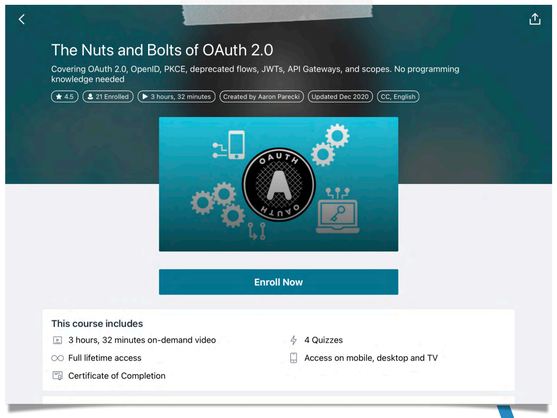
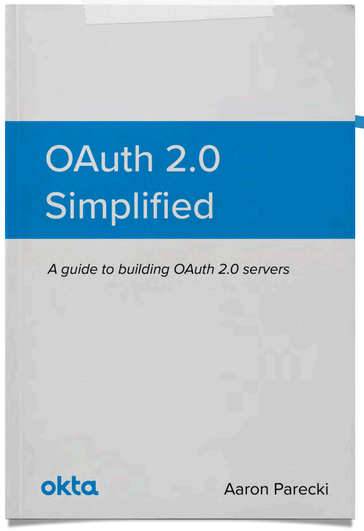
OAuth 2.0 and OpenID Connect

AARON PARECKI
@aaronpk
aaronpk.com





okta

IETF®

[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-parecki-oauth-v2-1) 00 01

OAuth Working Group — D. Hardt
Internet-Draft — SignIn.Org
Intended status: Standards Track — A. Parecki
Expires: 5 August 2021 — Okta
T. Lodderstedt
yes.com
1 February 2021

The OAuth 2.1 Authorization Framework
draft-ietf-oauth-v2-1-01

Abstract

The OAuth 2.1 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and an authorization service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 2.0 Authorization Framework described in RFC 6749.

[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-parecki-oauth-browser-based-apps)
00 01 02 03 04 05 06 07

Open Authentication Protocol — A. Parecki
Internet-Draft — Okta
Intended status: Best Current Practice — D. Waite
Expires: April 5, 2021 — Ping Identity
October 02, 2020

OAuth 2.0 for Browser-Based Apps
draft-ietf-oauth-browser-based-apps-07

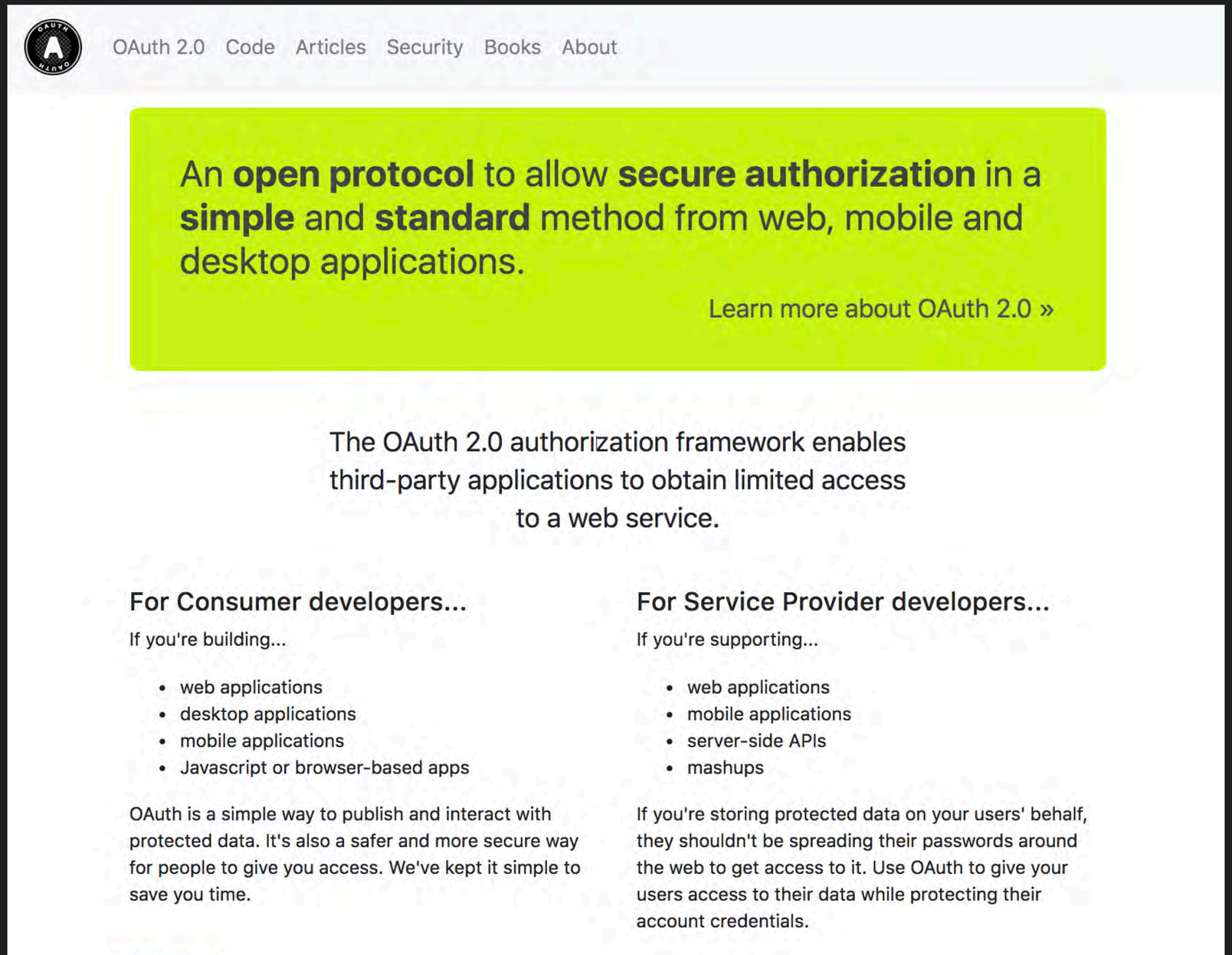
Abstract

This specification details the security considerations and best practices that must be taken into account when developing browser-based applications that use OAuth 2.0.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

oauth.net


OAuth 2.0
Code
Articles
Security
Books
About
An **open protocol** to allow **secure authorization** in a **simple** and **standard** method from web, mobile and desktop applications.
Learn more about OAuth 2.0 »
The OAuth 2.0 authorization framework enables third-party applications to obtain limited access to a web service.
For Consumer developers...
If you're building...
web applications
desktop applications
mobile applications
Javascript or browser-based apps
OAuth is a simple way to publish and interact with protected data. It's also a safer and more secure way for people to give you access. We've kept it simple to save you time.
For Service Provider developers...
If you're supporting...
web applications
mobile applications
server-side APIs
mashups
If you're storing protected data on your users' behalf, they shouldn't be spreading their passwords around the web to get access to it. Use OAuth to give your users access to their data while protecting their account credentials.

WHY OAUTH?

Updated by: 8252 PROPOSED STANDARD
Errata Exist
Internet Engineering Task Force (IETF) D. Hardt, Ed.
Request for Comments: 6749 Microsoft
Obsoletes: 5849 October 2012
Category: Standards Track
ISSN: 2070-1721

The OAuth 2.0 Authorization Framework

Abstract

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849.

Status of This Memo

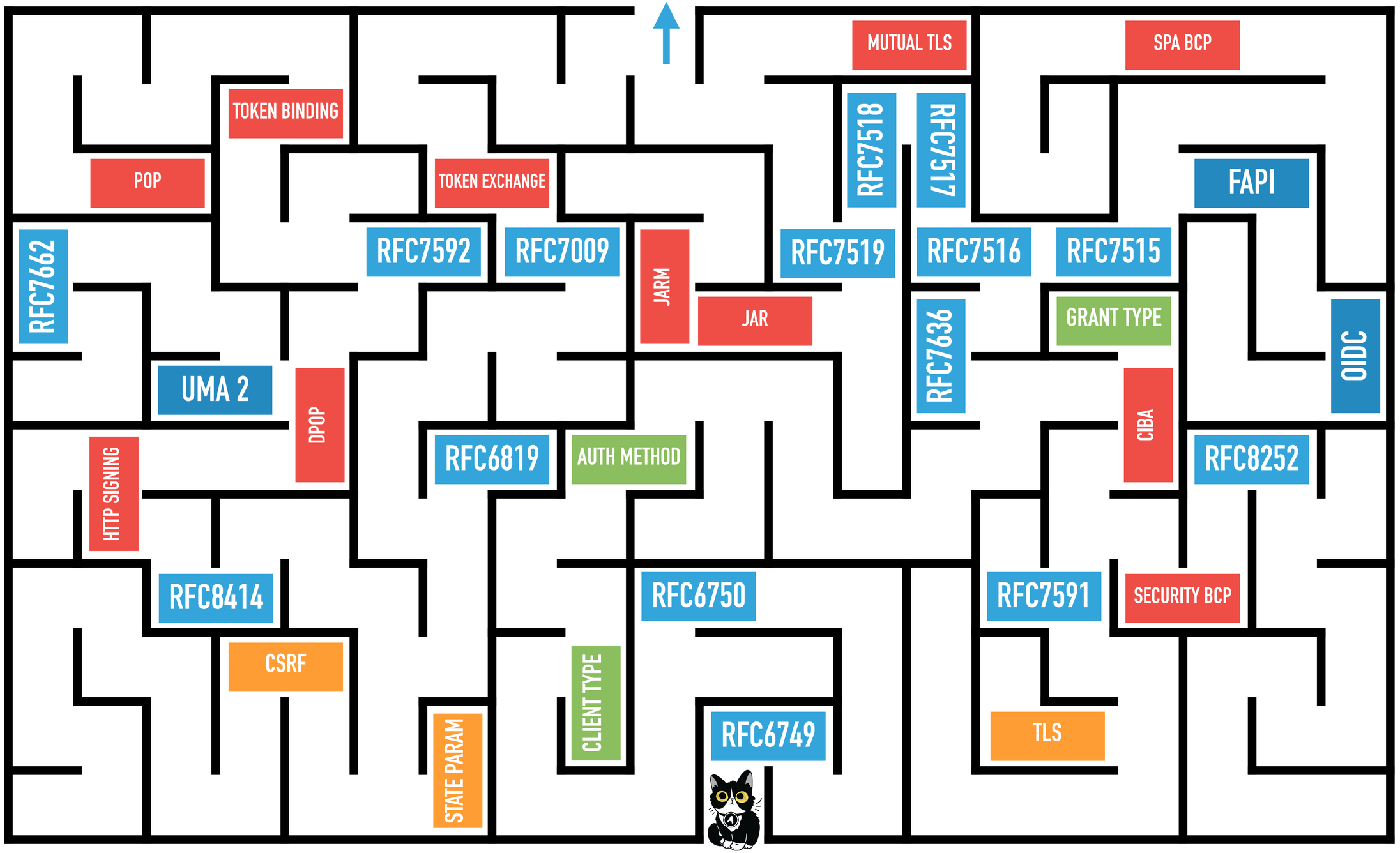
This is an Internet Standards Track document.

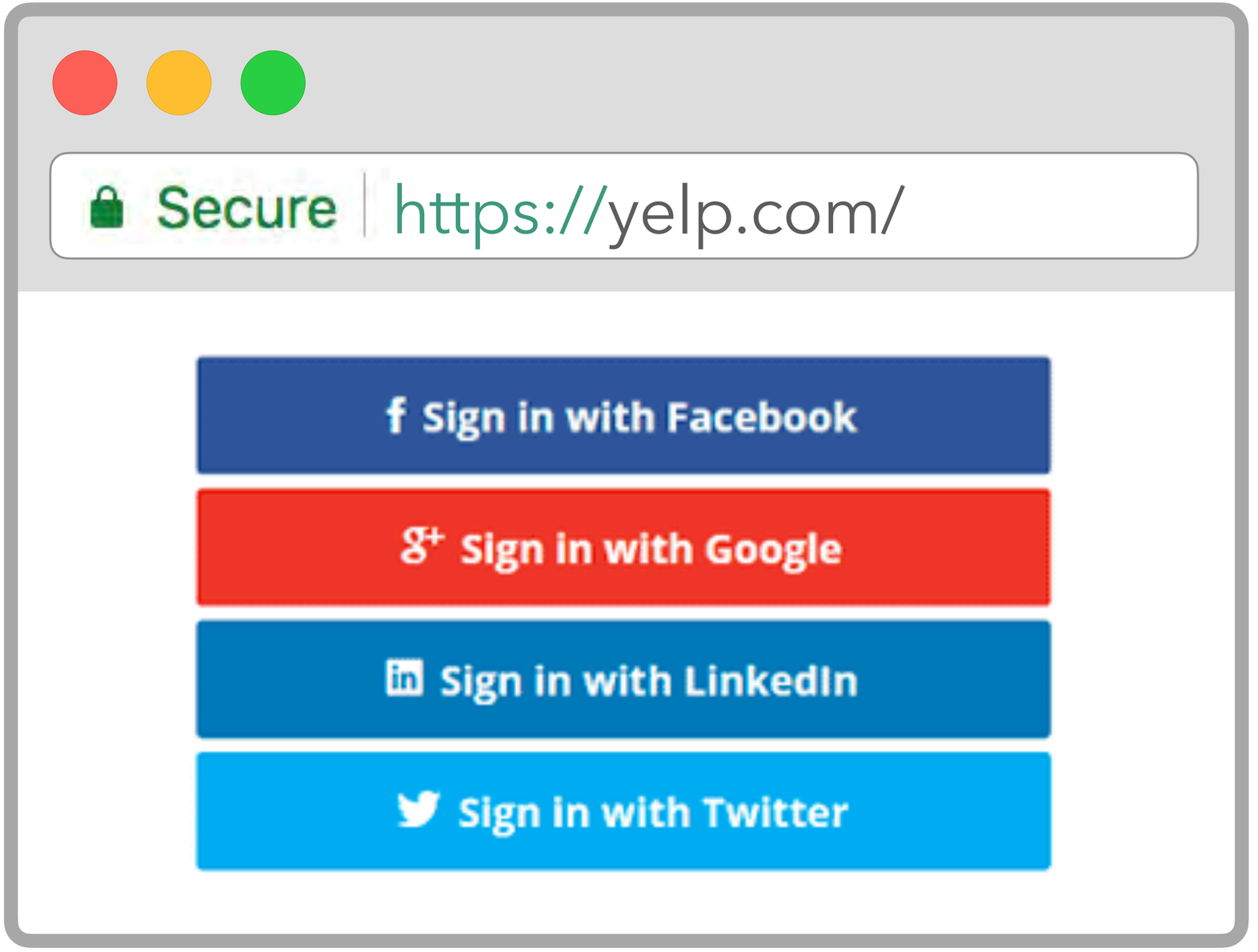
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6749.

Table of Contents

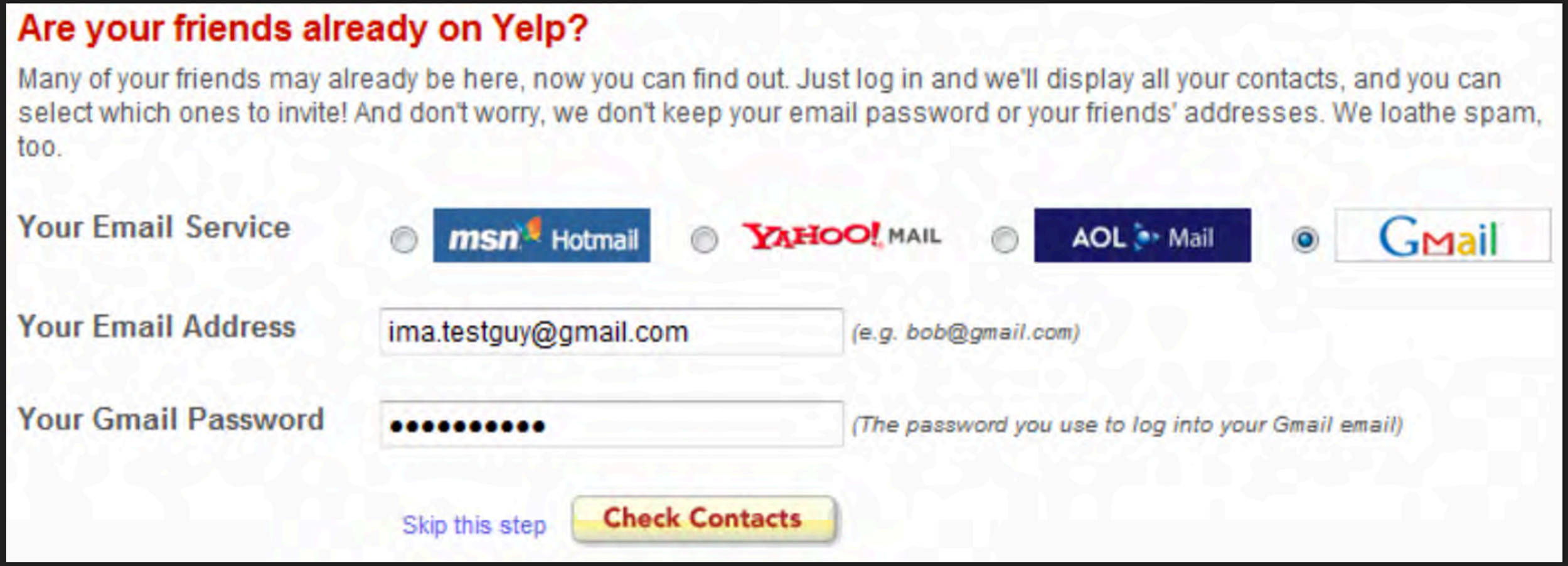
BUILDING YOUR APPLICATION




Secure
https://yelp.com/
Sign in with Facebook
Sign in with Google
Sign in with LinkedIn
Sign in with Twitter

LIMIT/DELEGATE ACCESS TO DATA

THE PASSWORD ANTI-PATTERN

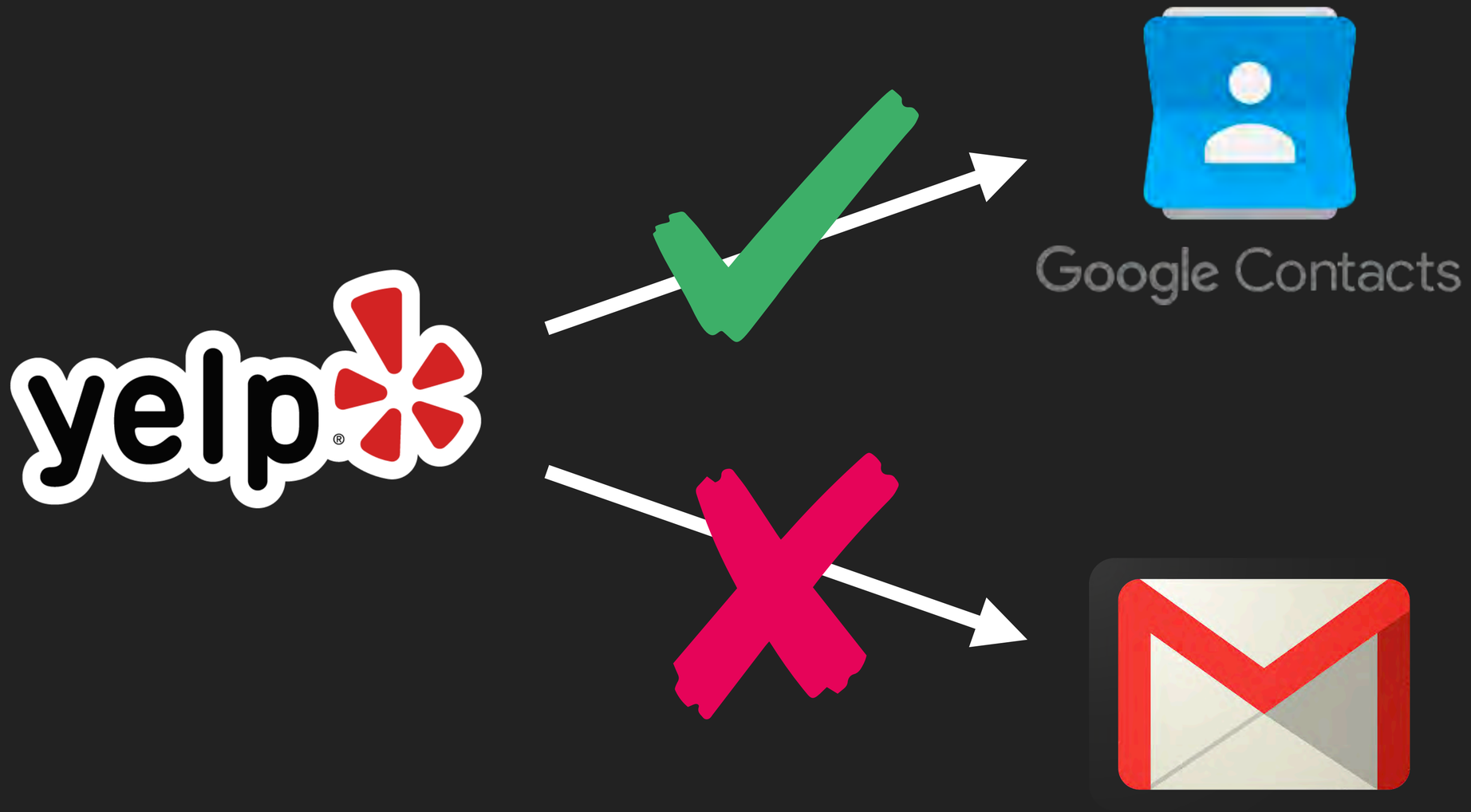


THE PASSWORD ANTI-PATTERN

facebook.com ~2010

WHY IS THIS BAD?

- Even though it only needs access to some data...
- You've given the app access to **all data**
- There's no way to revoke the app's access
- You place all your trust in the app


yelp
Google Contacts

so...

how can I let an app

access my data

without giving it my password?

Authorization Server

Access Token

Resource (API)

https://unsplash.com/photos/GJY1eAw6tn8

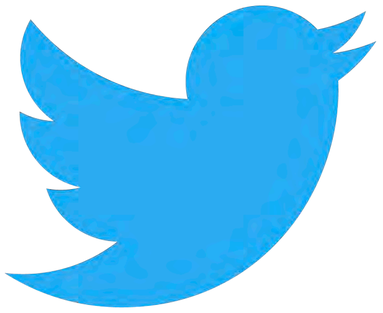

yelp


Google Contacts


last.fm

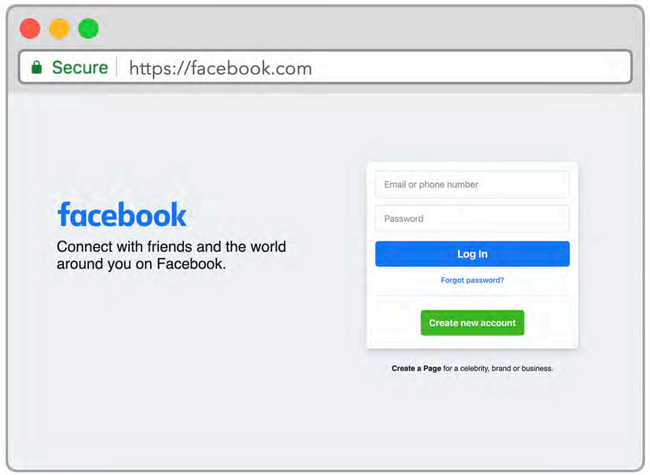

Spotify

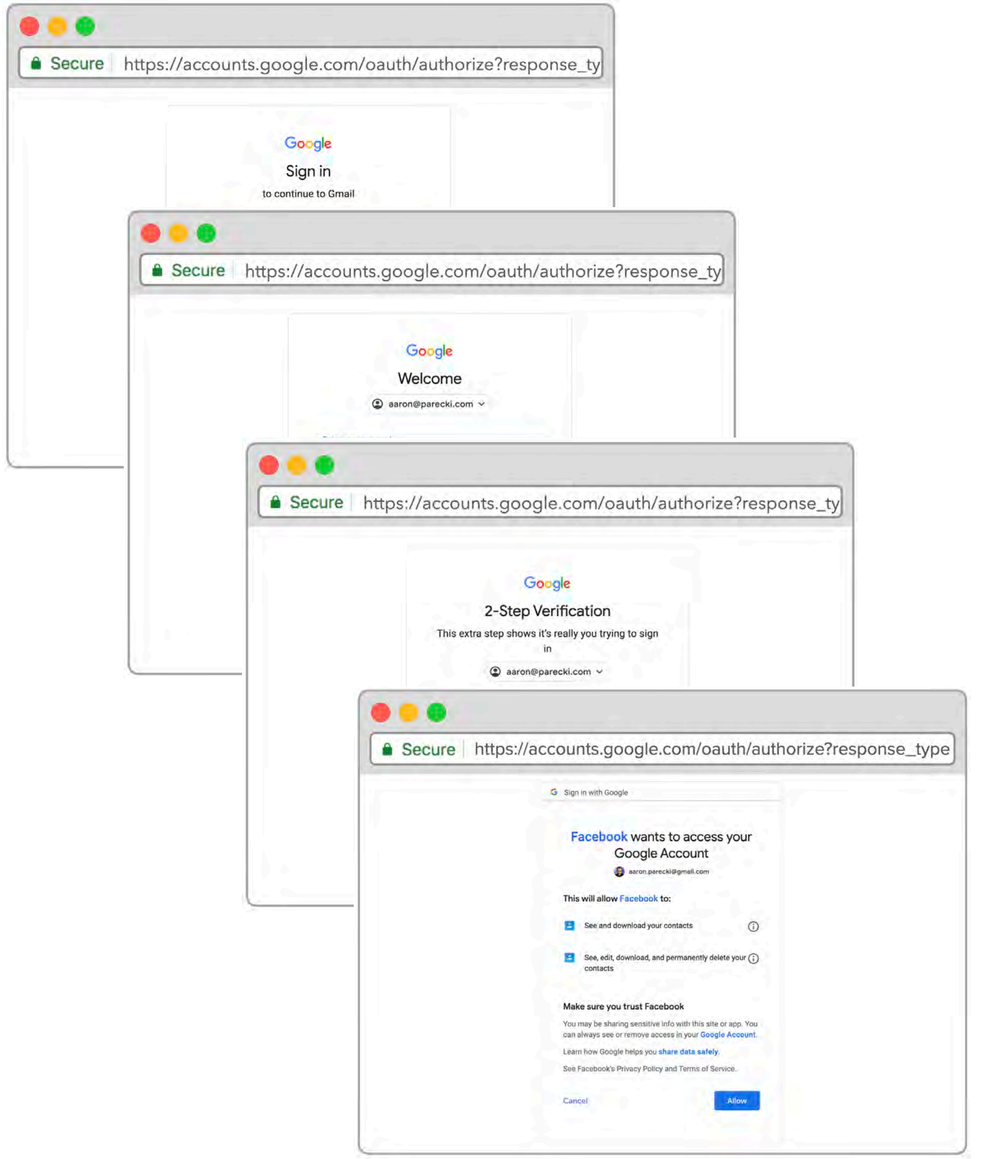

buffer

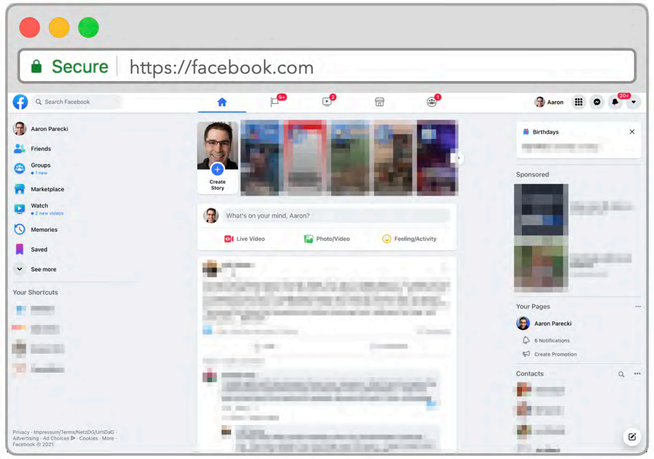


Application

OAuth Server







Sign in with Google

Facebook wants to access your Google Account

 aaron.parecki@gmail.com

This will allow Facebook to:

- See and download your contacts
- See, edit, download, and permanently delete your contacts

Make sure you trust Facebook

You may be sharing sensitive info with this site or app. You can always see or remove access in your **Google Account**.

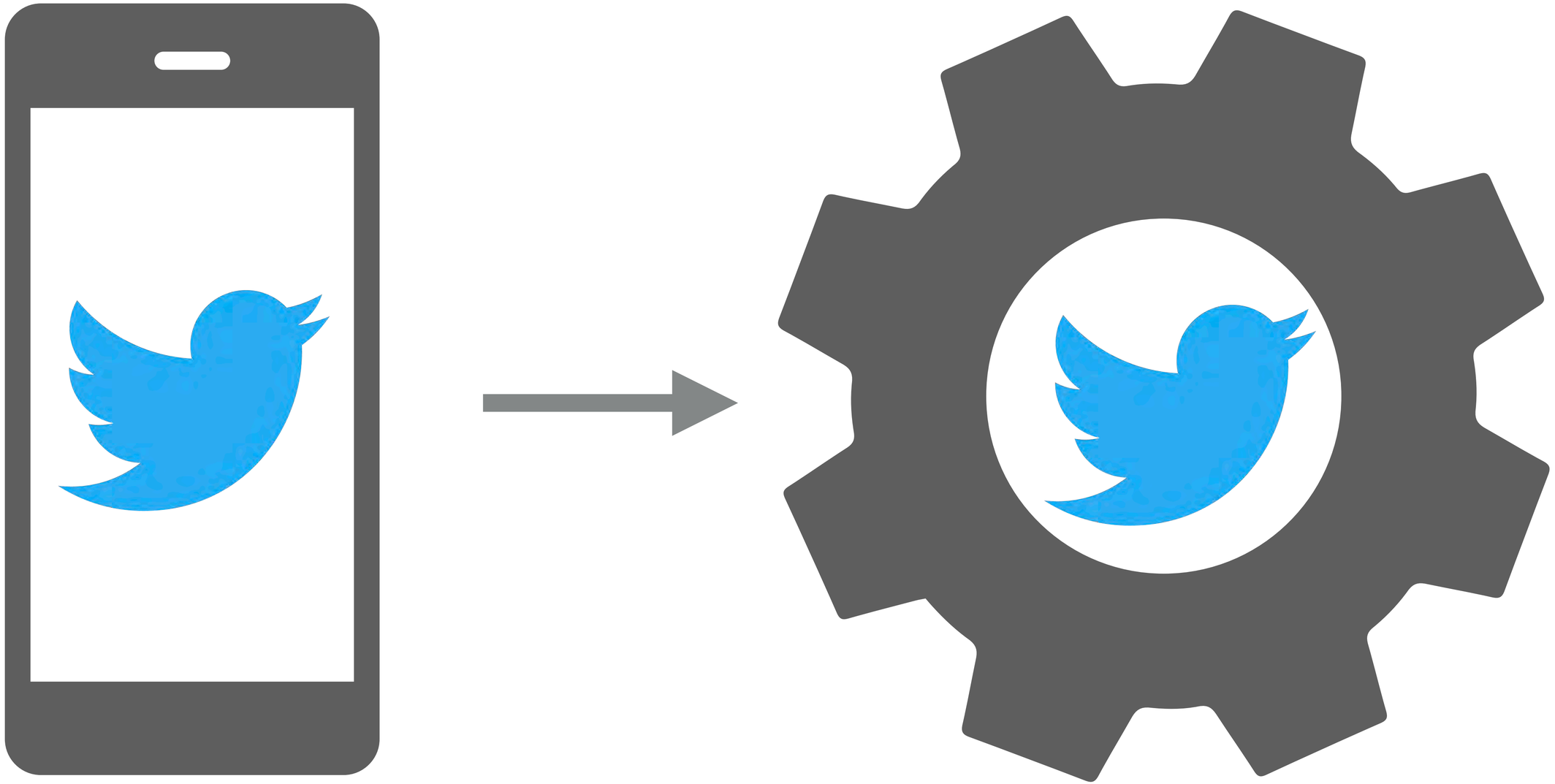
Learn how Google helps you **share data safely**.

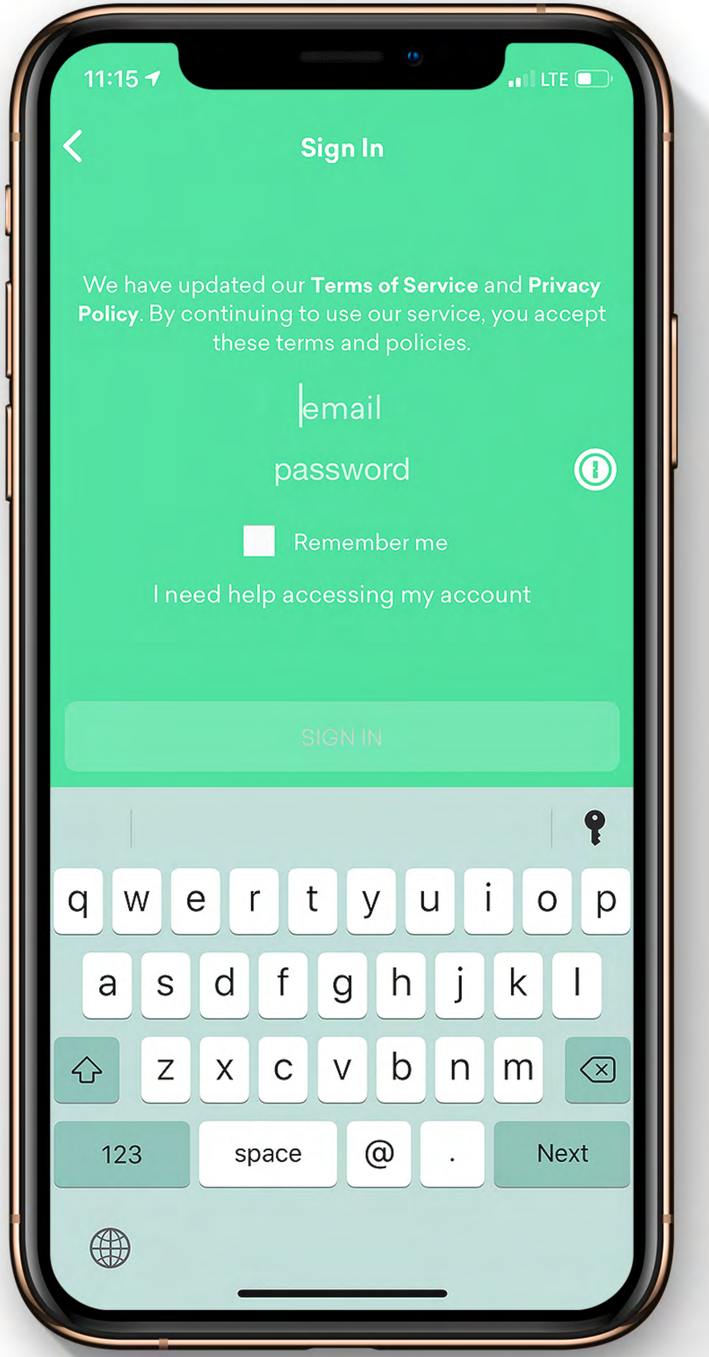
See Facebook's Privacy Policy and Terms of Service.

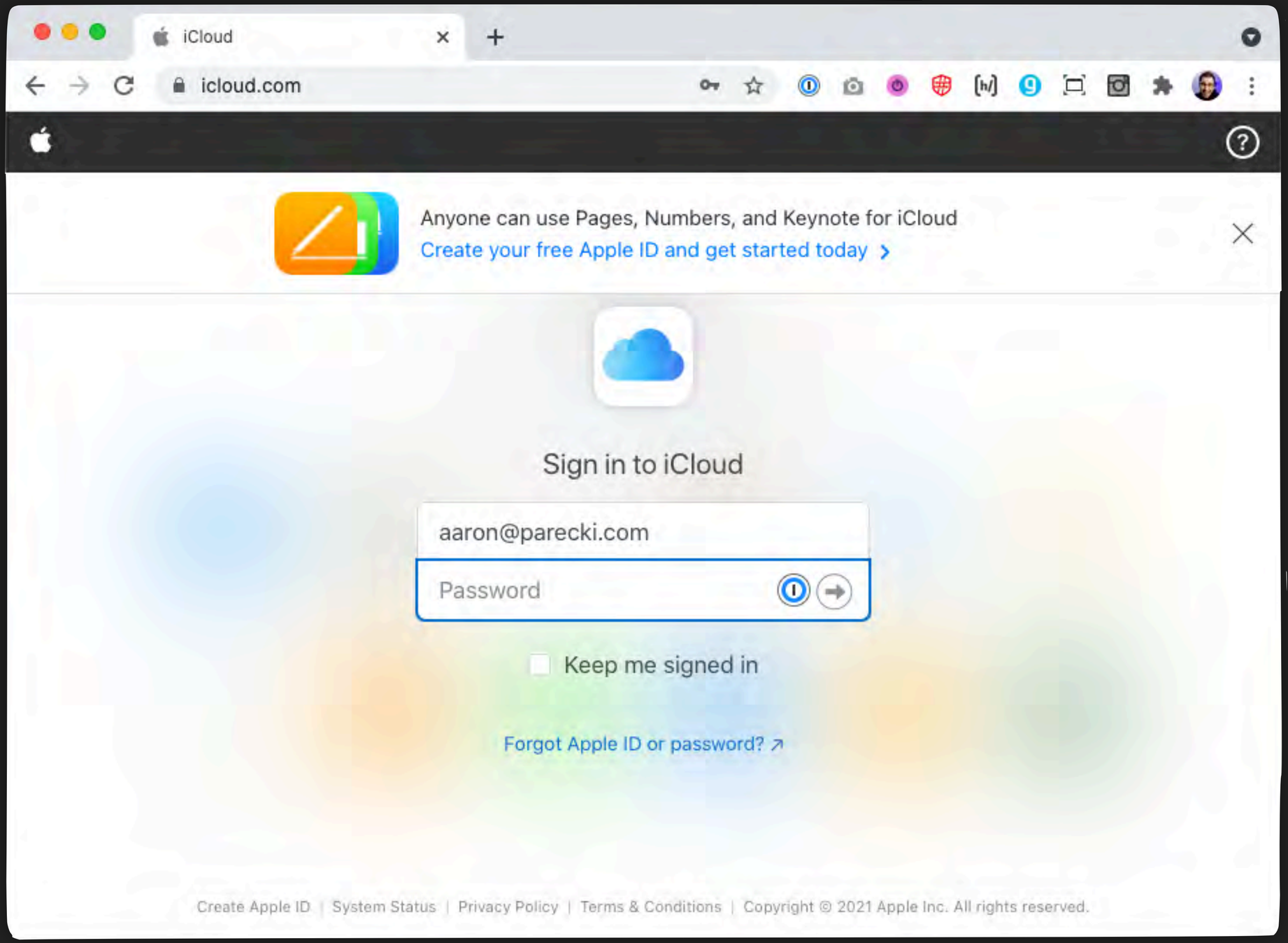
Cancel

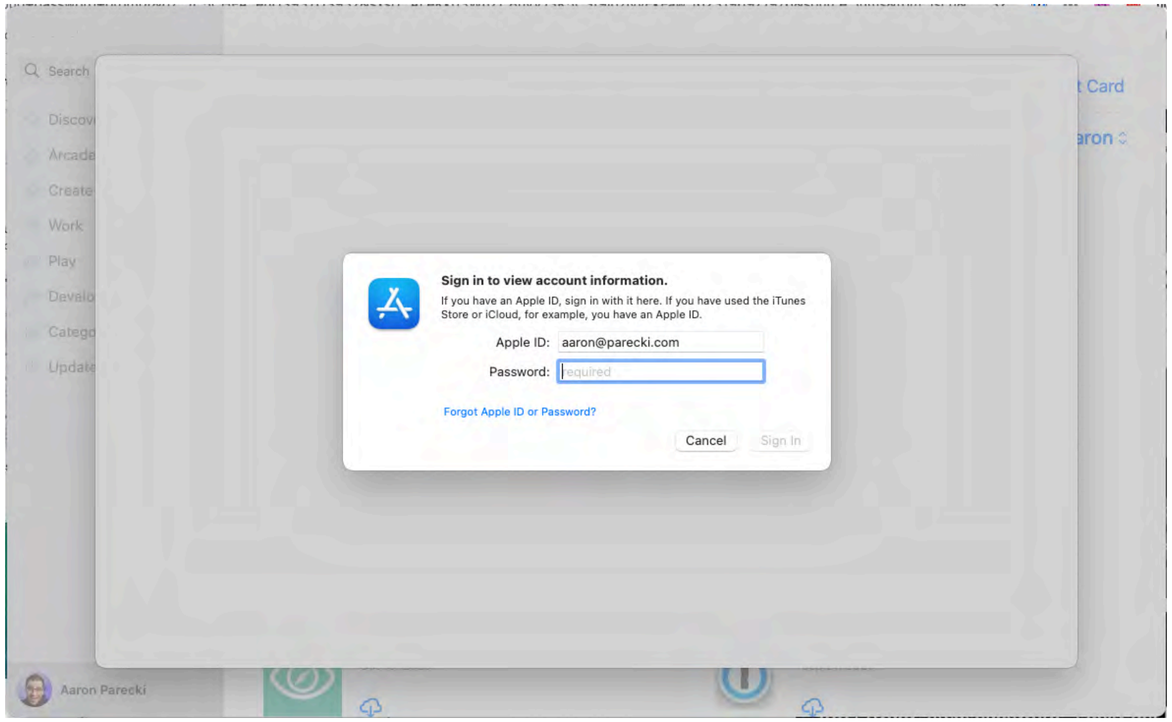
Allow

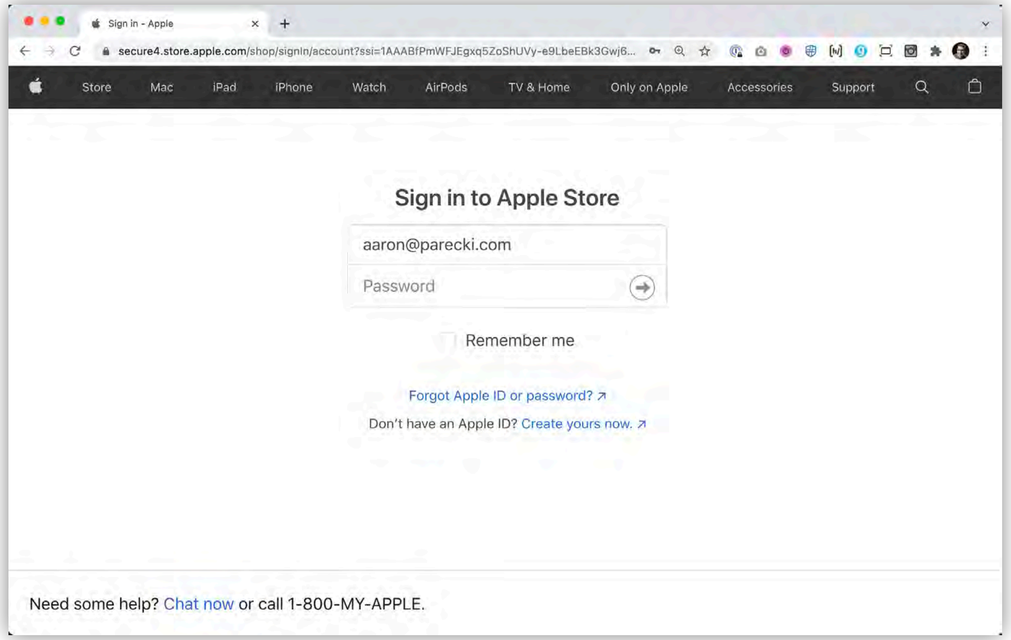
WHAT ABOUT FIRST PARTY APPS?

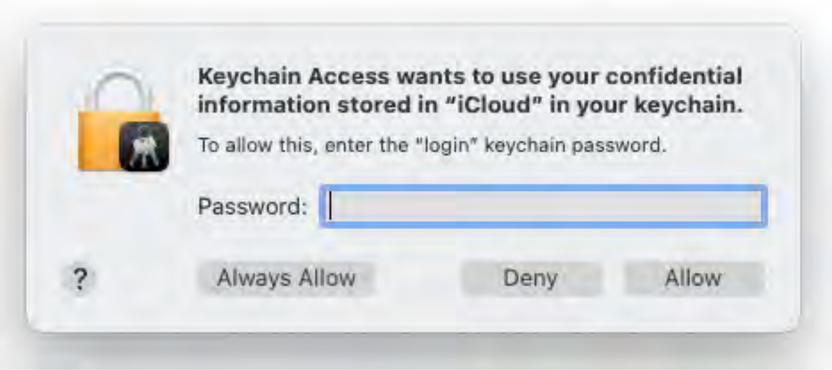


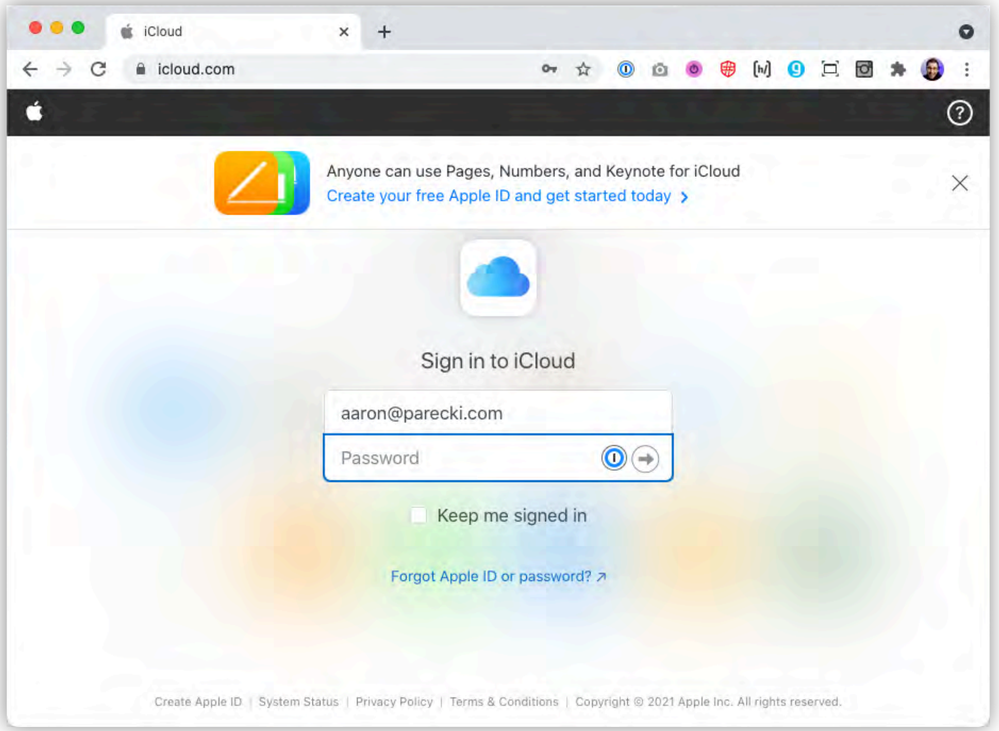

11:15
LTE
Sign In
We have updated our Terms of Service and Privacy Policy. By continuing to use our service, you accept these terms and policies.
email
password
Remember me
I need help accessing my account
SIGN IN
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
Next

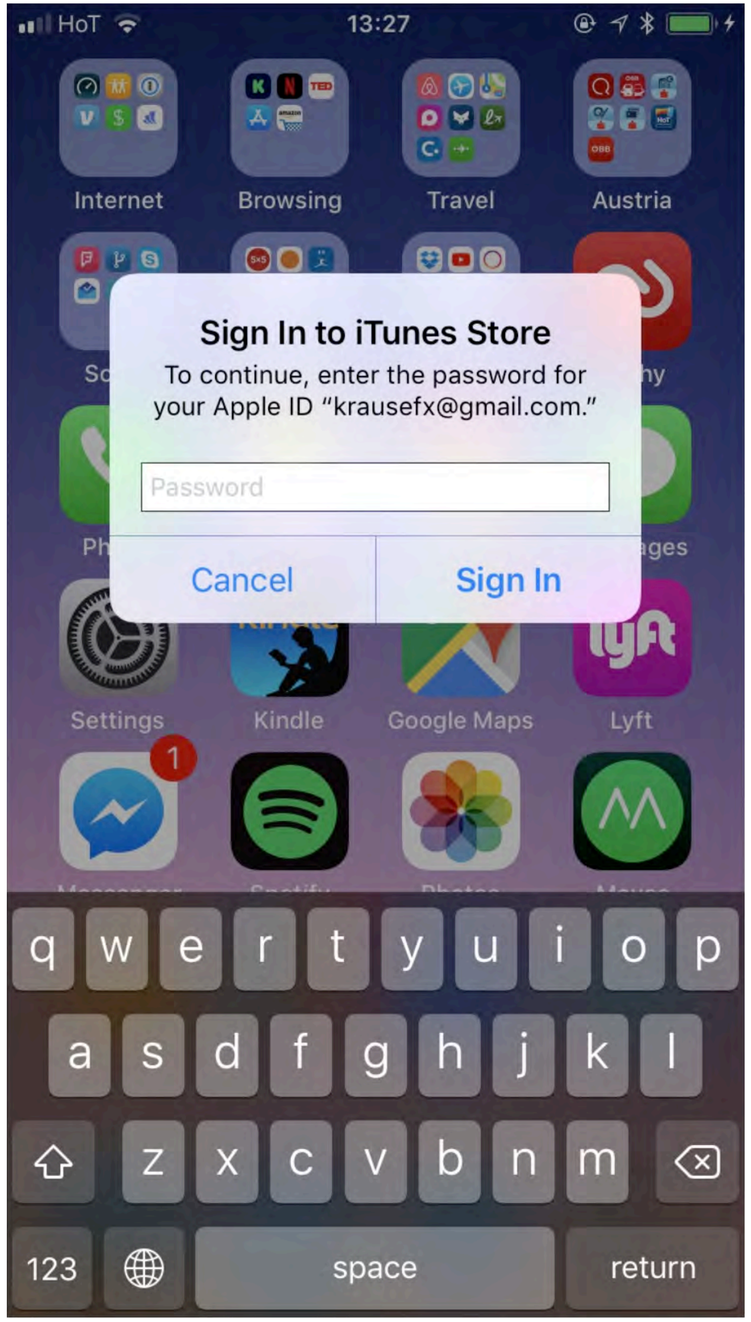

iCloud
icloud.com
Anyone can use Pages, Numbers, and Keynote for iCloud
Create your free Apple ID and get started today ›
Sign in to iCloud
aaron@parecki.com
Password
Keep me signed in
Forgot Apple ID or password? ↗
Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2021 Apple Inc. All rights reserved.

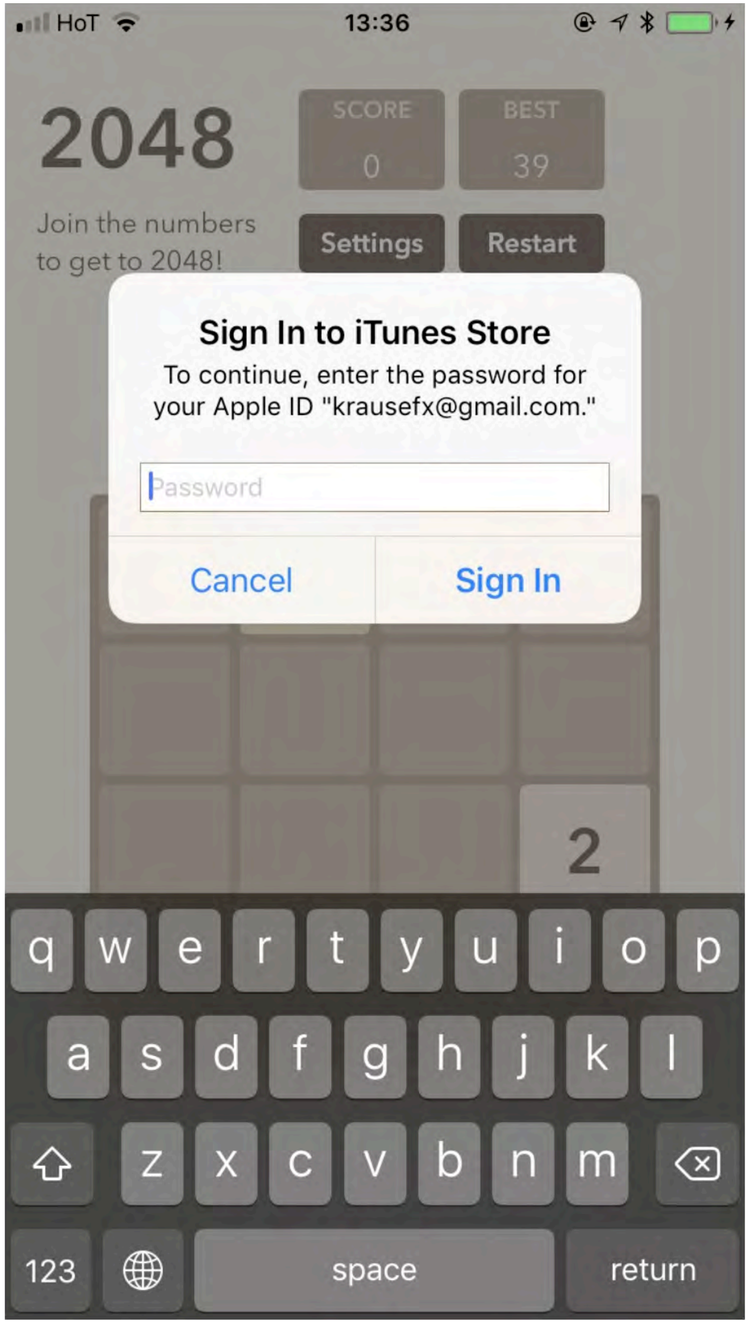

Search
Sign in to view account information.
If you have an Apple ID, sign in with it here. If you have used the iTunes Store or iCloud, for example, you have an Apple ID.
Apple ID: aaron@parecki.com
Password: required
Forgot Apple ID or Password?
Cancel
Sign In
Aaron Parecki


Sign in - Apple
secure4.store.apple.com/shop/signIn/account?ssi=1AAABfPmWFJEgxq5ZoShUVy-e9LbeEBk3Gwj6...
Store
Mac
iPad
iPhone
Watch
AirPods
TV & Home
Only on Apple
Accessories
Support
Sign in to Apple Store
aaron@parecki.com
Password
Remember me
Forgot Apple ID or password?
Don't have an Apple ID? Create yours now.
Need some help? Chat now or call 1-800-MY-APPLE.

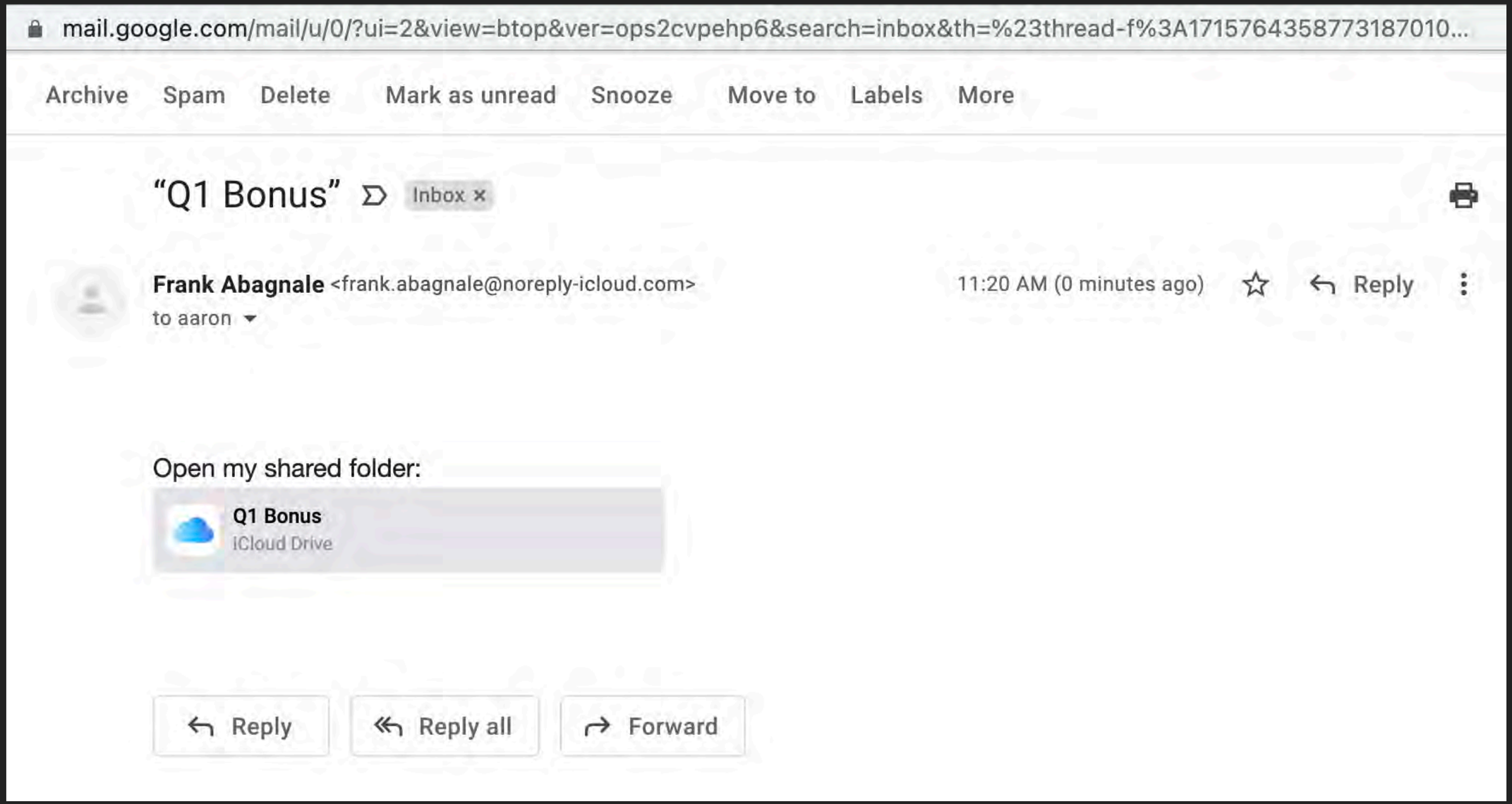

Keychain Access wants to use your confidential information stored in "iCloud" in your keychain.
To allow this, enter the "login" keychain password.
Password:
?
Always Allow
Deny
Allow

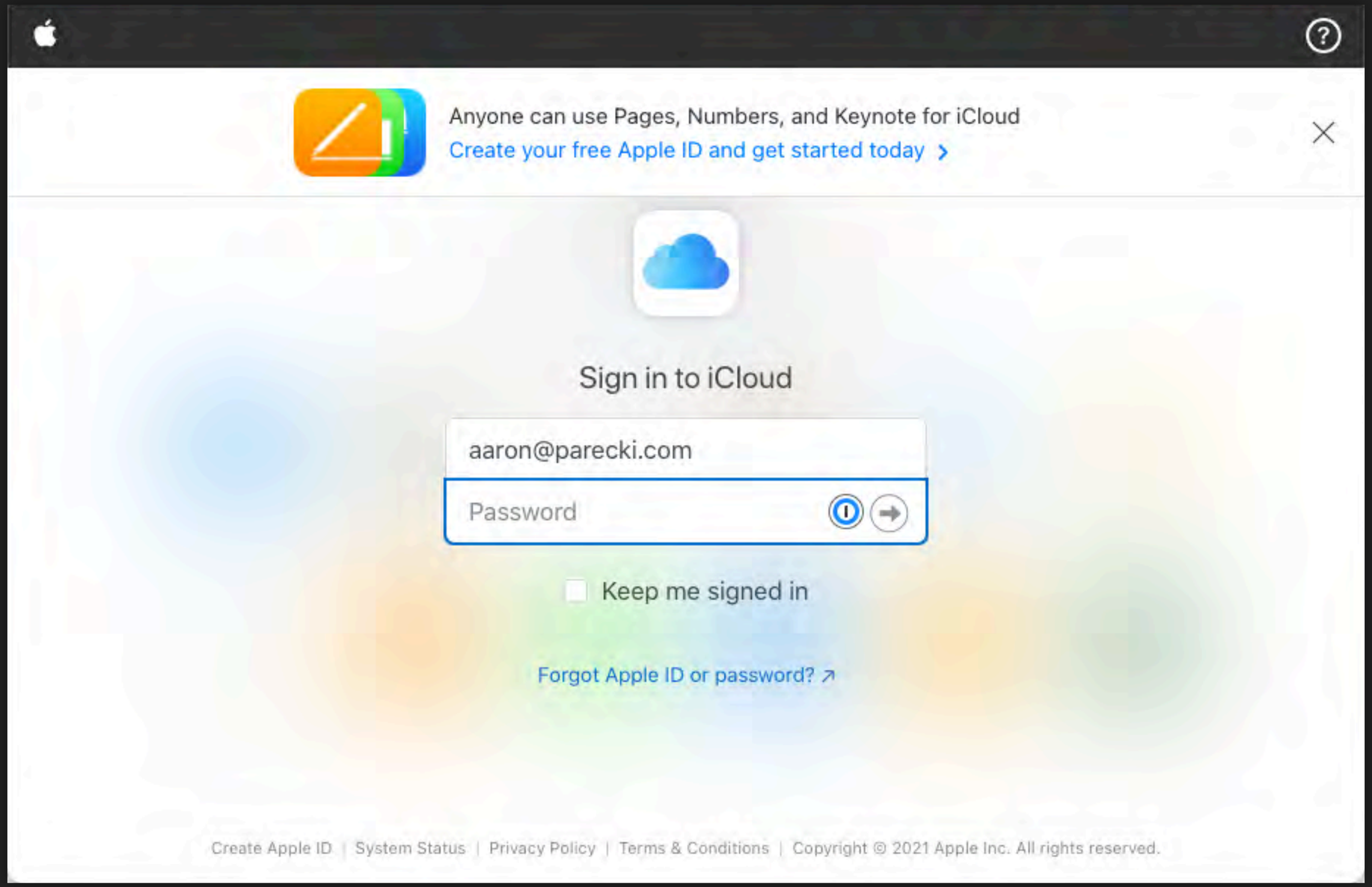

iCloud
icloud.com
Anyone can use Pages, Numbers, and Keynote for iCloud
Create your free Apple ID and get started today
Sign in to iCloud
aaron@parecki.com
Password
Keep me signed in
Forgot Apple ID or password?
Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2021 Apple Inc. All rights reserved.

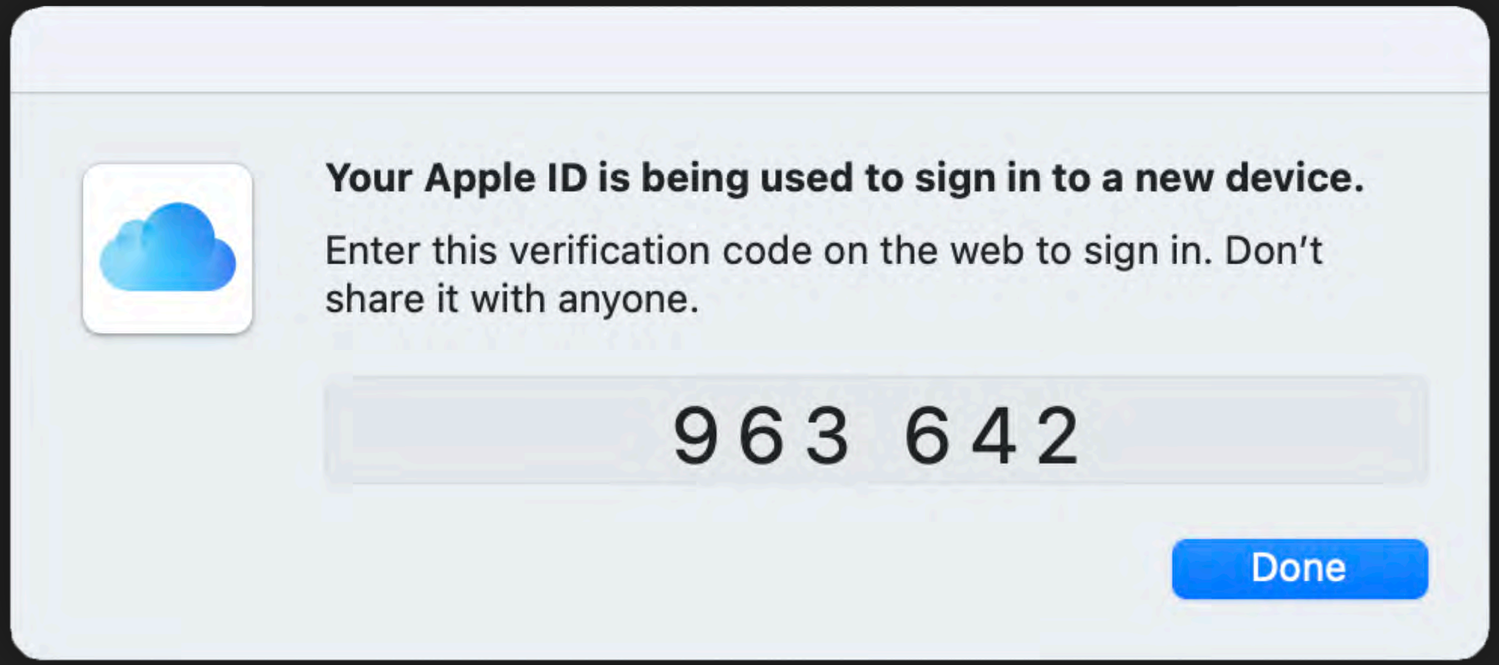




https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking


mail.google.com/mail/u/0/?ui=2&view=btop&ver=ops2cvpehp6&search=inbox&th=%23thread-f%3A1715764358773187010...
Archive
Spam
Delete
Mark as unread
Snooze
Move to
Labels
More
"Q1 Bonus"
Inbox ×
Frank Abagnale <frank.abagnale@noreply-icloud.com>
to aaron
11:20 AM (0 minutes ago)
Reply
Open my shared folder:
Q1 Bonus
iCloud Drive
Reply
Reply all
Forward


Anyone can use Pages, Numbers, and Keynote for iCloud
Create your free Apple ID and get started today ›
Sign in to iCloud
aaron@parecki.com
Password
Keep me signed in
Forgot Apple ID or password? ↗
Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2021 Apple Inc. All rights reserved.


Your Apple ID is being used to sign in to a new device.
Enter this verification code on the web to sign in. Don't share it with anyone.
963 642
Done

DOES MFA SOLVE THIS?

Phishable MFA

678328 is your Microsoft Azure verification code

Your Apple ID is being used to sign in to a new device.

Enter this verification code on the web to sign in. Don't share it with anyone.

963 642

Done

Google

Are you trying to sign in?

aaron@parecki.com

Device
Intel Mac OS X 10_15_7

Near
Düsseldorf, Germany

Time
Just now

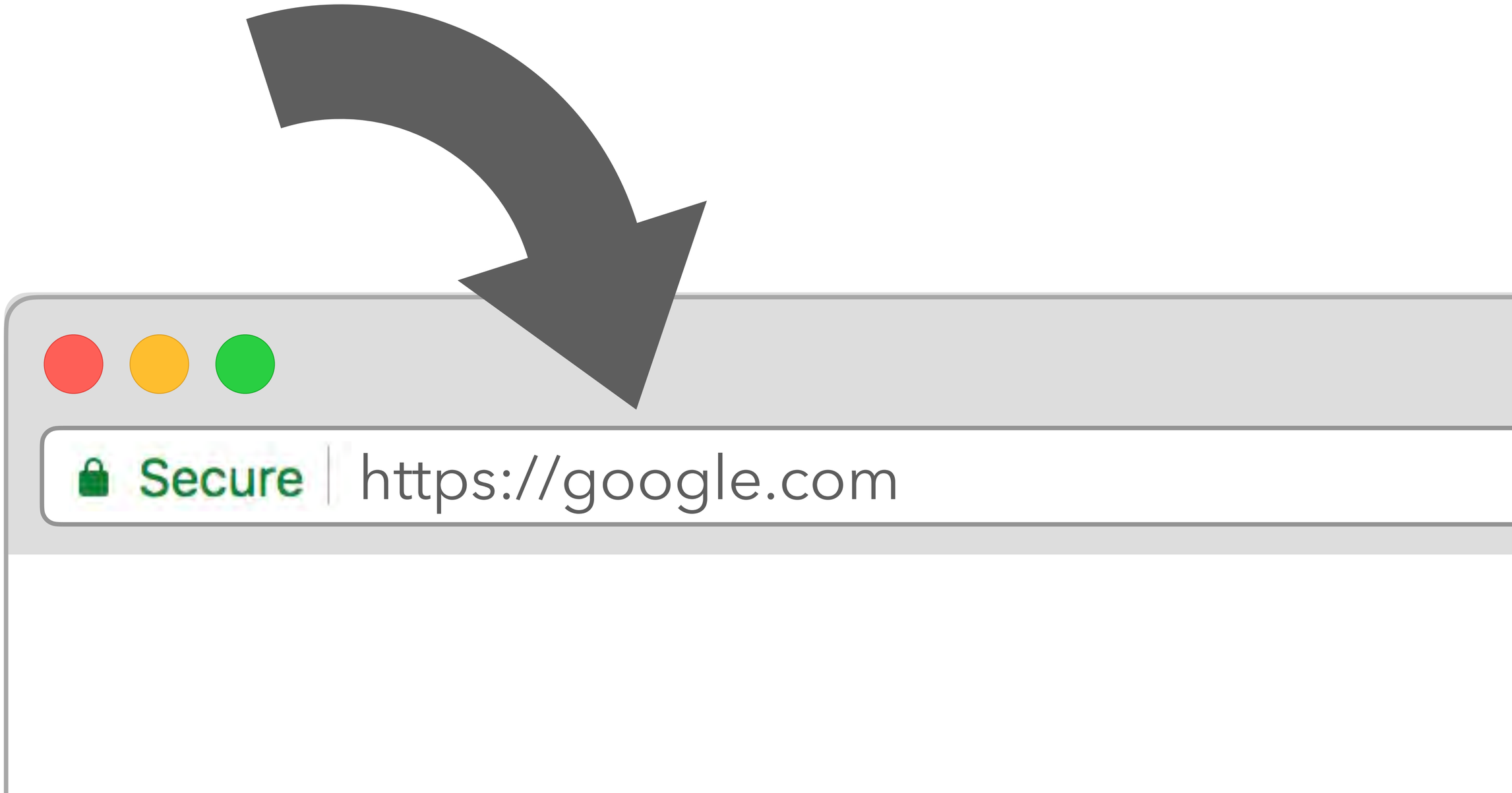
No, don't allow

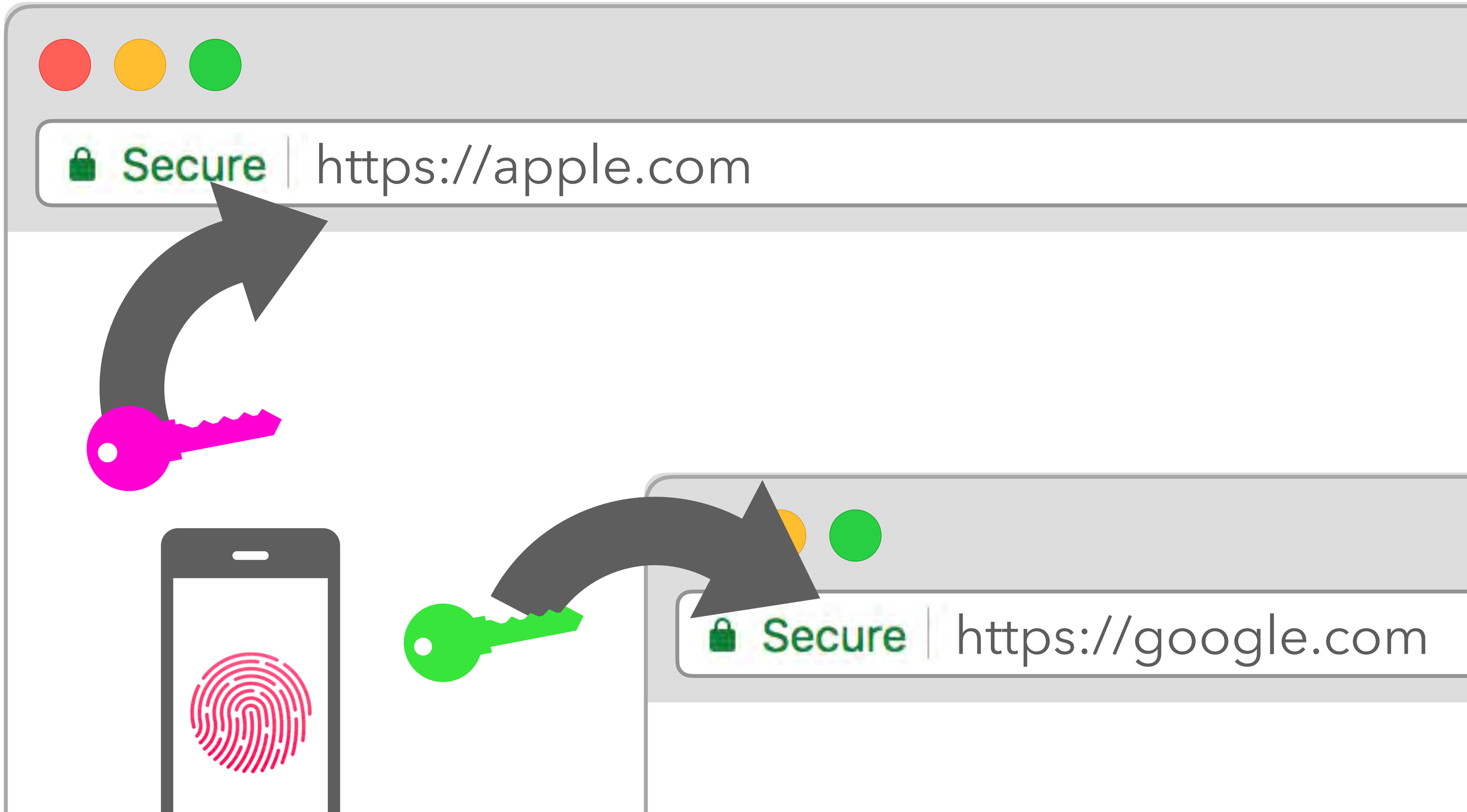
Yes, it's me

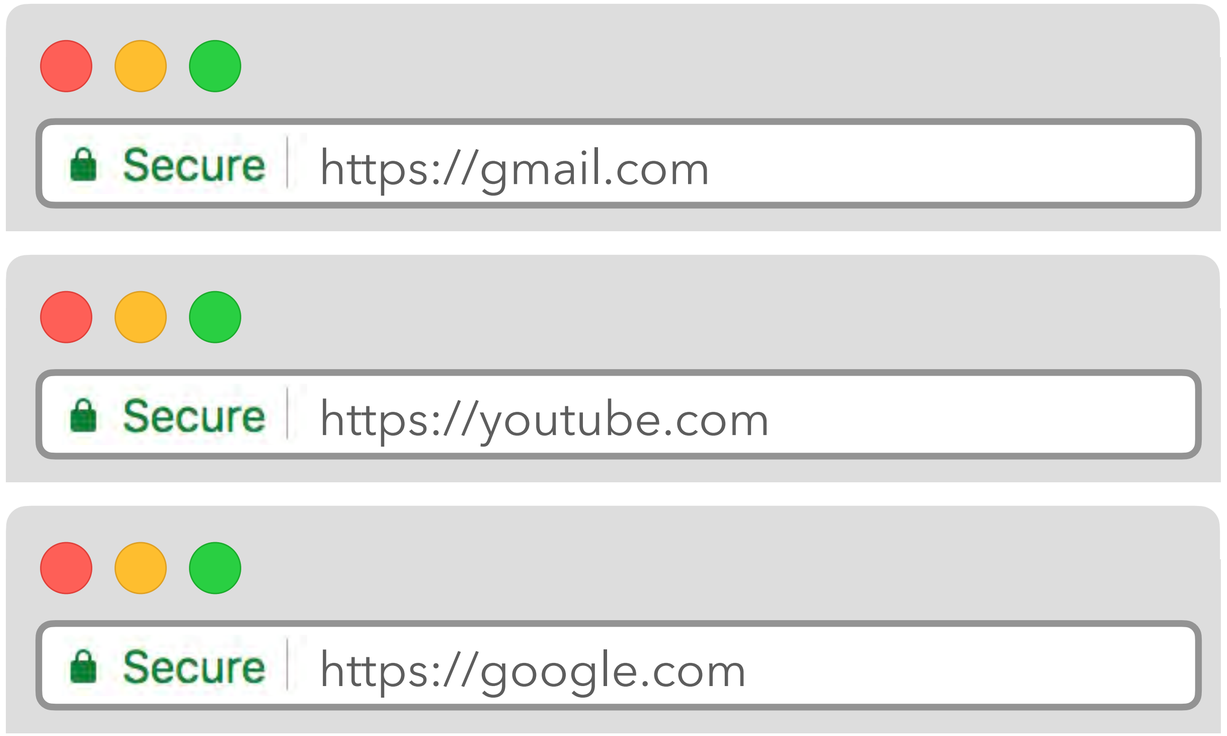
Non-Phishable MFA

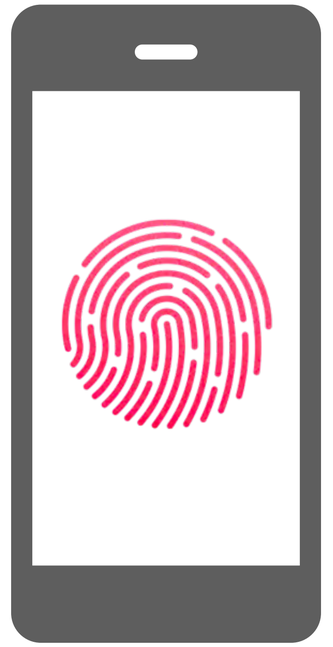
WebAuthn

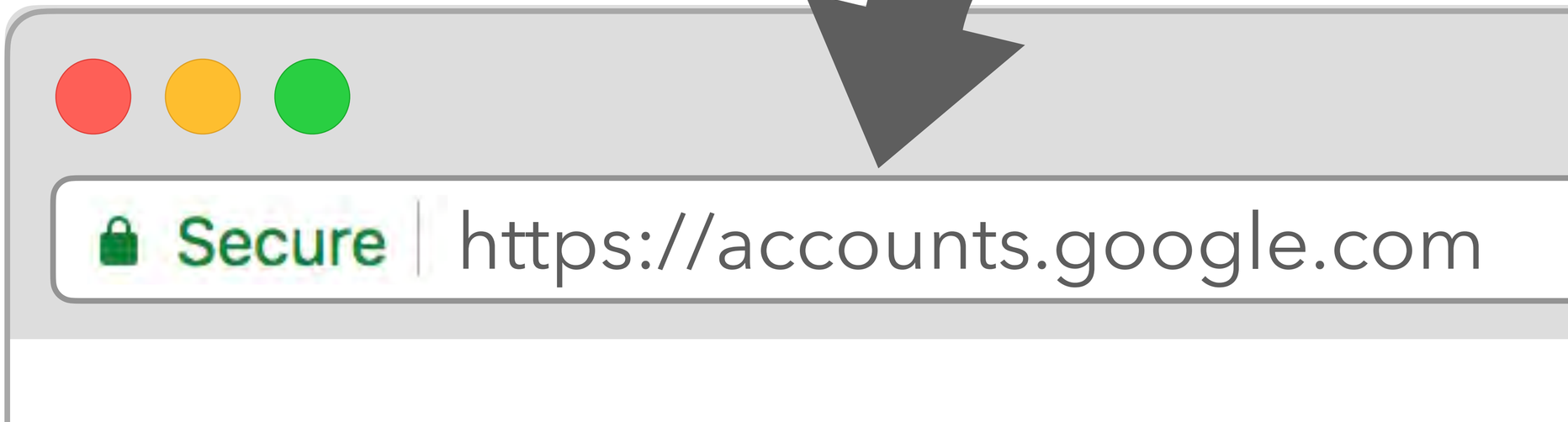
fido™


Secure
https://google.com


Secure
https://apple.com
Secure
https://google.com

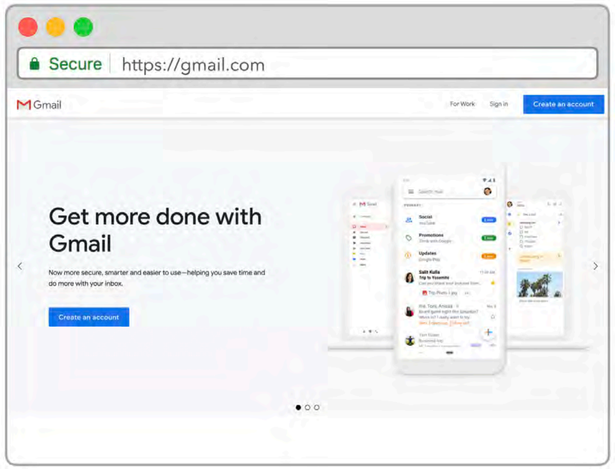

Secure
https://gmail.com
Secure
https://youtube.com
Secure
https://google.com

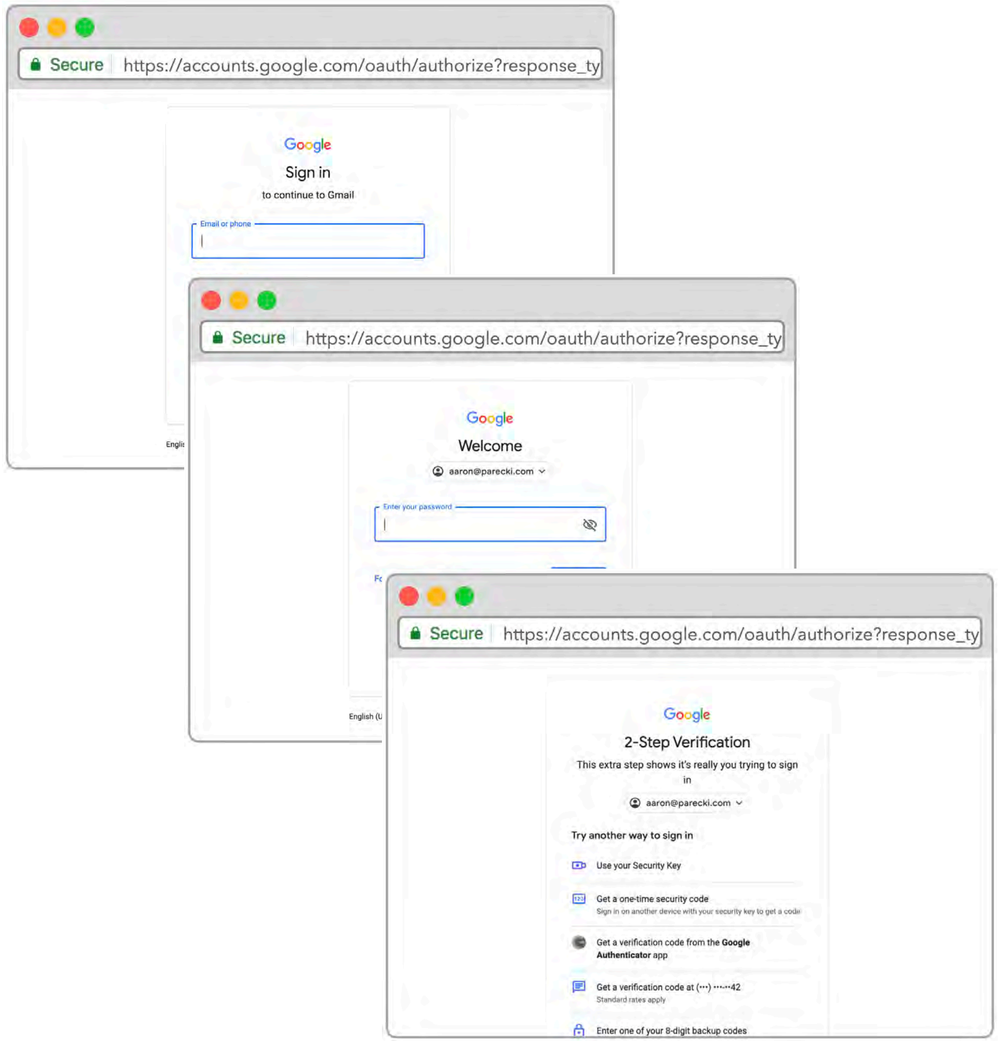


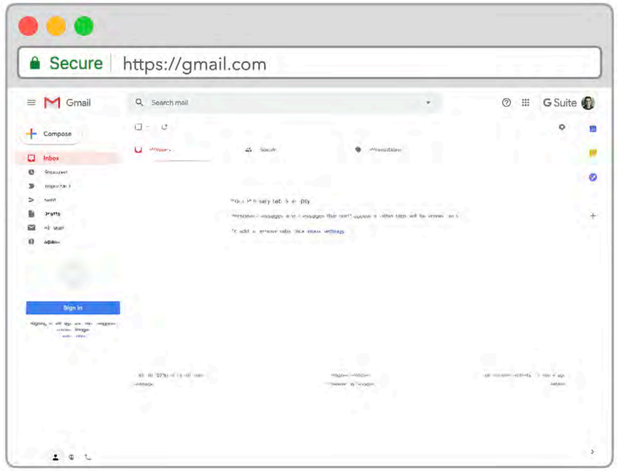

Secure
https://accounts.google.com

Application

OAuth Server

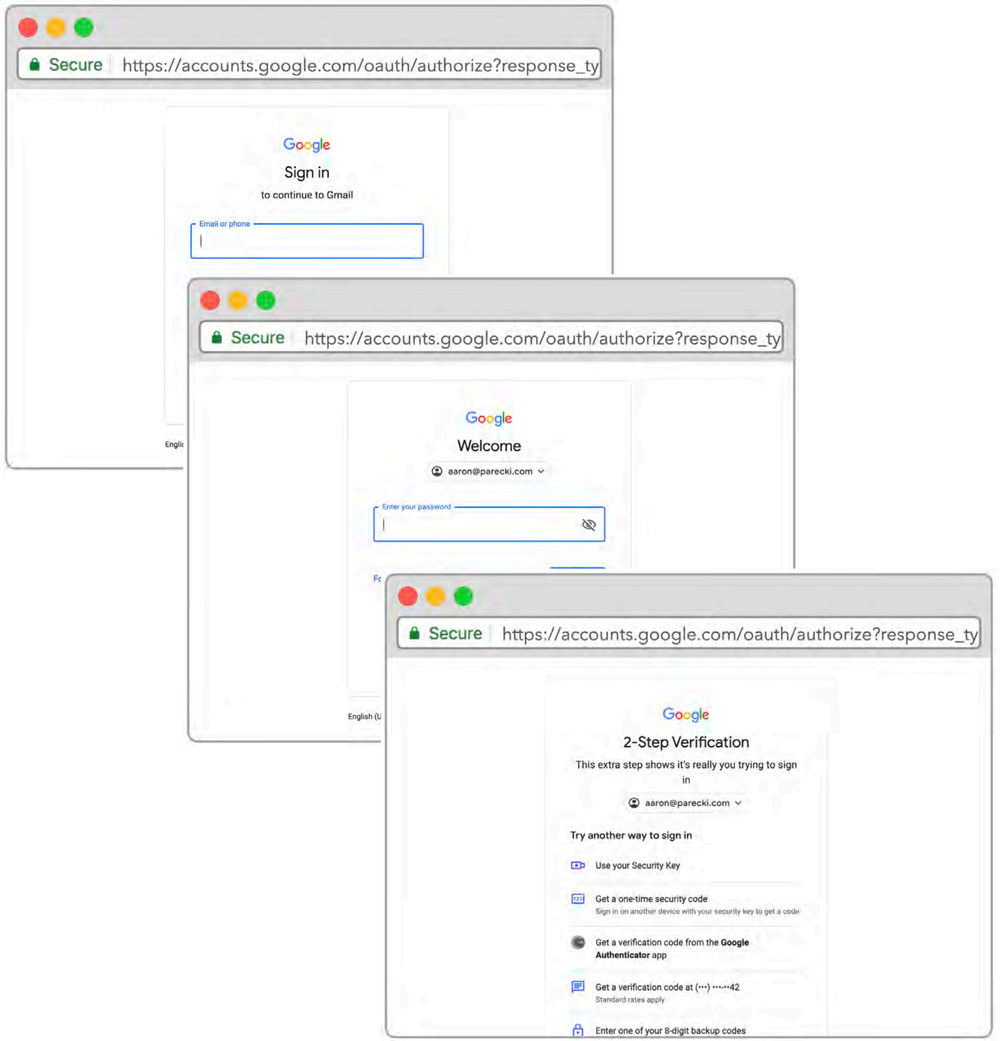






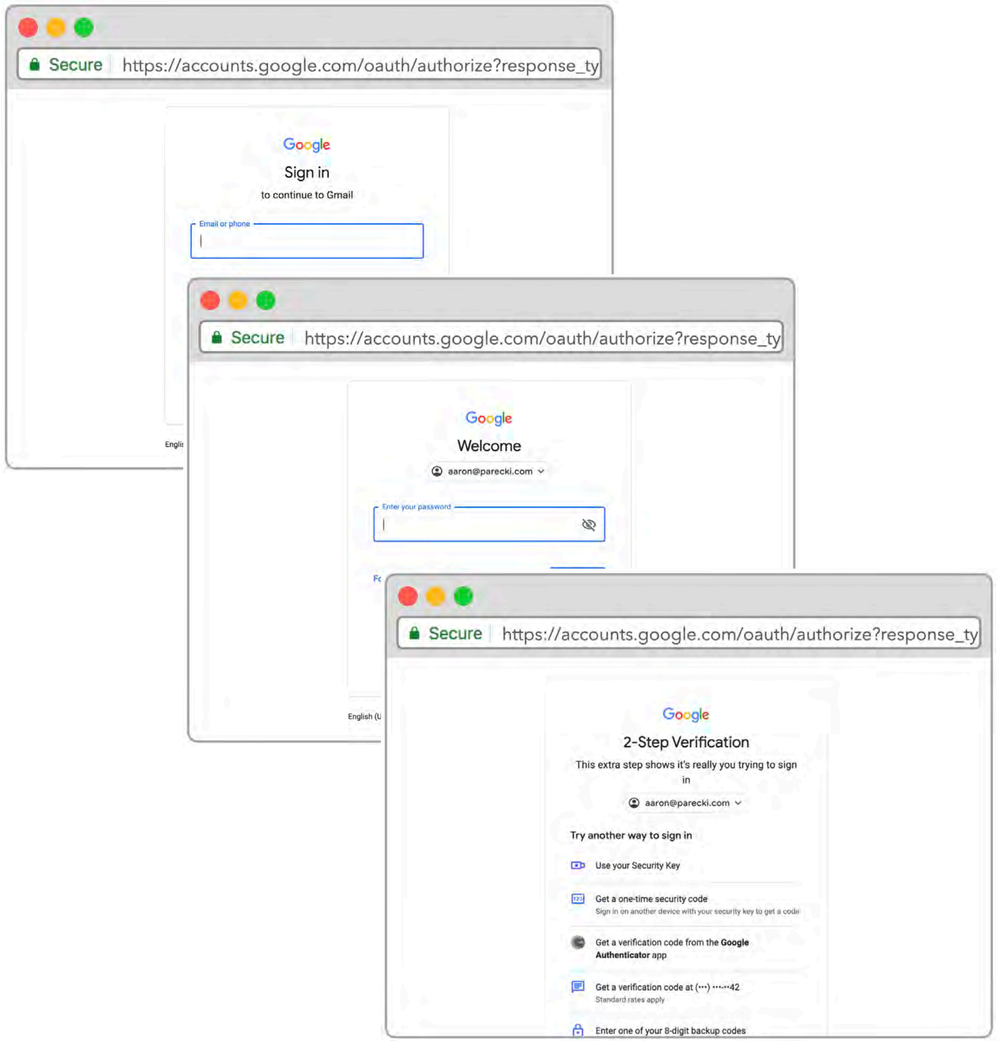
Application

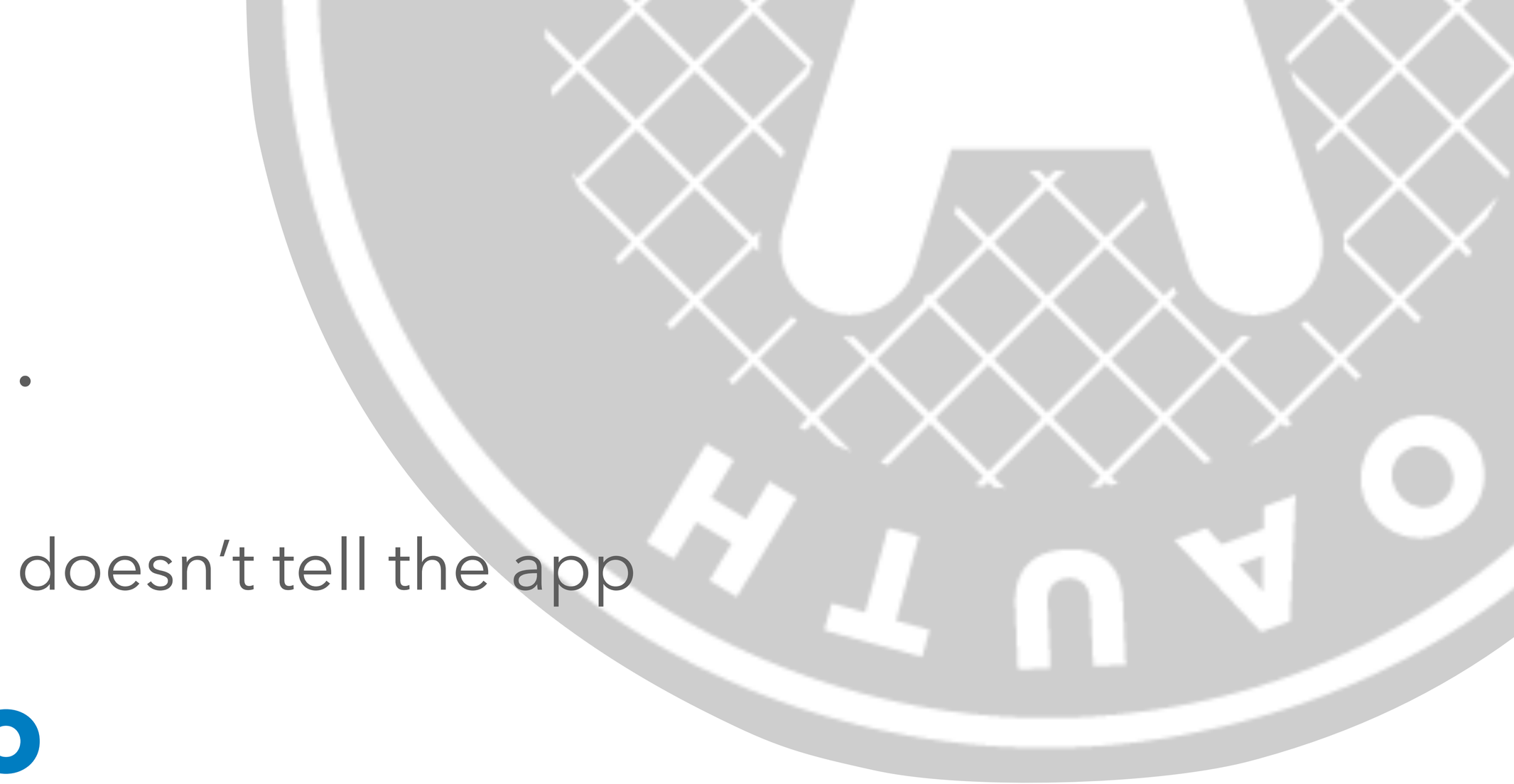
OAuth Server



Application

OAuth Server





but…

OAuth doesn’t tell the app

who

logged in

Accessing APIs

Identification

OAUTH VS OPENID CONNECT

Accessing APIs

Identification


OpenID
Connect


OAUTH
2
OAUTH

Gives the application a way to make API requests

Accessing APIs

Tells the application about the user authenticating

Identification

Gives the application a way to make API requests

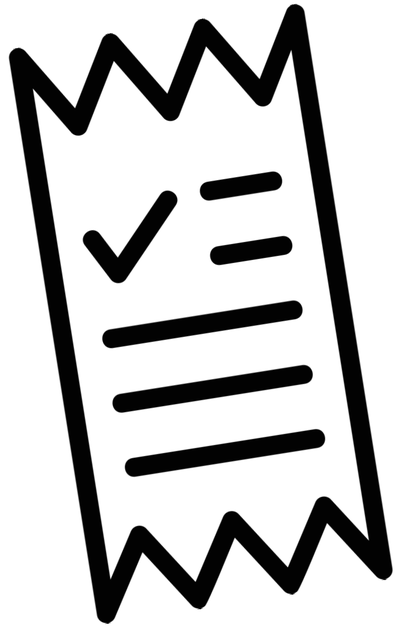
Access Token

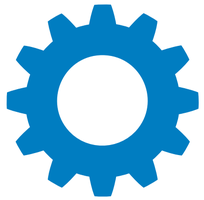
Tells the application about the user authenticating

ID Token

Access Token

ID Token





API

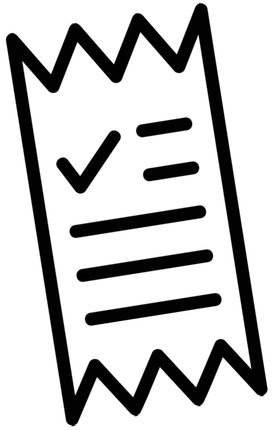
OAuth Server

Application

Access Token

Read by the API

ID Token



Read by the App

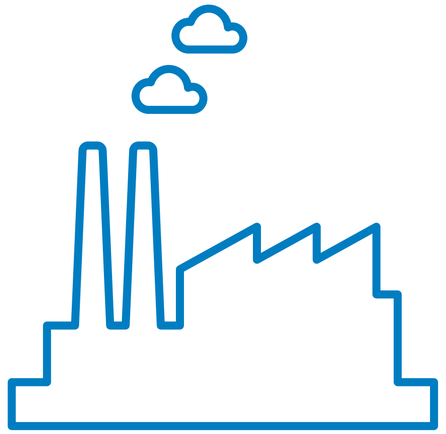
ROLES IN OAUTH

ROLES IN OAUTH

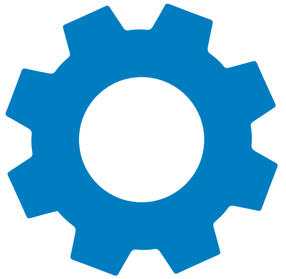
The User
(Resource Owner)

Device
(User Agent)

The Application
(Client)



OAuth Server
(Authorization Server)
aka the token factory



API
(Resource Server)

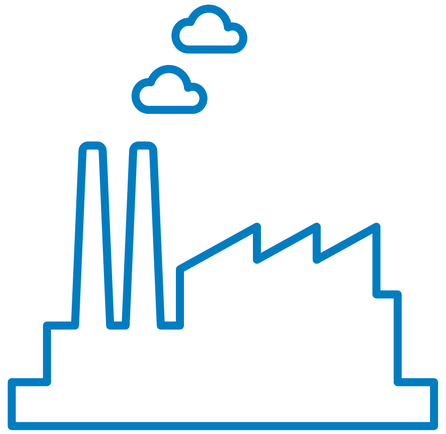
ROLES IN OAUTH

The User
(Resource Owner)

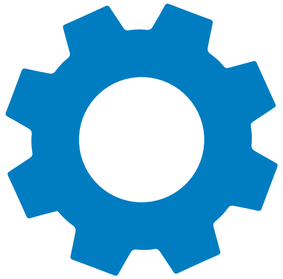
Device
(User Agent)

The Application
(Client)

Travis-CI.org



OAuth Server
(Authorization Server)
aka the token factory



API
(Resource Server)

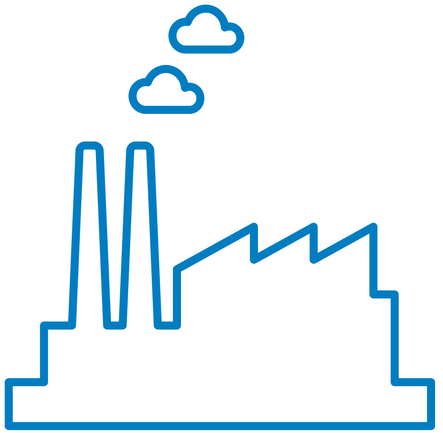
GitHub

ROLES IN OAUTH

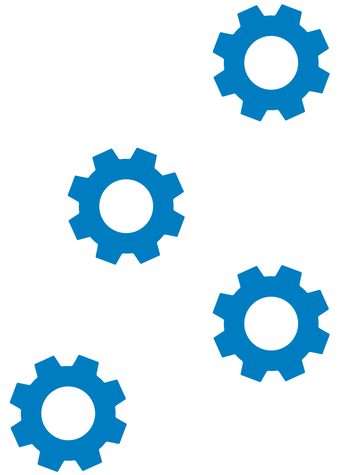
The User
(Resource Owner)

Device
(User Agent)

The Application
(Client)



OAuth Server
(Authorization Server)
aka the token factory



API
(Resource Server)

Okta

Microservices

OAUTH CLIENTS

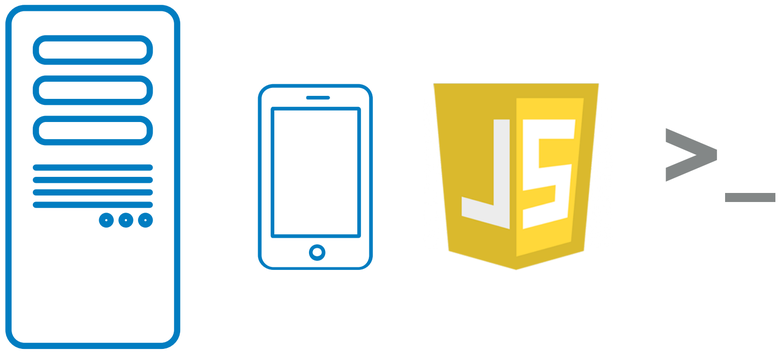
Goal of the Client:

Get an access token

Use the access token
to make API requests

OAUTH FLOWS

Authorization Code

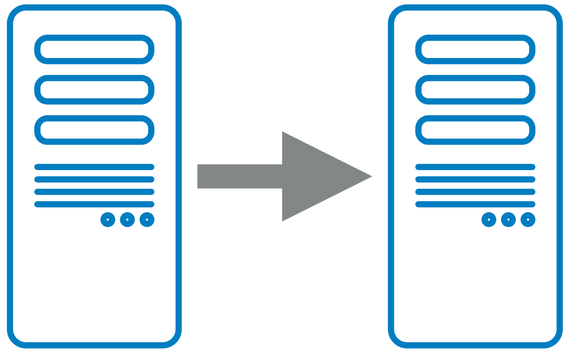


web mobile SPA CLI

Device Flow

CLI browserless devices

Client Credentials

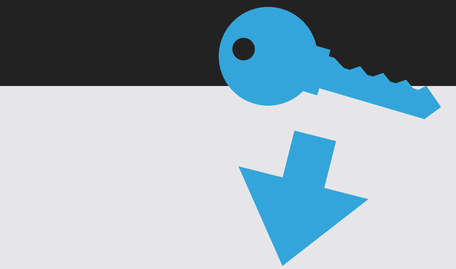


server-to-server

~~Implicit~~

~~Password~~

USING AN ACCESS TOKEN



```
POST /resource/1/update HTTP/1.1
Authorization: Bearer RsT5OjbzRn430zqMLgV3Ia
Host: api.authorization-server.com

description=Hello+World
```

Confidential Clients

Application running on a server

Has the ability to keep strings secret
since code is running in a trusted environment

Public Clients

The application can't keep strings secret

JavaScript/Single-Page apps: "view source"
Native apps: decompile and extract strings

GETTING READY:

CLIENT REGISTRATION

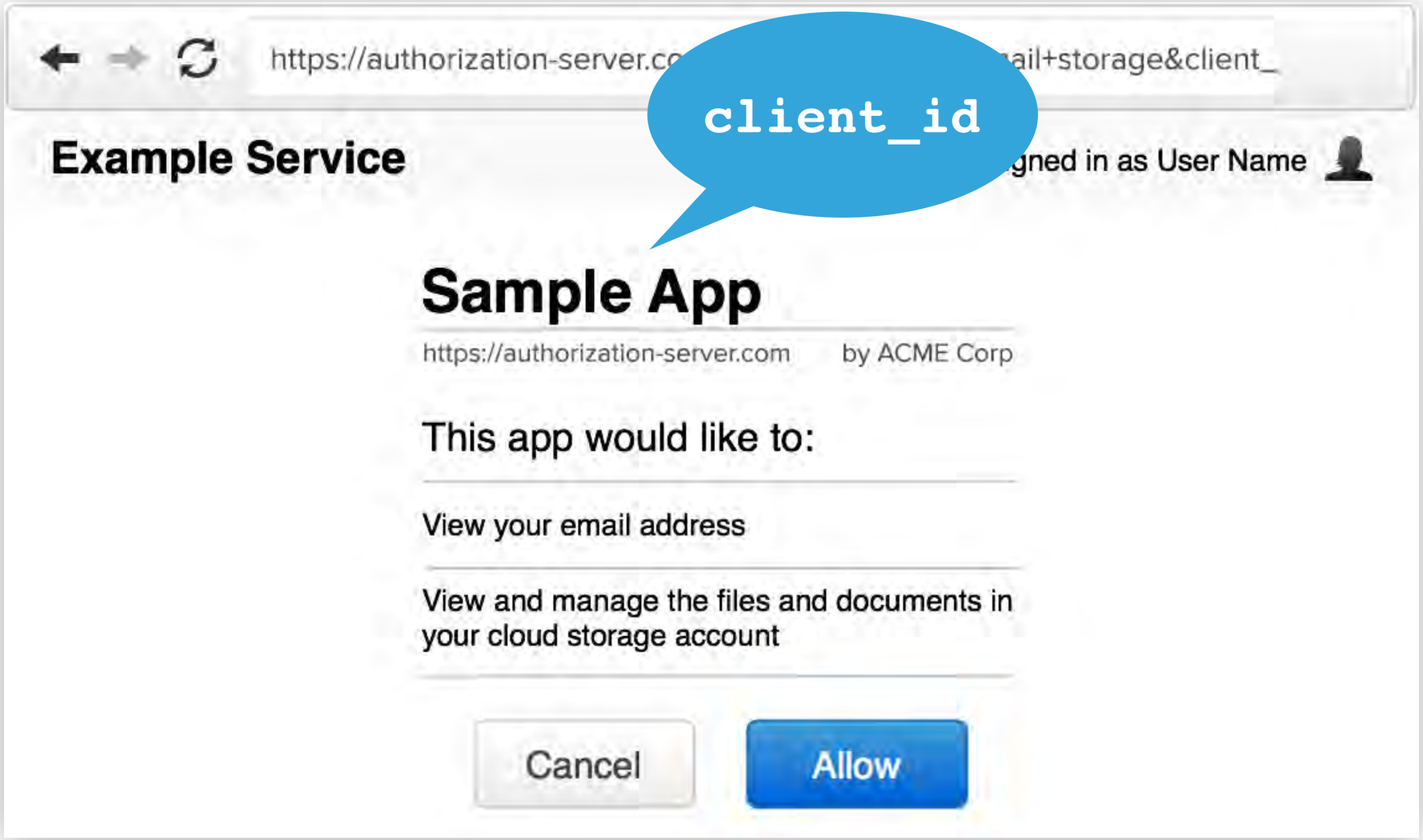
`client_id`

identifies the application

`client_secret`

the application's password

Authorization Interface



Create a new app integration

Sign-in method

Learn More

- (•) OIDC - OpenID Connect
  Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- ( ) SAML 2.0
  XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- ( ) SWA - Secure Web Authentication
  Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- ( ) API Services
  Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- (•) Web Application
  Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- ( ) Single-Page Application
  Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- ( ) Native Application
  Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Cancel Next

My App

Active ▾ View Logs

General Sign On Assignments Okta API Scopes

Client Credentials

Edit

Client ID

0oa847gxqiY8VOXNW357

Public identifier for the client that is required for all OAuth flows.

Client secret

••

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Ready to code

You can download a preconfigured sample app.

Download sample app

To get started using your custom app integration, see the "Sign Users In" section in the Okta Developer's guide

EXERCISE 1

oauth.school

"Getting Started"

GRANT TYPE:

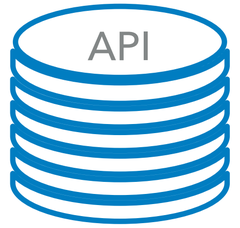
AUTHORIZATION CODE + PKCE

PKCE

(pronounced "pixie")

PROOF-KEY FOR CODE EXCHANGE

RFC 7636

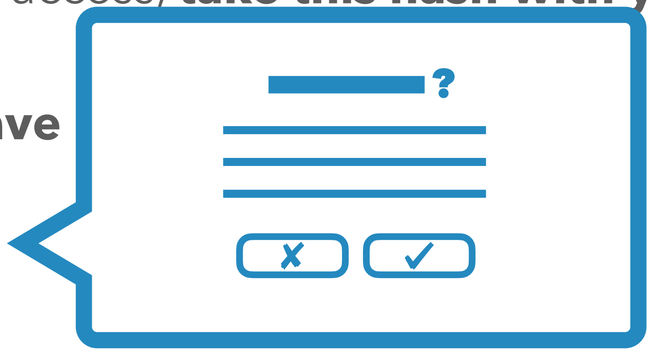


User: I'd like to use this great app

App: Hang on while I generate a new secret and hash it

App: Please go to the authorization server to grant me access, **take this hash with you**

User: I'd like to log in to this app, **here's the hash it gave**



AS: Here is a temporary code the app can use

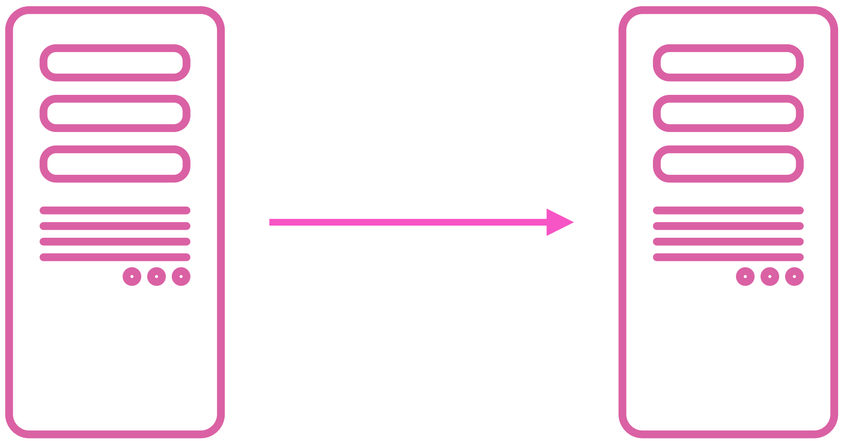
User: Here is the temporary code, please use this to get a token

App: Here's the code, **and the plaintext secret**, please give me a token

AS: **Let me verify the hash of that secret**... ok here is an access token!

App: Please let me access this user's data with this access token!

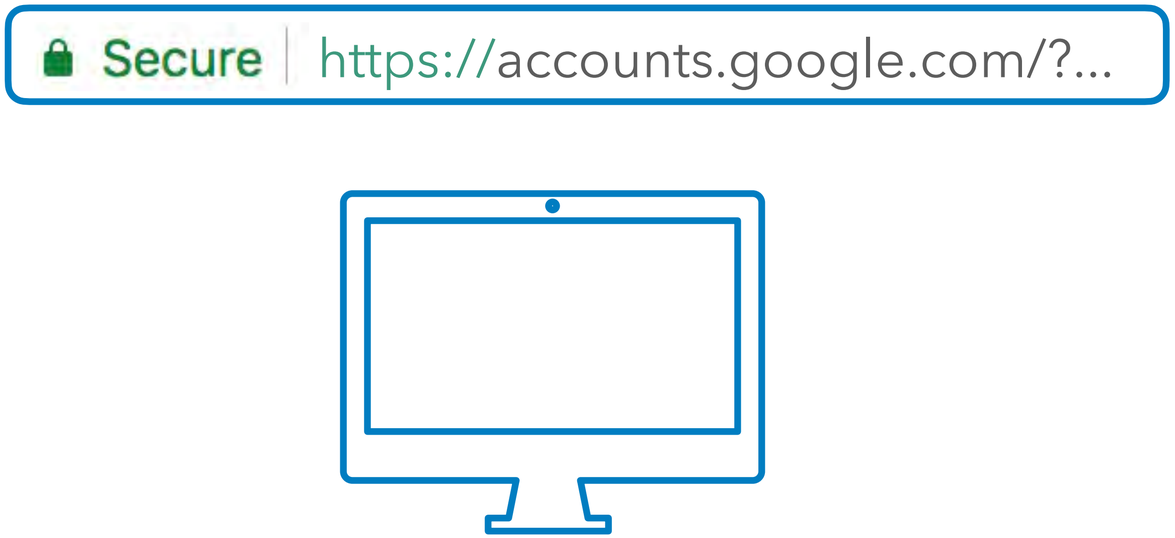
Back Channel



Sent from client to server

HTTPS request from client to server,
so requests cannot be tampered with

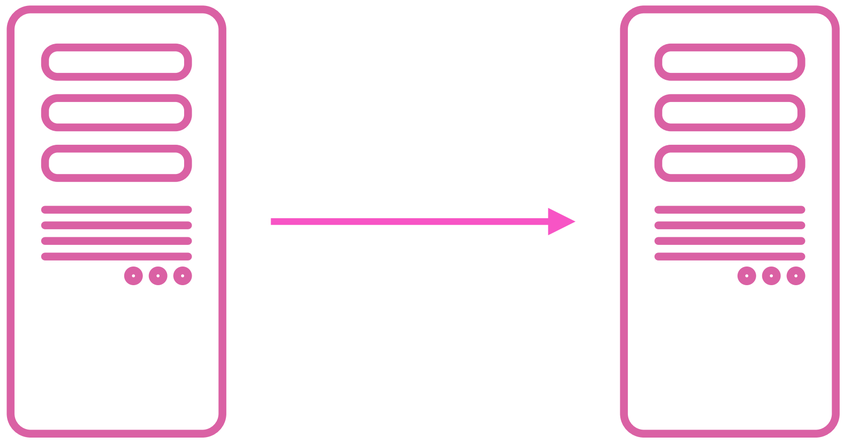
Front Channel



Passing data via the browser's address bar

The user, or malicious software,
can modify the requests and responses

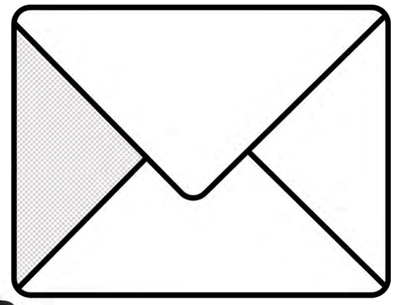
Back Channel Benefits

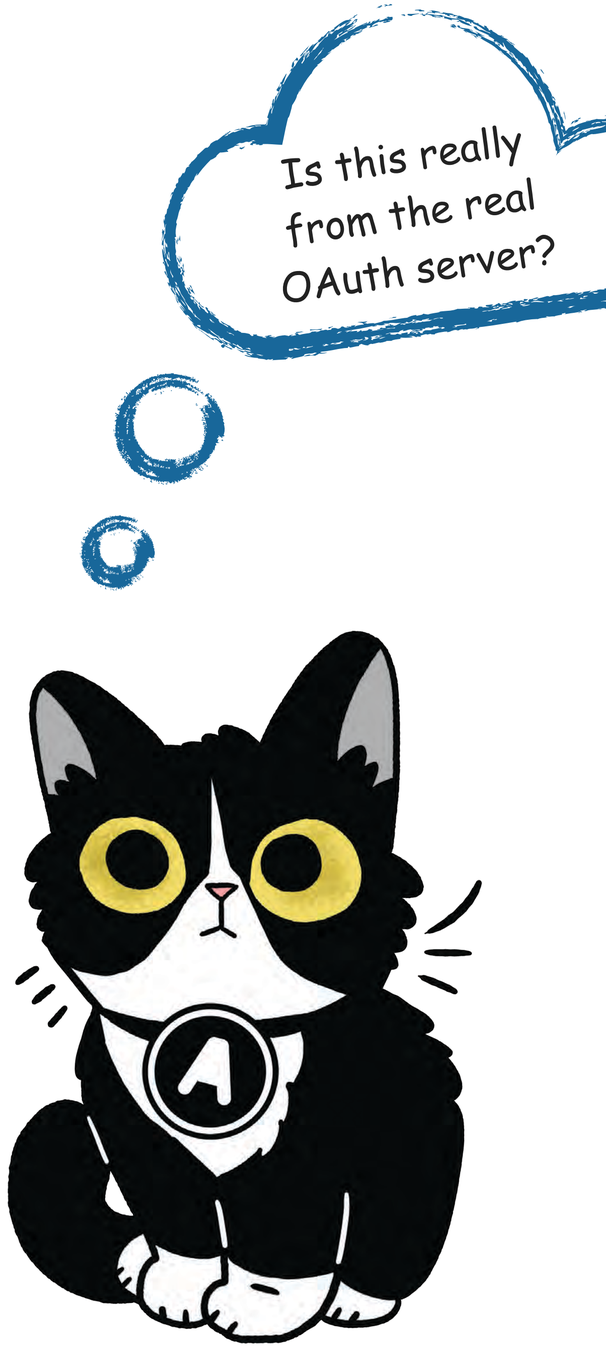


- The application knows it's talking to the right server
- Connection from app to server can't be tampered with
- Response from the server can be trusted because it came back in the same connection

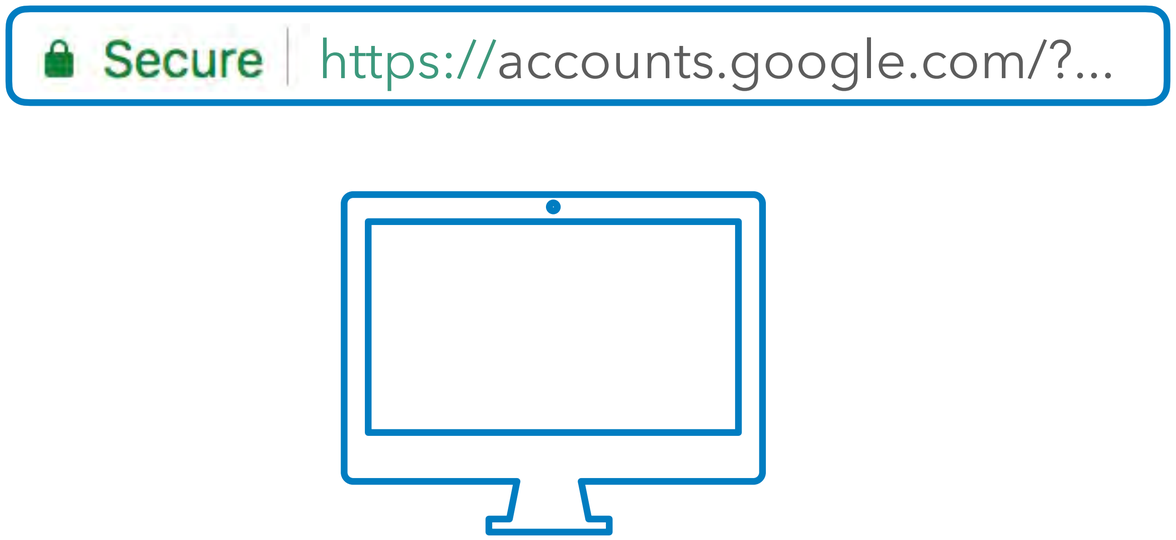
Back Channel

Front Channel





Front Channel Benefits



- The user being involved enables them to give consent
- Enables easier two-factor authorization integration
- Doesn't require the receiver to have a publicly routable IP (e.g. can work on a phone)

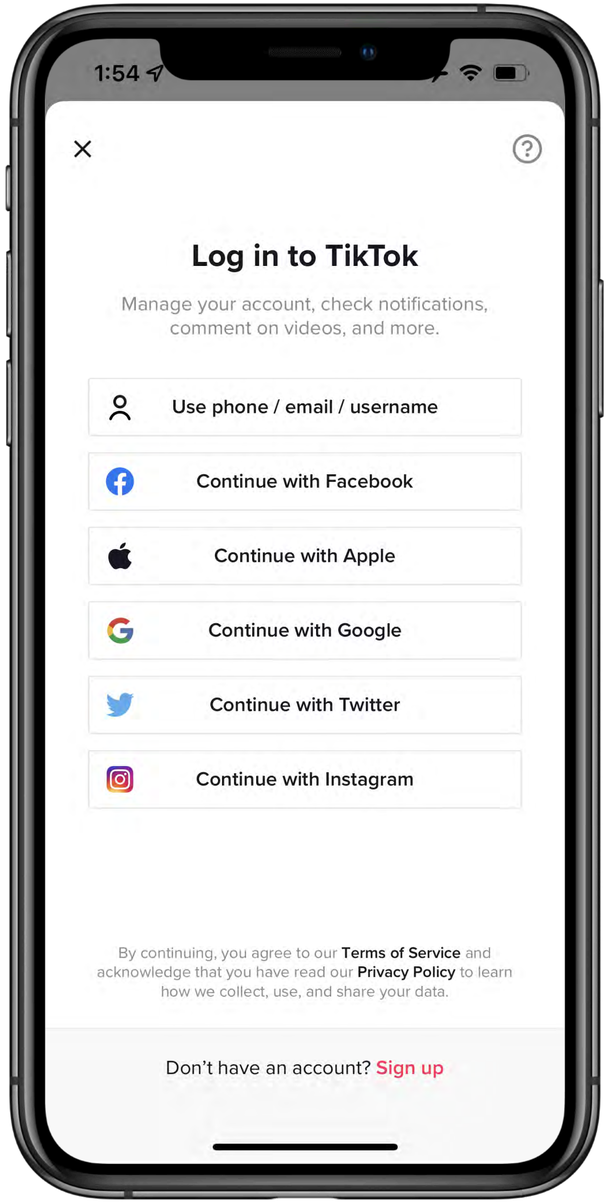
EXERCISE 2

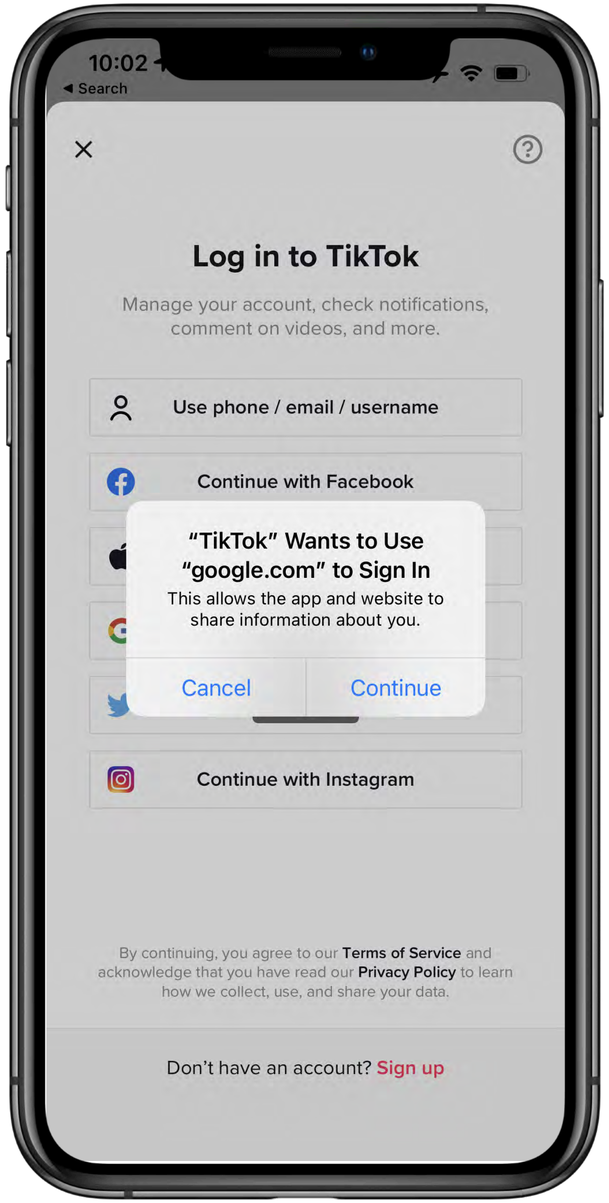
oauth.school

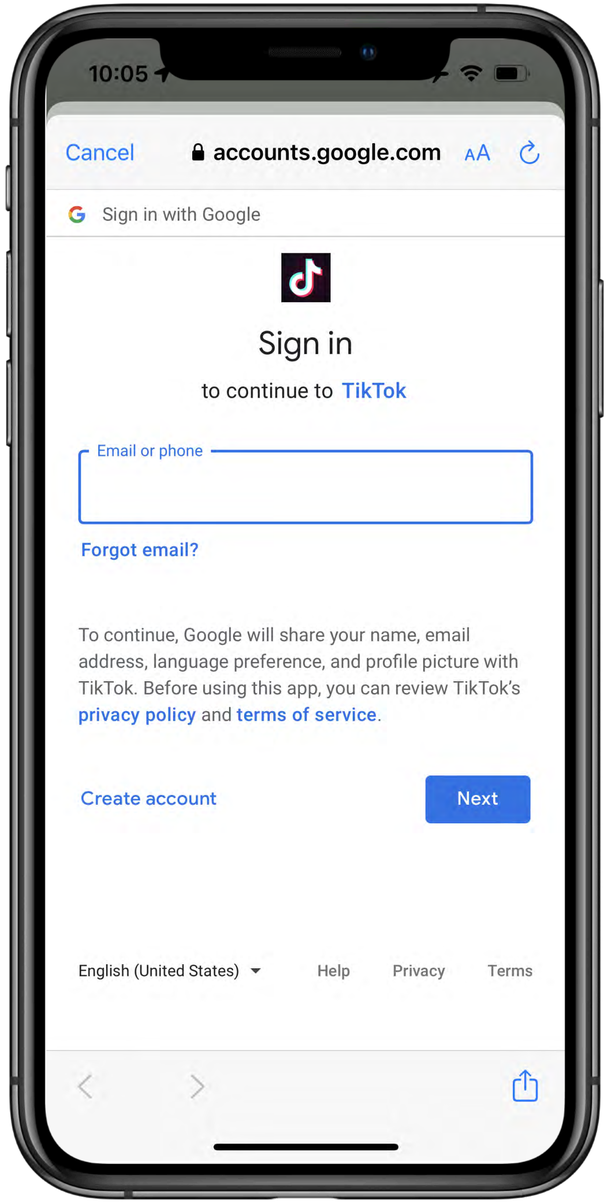
"OAuth for Web Applications"

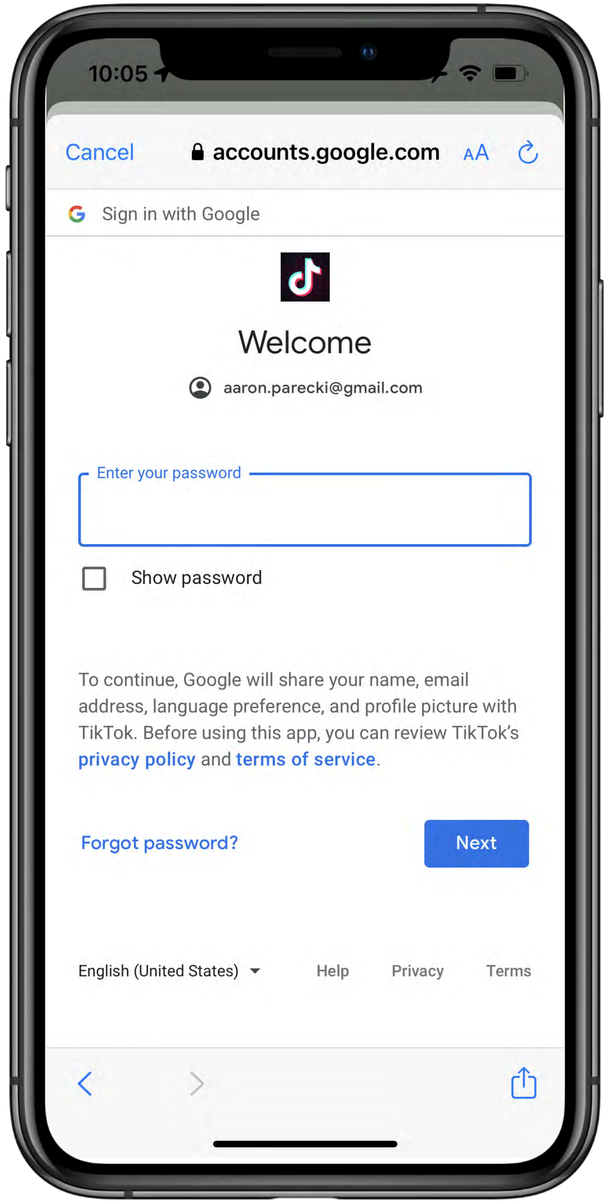
REFRESH TOKENS

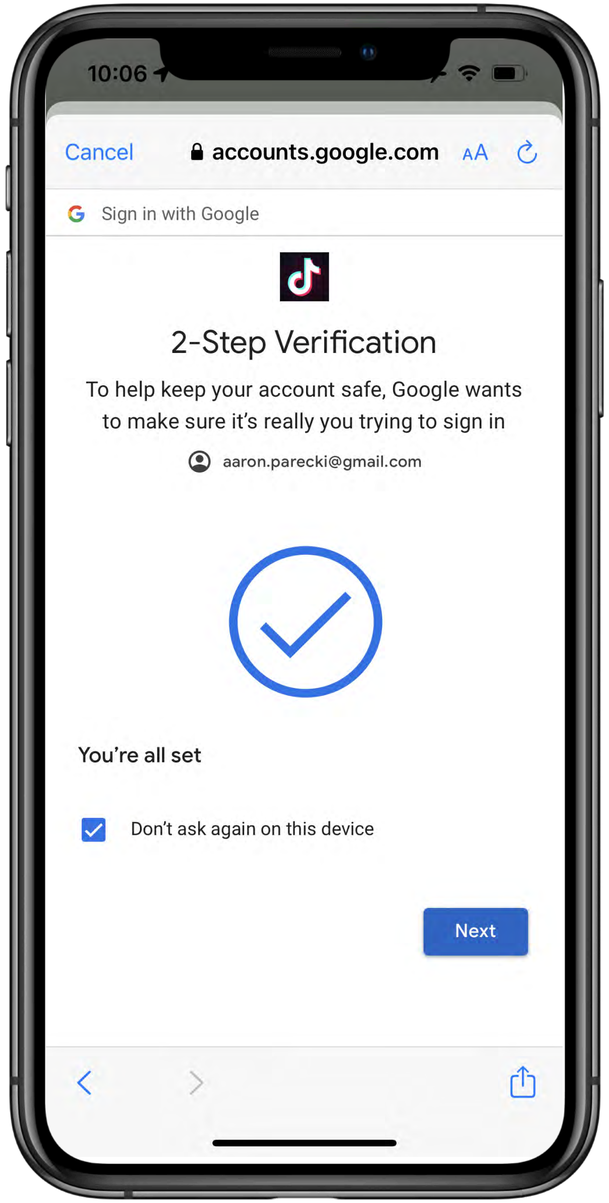
IOS OAUTH SEQUENCE

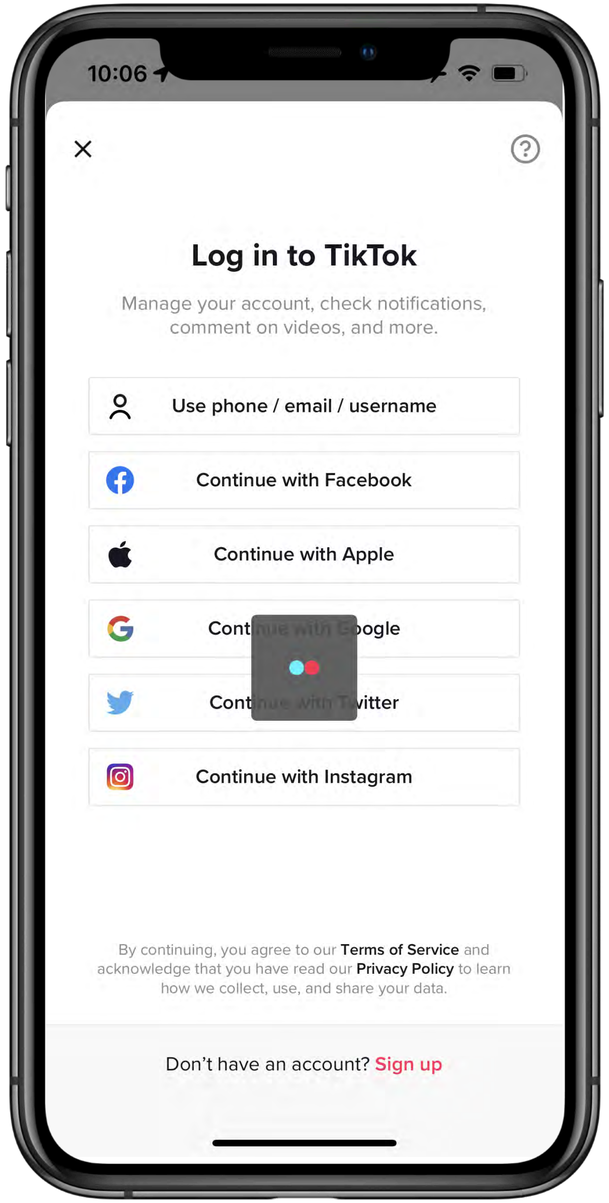

1:54
Log in to TikTok
Manage your account, check notifications, comment on videos, and more.
Use phone / email / username
Continue with Facebook
Continue with Apple
Continue with Google
Continue with Twitter
Continue with Instagram
By continuing, you agree to our Terms of Service and acknowledge that you have read our Privacy Policy to learn how we collect, use, and share your data.
Don't have an account? Sign up


10:02
Search
Log in to TikTok
Manage your account, check notifications, comment on videos, and more.
Use phone / email / username
Continue with Facebook
"TikTok" Wants to Use "google.com" to Sign In
This allows the app and website to share information about you.
Cancel
Continue
Continue with Instagram
By continuing, you agree to our Terms of Service and acknowledge that you have read our Privacy Policy to learn how we collect, use, and share your data.
Don't have an account? Sign up


10:05
Cancel
accounts.google.com
AA
Sign in with Google
Sign in
to continue to TikTok
Email or phone
Forgot email?
To continue, Google will share your name, email address, language preference, and profile picture with TikTok. Before using this app, you can review TikTok's privacy policy and terms of service.
Create account
Next
English (United States)
Help
Privacy
Terms


10:05
Cancel
accounts.google.com
AA
Sign in with Google
Welcome
aaron.parecki@gmail.com
Enter your password
Show password
To continue, Google will share your name, email address, language preference, and profile picture with TikTok. Before using this app, you can review TikTok's privacy policy and terms of service.
Forgot password?
Next
English (United States)
Help
Privacy
Terms

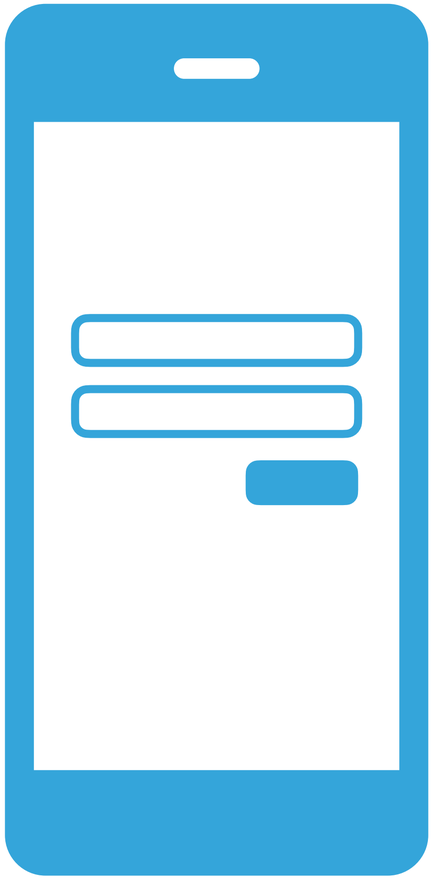

10:06
Cancel
accounts.google.com
AA
Sign in with Google
2-Step Verification
To help keep your account safe, Google wants to make sure it's really you trying to sign in
aaron.parecki@gmail.com
You're all set
Don't ask again on this device
Next


10:06
Log in to TikTok
Manage your account, check notifications, comment on videos, and more.
Use phone / email / username
Continue with Facebook
Continue with Apple
Continue with Google
Continue with Twitter
Continue with Instagram
By continuing, you agree to our Terms of Service and acknowledge that you have read our Privacy Policy to learn how we collect, use, and share your data.
Don't have an account? Sign up

authorization request

user authenticates

access token & refresh token



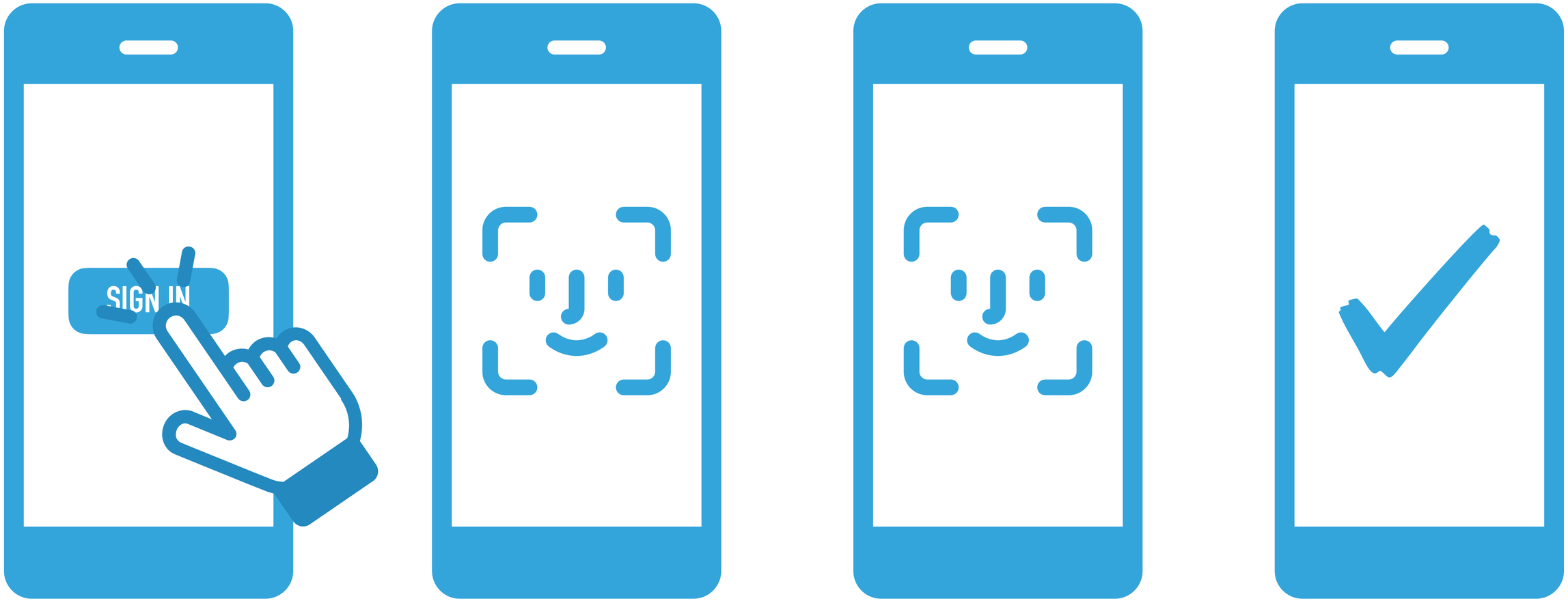
store refresh token in secure storage

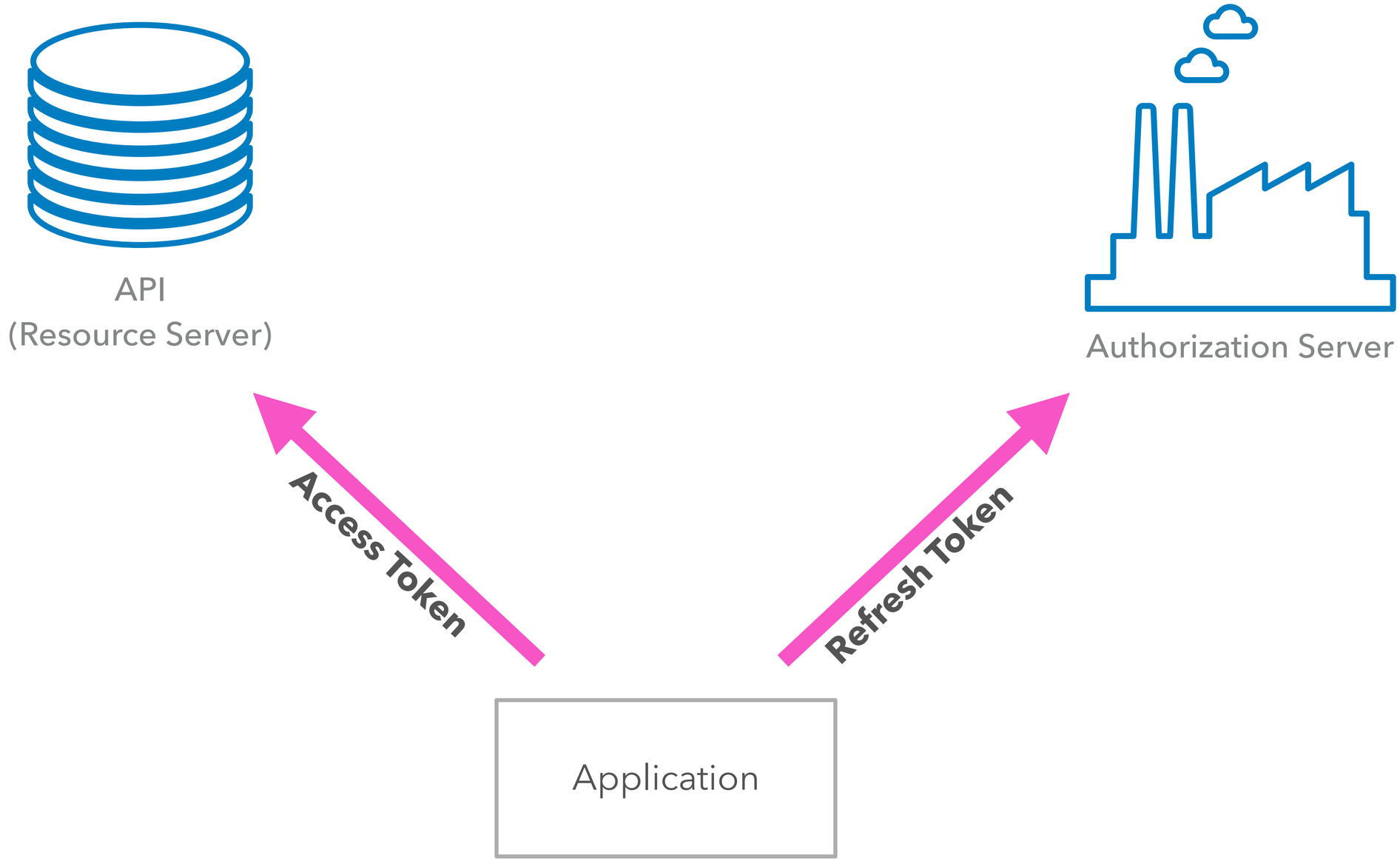
already has
refresh token

biometrics unlock
refresh token

use refresh token
to get new access token

new access token
& refresh token




API
(Resource Server)
Authorization Server
Access Token
Refresh Token
Application

EXERCISE 3

oauth.school

"Refresh Tokens"

WHERE IS THE BEST PLACE TO

STORE TOKENS?

Storage Options for JS Apps

LocalStorage

SessionStorage

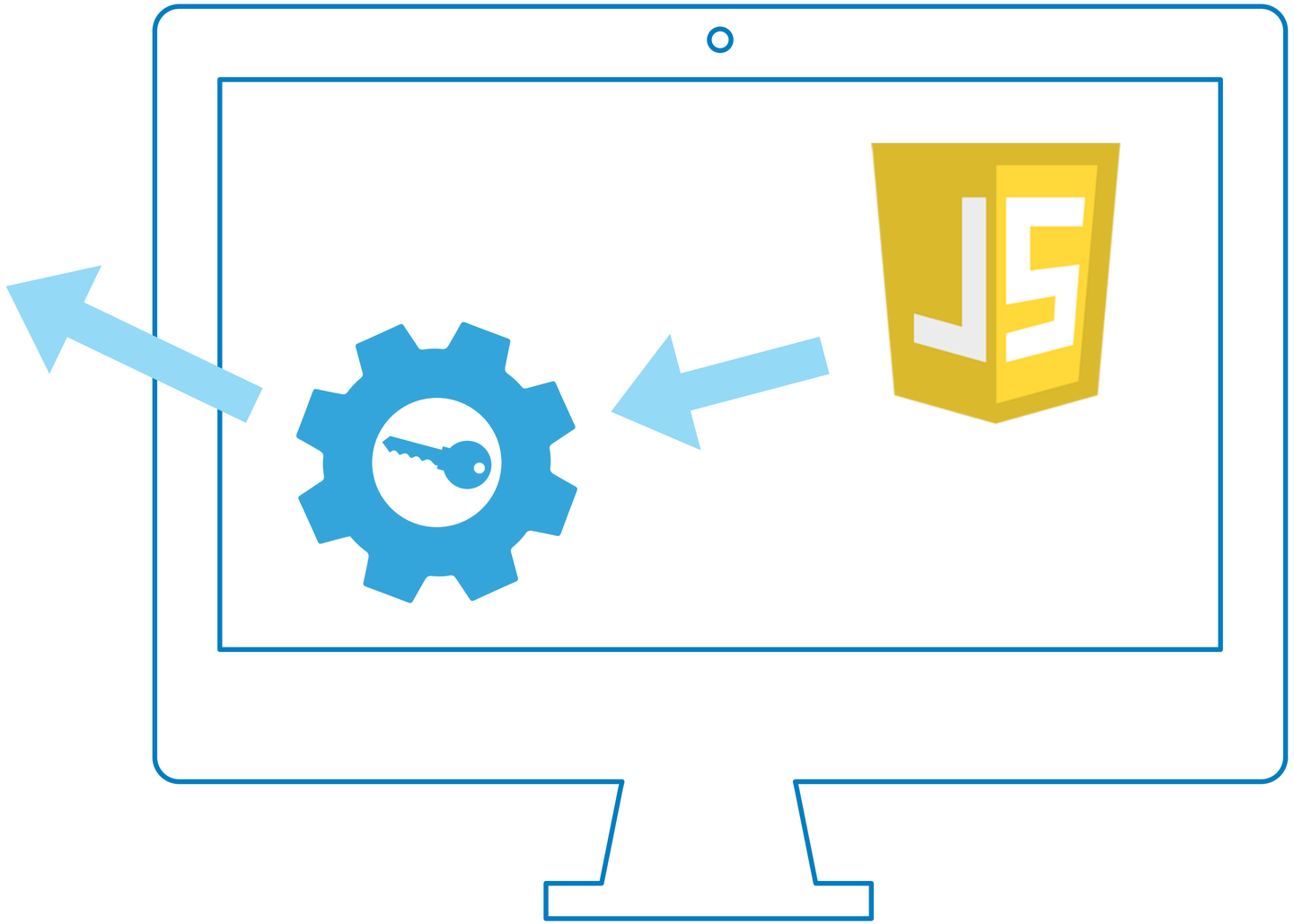
Cookies

XSS

Cross-Site Scripting

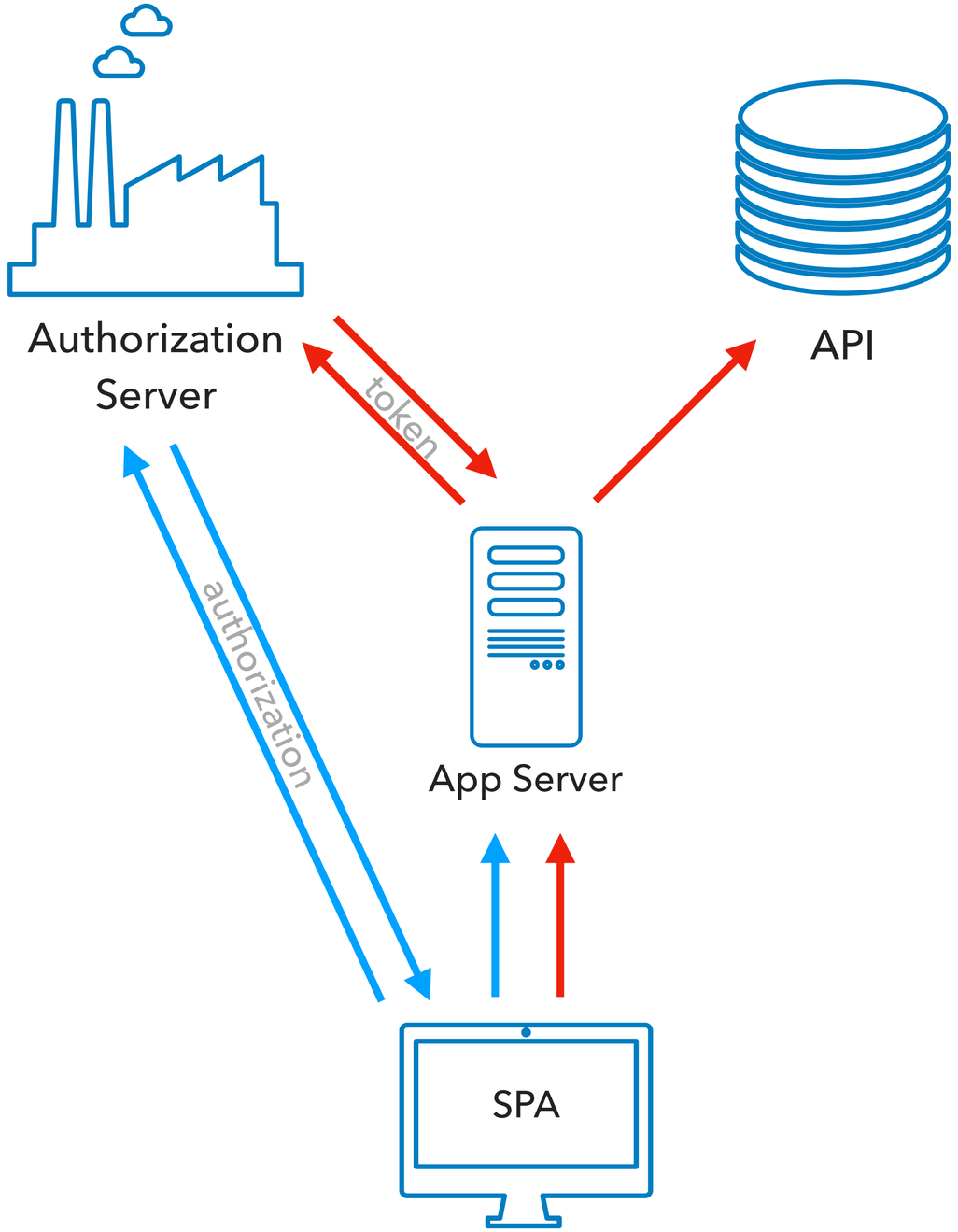
If your JavaScript can see the access token, so can an attacker using XSS

Service Worker



If your JavaScript can't see the access token, neither can an attacker!

Backend for your Frontend



Access token is never sent to the browser.

XSS is limited to the attacker telling your app server to make requests.

OPENID CONNECT:

WHO LOGGED IN?


OpenID
Connect

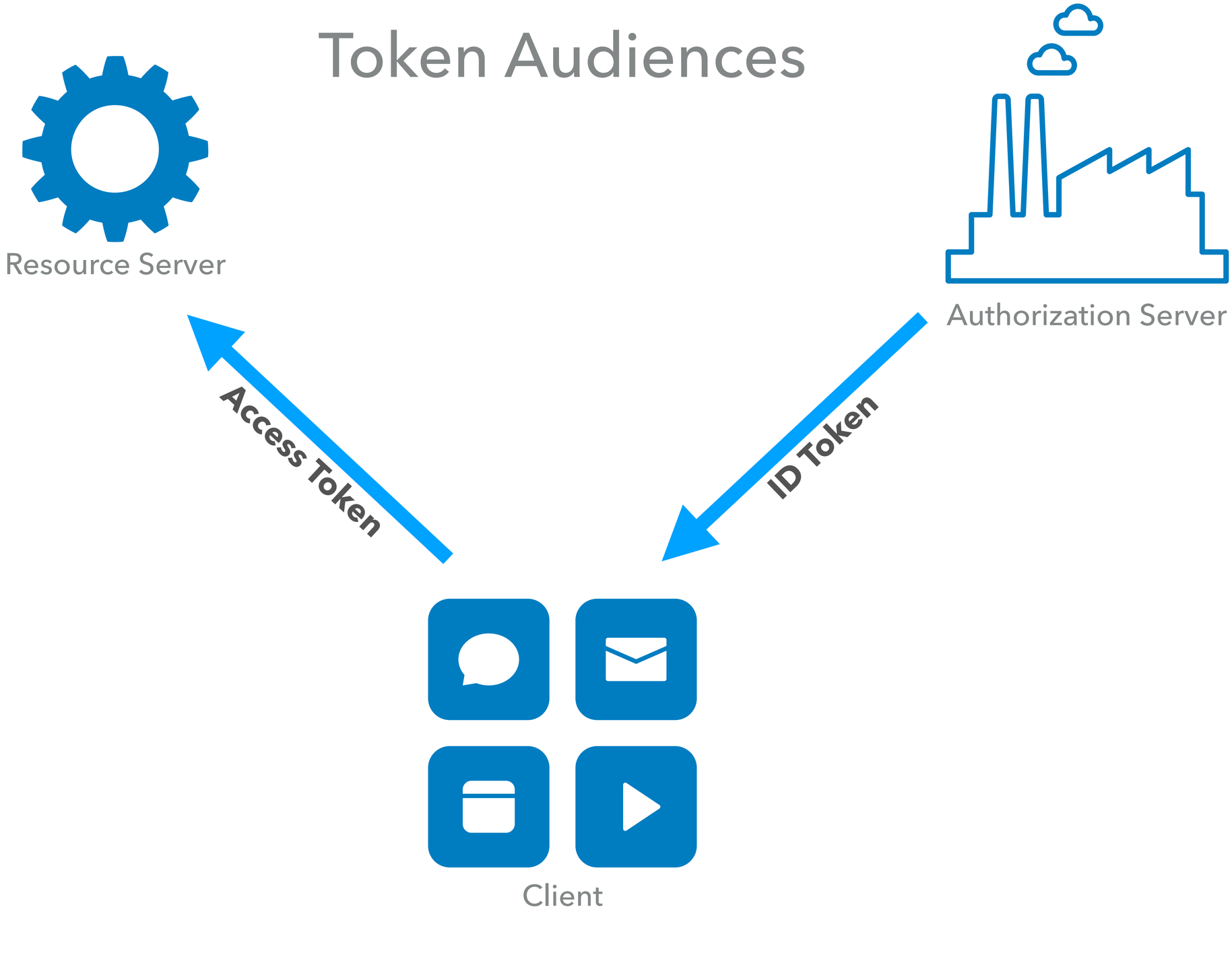

OAUTH
2
OAUTH

New token type: ID Token

An ID token encodes user information

This may look like an access token if your access tokens are also JWTs, but they are not the same!

Token Audiences



ID Token: JWT


```
eyJraWQiOiJiRmxZbmkzLXRhMXFSa0lFellHc2tLeFFRVUJvczZnOU9RQnRmNm9xcUxJIiwiYWxnI
joiUlMyNTYifQ

.

eyJzdWIiOiIwMHVjcTNid2o0V25JcTNnejBoNyIsIm5hbWUiOiJQYWRtYS0yIEdvdmluZGFyYWphb
HUiLCJsb2NhbGUiOiJlbi1VUyIsInZlciI6MSwiaXNzIjoiaHR0cHM6Ly9wYWRtYWdvdmluZGFyYW
phbHUub2t0YXByZXZpZXcuY29tL29hdXRoMi9kZWZhdWx0IiwiYXVkIjoiMG9hZDlydTd0endmNUF
qcGIwaDcgIiwiaWF0IjoxNTI0NTk0OTEwLCJleHAiOjE1MjQ1OTg1MTAsImp0aSI6IklELklfNUc4
RzhWdXowMHJvYl9aSzlja3J0T0pseVdwNzhxMU5naGV2QlJ6dkEiLCJhbXIiOlsicHdkIl0sImlkc
CI6IjAwb2NxM2J3aTFoTnpRT3B5MGg3Iiwibm9uY2UiOiJhYmMiLCJwcmVmZXJyZWRfdXNlcm5hbW
UiOiJwYWRtYS5nb3ZpbmRhcmFqYWx1QG9rdGEuY29tIiwiZ2l2ZW5fbmFtZSI6IlBhZG1hIiwibWl
kZGxlX25hbWUiOiJLcmlzaG5hIiwiZmFtaWx5X25hbWUiOiJHb3ZpbmRhcmFqYWx1Iiwiem9uZWlu
Zm8iOiJBbWVyaWNhL0xvc19BbmdlbGVzIiwidXBkYXRlZF9hdCI6MTUyNDU5NDM2MSwiYXV0aF90a
W1lIjoxNTI0NTk0OTA3fQ

.

HvMYW8XbdCf1BW-
ZfHQ1odaAYJjZqKkh1NUkHW0clk6J7pYunn8jllbIp0IhSjcCn6PBIlZPrrE0dkuyjvdHjVI8ALQN
wtM7FnIs9H6gCH0oONx4EL4K-Ef4d_w46qeqsCwMClvNoaE3c2I5-kON-
uJUlaefbnr6Al_y9z5mvLyDynf9IjrOyTPoIrgk9V46l28Aulp4dJhqBtZfpYyVbKrXawHSO5FvKT
DMPBhQgxt0_6PKG7sSkhbMeBicIc35SJJaXt81KSfkYDUp5s1UQ74ATHrtLe7HMU1yp_KajgYUKxM
XO5NiXpeNEHzarAOWzLHblrQcgkpuJbY3KM1HHg
```

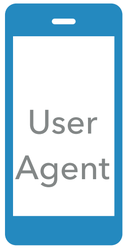
Decoded ID Token

```
header
.
{
  "sub": "{USER_ID}",
  "iss": "https://authorization-server.com/oauth2/ausd1nry9hBoyvKrY0h7",
  "aud": "{CLIENT_ID}",
  "iat": 1524237221,
  "exp": 1524240821,
  "nonce": "{NONCE}",
  "auth_time": 1524606562
}
.
signature
```

OpenID Connect - Authorization Code Flow + PKCE

Front Channel

```
https://authorization-server.com/auth?
   response_type=code&
   client_id=CLIENT_ID&
   redirect_uri=REDIRECT_URI&
   scope=openid+profile&
   state=xyz1234&
   nonce=1029385476&
   code_challenge=CODE_CHALLENGE&
   code_challenge_method=S256
```



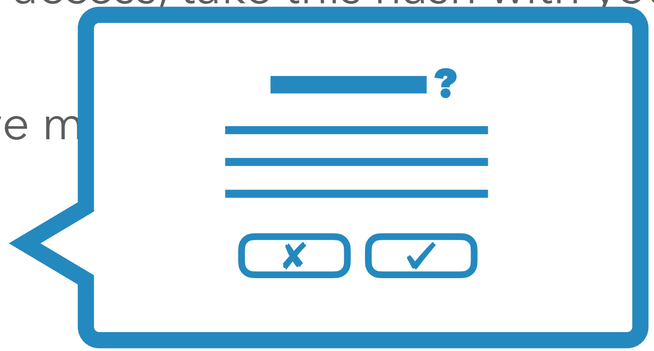
App

User: I'd like to use this great app

App: Hang on while I generate a new secret and hash it

App: Please go to the authorization server to grant me access, take this hash with you

User: I'd like to log in to this app, here's the hash it gave m



AS: Here is a temporary code the app can use

User: Here is the temporary code, please use this to get an access token and ID token

App: Here's the code, and the plaintext secret, please give me a token

AS: Let me verify the hash of that secret... ok here are the tokens!

App parses the ID token for the information it needs

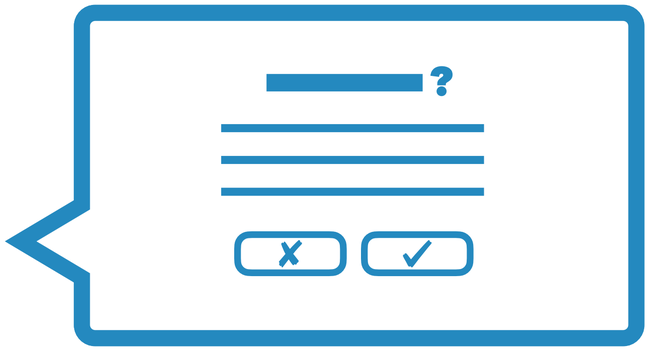
OPENID CONNECT AUTH CODE + PKCE

OPENID CONNECT IMPLICIT FLOW

User: I'd like to use this great app

App: Please go to the authorization server to grant me access

User: I'd like to log in to this app



AS: Here is an ID token!

User: Here is the ID token

App validates ID token signature and all claims

Implicit Flow and OpenID Connect

- What's actually deprecated is issuing access tokens in the authorization response
- OpenID Connect hybrid response modes
  - ~~"token id_token"~~ "code id_token" "id_token"
- ID Token front channel leakage is still a risk

EXERCISE 4

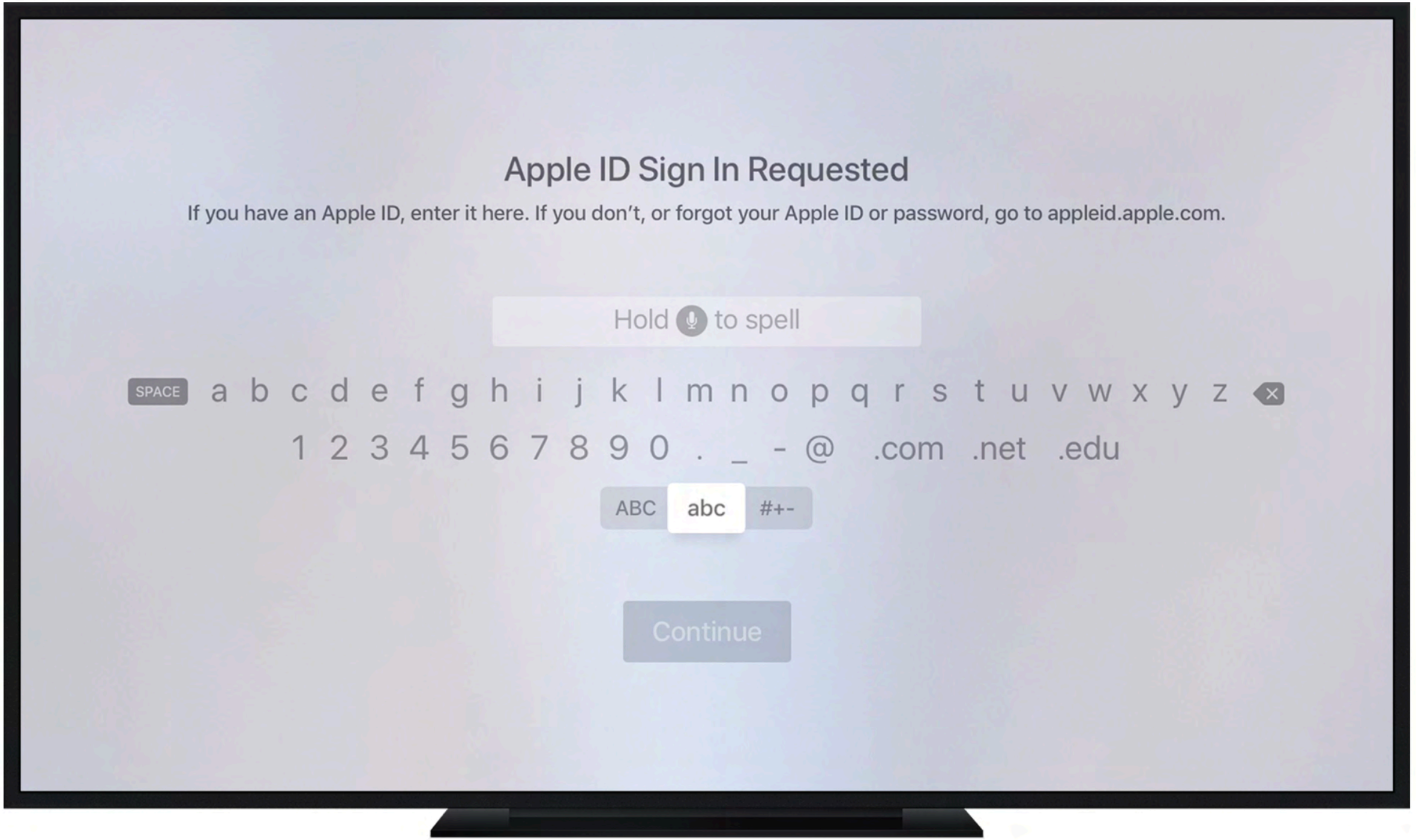
oauth.school

"OpenID Connect"

GRANT TYPE:

DEVICE CODE

BROWSERLESS DEVICES


Apple ID Sign In Requested
If you have an Apple ID, enter it here. If you don't, or forgot your Apple ID or password, go to appleid.apple.com.
Hold to spell
SPACE a b c d e f g h i j k l m n o p q r s t u v w x y z
1 2 3 4 5 6 7 8 9 0 . _ - @ .com .net .edu
ABC abc #+-
Continue

Sign In to Activate SYFY

For full episodes and more, sign in with your TV provider account.

To sign in on your PC, notebook or mobile device, go to:

syfy.com/appletv

When prompted, enter the following activation code:

NKLDD5D

Get New Code

ACTIVATE

STEP 1:

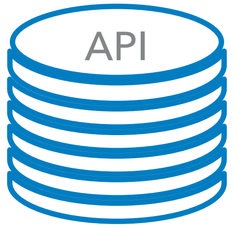
Visit abc.com/activate on your computer or mobile device

STEP 2:

Enter the following code:

Z	N	Z	M	H	Z	W

refresh code



User: I'd like to use this great app

Device: A user would like to log in

AS: Here's a temporary code, check back every 5 sec for the next 5 minutes

Device: Go to this URL and enter this code

User: I'd like to log in to "The Best App Ever", it wants to access my photos

AS: Ok, I'll let the device know you allowed it next time it checks in

Device: Here is the temporary code, has the user logged in yet?

AS: Here is an access token!

Device: Please let me access this user's data with this access token!

RESOURCES

OAuth 2.0 Servers

Written by Aaron Parecki

OAuth 2.0 is the modern standard for securing access to APIs.

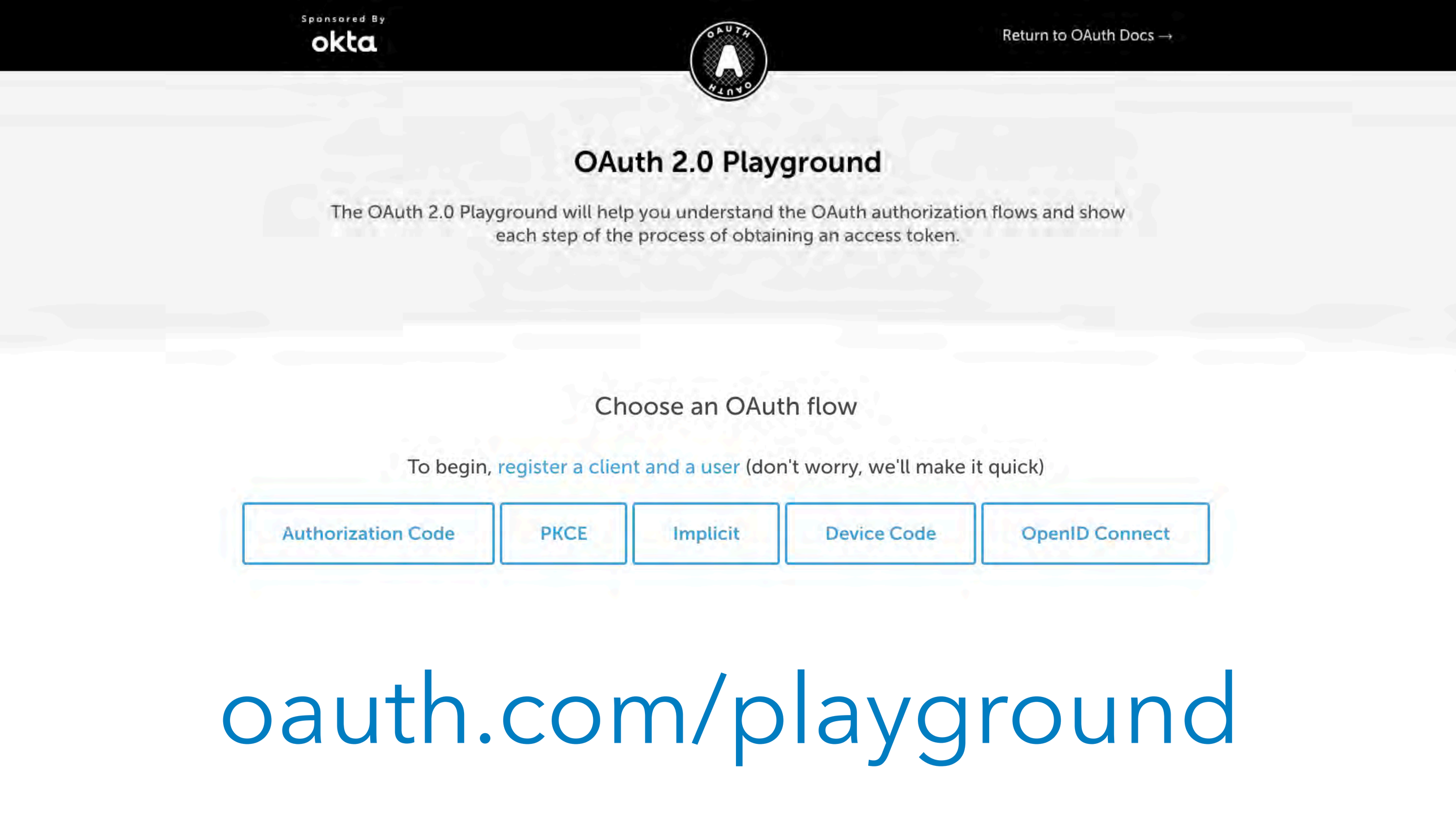
Read on for a complete guide to building your own authorization server.

Learn about OAuth 2.0 | Solve it with Okta

Table of Contents

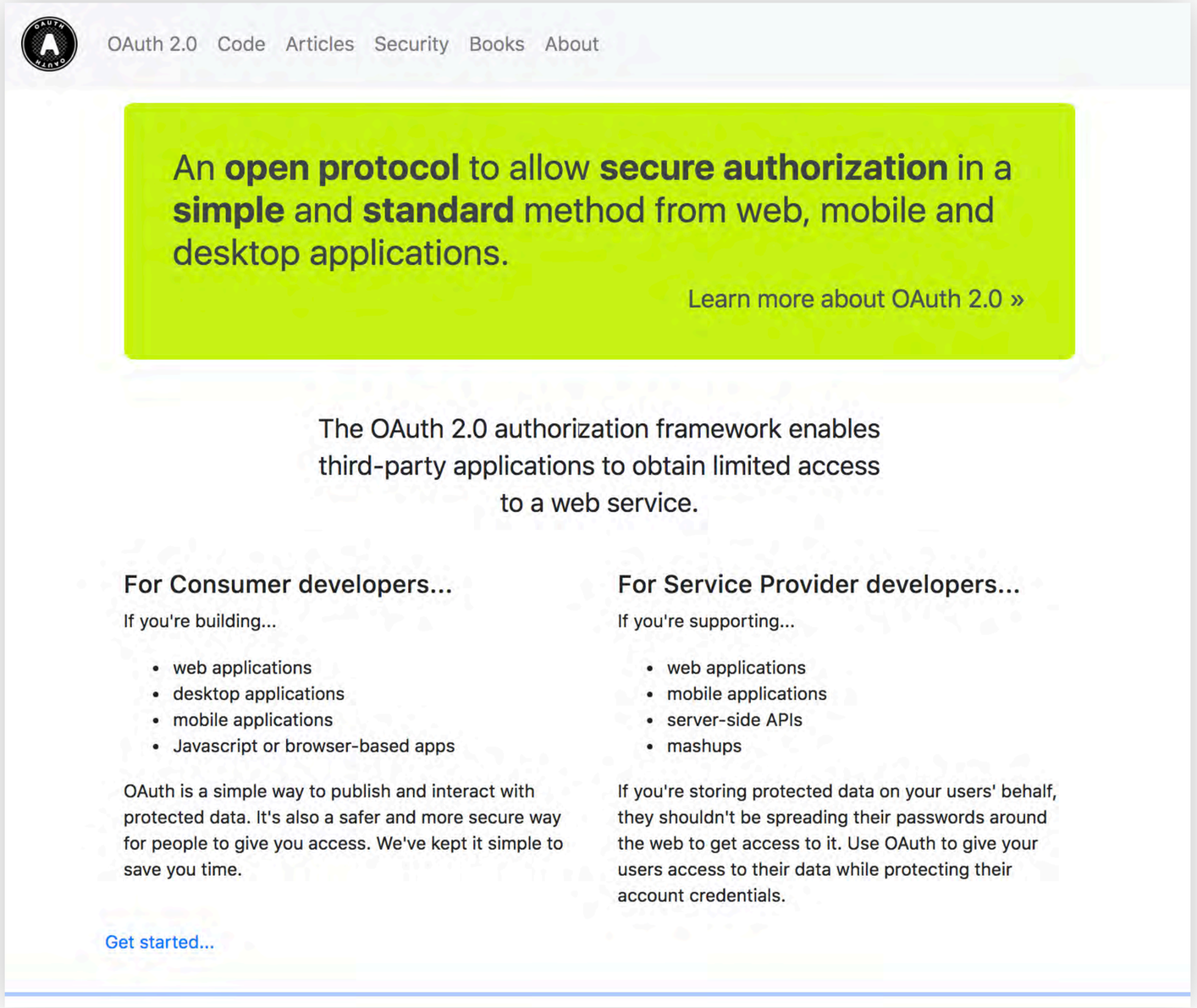
Search for a Topic

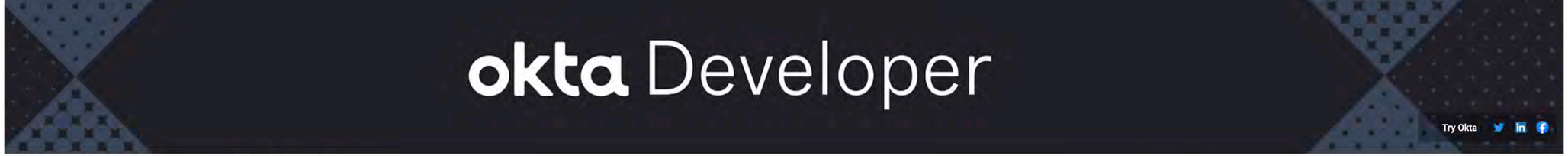
oauth.com



oauth.com/playground

oauth.net

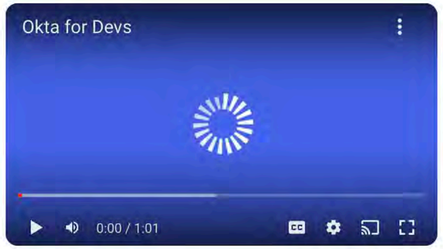

OAuth 2.0
Code
Articles
Security
Books
About
An **open protocol** to allow **secure authorization** in a **simple** and **standard** method from web, mobile and desktop applications.
Learn more about OAuth 2.0 »
The OAuth 2.0 authorization framework enables third-party applications to obtain limited access to a web service.
For Consumer developers...
If you're building...
web applications
desktop applications
mobile applications
Javascript or browser-based apps
OAuth is a simple way to publish and interact with protected data. It's also a safer and more secure way for people to give you access. We've kept it simple to save you time.
For Service Provider developers...
If you're supporting...
web applications
mobile applications
server-side APIs
mashups
If you're storing protected data on your users' behalf, they shouldn't be spreading their passwords around the web to get access to it. Use OAuth to give your users access to their data while protecting their account credentials.
Get started...



OktaDev
@OktaDev
43.9K subscribers

Subscribe

HOME VIDEOS SHORTS LIVE PLAYLISTS COMMUNITY CHANNELS ABOUT



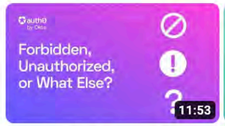
Okta for Devs

1,407 views • 3 months ago

At Okta, we believe in providing developers with the tools and information they need to add customer identity to their applications. Each month, 2.8 million developers turn to Okta and Auth0 for technical content, videos, podcasts, identity tools, and more. From building and implementation, to education and hands-on workshops, we support the developers every step of the way...

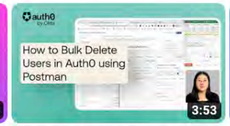
READ MORE

Videos ▶ Play all



Forbidden, Unauthorized, or What Else?

64 views • 7 hours ago



How to Bulk Delete Users in Auth0 Using Postman

93 views • 1 day ago

CC

Syncing Stripe with Auth0 Using Actions

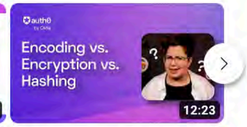
138 views • 5 days ago

How SAML Authentication Works

831 views • 7 days ago

Multi-factor Authentication (MFA) - Add More Security t...

189 views • 12 days ago



Encoding, Encryption and Hashing -- What's the...

626 views • 2 weeks ago

What is OAuth and OpenID Connect? ▶ Play all

What's New With OAuth and OIDC?

OktaDev
33K views • 2 years ago

How to Hack OAuth

OktaDev
35K views • 2 years ago

What is OAuth and why does it matter? - OAuth in Five...

OktaDev
109K views • 3 years ago

CC

What's the difference between Confidential and...

OktaDev
21K views • 3 years ago

OAuth 2.0 access tokens explained

OktaDev
134K views • 4 years ago

CC

OAuth Phishing? - OAuth in Five Minutes

OktaDev
6.9K views • 2 years ago

youtube.com/oktadev

The Nuts and Bolts of OAuth 2.0

Covering OAuth 2.0, OpenID, PKCE, deprecated flows, JWTs, API Gateways, and scopes. No programming knowledge needed

4.5 | 21 Enrolled | 3 hours, 32 minutes | Created by Aaron Parecki | Updated Dec 2020 | CC, English

Enroll Now

This course includes

- 3 hours, 32 minutes on-demand video
- 4 Quizzes
- Full lifetime access
- Access on mobile, desktop and TV
- Certificate of Completion

oauth2simplified.com/course

Advanced OAuth Security

Learn the high-security OAuth extensions described in FAPI: PAR, JAR, JARM, DPoP, Mutual TLS, and HTTP Signatures

Bestseller 4.7 ★★★★½ (42 ratings) 463 students

Created by Aaron Parecki

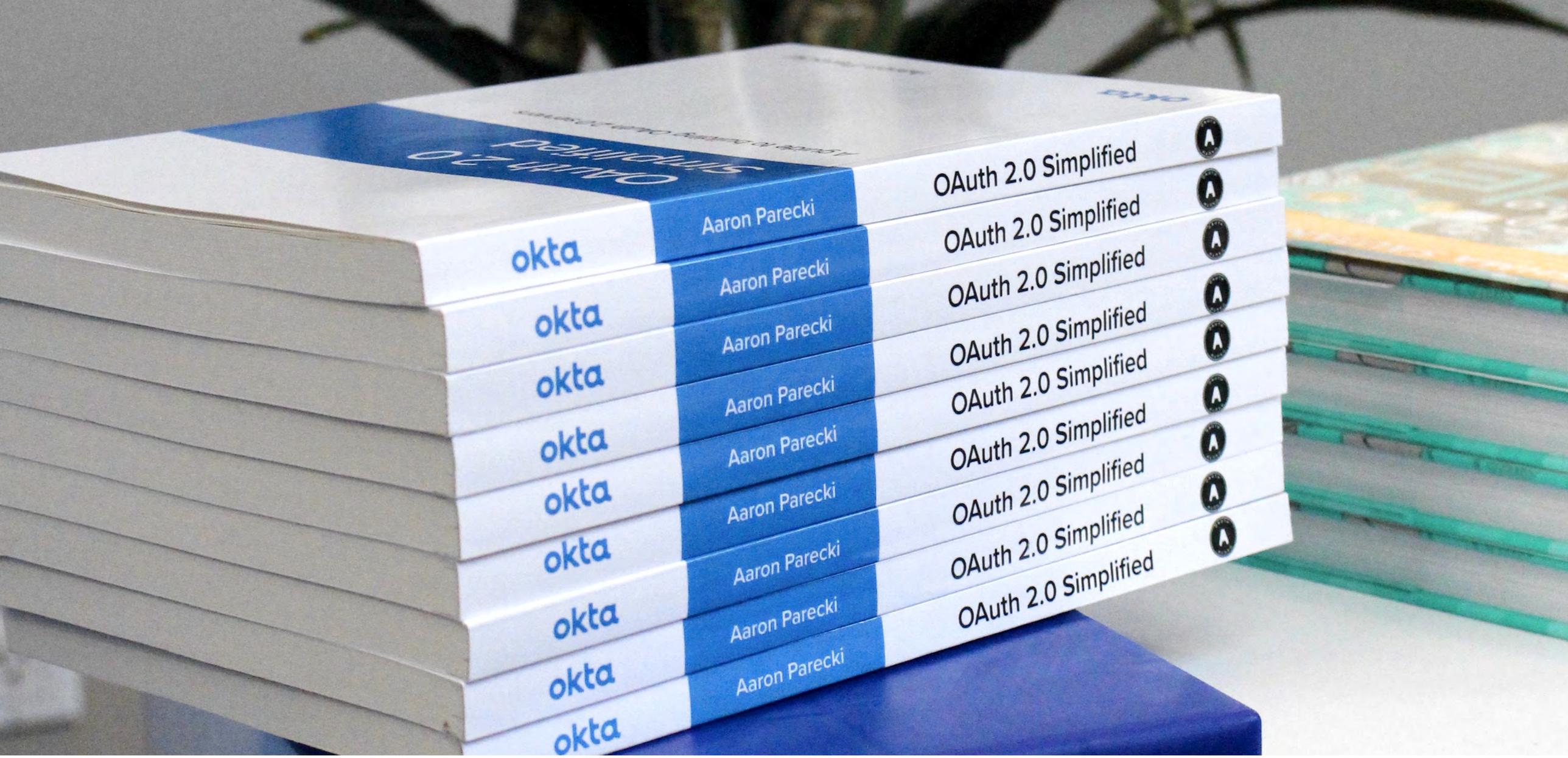
Last updated 12/2022

English

English

Add to cart

oauth2simplified.com/advanced-oauth



oauth2simplified.com

Thank You!

@aaronpk

oauth2simplified.com