

# Password-less Login at Skyscanner



Michael Baldock – Senior Software Engineer at Skyscanner

Twitter (X): @MichaelBaldock

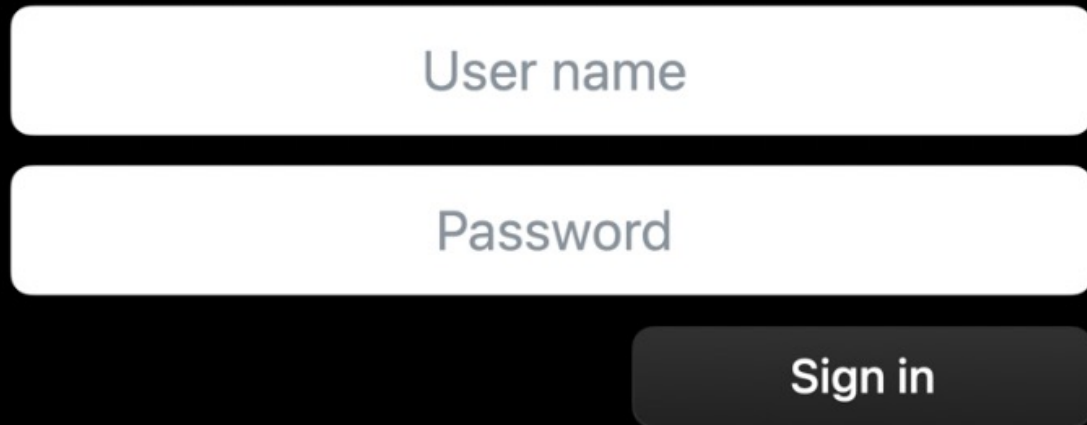
# Contents

- The Problem With Passwords
- Product Expectations
- How did we build it?
- Did we solve the problems?
- Web Authn & Passkeys



# The Problems With Passwords





User name

Password

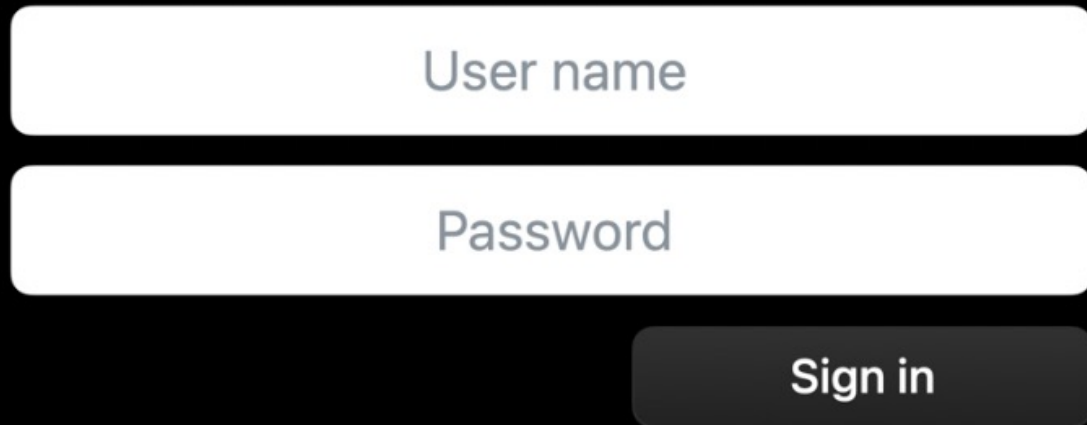
Sign in

# The Email Password Form

Simple to Use

Users know what's expected

*Source: Verizon 2023 Data Breach Investigations Report*



User name

Password

Sign in

# Industry lessons

Protecting Secrets is Hard

Phishing is very common

Weak & reused passwords make problems worse

*Source: Verizon 2023 Data Breach Investigations Report*

Stolen data	% of breaches
-------------	---------------

Email addresses 2.8%

Passwords	2.3%
-----------	------

U usernames 1.6%

# Data Breach Statistics

Email & Passwords are the most stolen form of data

Huge numbers of credential exist on the internet black market

Company	Date	User Records Breached
---------	------	-----------------------

Yahoo 2013 & 2014 3,000,000,000

Sina Weibo	2020	538,000,000
------------	------	-------------

Marriott International 2014-2018 500,000,000

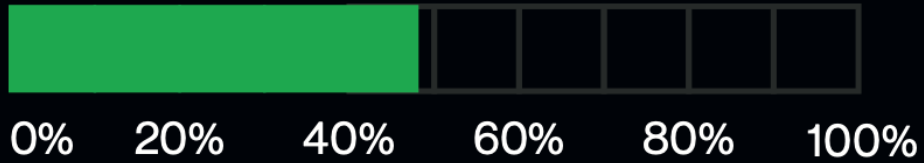
Adult Friend Finder	2016	412,200,000
---------------------	------	-------------

MySpace 2013 359,420,698

Source: <https://www.uswitch.com/broadband/studies/data-breaches-report/#most-commonly-stolen-data>

2023

49%



## Credential theft is on the rise

49% of breaches by external actors involved use of stolen credentials

This statistic has increased by 12% since 2020

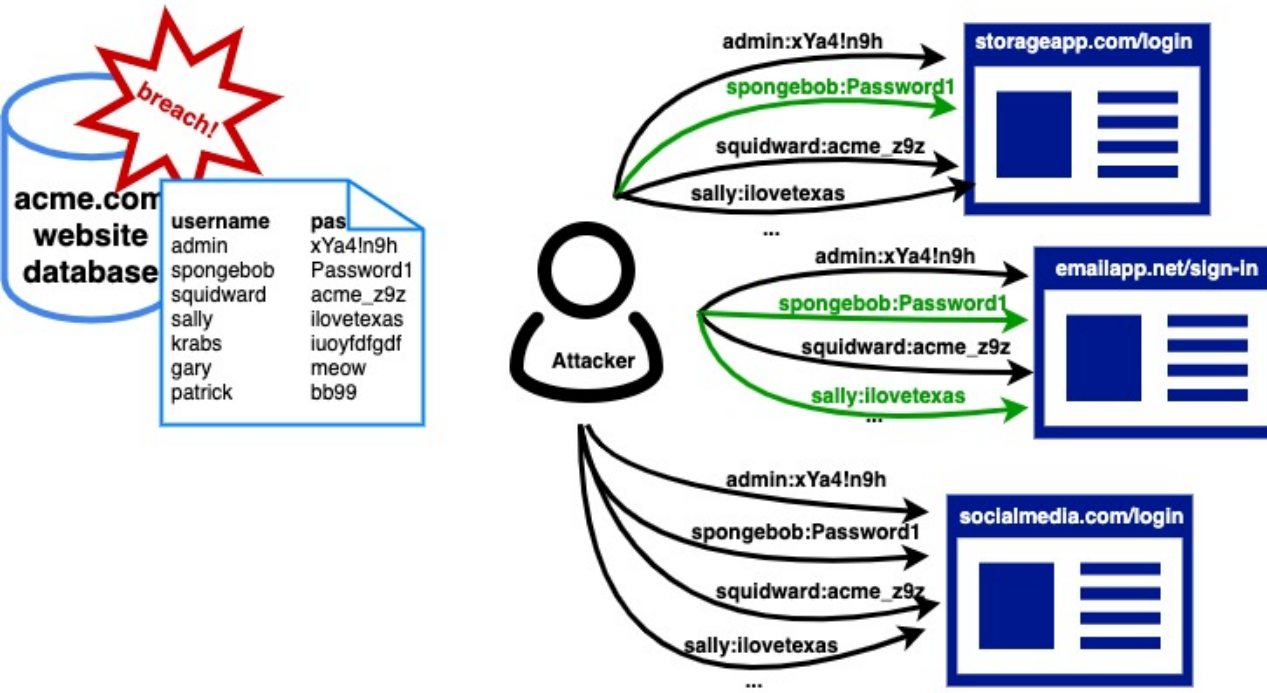
2020

37% of breaches stole or used credentials



Source: <https://www.uswitch.com/broadband/studies/data-breaches-report/#most-commonly-stolen-data>

# Credential Stuffing



Inject stolen credentials into login forms across the internet.

Can lead to account takeover, or increase the value of known 'good' credentials



TECH

**Amazon hit with \$887 million fine by European privacy watchdog**

**Google's \$400m penalty and impact of the 5 heftiest data privacy fines on 2023 ad plans**

News

**Meta slapped with 5.5 mn euro fine for EU data breach**

# The Consequences of Data Breaches

Must notify (ICO) authority within 72 hours

**Are your users telling you something?**

**35% of travellers who logged in  
'*successfully*' with a password had gone  
through the forgot password flow**



**So how can you protect your  
business and your users?**

**Don't allow passwords!**



# Product Designs



Product Expectation


# Sign In With Apple

The *simplest*  
passwordless option



Apple ID

Cancel



Create an account for Homely using your Apple ID  
ryan.christoffel@homely.com

NAME Ryan Christoffel

Continue

# Frictionless Signup

The existing flow already had very little friction



## Previous Flow

1.

Email:

Password:

2.



You've signed up

# Frictionless Signup

But we can make it even smoother!

No Password or  
Passcode required at  
sign-up



# Password-less Flow

1.

What's your  
email address?

2.



You've signed up

Product Expectation

# Help Lost Travellers

A social sign-up should be able to log back in with their email without friction



1 year later...



**What's your  
email address?**

4-digit verification code

--	--	--	--



**You've signed in**





# Product Expectations Summary

Sign-up with only an email

A *social* sign-up should be able to log back in using their email & a passcode



# Technical Requirements

- We continue to integrate with Auth0
- We (and Auth0) use OAuth as our Identity protocol

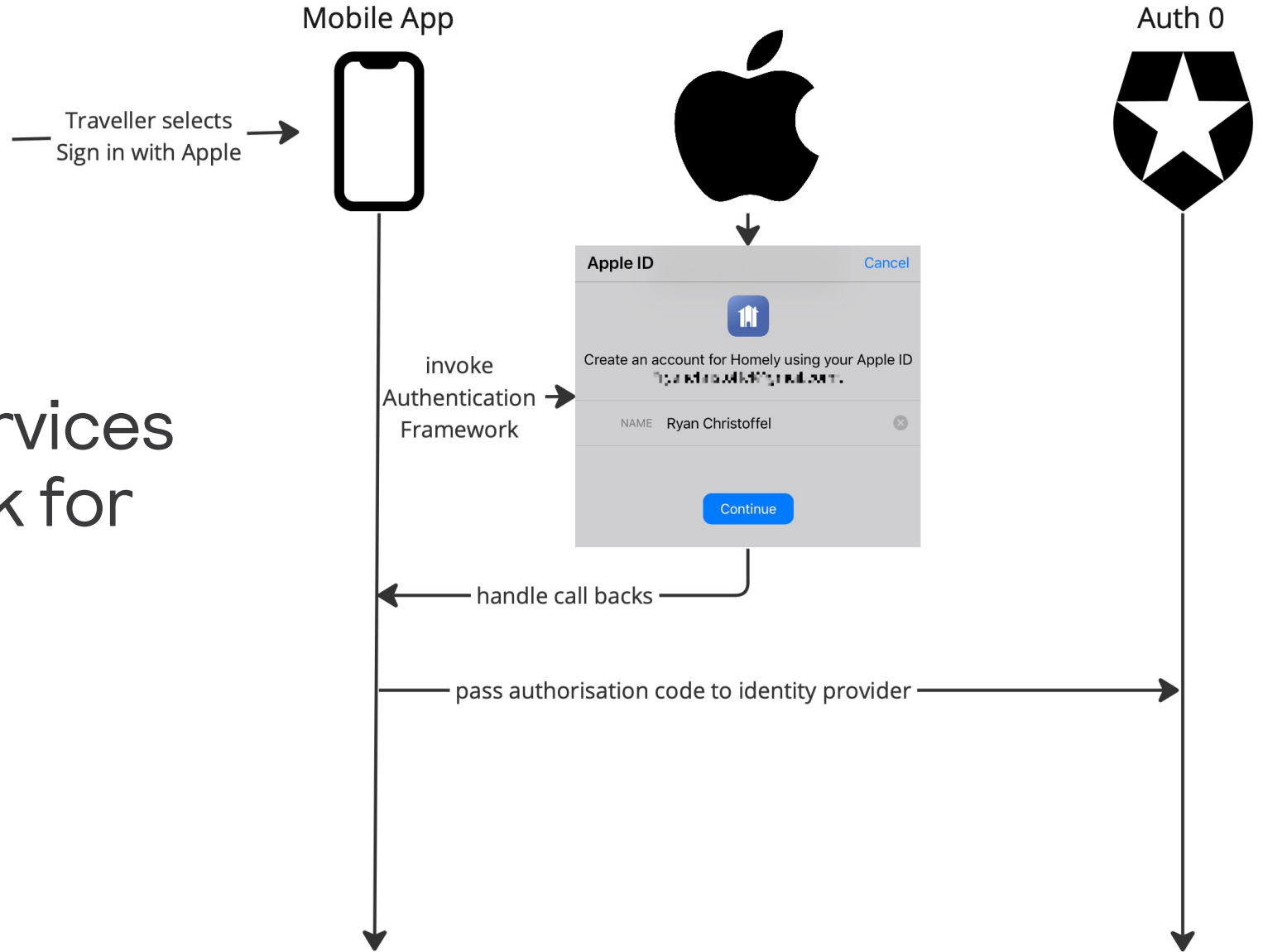


# So how did we Build it then?



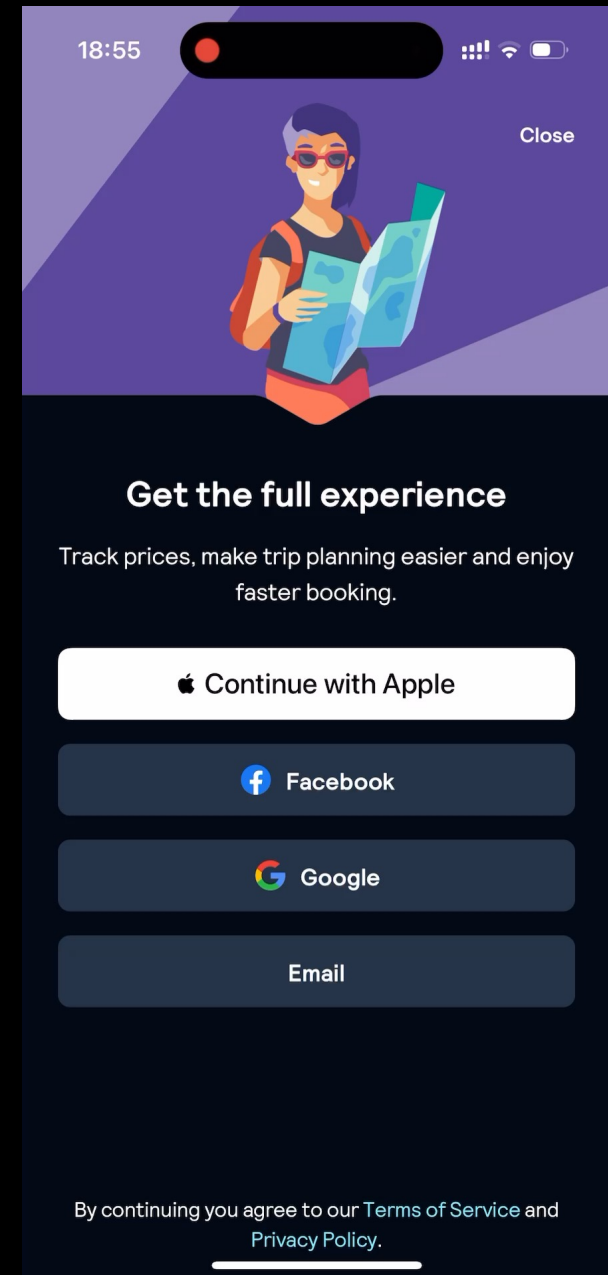
# Sign In With Apple

Authentication Services  
does the hard work for  
you



# Sign In With Apple Demo

Sign In With Apple is a simple workflow for users and engineers



# Passwordless Auth0 Interface Options

What's your email address?

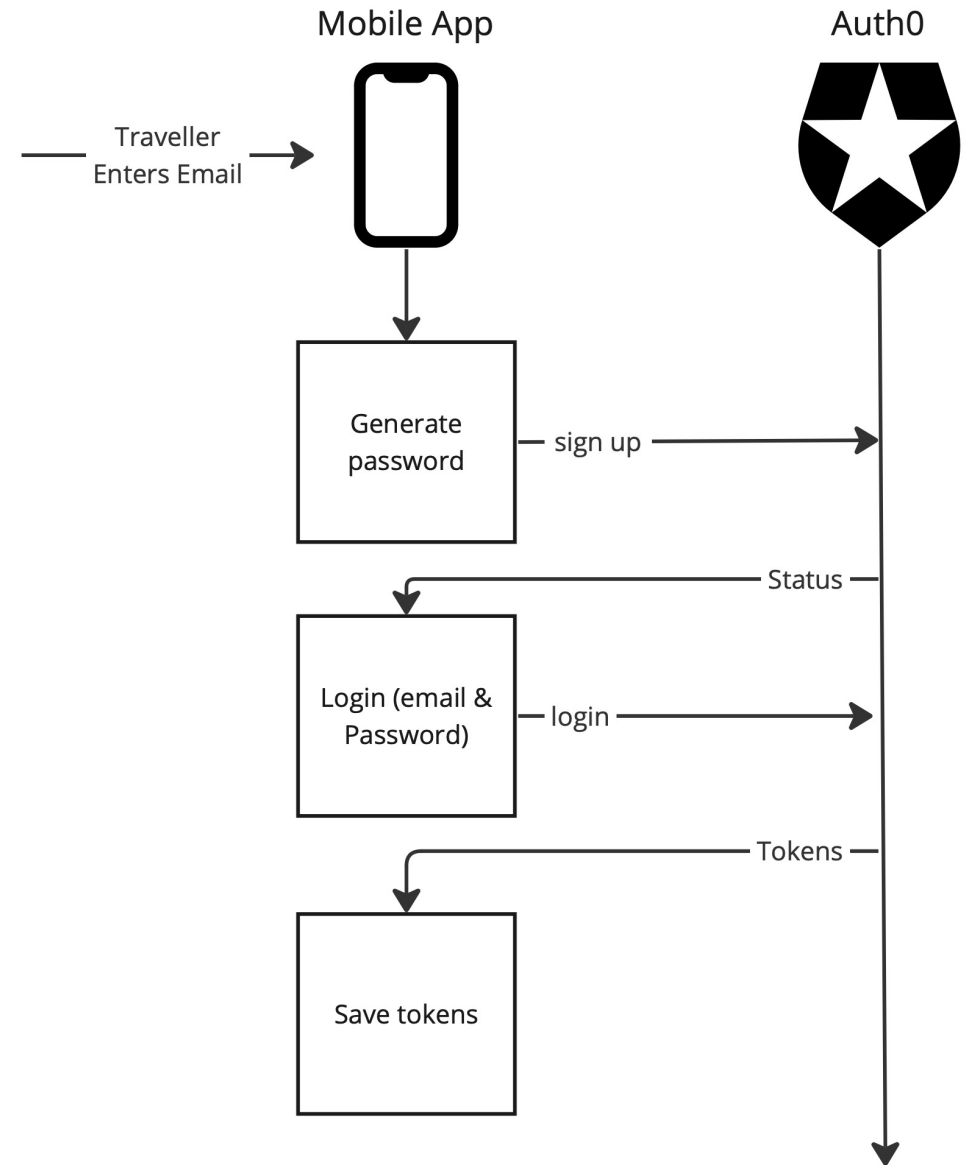
Auth0 APIs:

API	Process	Requirements
Password-less Signup	<ol style="list-style-type: none"><li>1. Send OTP to an email</li><li>2. Sign-up with username <i>and</i> OTP</li></ol>	<div>username REQUIRED</div> <div>otp REQUIRED</div>
Email & Password Sign-up	<ol style="list-style-type: none"><li>1. User enters credentials</li><li>2. Sign-up to create an account</li></ol>	<div>email REQUIRED</div> <div>password REQUIRED</div>



# Here's the Trick

We allow one password,  
one time only



# Is this a security risk?

- Our passwords are generated, they will not appear in leaks from other websites
- If we are hacked, then there are *no* password in our system.









# Sign up Demo

## Password-less Login in Skyscanner App




19:19    


<

**What's your email address?**

**Next**

for skyscanner.net carlos55.cactus@gmail.com for skyscanner.net Michael.baldock@skyscan... 

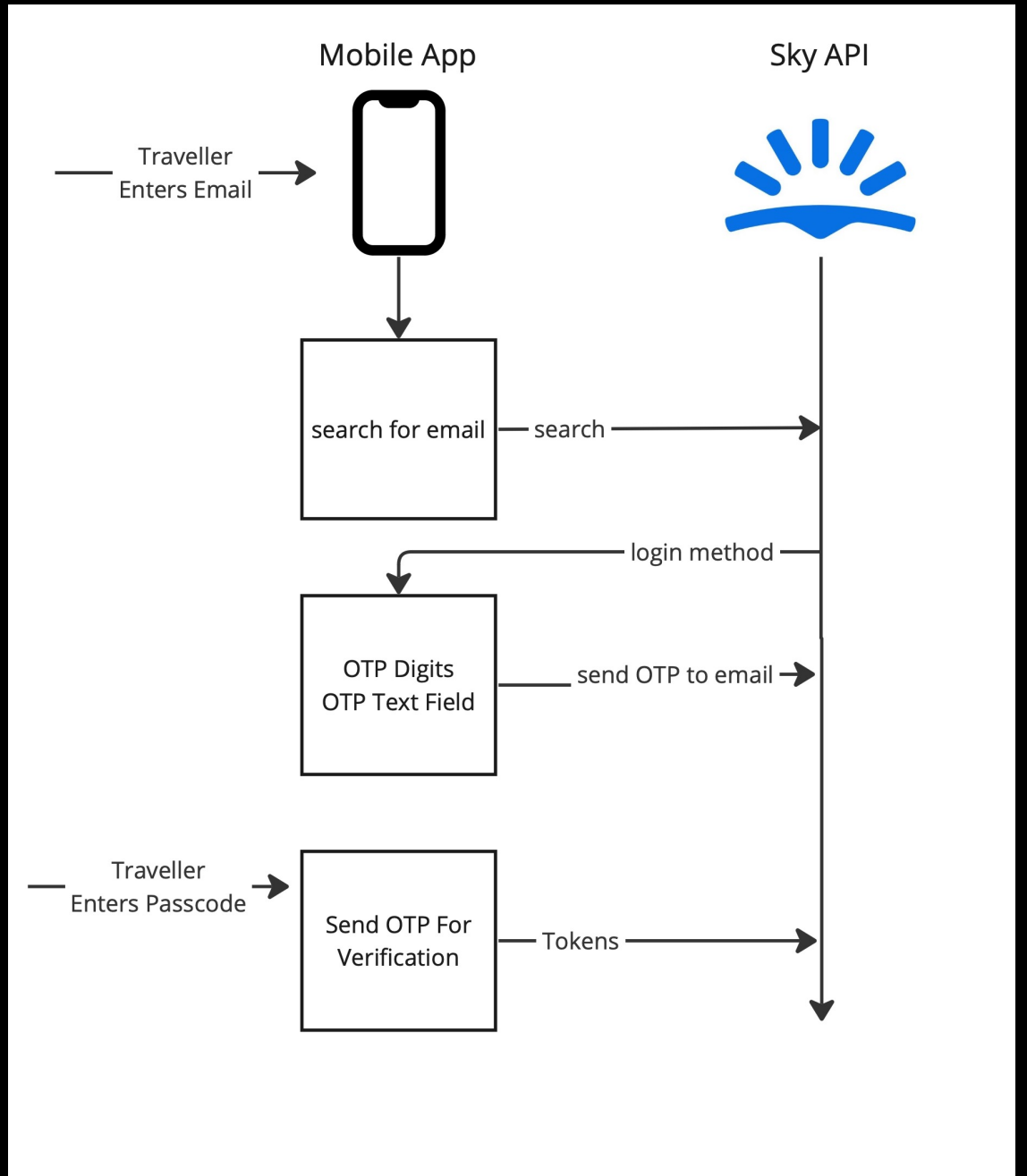
q w e r t y u i o p  
a s d f g h j k l  
⬆ z x c v b n m ⬇  
123 😊 space @ . next

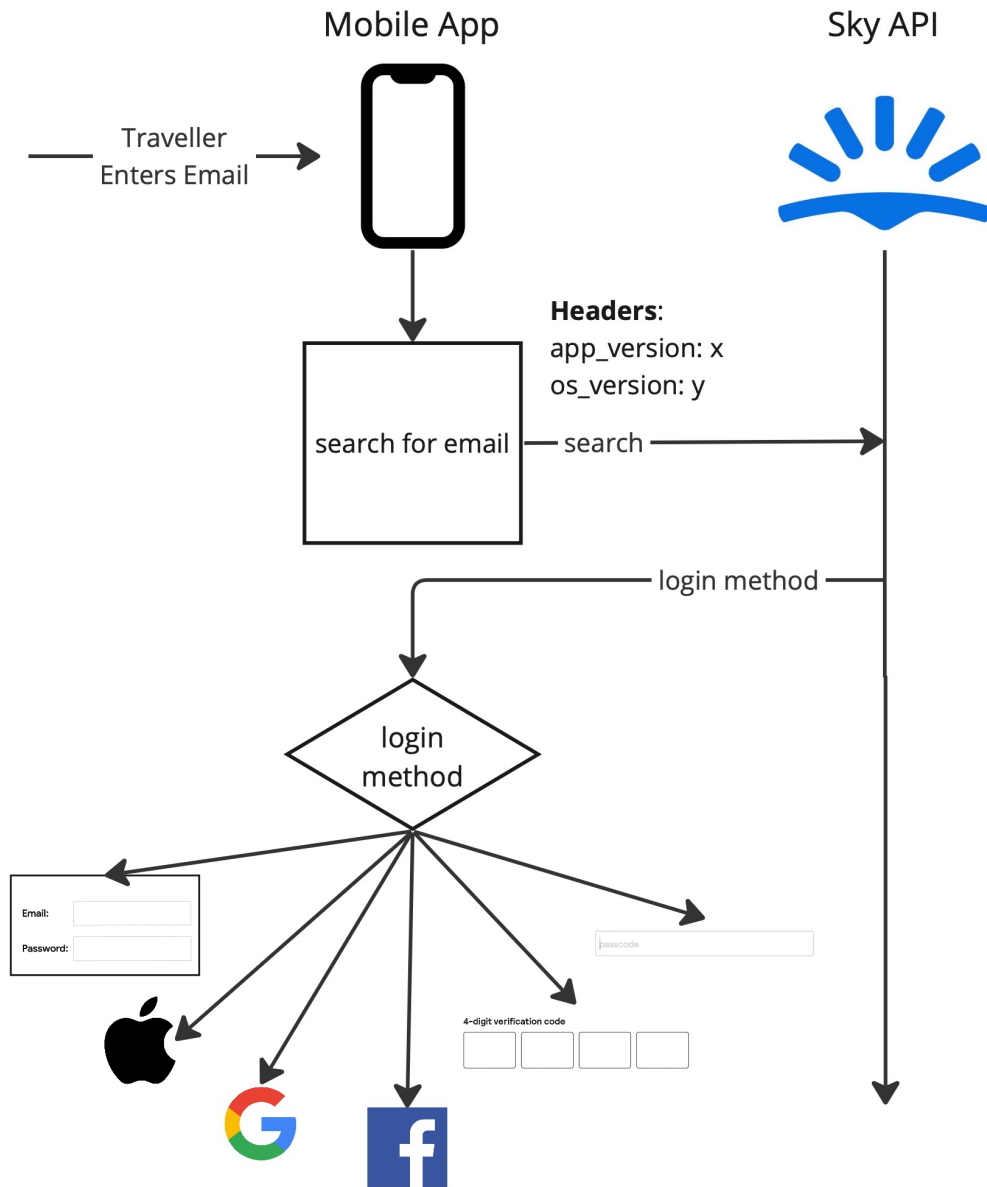


# Handling Login

Pass the email to the API.

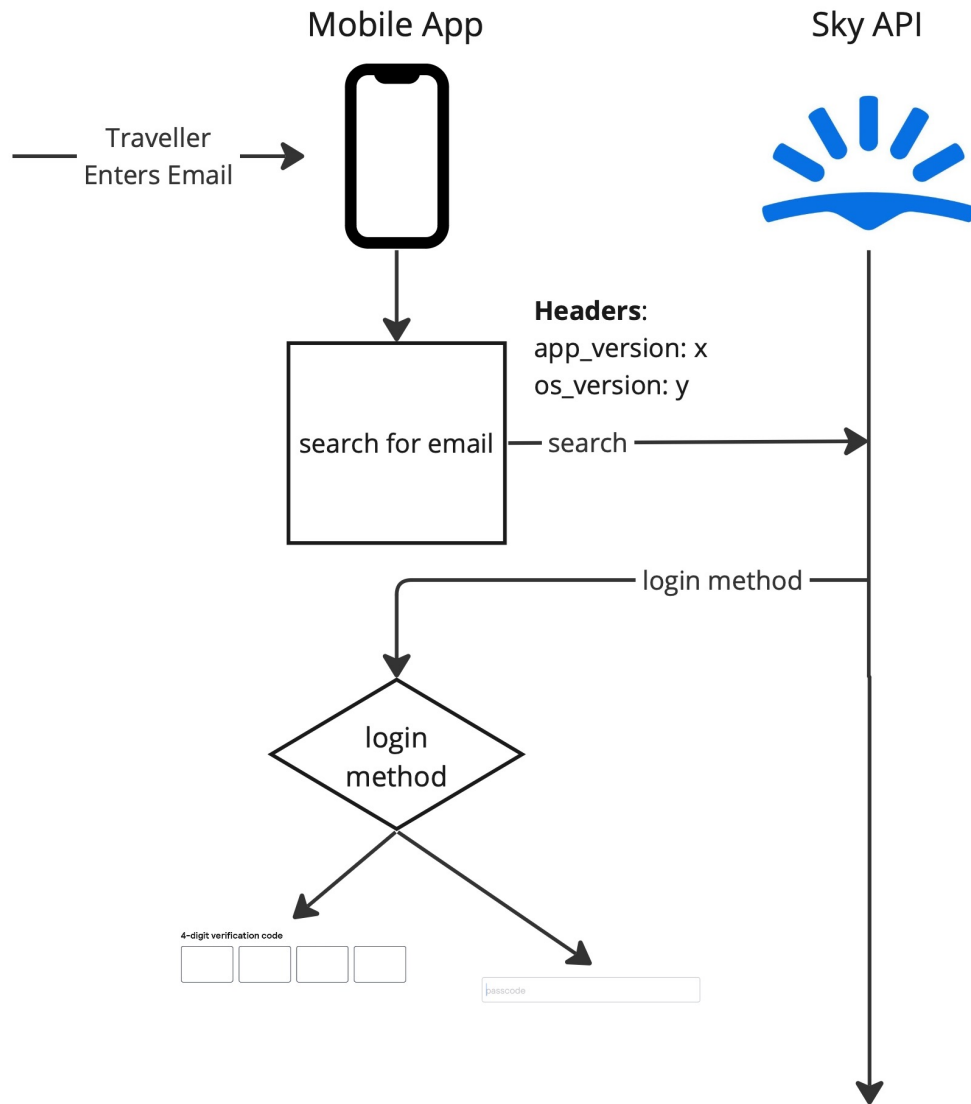
The API tells the front-end how to login





# Server Driven UI – Login Method

Rolling out the new feature could be managed by the back-end



# A little piece of Server Driven UI

We have only kept the flexibility to switch between 4 digit and any character passcodes

# Login With OTP Demo

Login with a One Time  
Passcode

A screenshot of a mobile application interface for login. At the top, the status bar shows the time 19:24, a red indicator light, and signal/battery icons. Below the status bar is a back arrow icon. The main heading is "What's your email address?". Below this is a text input field containing the email address "Michael.baldock@skyscanner.net". At the bottom of the screen is a blue button labeled "Next". A virtual keyboard is visible at the bottom, with keys for letters, numbers, and symbols. A globe icon is located at the very bottom of the screen.

**So how did  
passcodes  
perform?**



# 90% reduction in errors

Wrong password errors  
Forgot password flow errors  
No account exists errors



**25% increase in  
login success rate**





**170% increase in travellers logging in during checkout**

**35% increase in booking travellers who are logged in**



# The Results were good!

- And... Skyscanner Won a European Identity Award for Authentication!



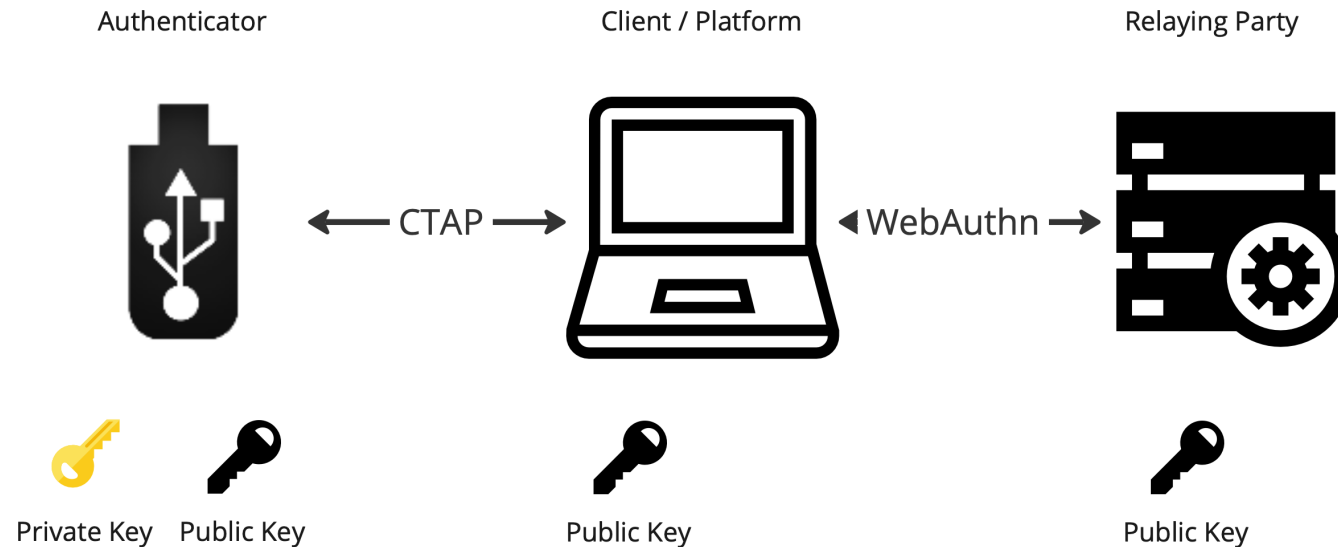
# Web Authn & Passkeys

(the next chapter)



# Web Authn

- Web Authn is an authentication protocol developed by FIDO alliance
  - **Fast Identity Online**

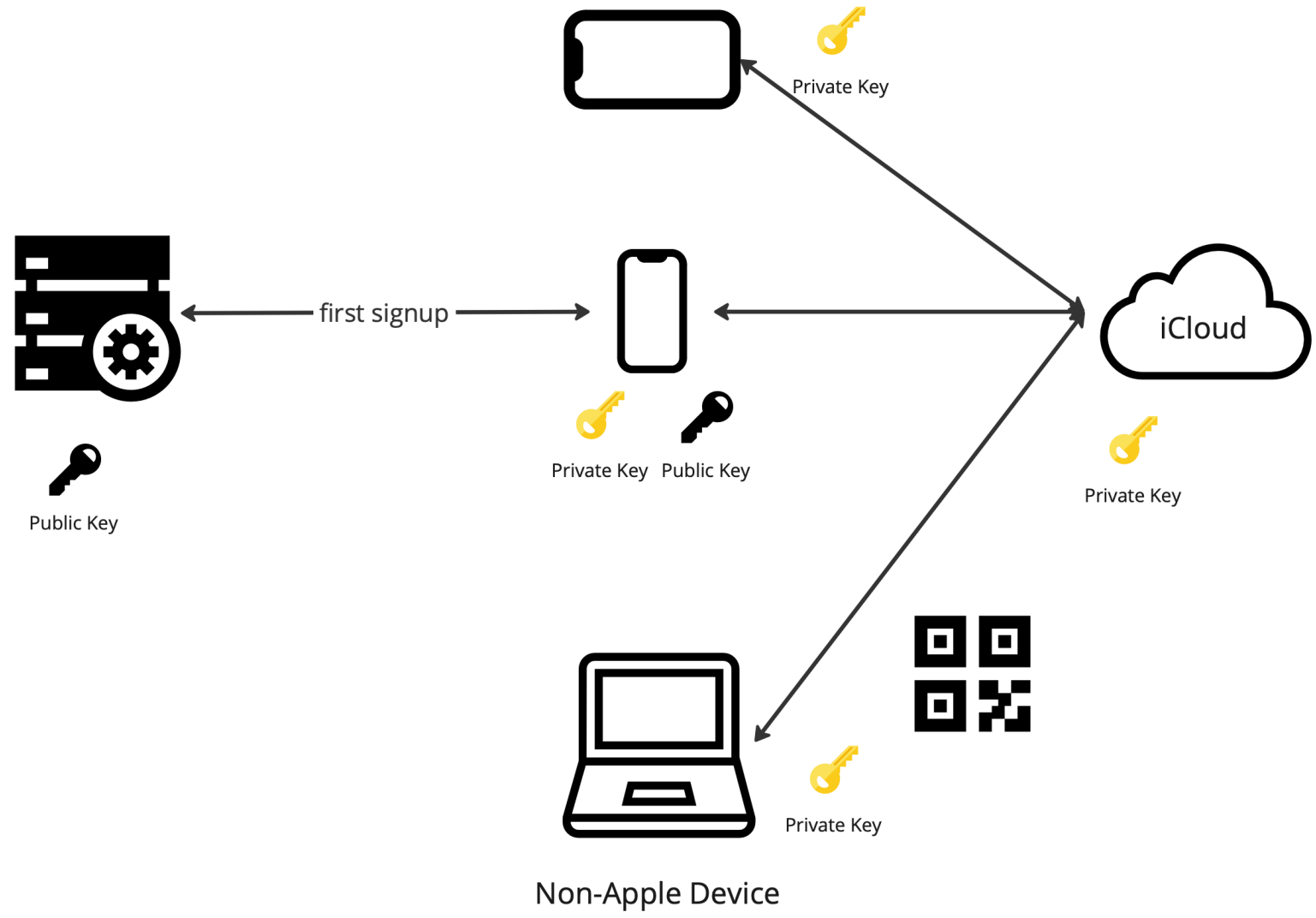


# & Passkeys...

- iOS 16 Apple release Passkeys
  - They are synced through your keychain
- Passkeys use the standard protocol developed by the FIDO alliance, also adopted by Google and Microsoft
- Passkeys can be sent from iCloud to other platforms using a QR code



# Passkeys



# Thanks for listening!

I hope this gave you some ideas about *why* to move away from passwords, and insight into how to go about it with iOS.

Twitter (X): @MichaelBaldock

