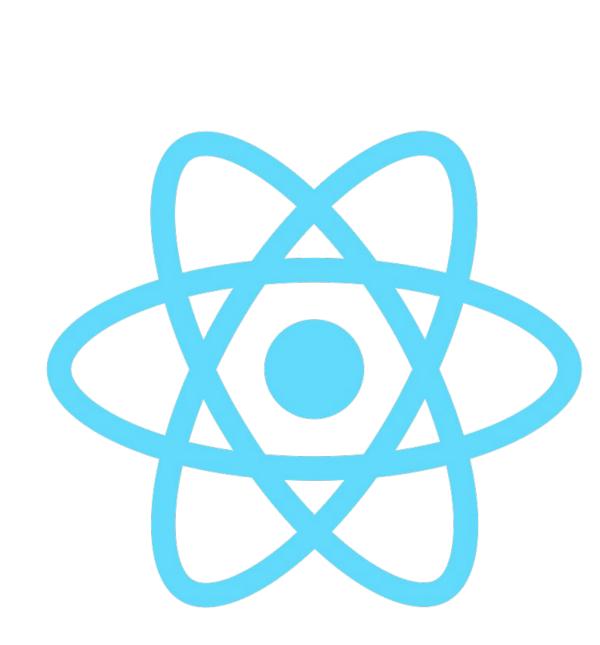
Authorization Code Flow Back Channel + Front Channel





Authorization Code + PKCE Front Channel Only



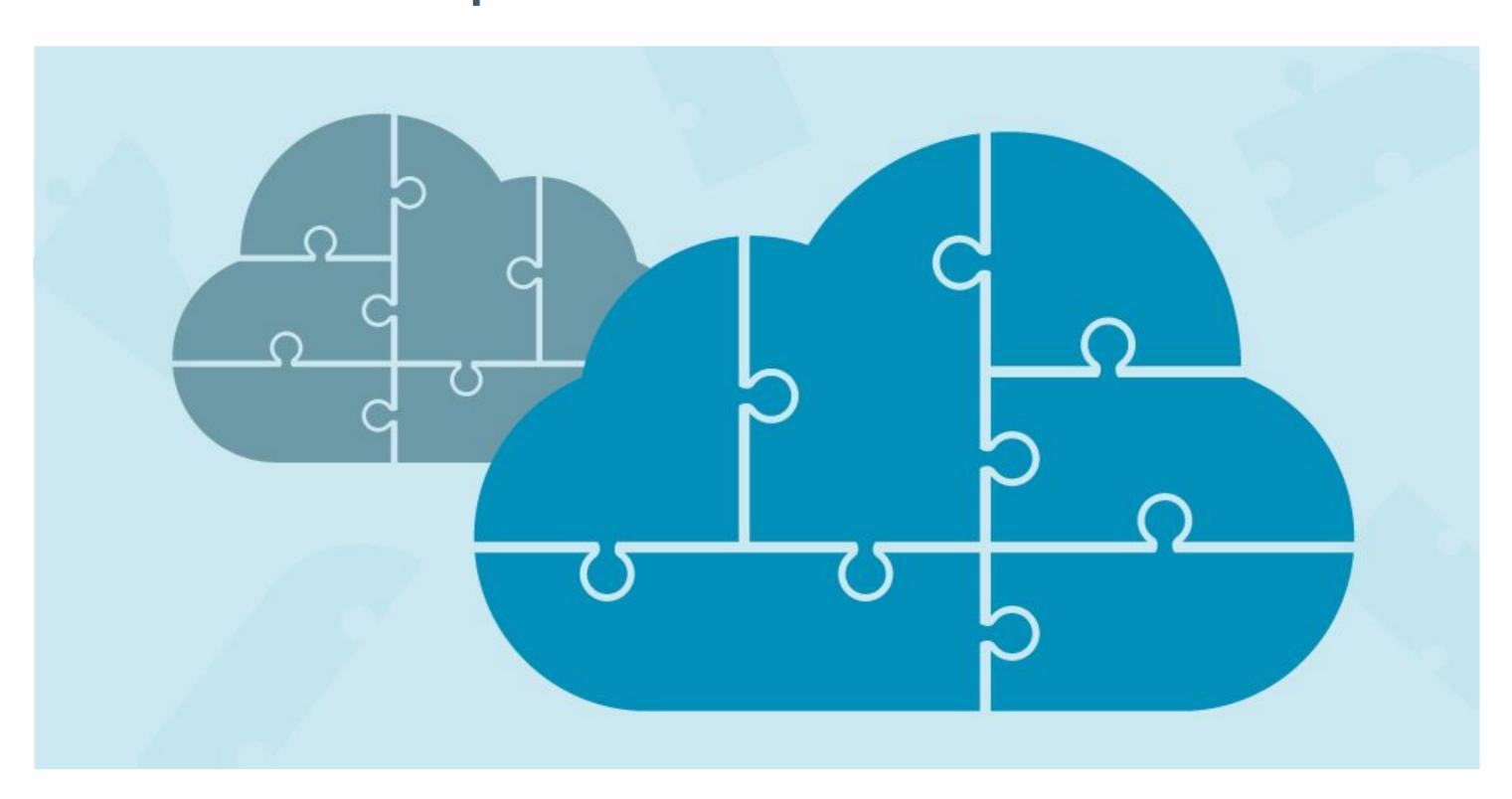


SPA/Mobile





Client Credentials Flow *Back Channel Only* Machine-to-Machine example: microservices





FOUNDATION SUMMARY





1.2. Protocol Flow

< (D) Authomization Count	Owner
<pre><-(B) Authorization Grant +</pre>	
+	
(C) Authorization Grant>	
<-(D) Access Token	Server
+	
(E) Access Token>	Resource Server
<-(F) Protected Resource	
	+ (E) Access Token>

CLIENT

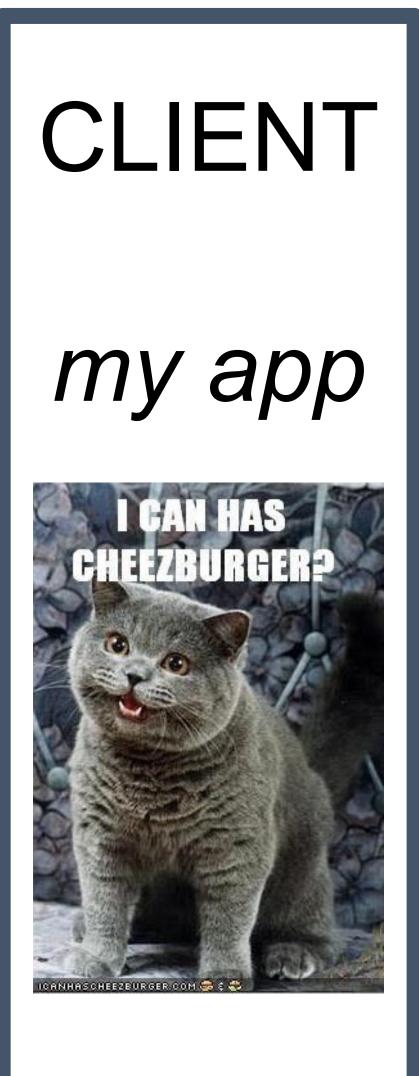
my app







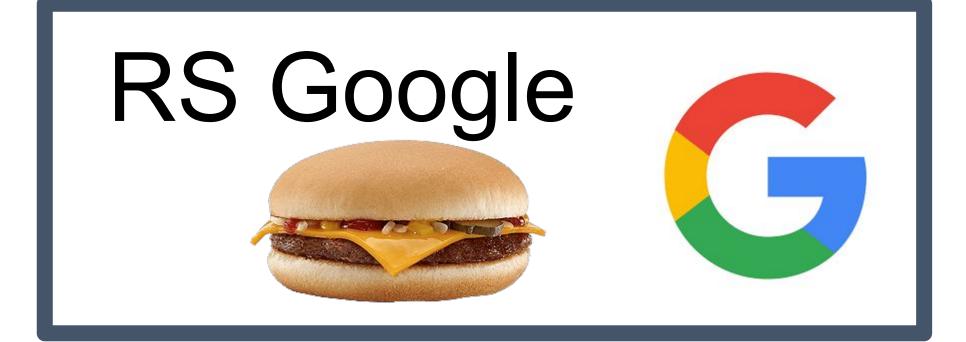


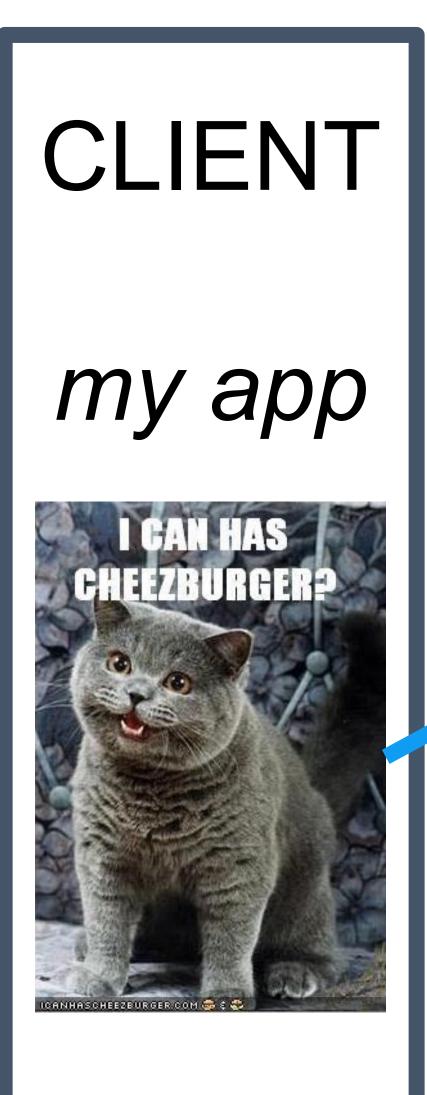


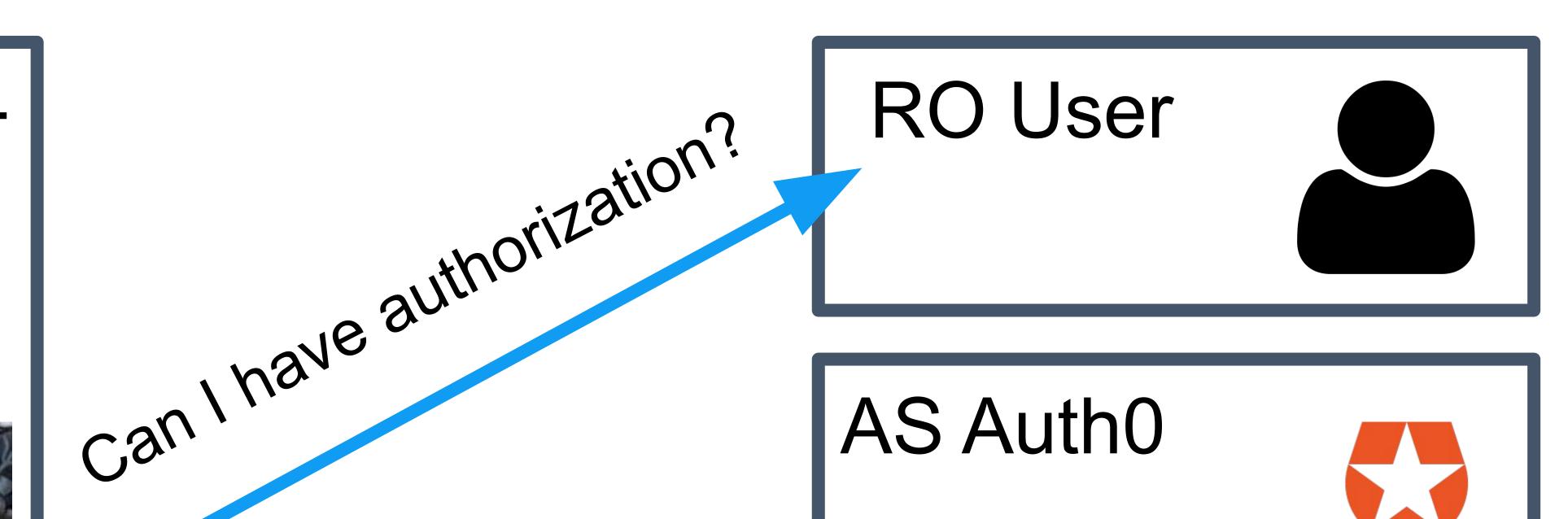






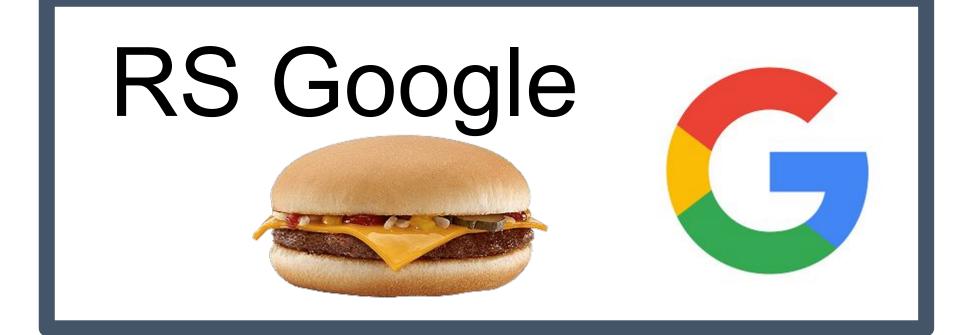






AS Auth0





https://auth-server.com/authorize? response type=code&

client id=client id123&

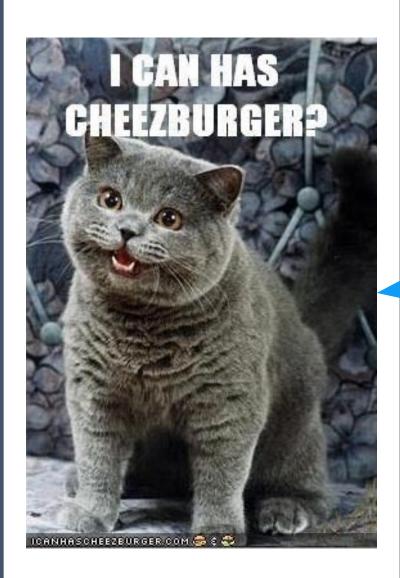
redirect uri=https://example.com/callback&

scope=openid+profile+email&

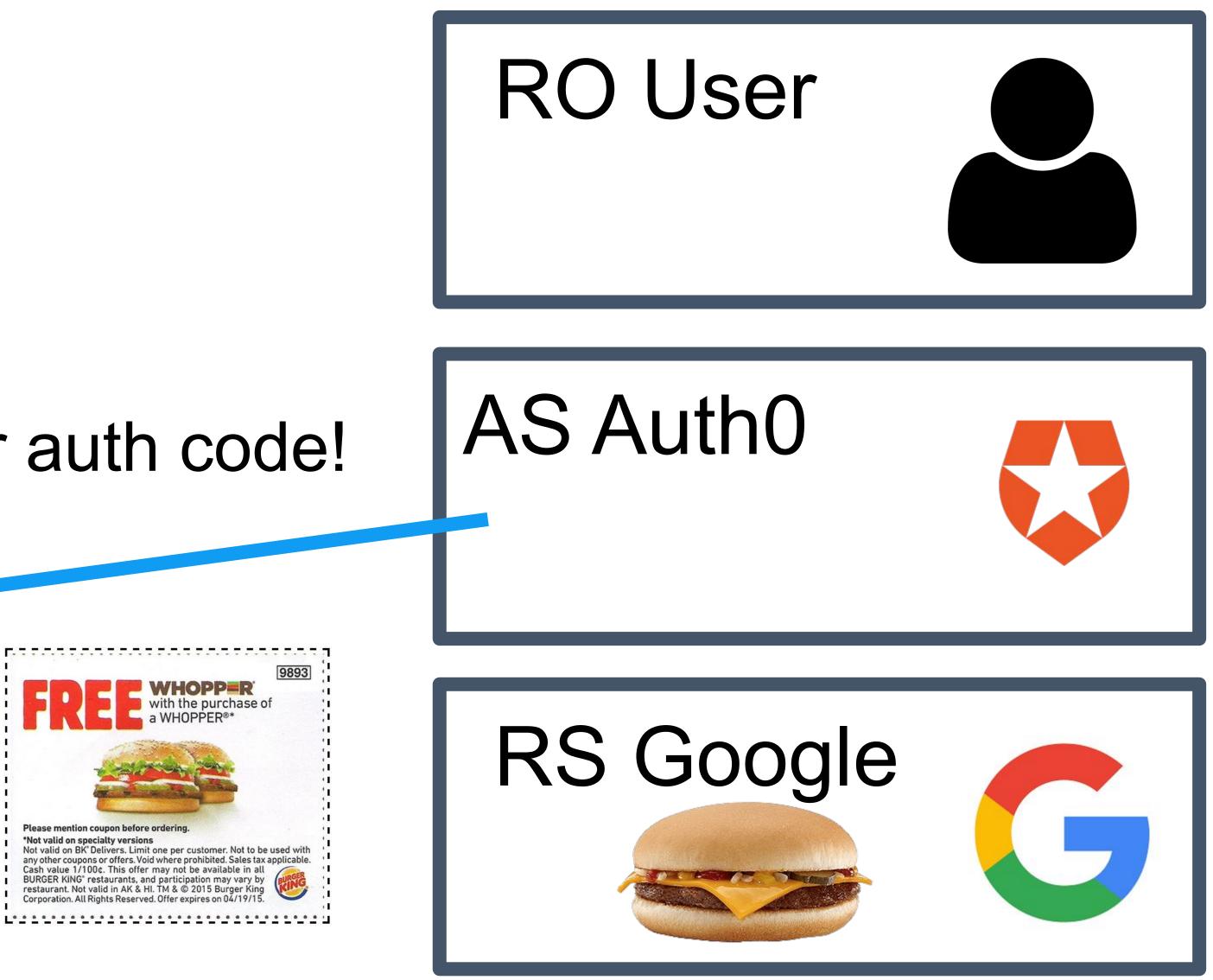
state=some random string

CLIENT

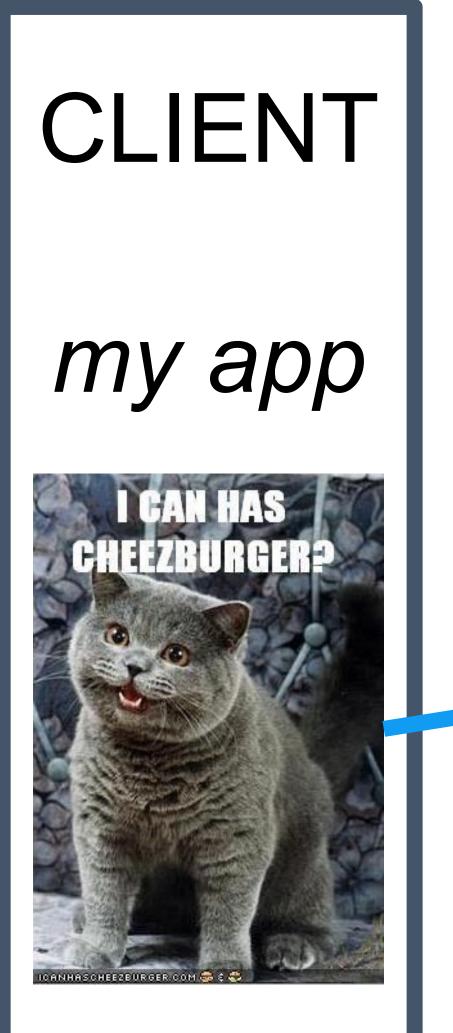
my app

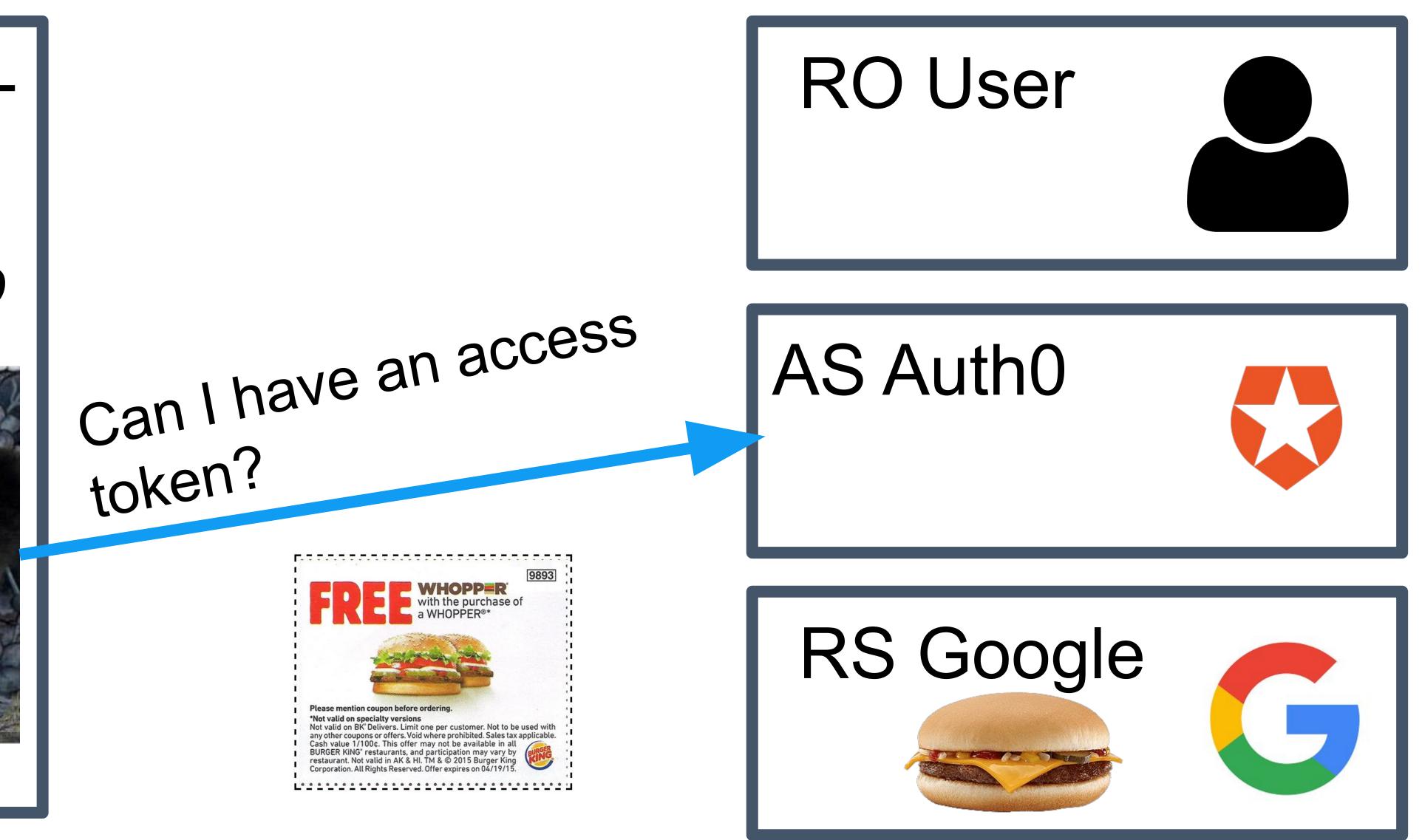


Here's your auth code!



https://example.com/callback? code=123& state=some random string

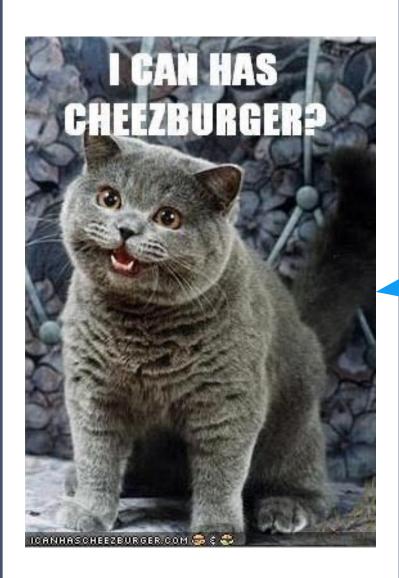




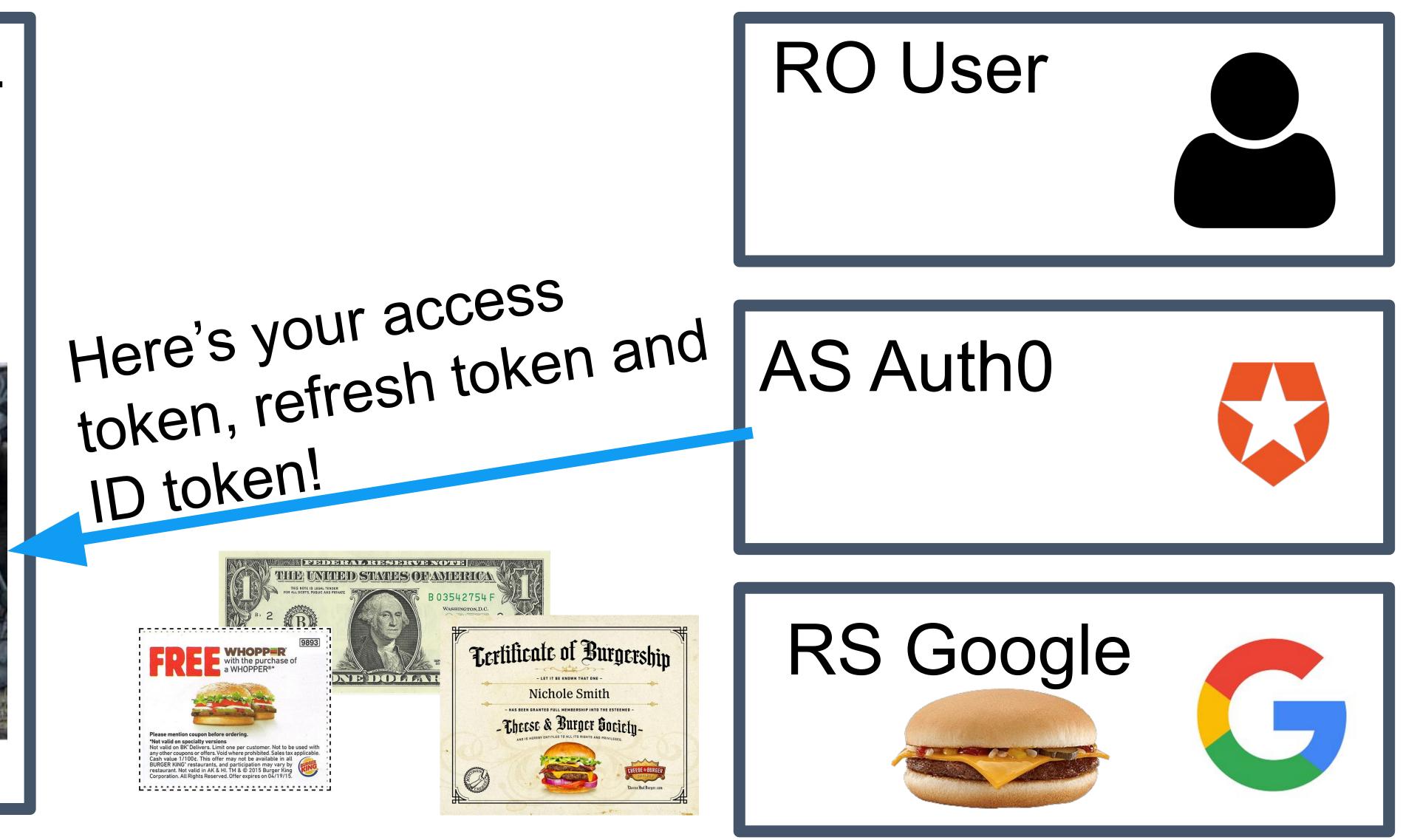
POST https://auth-server.com/token
grant_type=authorization_code&
code=123&
redirect_uri=https://example.com/callback&
client_id=client_id123&



my app



ID token!

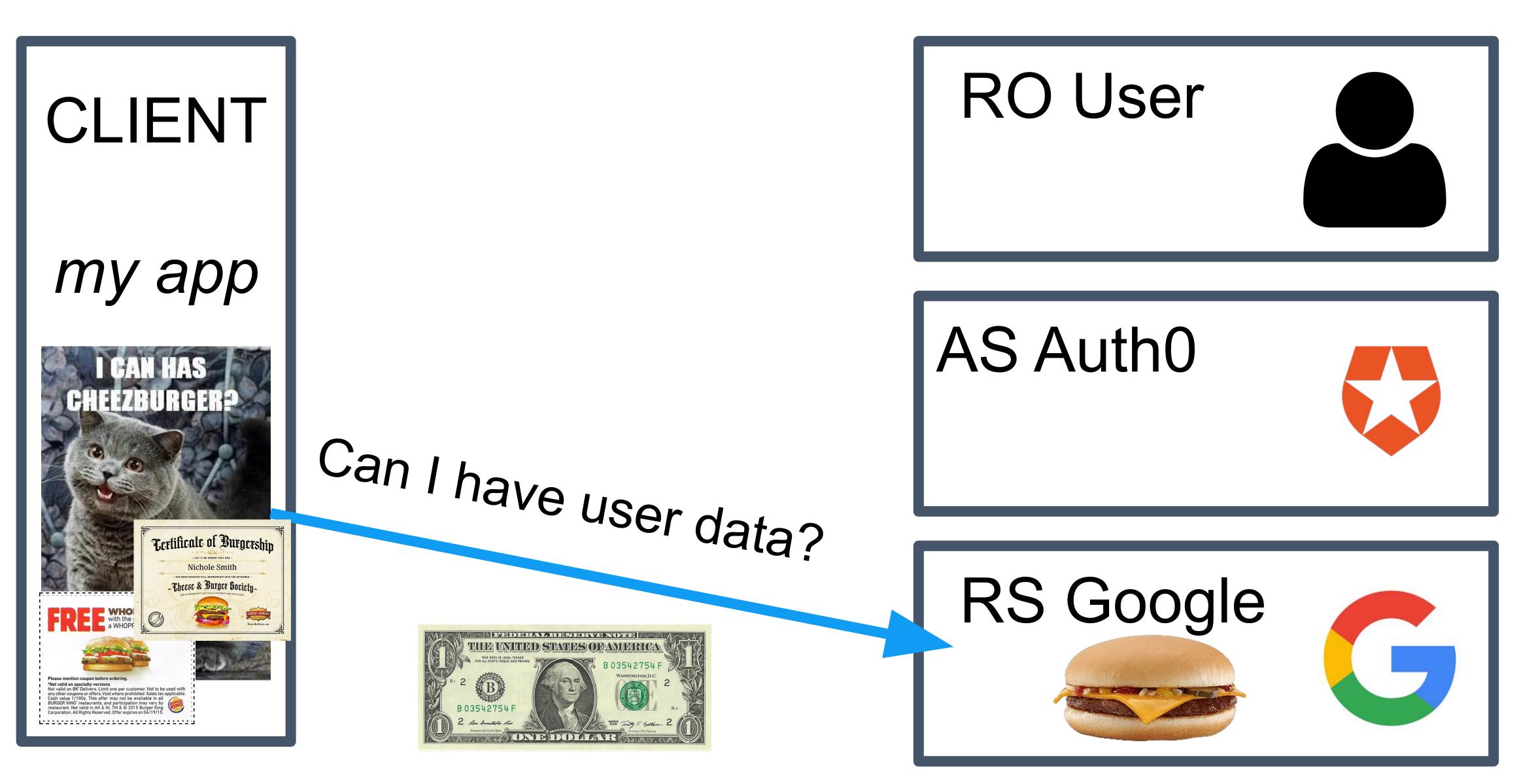


🥚 🔴 🔴

HTTP/1.1 200 OK Content-Type: application/json Cache-Control: no-store Pragma: no-cache

"access_token":"LSDLFJSDFKLK123", "token_type":"bearer", "expires_in":3600, "refresh_token":"DSLFSLKDF12321",

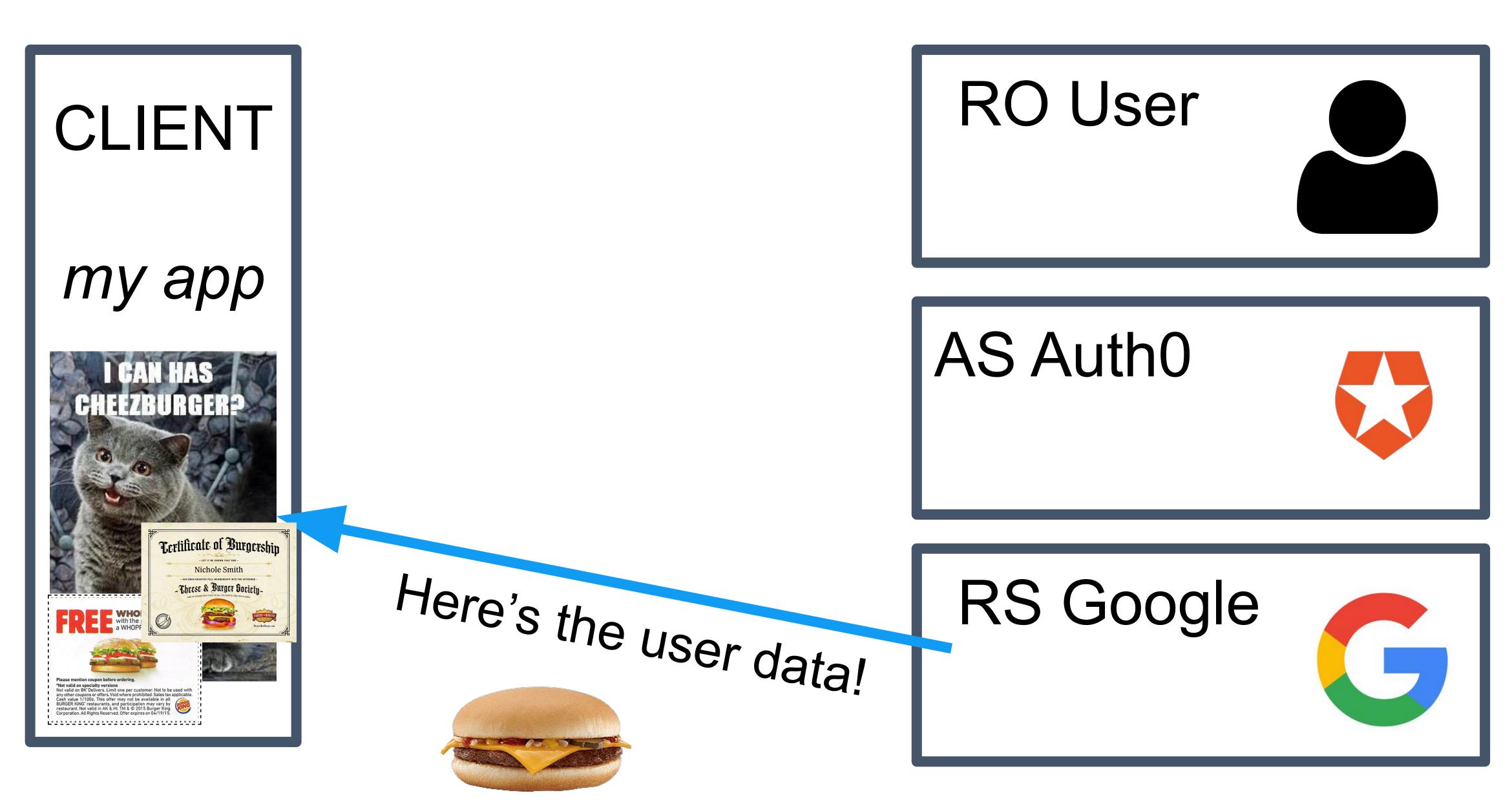
"id_token": "eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJzdWIiOiIxMjM0NTY30DkwIiwibmFtZSI6Ikpva G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ. SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c"





POST /user/123 HTTP/1.1 Host: google.com

Authorization: Bearer asdasdlq323342"



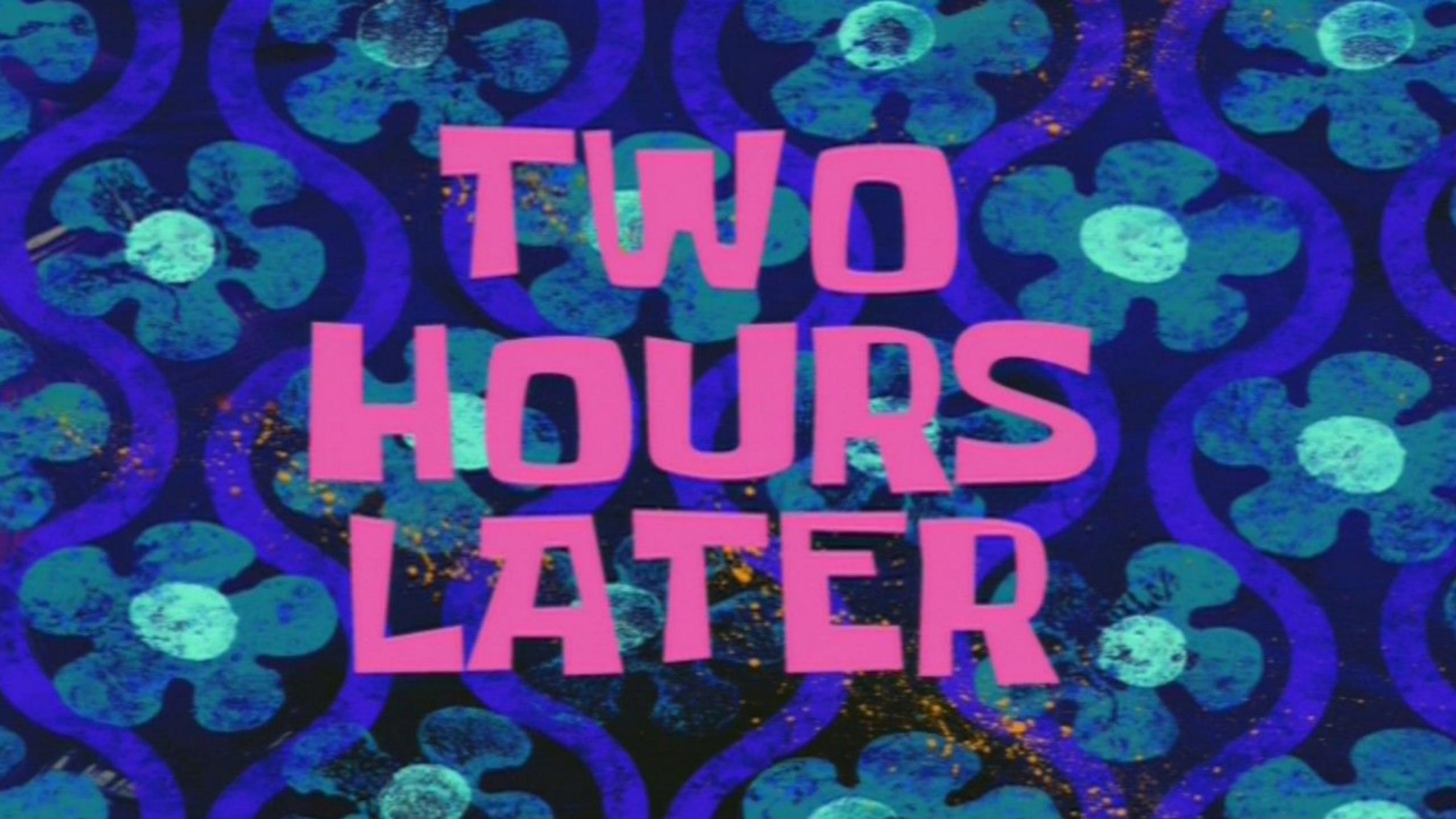
```
.
  "displayName": "Stephanie Chamblee",
  "id": _____
  "user_id": "______
  "name": {
    "familyName": "Chamblee",
    "givenName": "Stephanie"
  },
  "emails": [
      "value": "stephaniejoychamblee@gmail.com"
  ],
  "locale": "en",
  "nickname": "stephaniejoychamblee"
ി
```

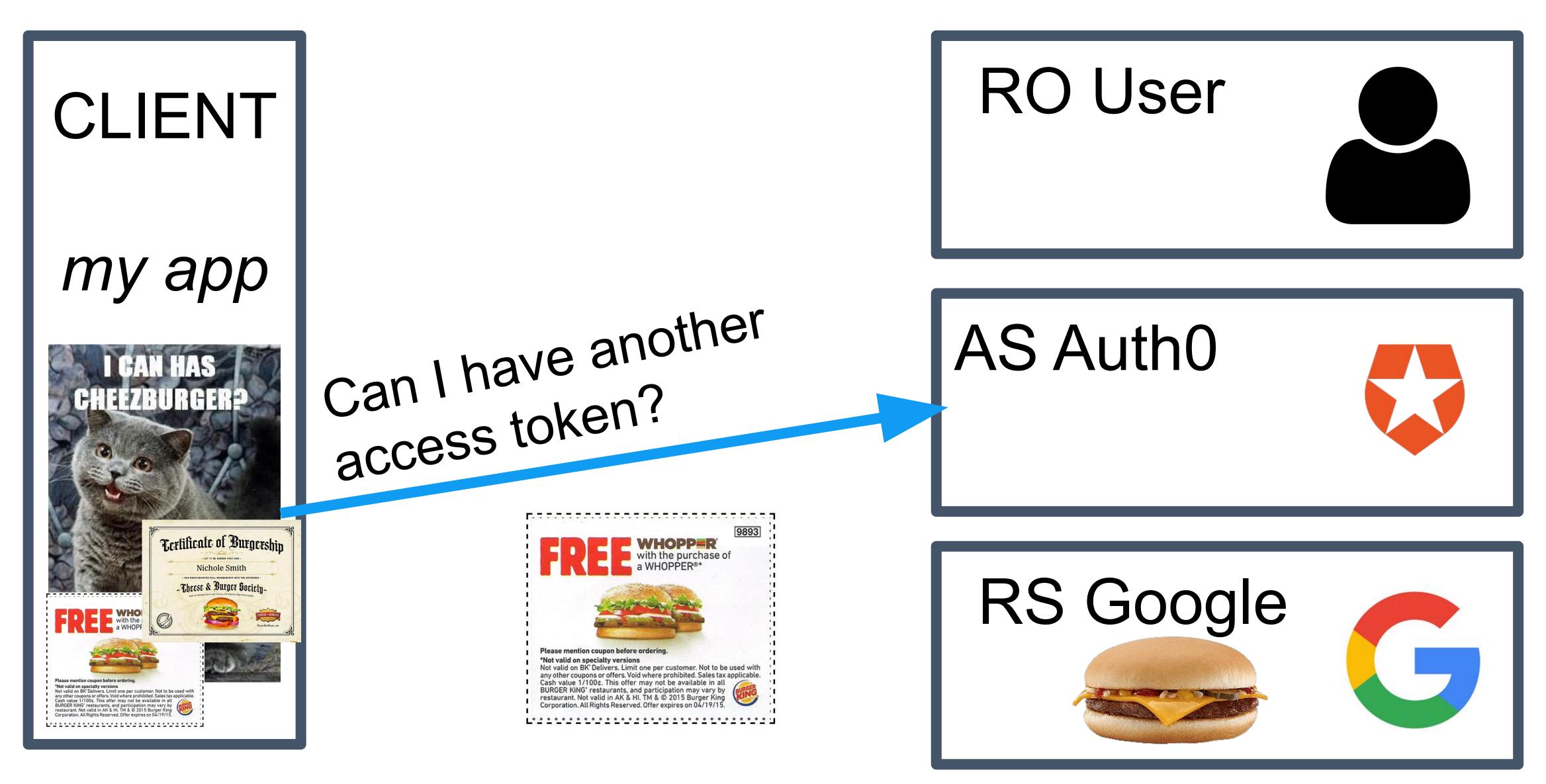
"picture": "https://lh3.googleusercontent.com/a-/AAuE7mDOBfvvtIJgdy7FqJecZ0bGjUhCqUWcX-_Jw833HA",







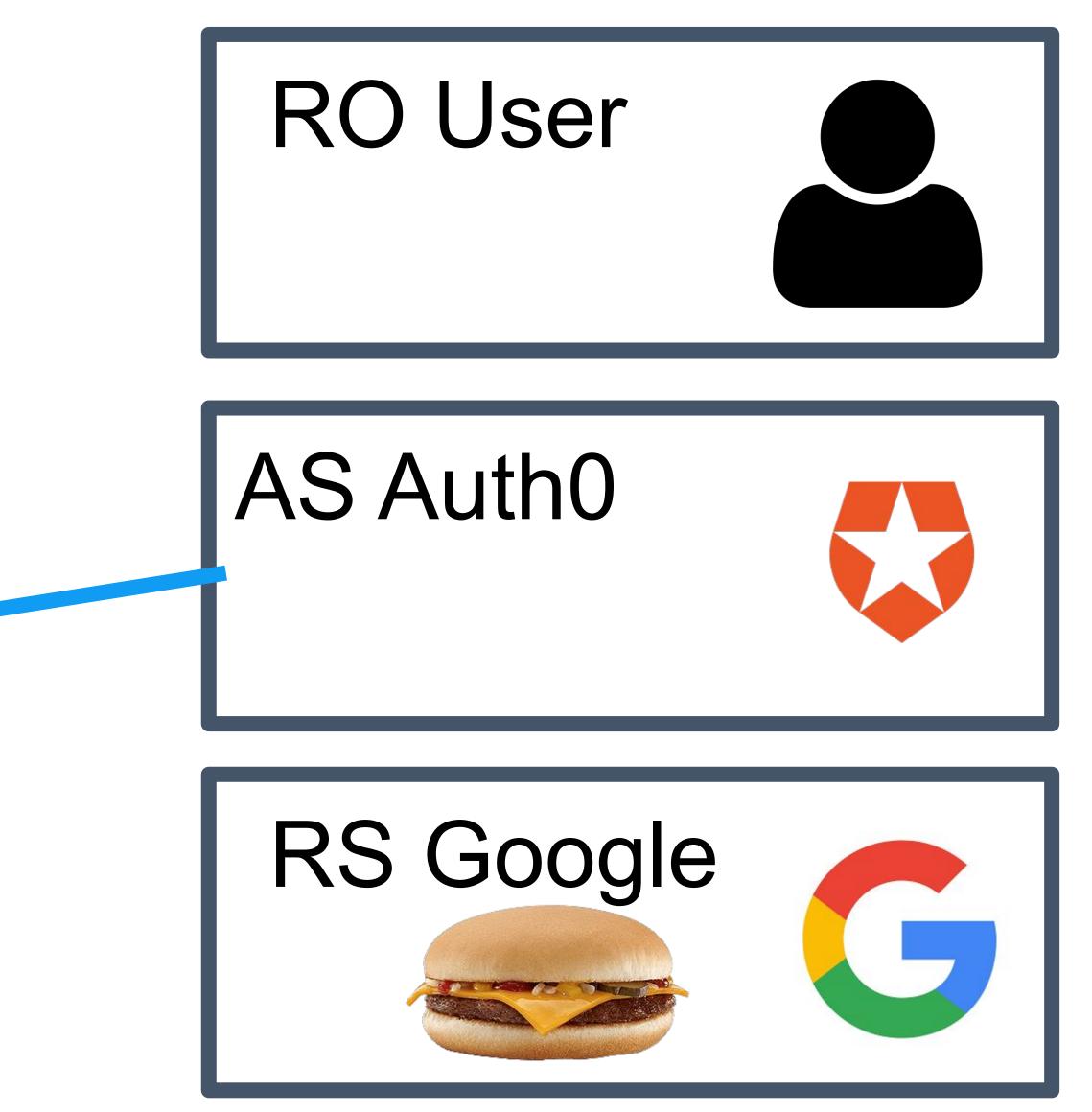


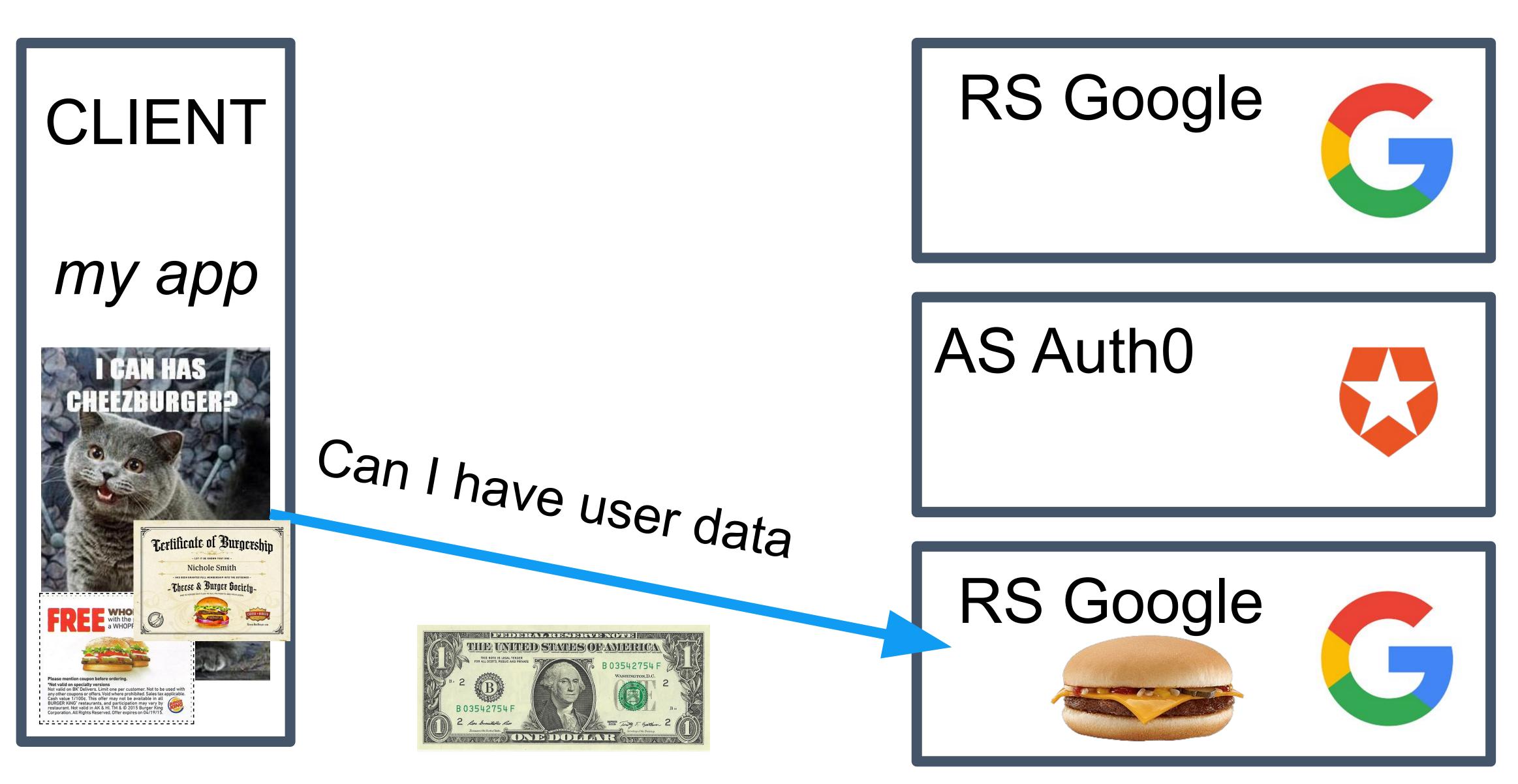




Here's another access token!



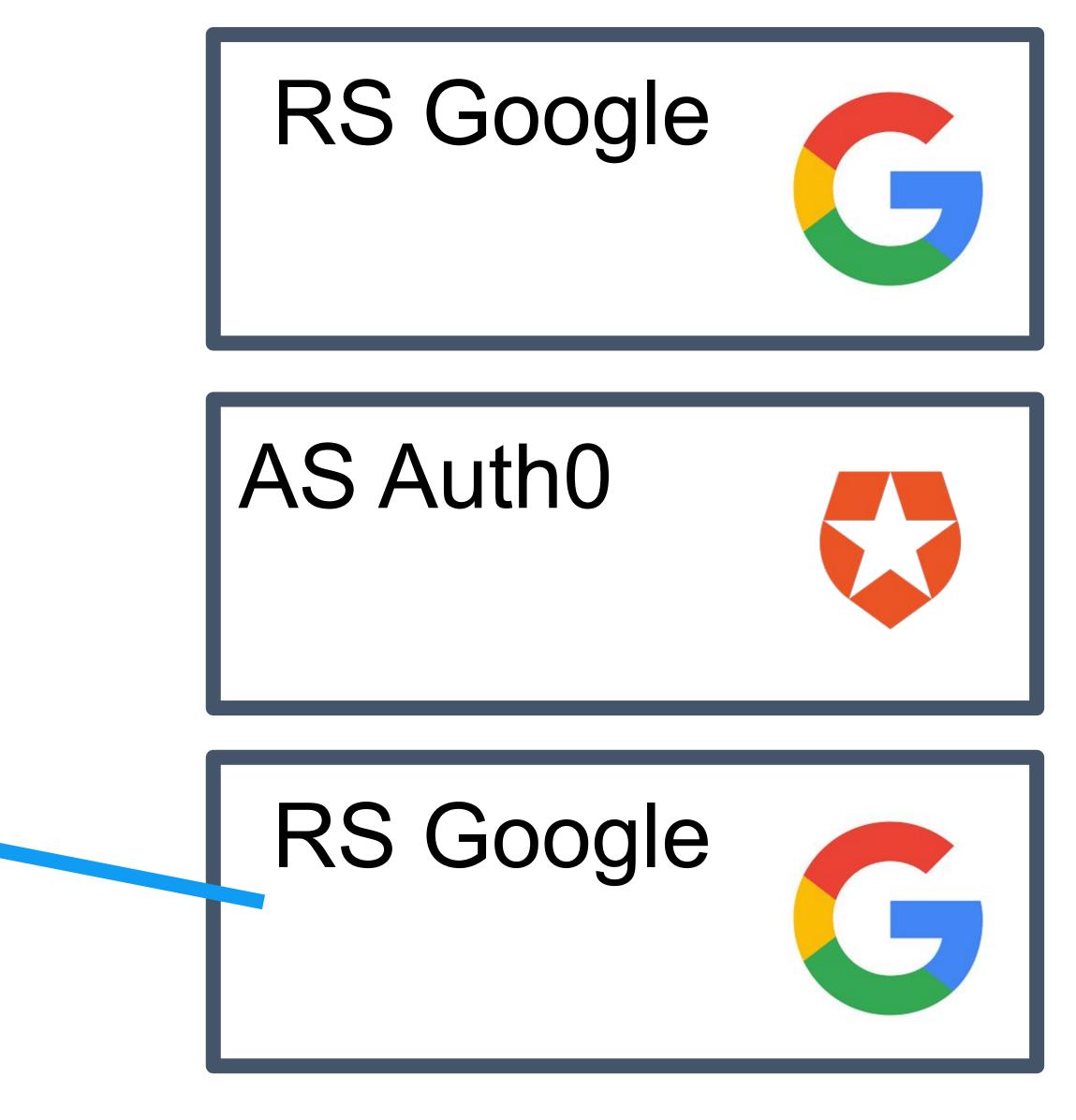
















Summary

CONTEXT Open Standards Brief History of Identity

FOUNDATION

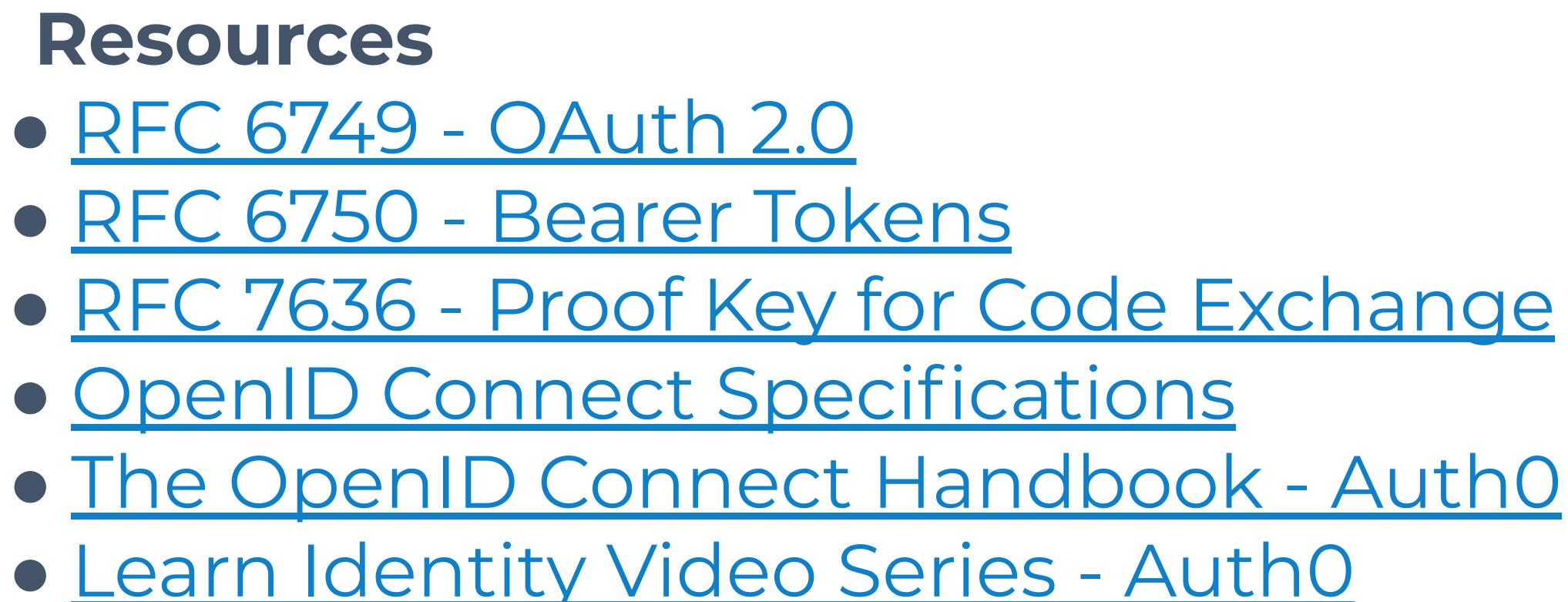
Four roles in OAuth

Tokens

1

Authorization Flows

OAUTH & OIDC AUTHORIZATION CODE FLOW OAuth 2.0 & OpenID Connect (OIDC) Walkthrough





Thanks

Stephanie Chamblee Østephchamblee

