

Privacy and Your Apps

Session 702

Georgios Kontaxis, Privacy Engineering
Katie Skinner, Privacy Engineering

“People have entrusted us with their most personal information. We owe them nothing less than the best protection that we can possibly provide.”

Tim Cook, White House Cybersecurity Summit, February 2015

Agenda

Best practices

Updates

Features

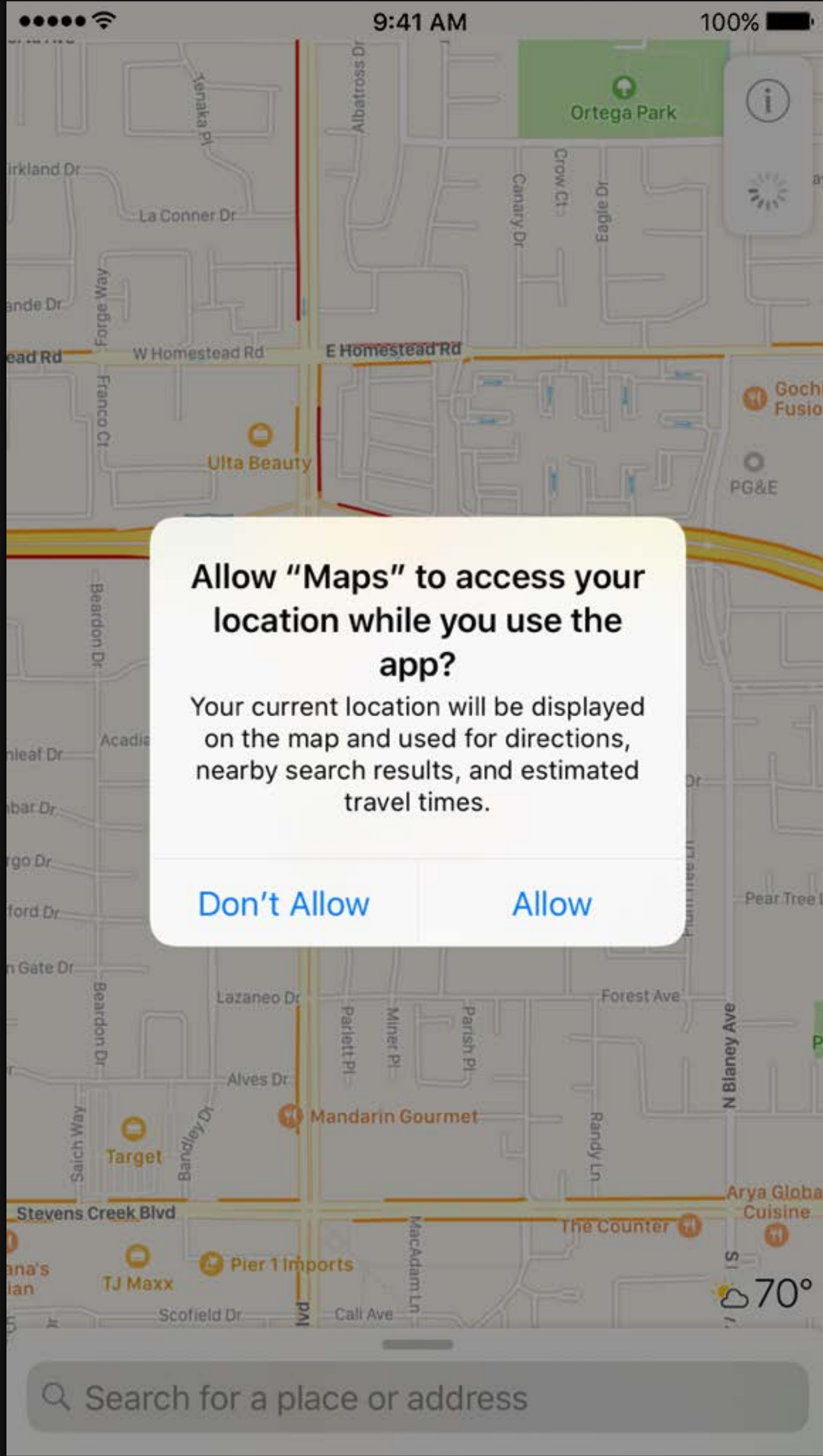
Transparency, Consent, and Control



Transparency about the use of data

Consent before collecting data

Users in control of their privacy



Allow "Maps" to access your location while you use the app?

Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.

Don't Allow

Allow

Search for a place or address

70°



9:41 AM

100%

[← Privacy](#)

Location Services

Location Services



Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. [About Location Services & Privacy...](#)

Location Services settings also apply to your Apple Watch.

Share My Location [>](#)



Calendar

While Using [>](#)



Camera

While Using [>](#)



Home

While Using [>](#)



Maps

While Using [>](#)



Siri & Dictation

While Using [>](#)



Weather

While Using [>](#)

System Services [>](#)

A hollow arrow indicates that an item may receive your location under certain conditions.

A purple arrow indicates that an item has recently used your location.

A gray arrow indicates that an item has used your location in the last 24 hours.

Identifying Devices and Users



Random

Anonymous

Short-lived

Easy to reset

OS-provided APIs

Universally Unique Identifier

Random

128-bit values

```
let uuid = UUID()
```

Call 1

8E2F725B-9E3B-459D-89C9-DAC743C174B4

Call 2

5C8E2D37-1C56-44B3-974A-928FE4D6C00C

Call 3

AD748A3A-56C2-4587-A5E2-713C7DBBEED6

Vendor Identifier

Same for apps with the same team ID

Resets when all vendor apps are uninstalled

```
let idForVendor = UIDevice.current.identifierForVendor
```

Team ID 1	App 1	BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376
Team ID 1	App 2	BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376
Team ID 2	App 1	045051D9-EED8-4D35-B2E2-62E6455CAD69

Vendor Identifier

Same for apps with the same team ID

Resets when all vendor apps are uninstalled

```
let idForVendor = UIDevice.current.identifierForVendor
```

Team ID 1	App 1	BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376
Team ID 1	App 2	BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376
Team ID 2	App 1	045051D9-EED8-4D35-B2E2-62E6455CAD69

Tailoring Data Collection to Your Needs



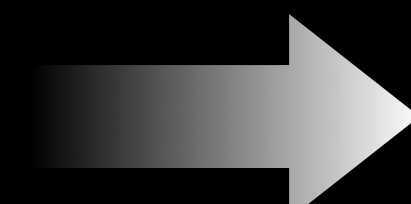
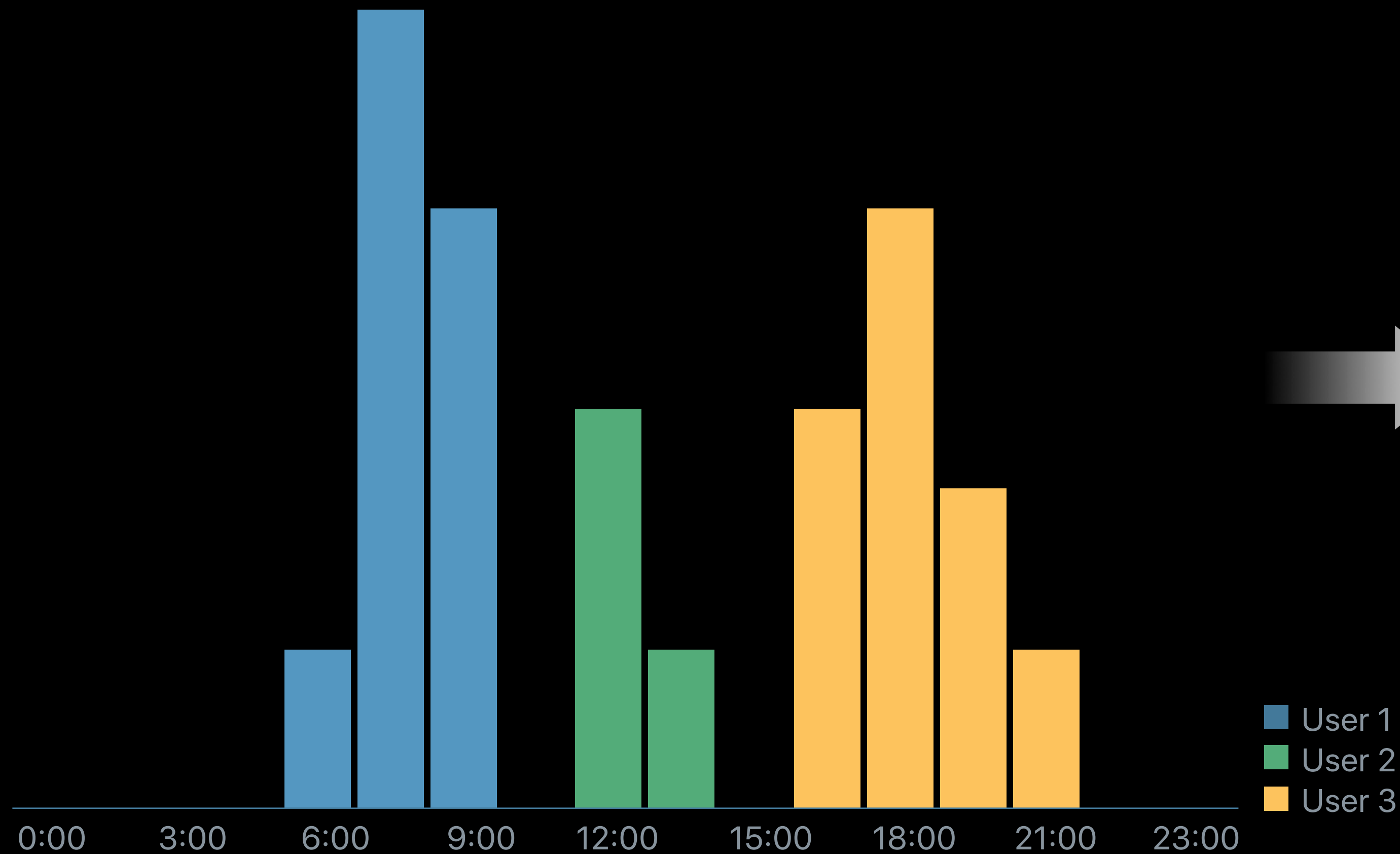
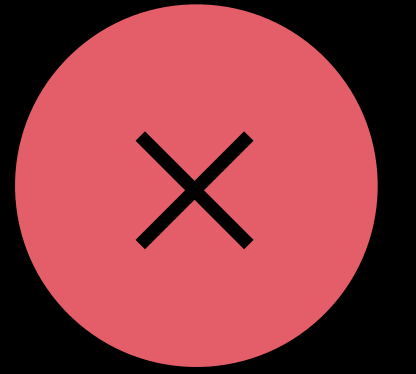
Aggregation

Sampling

On-device processing

Raw Data May Reveal Additional Information

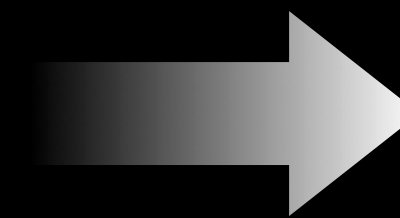
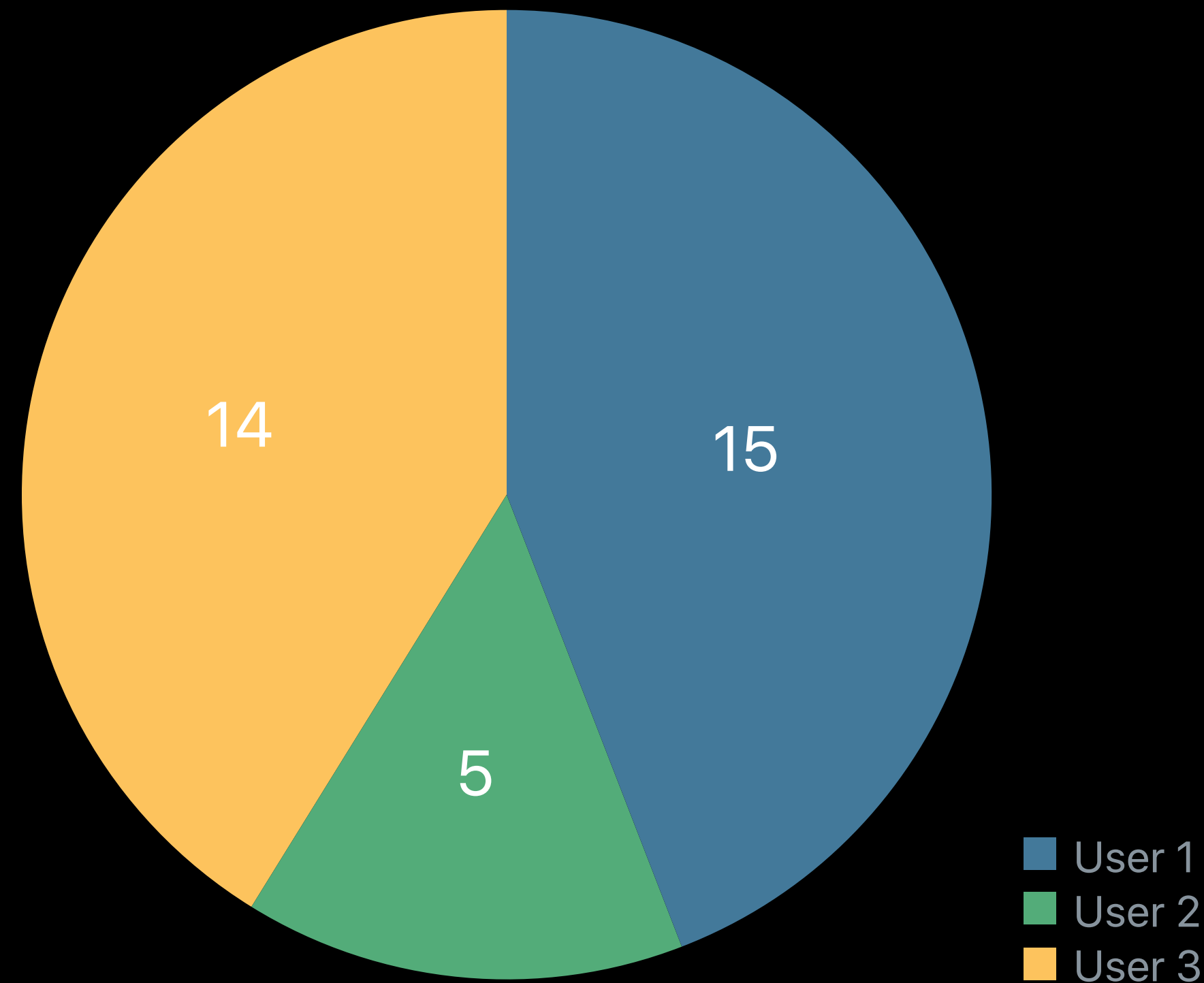
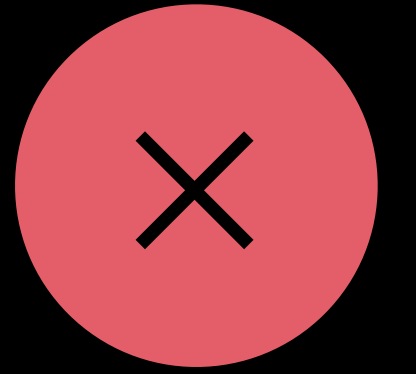
How frequently do users engage with my latest feature?



User 1 is a morning person
User 2 uses the app during lunch
User 3 prefers the night

Raw Data May Reveal Additional Information

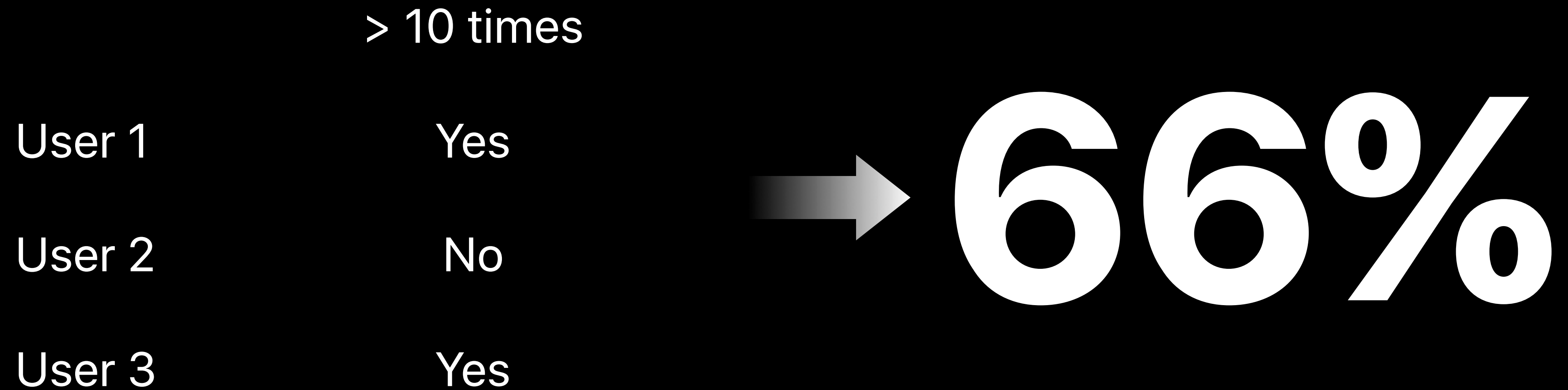
How frequently do users engage with my latest feature?



User 1 likes the feature the most
User 2 likes the feature the least

Aggregation Focuses on the Big Picture

How many users engage with my feature more than 10 times?



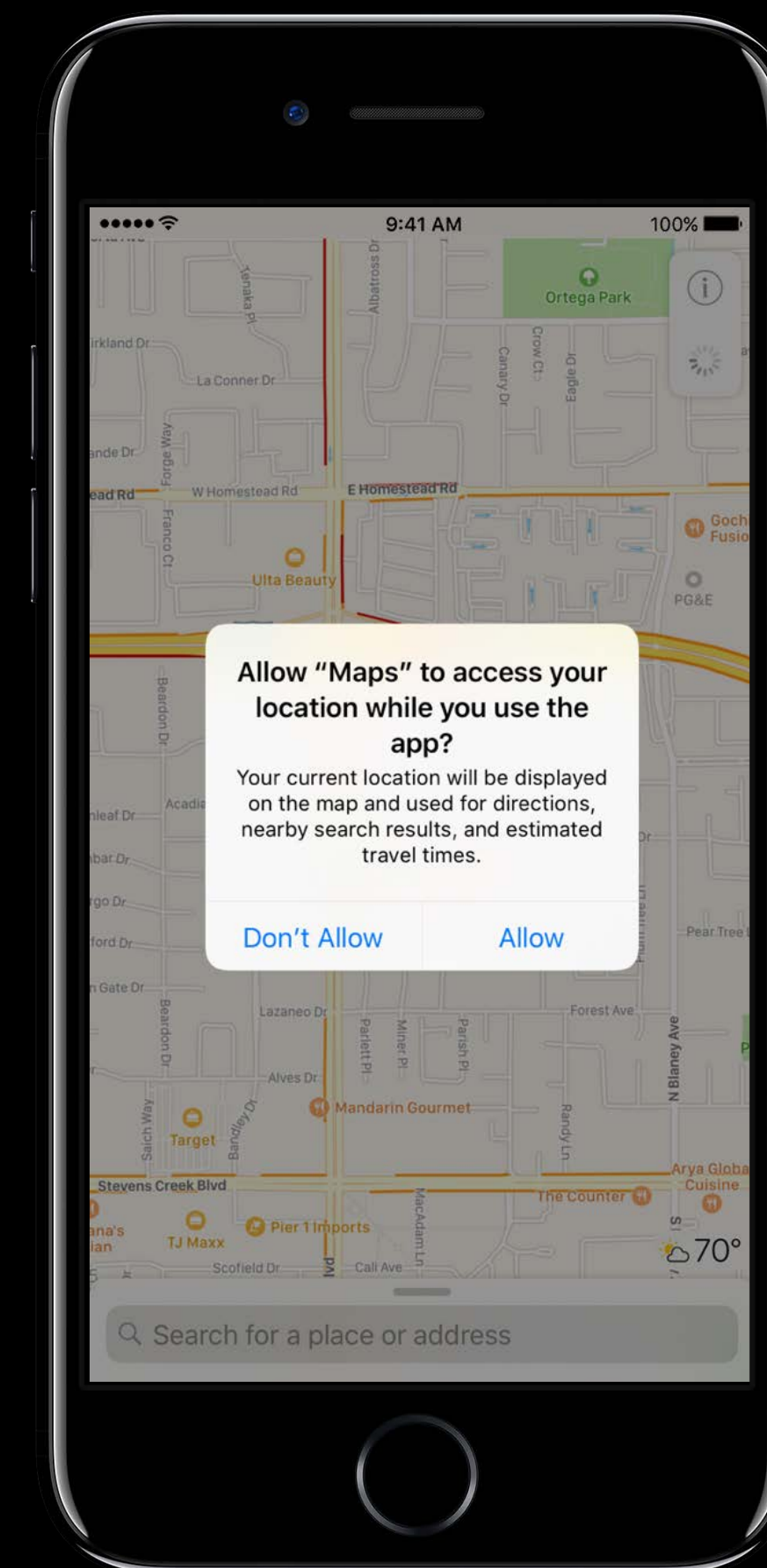
Updates

Prompting with Purpose

Some access requests require a purpose string

Specific ask enables informed user decisions

```
Info.plist: NSLocationUsageDescription
```

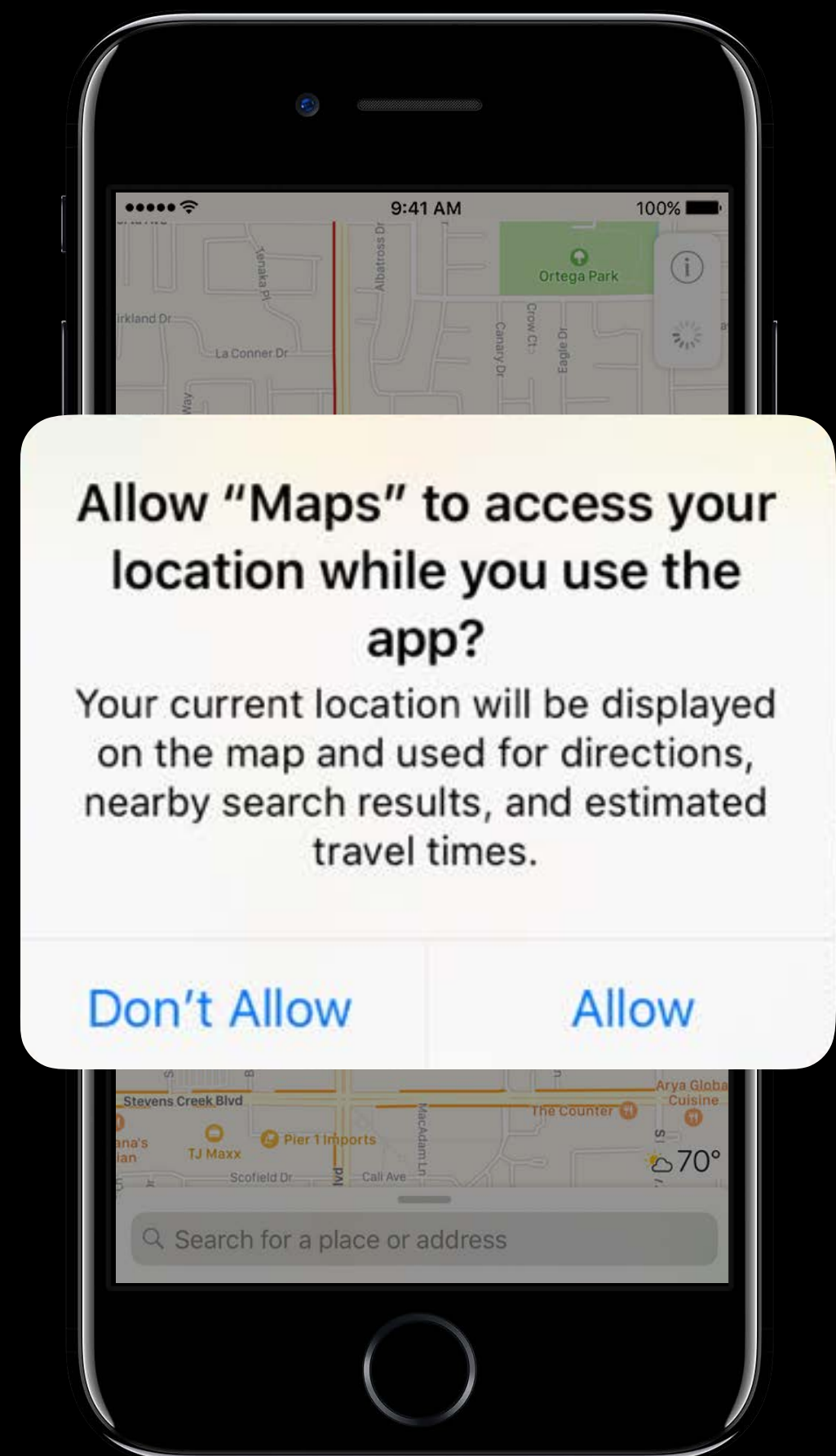


Prompting with Purpose

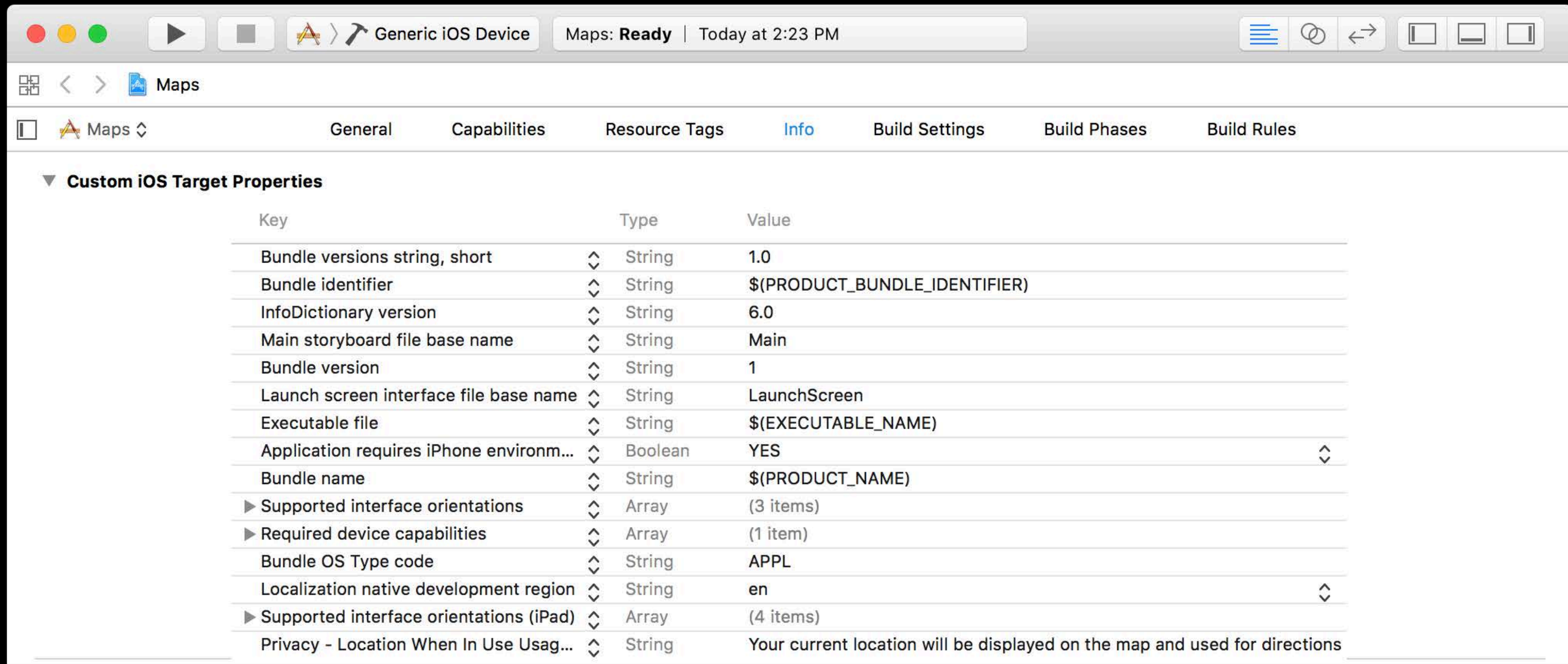
Some access requests require a purpose string

Specific ask enables informed user decisions

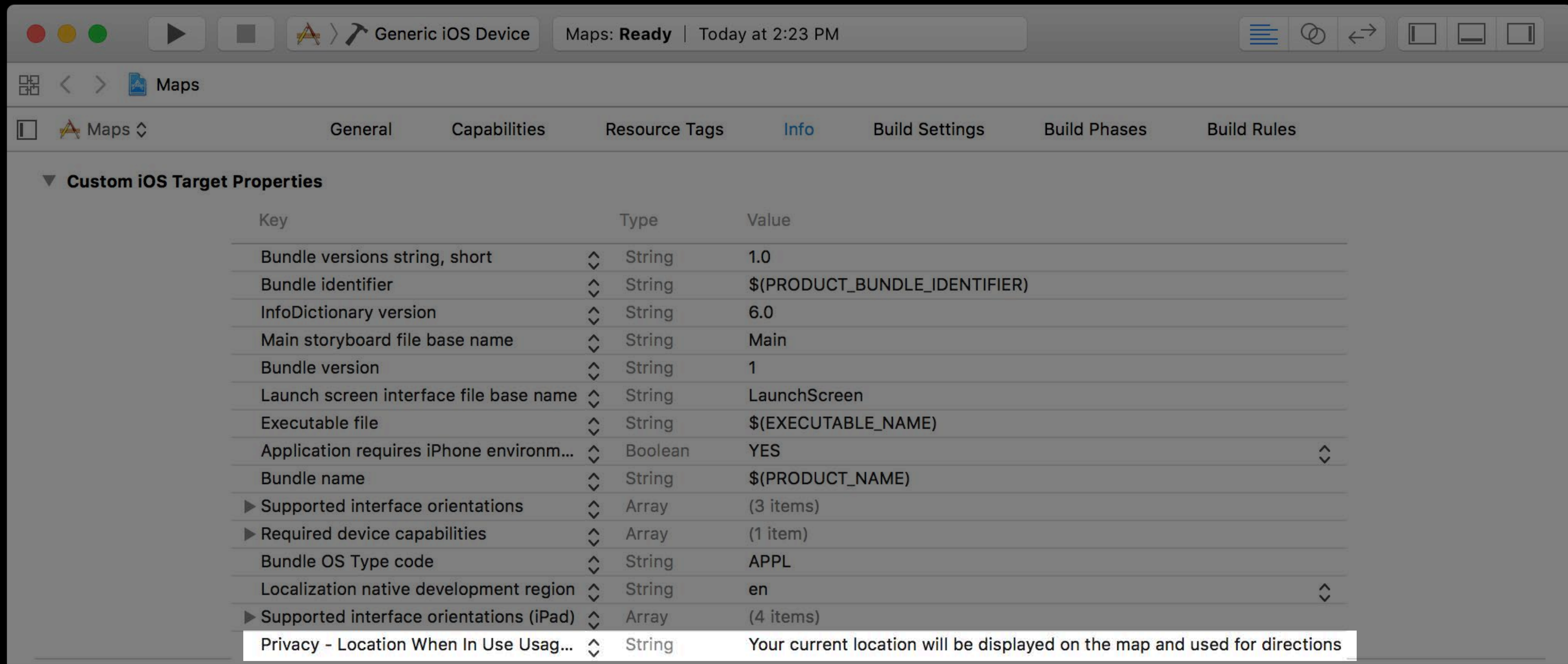
```
Info.plist: NSLocationUsageDescription
```



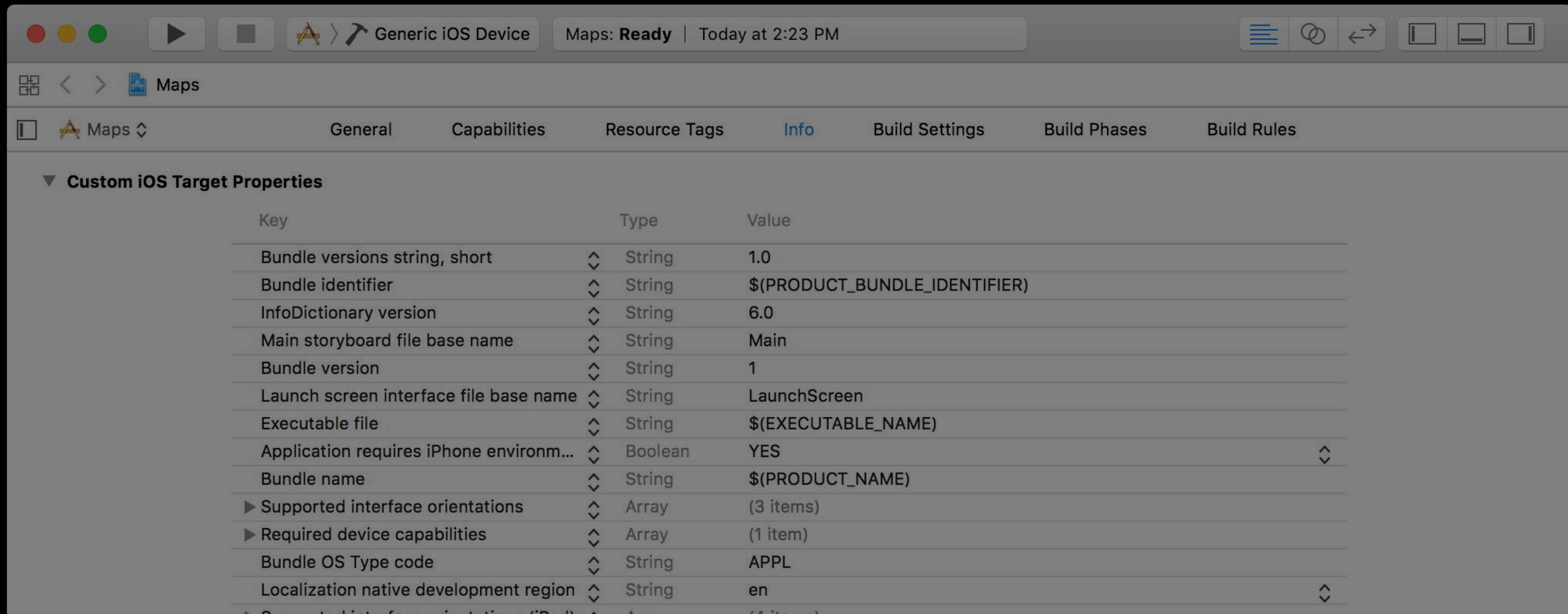
Add Purpose String in Xcode



Add Purpose String in Xcode



Add Purpose String in Xcode



Privacy - Location When In Use Usag... String Your current location will be displayed on the map and used for directions

Purpose Strings are Mandatory

Exception Type: EXC_CRASH (SIGABRT)

Application Specific Information:

This app has crashed because it attempted to access privacy-sensitive data without a usage description.

The app's Info.plist must contain a NSCameraUsageDescription key with a string value explaining to the user how the app uses this data.

Purpose String Required

iOS 10

Contacts

Camera

CallKit

Calendar

Photos

Speech Recognition

Reminders

Health

SiriKit

Location

HomeKit

TV Provider

Bluetooth Sharing

Media Library

Microphone

Motion and Fitness

Purpose String Required

iOS 11

Contacts

Camera

CallKit

Calendar

Photos

Speech Recognition

Reminders

Health

SiriKit

Location

HomeKit

TV Provider

Bluetooth Sharing

Media Library

NFC

Microphone

Motion and Fitness

San Francisco

Mostly Cloudy

60°

Thu		54
Now		18
		59
Friday		63 53
Saturday		62 52
Sunday		63 51
Monday		67 51
Tuesday		67 52
Wednesday		68 54
Thursday		66 53

Allow "Weather" to access your location even when you are not using the app?

Your location is used to show local weather in the Weather app and widget.

[Don't Allow](#) [Allow](#)



9:41 AM



San Francisco

Cloudy

58°

Allow "Weather" to access your location?

Your location is used to show local weather in the Weather app and widget.

Only While Using the App

Always Allow

Don't Allow

Thursday 63 53

Now 3PM

58° 62°

Friday 63 52

Saturday 62 51

Sunday 63 51

Monday 67 52

Tuesday 66 52

Wednesday 67 54



CoreLocation—When In Use

NEW

Support When In Use location authorization

```
CLLocationWhenInUseUsageDescription
```

```
CLLocationAlwaysAndWhenInUseUsageDescription
```

Ask for location in a meaningful way

- Prompt in the right context
- Start with When In Use

CoreLocation—Legacy Apps

Linked against iOS 10

When In Use undefined

Compatibility warning

CoreLocation—Legacy Apps

Linked against iOS 10

When In Use undefined

Compatibility warning

Allow "Potloc" to access your location?

App explanation for always: "Your location will be used for demonstration purposes all the time."

If you only allow access to your location while you are using the app, some features may not work while this app is in the background.

Only While Using the App

Always Allow

Don't Allow

CoreLocation—Legacy Apps

Linked against iOS 10

When In Use and Always defined

CoreLocation—Legacy Apps

Linked against iOS 10

When In Use and Always defined

Allow "Potloc" to access your location?

App explanation for always: "Your location will be used for demonstration purposes all the time."

App explanation for while using: "Your location will be used for demonstration purposes only when you are using the app"

Only While Using the App

Always Allow

Don't Allow

Photos



NEW

Image picker without prompting for access

Write only support

Authorization will be reset on upgrade

Photos—Image Picker

NEW

Does not require explicit authorization

Access to photos or videos the user chooses

Great for rare actions within your app

```
UIImagePickerController
```


Photos—Write-only

NEW

Ability to add items to the Photo Library

`NSPhotoLibraryAddUsageDescription`

Does not enable read

`UIImageWriteToSavedPhotosAlbum`

`UISaveVideoAtPathToSavedPhotosAlbum`

**“Vacation” Would Like to Add
to your Photos**

Save some awesome photos and
videos!

Don't Allow

OK

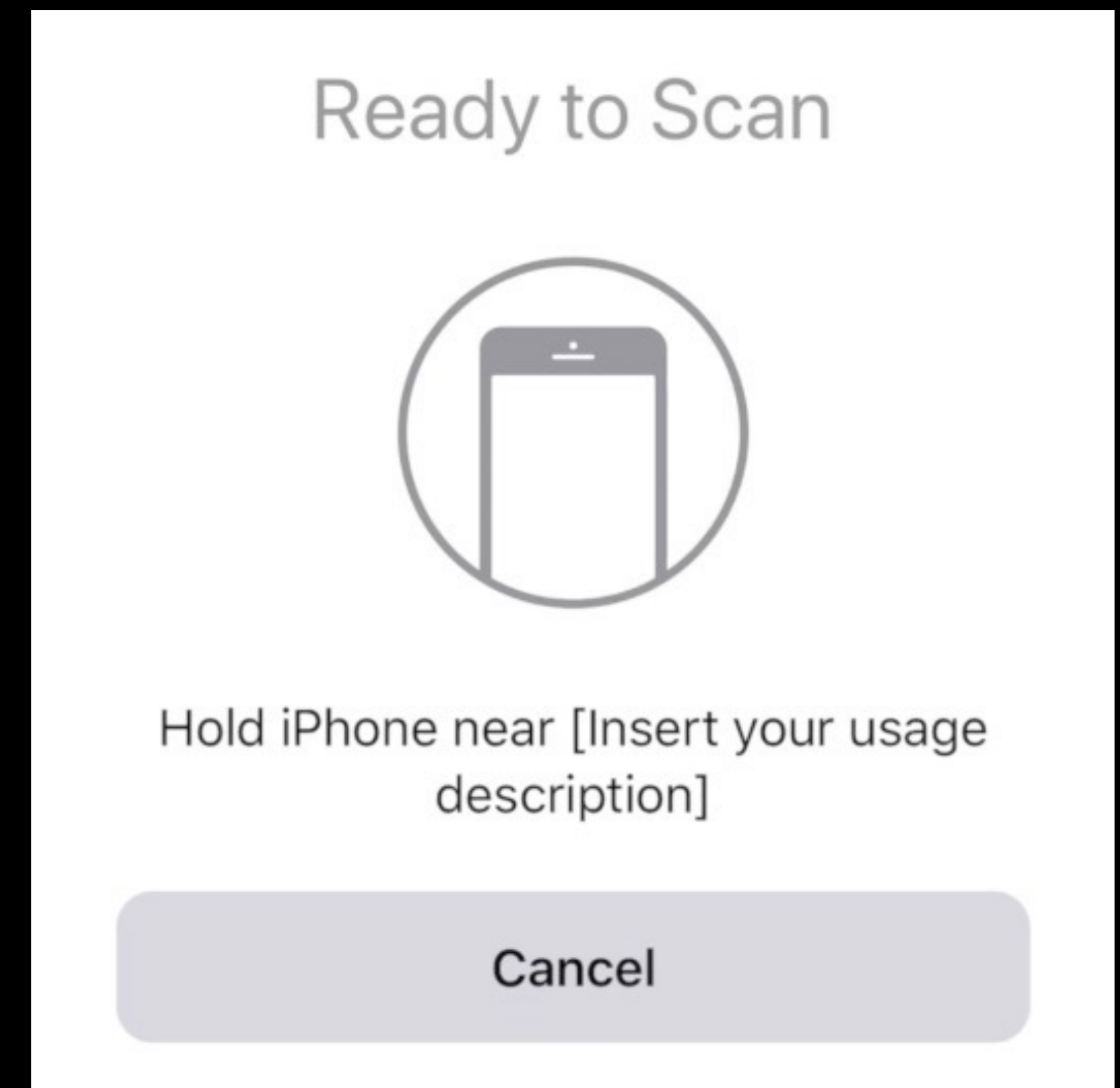
CoreNFC

NEW

Scan for nearby NFC tags

In the foreground

`NFCReaderUsageDescription`



Microphone—watchOS



NEW

Recording allowed to continue in the background

Recording possible without the built-in modal UI

Requires microphone authorization

Indicator on watch face

NEW



MusicKit

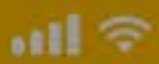
NEW

Token unlocks features based and personalized and non-personalized APIs

Seamless authentication through a Music token

User's consent is necessary

Control over the apps authorized



9:41 AM

100%



Settings



Save your Shazams

SIGN UP / LOG IN

**"Shazam" would like to
access Apple Music, your
music and video activity, and
your media library.
...to play full songs**

Don't Allow

OK

STREAM



Ap

CONTINUE



Sp

CONTINUE

Play any
Shazam.

leaving

USEFUL STUFF

Notifications >

Shazam on app start

Auto Shazam: Press and hold the Shazam button on home to start Auto Shazam

REMOVE ADS

Upgrade Shazam >

Safari View Controller

iOS 11

NEW

Safari and other apps get their own cookies and website data

Clearing website data in Safari also clears the data in your app




Domain

apple.com

example.org



Cookie

 = iphone 7

 = john appleseed

Safari View Controller

iOS 11

NEW

Safari and other apps get their own cookies and website data

Clearing website data in Safari also clears the data in your app



Features

Katie Skinner, Privacy Engineering

On-Device Processing

On-Device Processing

Benefits

Works anywhere

Network latency

Performance



120x

On-Device Processing

Privacy benefits

Access to user data

Security built in to iOS

- Keychain, data protection

Lower risk

On-Device Processing

Frameworks

NEW

CoreML

VisionKit

ARKit

NLP

Introducing Core ML

Hall 3

Tuesday 3:10PM

DeviceCheck

iOS, tvOS

DeviceCheck



NEW

Identifying devices

- Did this device already consume a free trial?
- Has this device paid for content but not linked that purchase to an account?
- Was this device previously used by an abusive user?
- Was this device previously used for fraudulent activities?

DeviceCheck

NEW

Assign state to a device

Privacy friendly

DeviceCheck



NEW

Per device, per developer data stored by Apple

Two bits and a timestamp

Until developer resets

- Erase install

Input to business logic

DeviceCheck

NEW

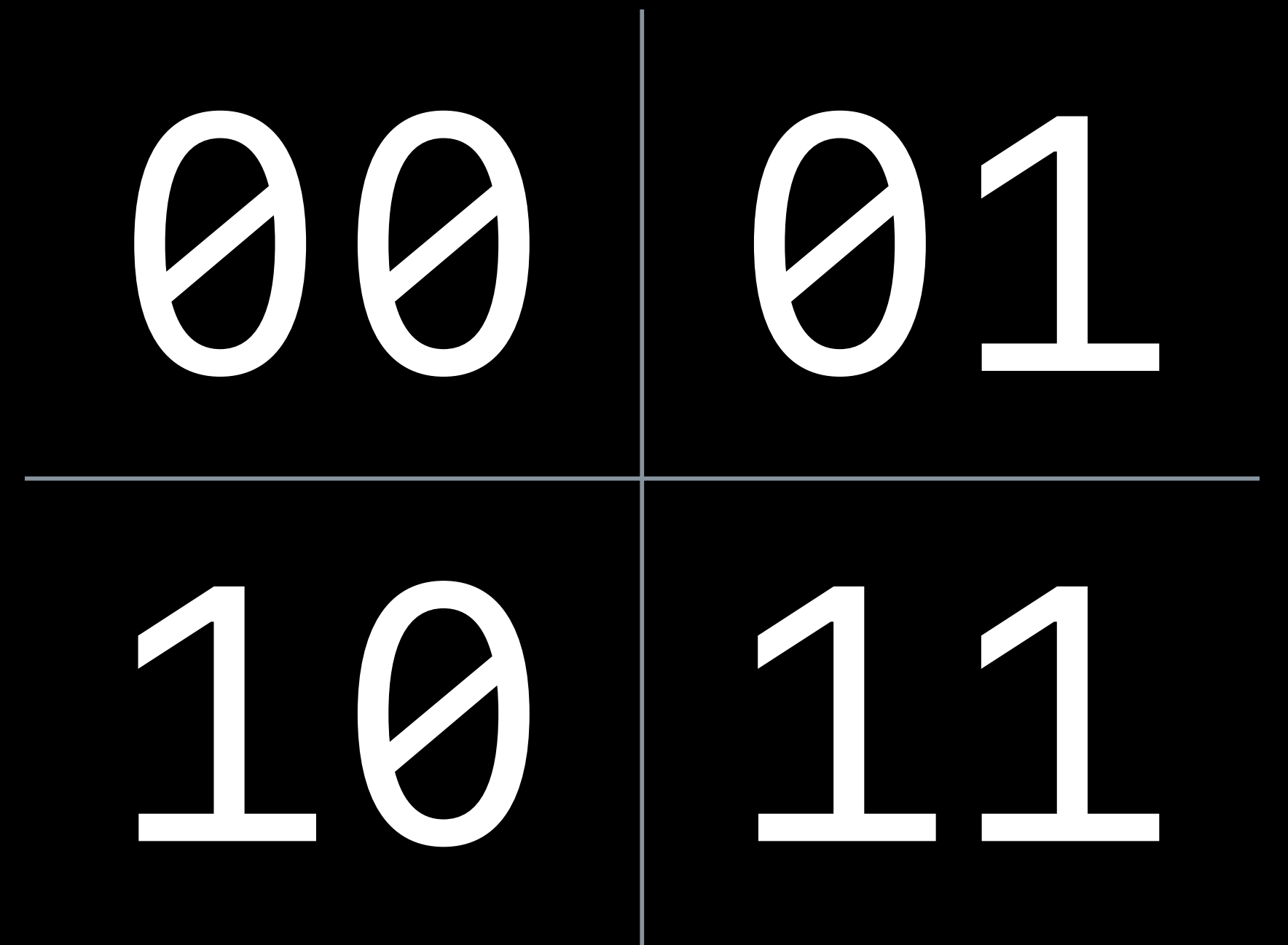
Per device, per developer data stored by Apple

Two bits and a timestamp

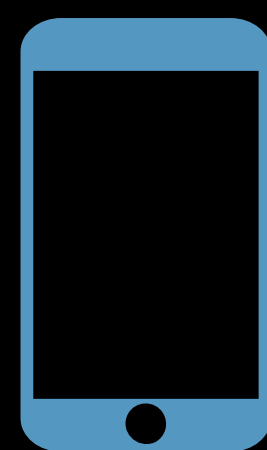
Until developer resets

- Erase install

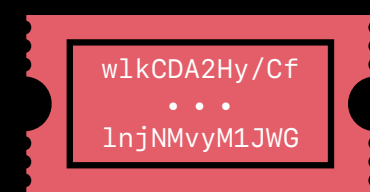
Input to business logic



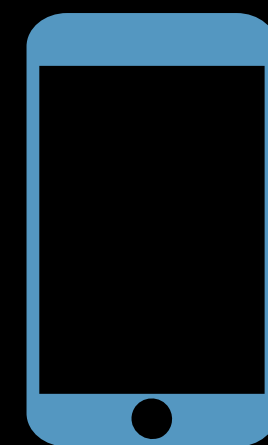
DeviceCheck



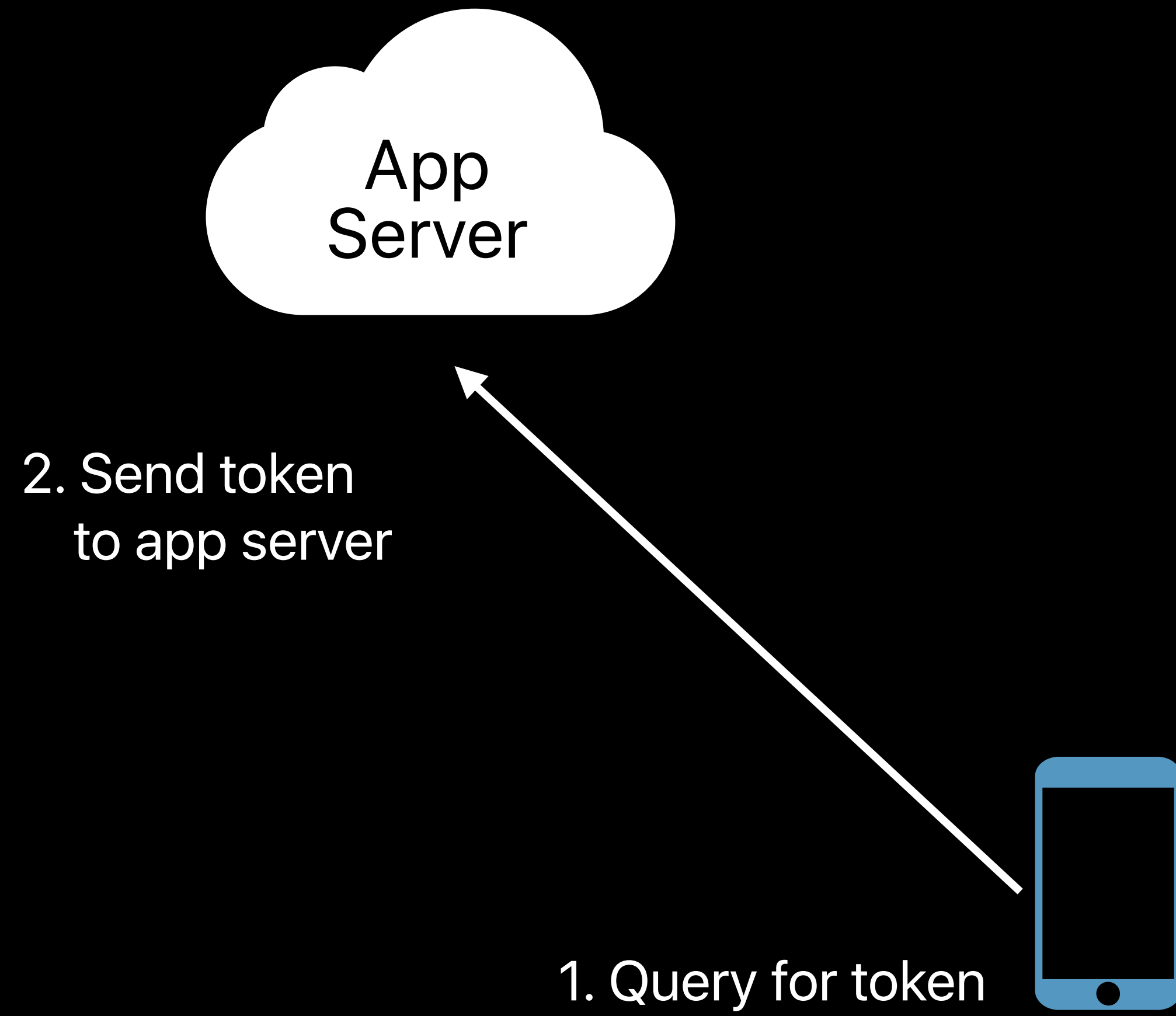
DeviceCheck



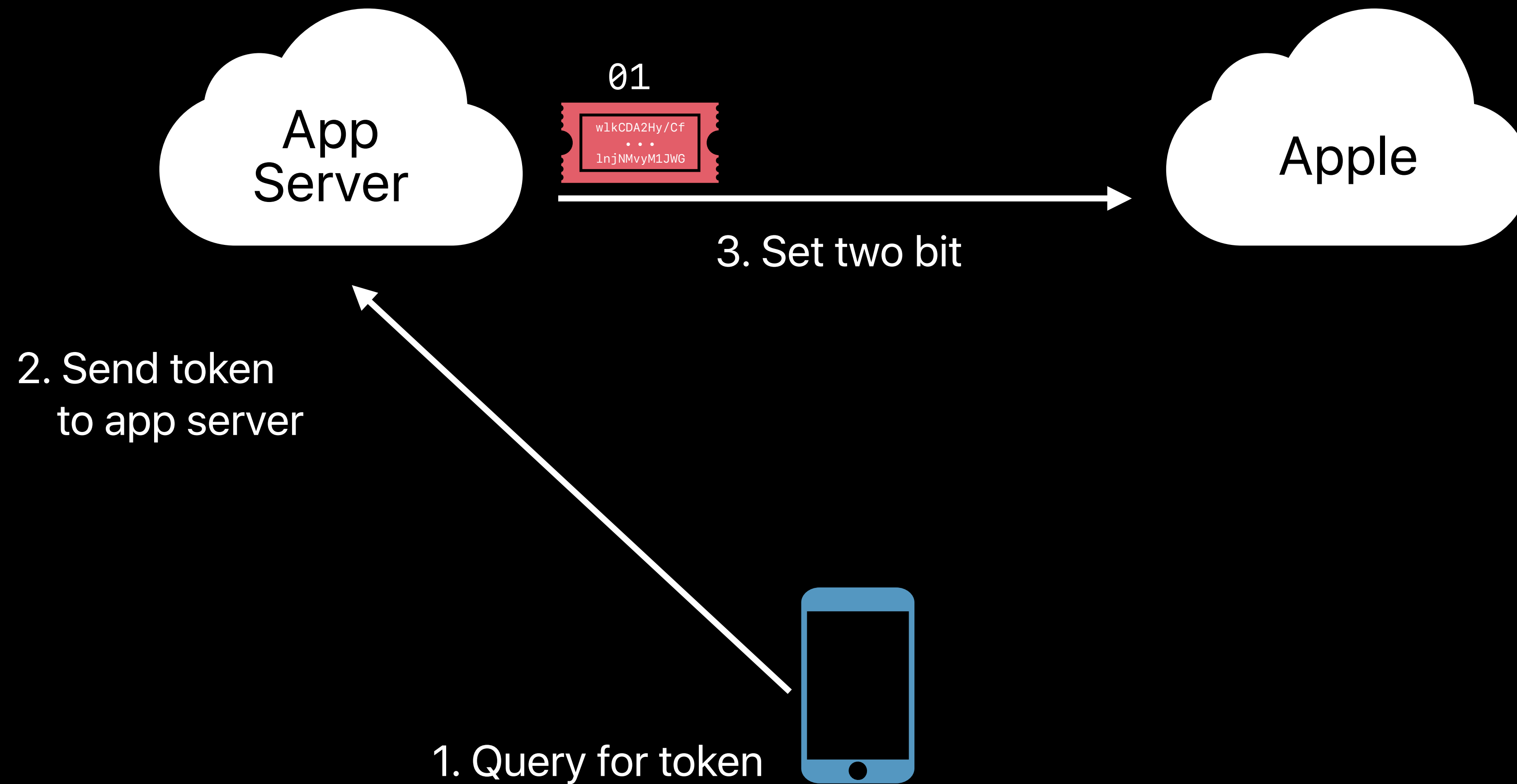
1. Query for token



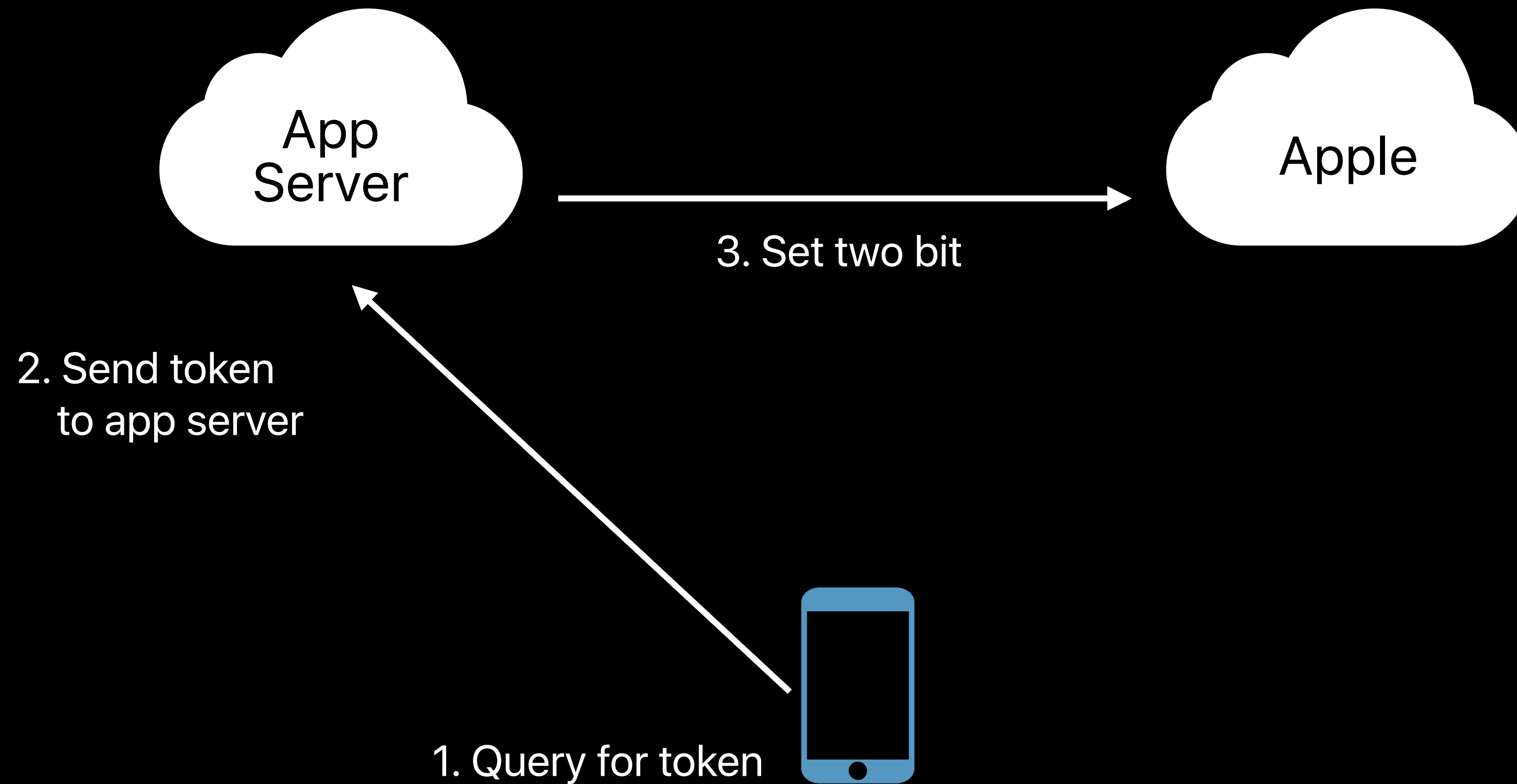
DeviceCheck



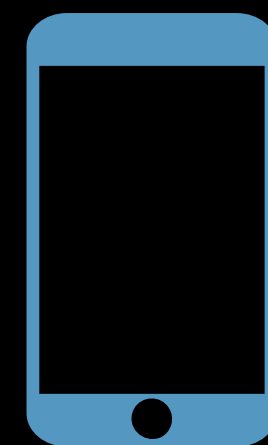
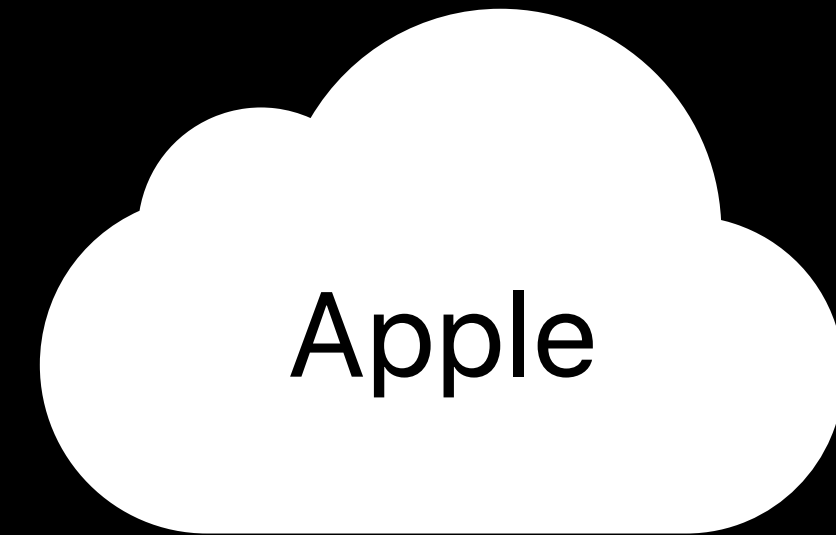
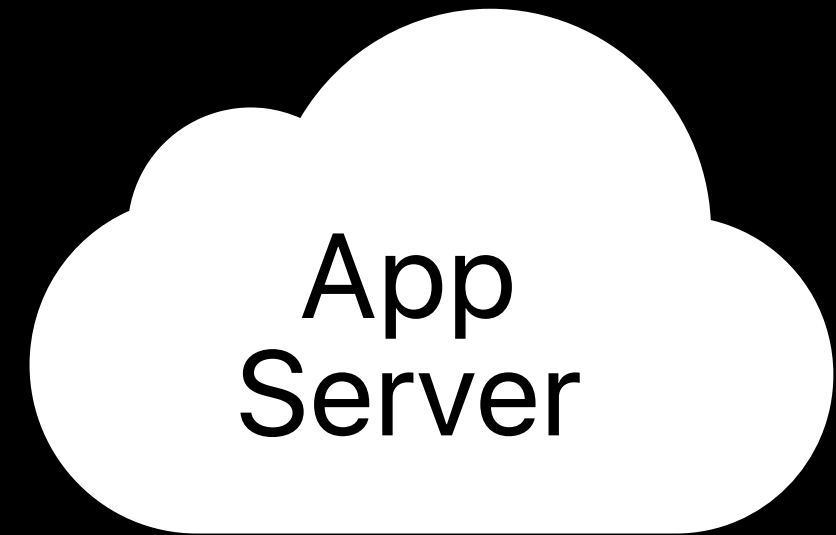
DeviceCheck



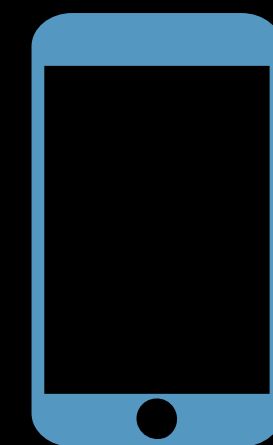
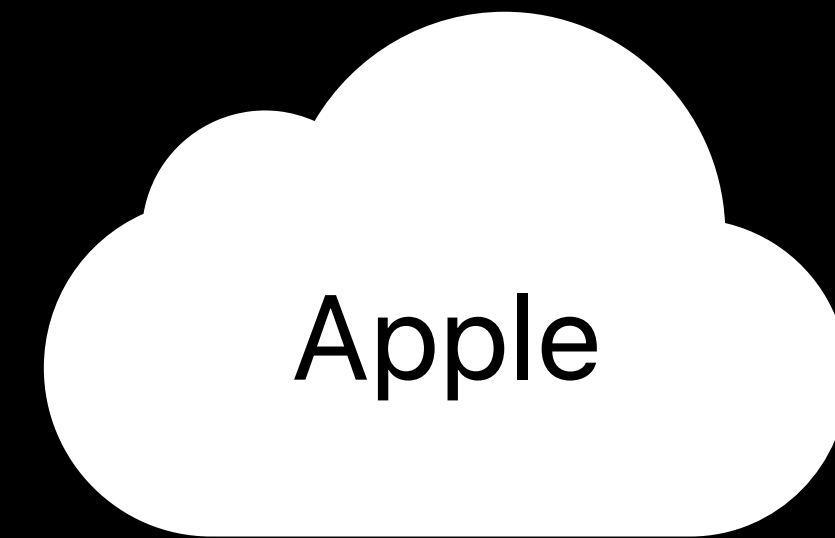
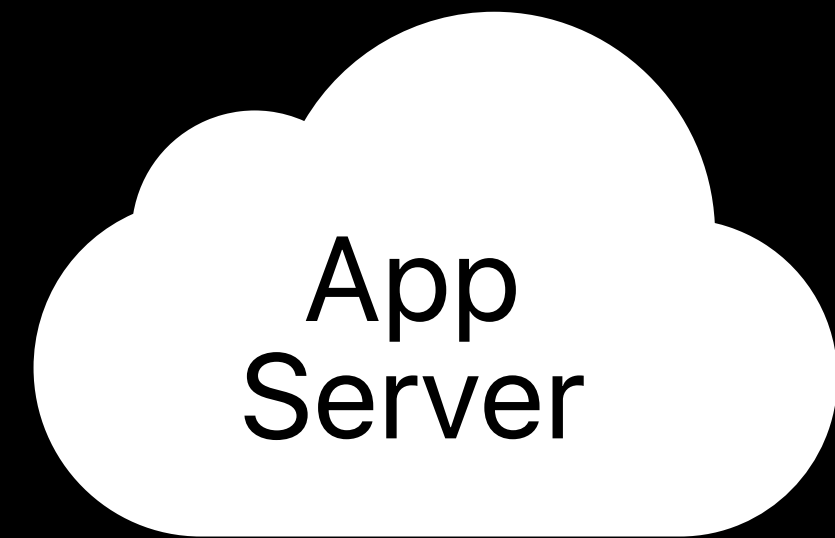
DeviceCheck



DeviceCheck

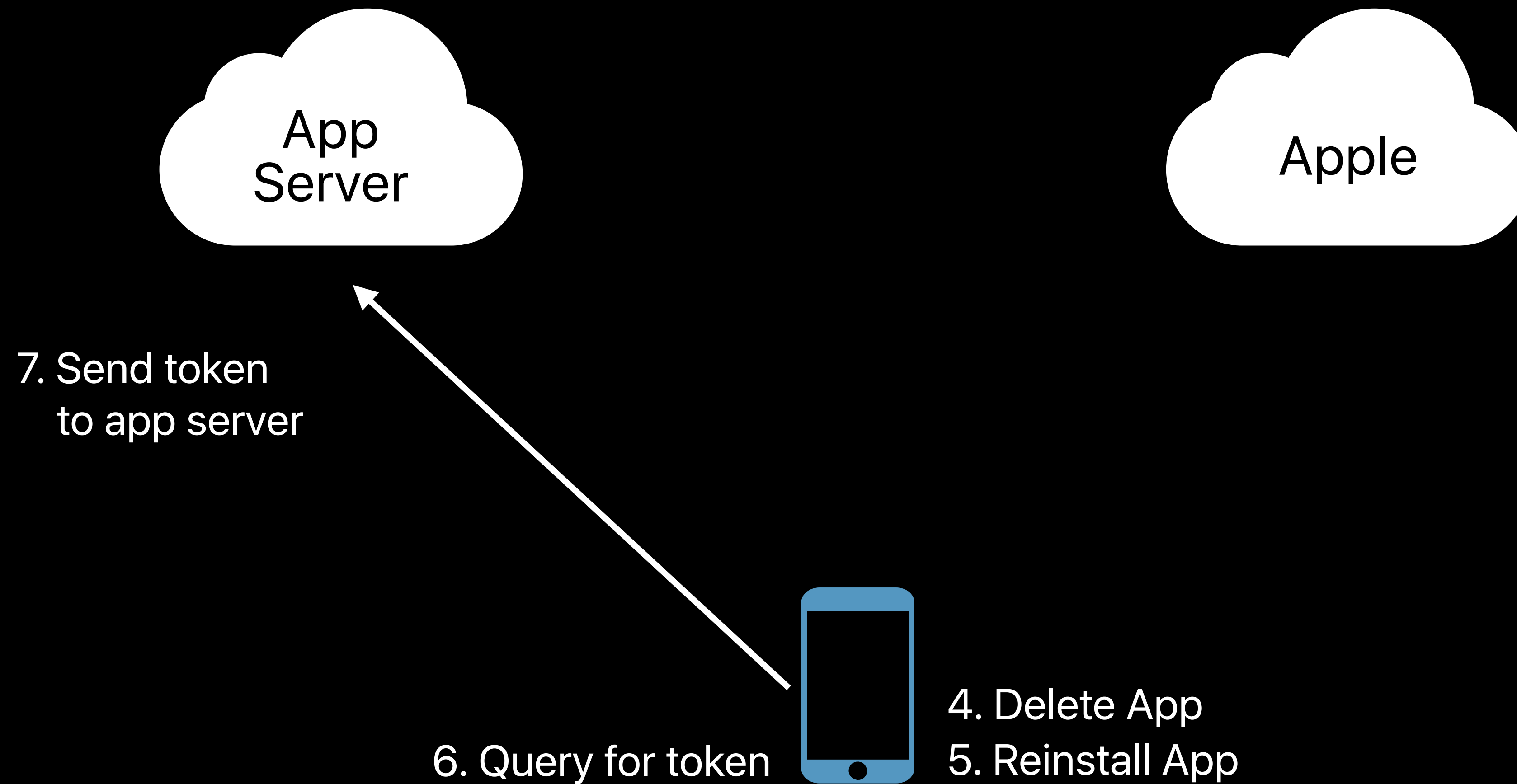


DeviceCheck

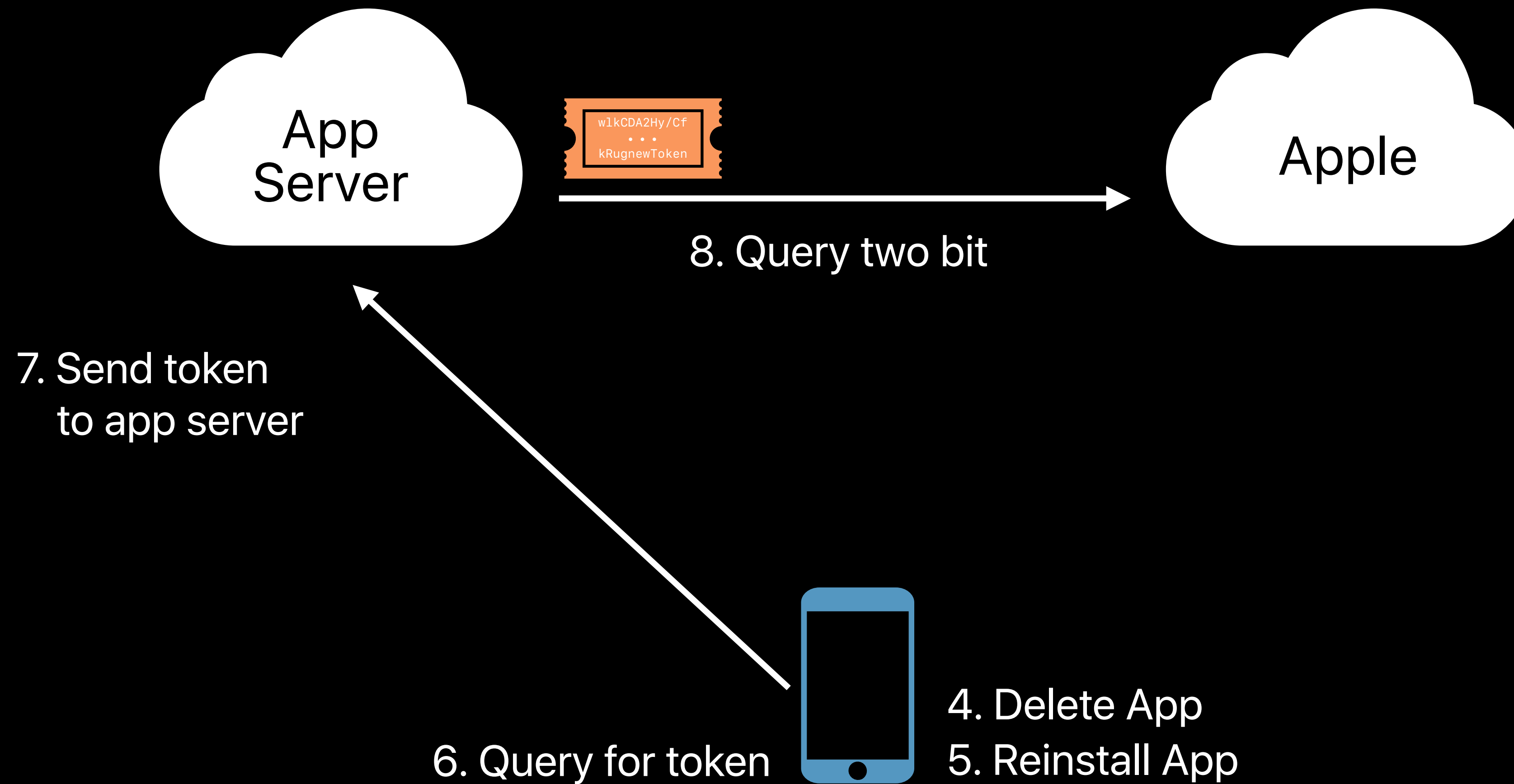


- 4. Delete App
- 5. Reinstall App

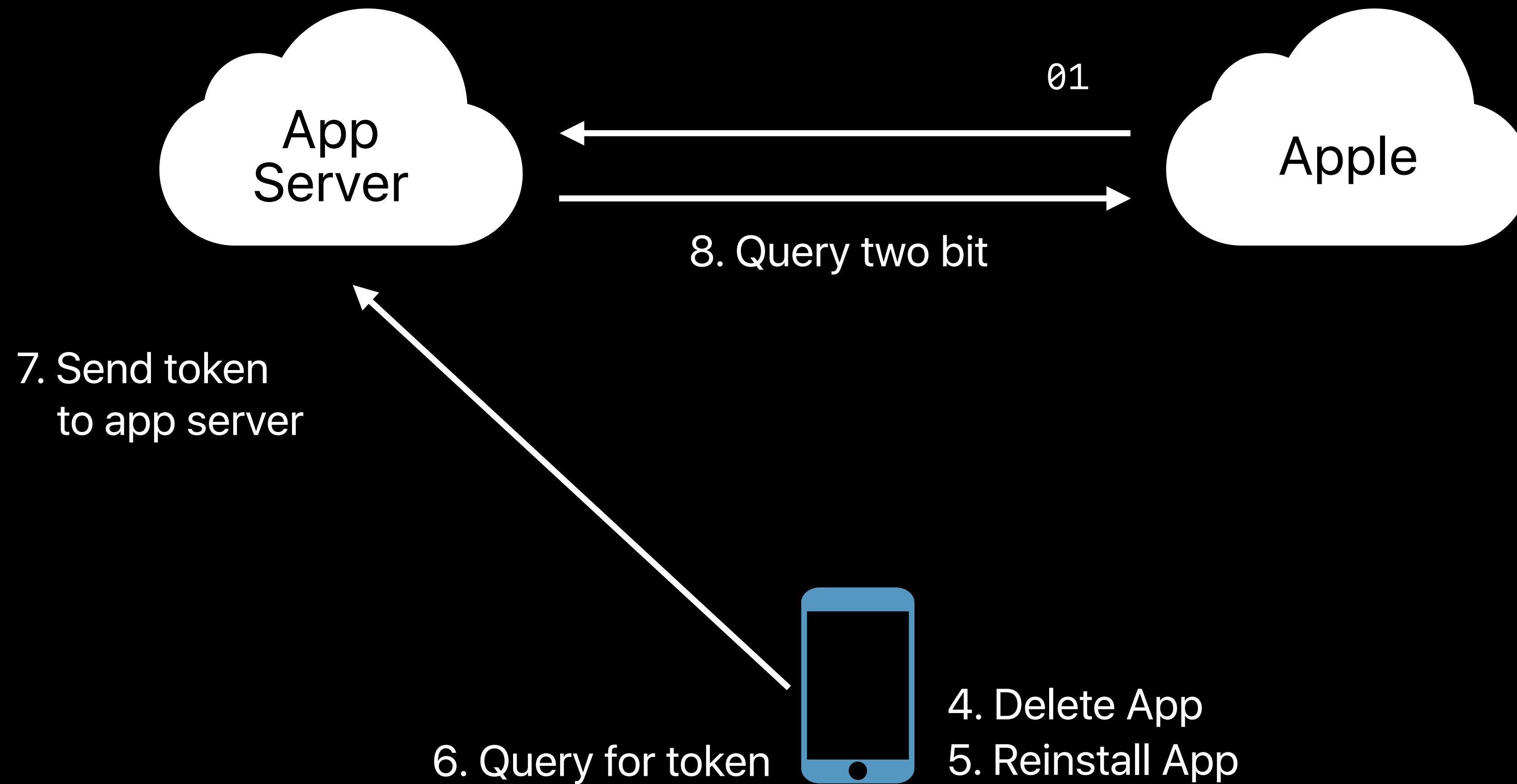
DeviceCheck



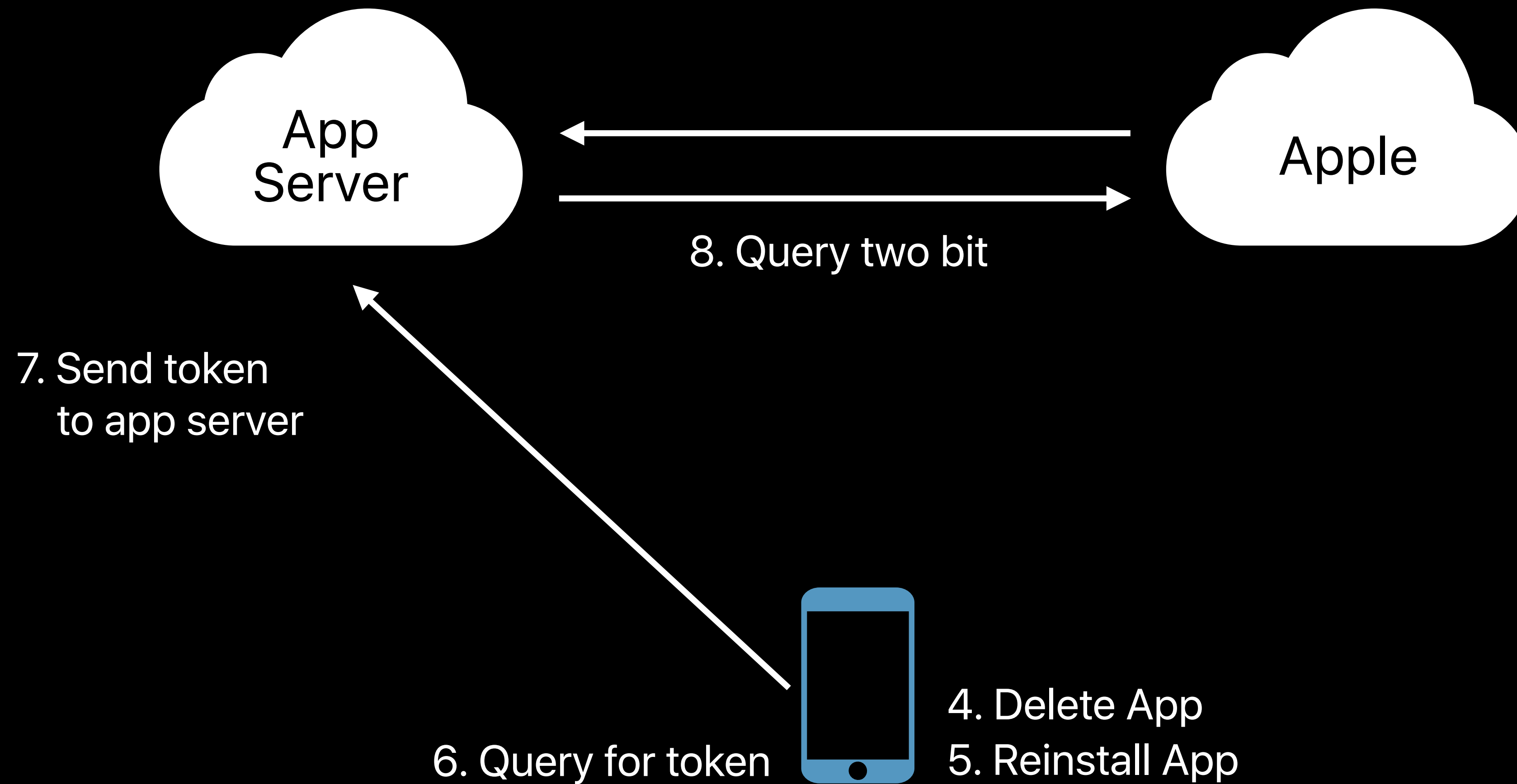
DeviceCheck



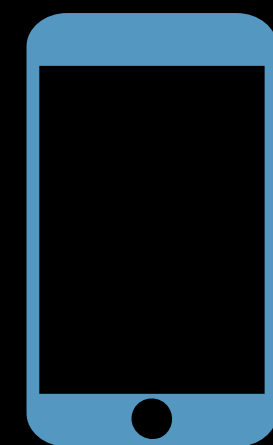
DeviceCheck



DeviceCheck

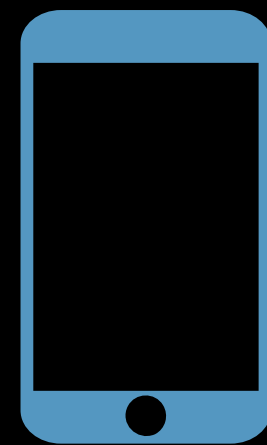


DeviceCheck

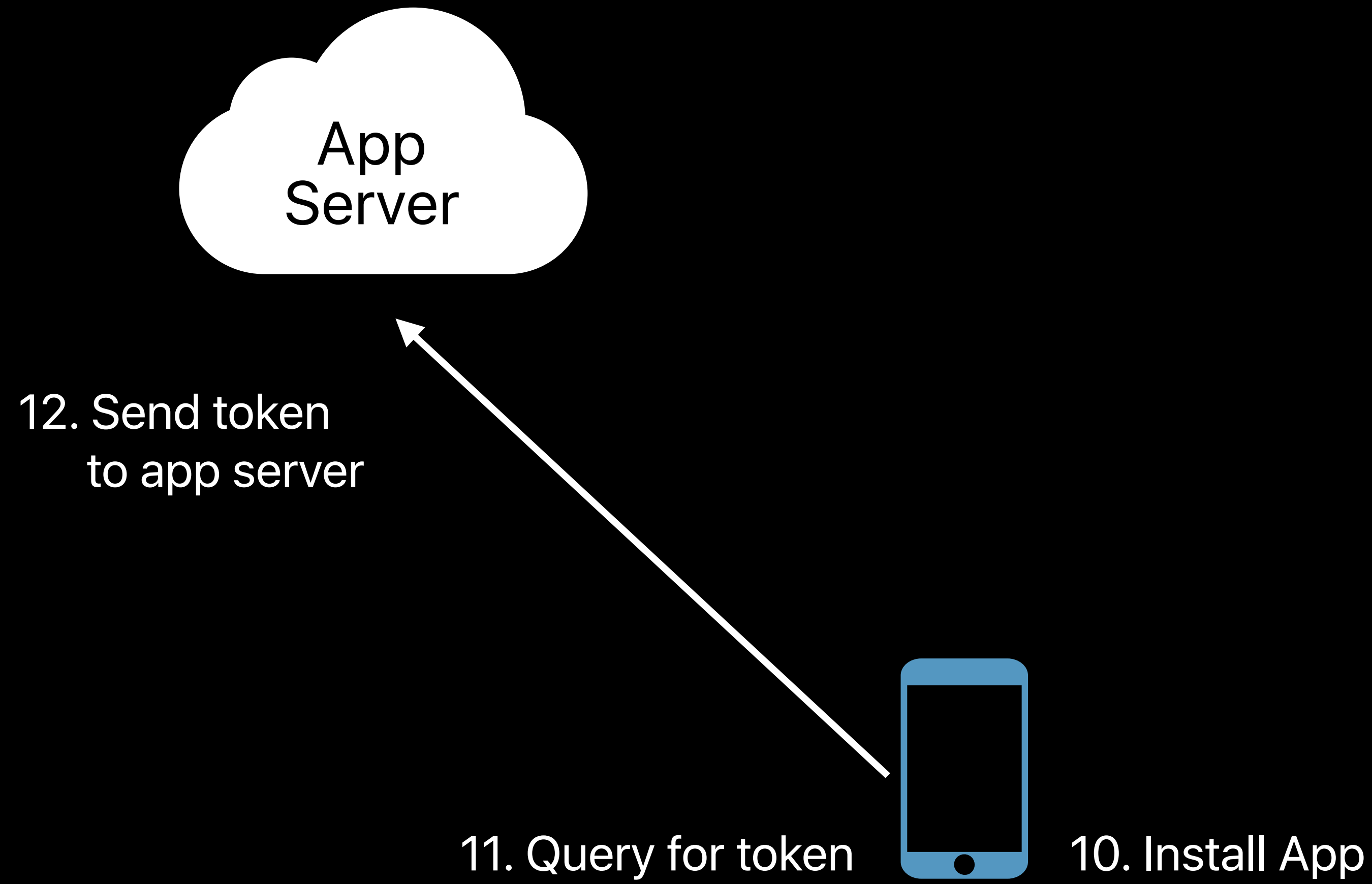


DeviceCheck

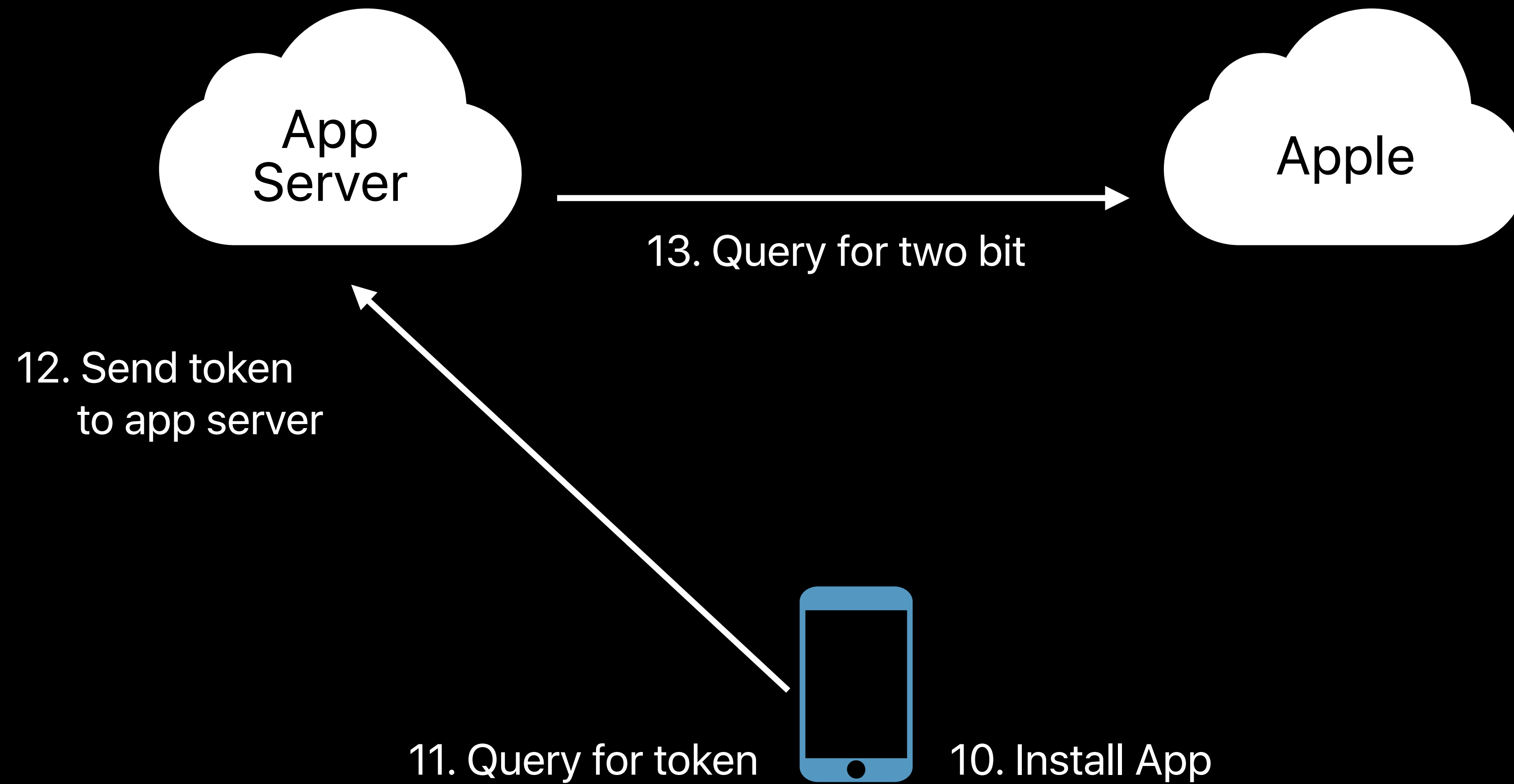
Georgios' iPhone



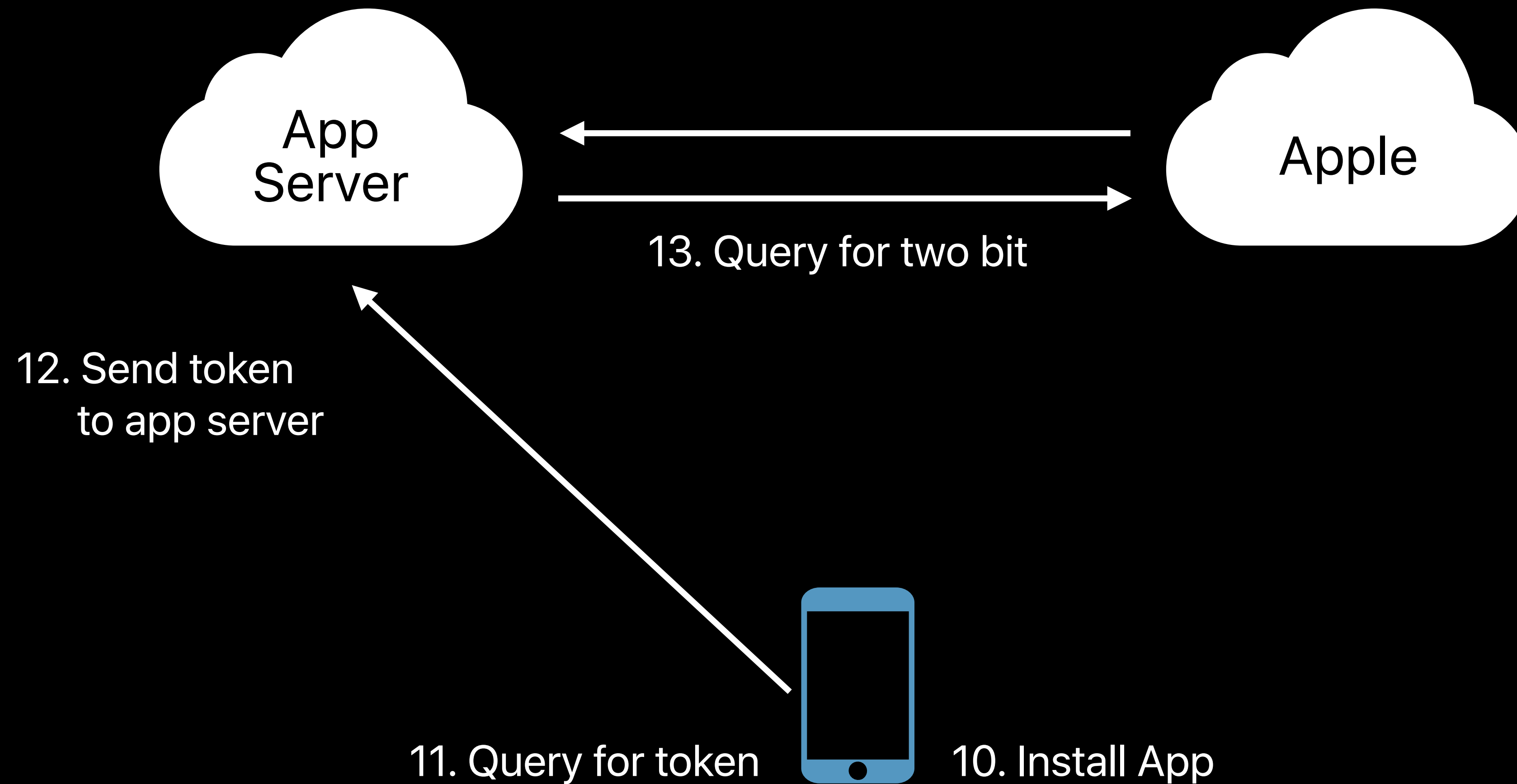
DeviceCheck



DeviceCheck



DeviceCheck



DeviceCheck

Query

Request to Apple to query bit state

```
{  
  "device_token" : "w1kCDA2Hy/CfMqVASHs1BAR/0sAiuRIUm5jQg0a..."  
  "transaction_id" : "5b737ca6-a4c7-488e-b928-8452960c4be9",  
  "timestamp" : 1487716472000  
}
```

DeviceCheck

Response

Response from Apple with the bit state

```
{  
  "bit0" : true,  
  "bit1" : true,  
  "last_update_time": "2017-02"  
}
```

Last update rounded to the month

DeviceCheck

Update

Update bit state

```
{  
  "device_token" : "w1kCDA2Hy/CfMqVASHs1BAR/0sAiuRIUm5jQg0a..."  
  "transaction_id" : "5b737ca6-a4c7-488e-b928-8452960c4be9",  
  "timestamp" : 1487716472000,  
  "bit0" : true,  
  "bit1" : false  
}
```

DeviceCheck

Best practices

Handle resold or transferred devices

Relevancy based on age

Part of your app logic not sole source

Should not affect UI

- e.g. "Welcome Back!"

Identifying Devices the Right Way

Use platform supported identifiers

- Application Identifier, Vendor Identifier, Advertising Identifier

Will continue to remove entropy

Will continue to provide user control of entropy sources

Will continue to remove functionality that is being abused to uniquely identify users

Intelligent Tracking Prevention

Safari

Intelligent Tracking Prevention



NEW

Does not block content

Dynamically detects online tracking

- On-device classifier

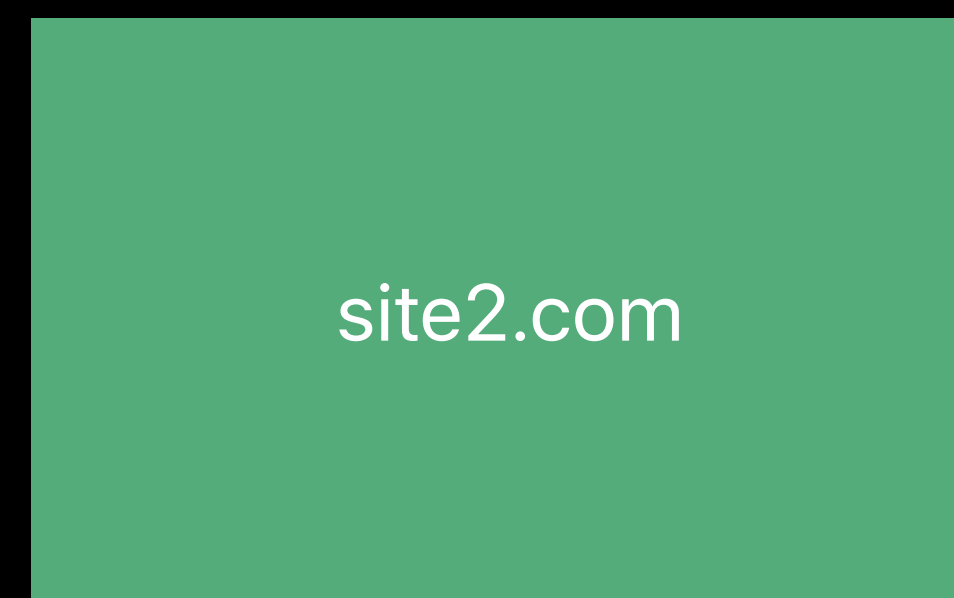
Hinders tracking

- Isolates
- Periodically purges

User interaction temporarily whitelists domains

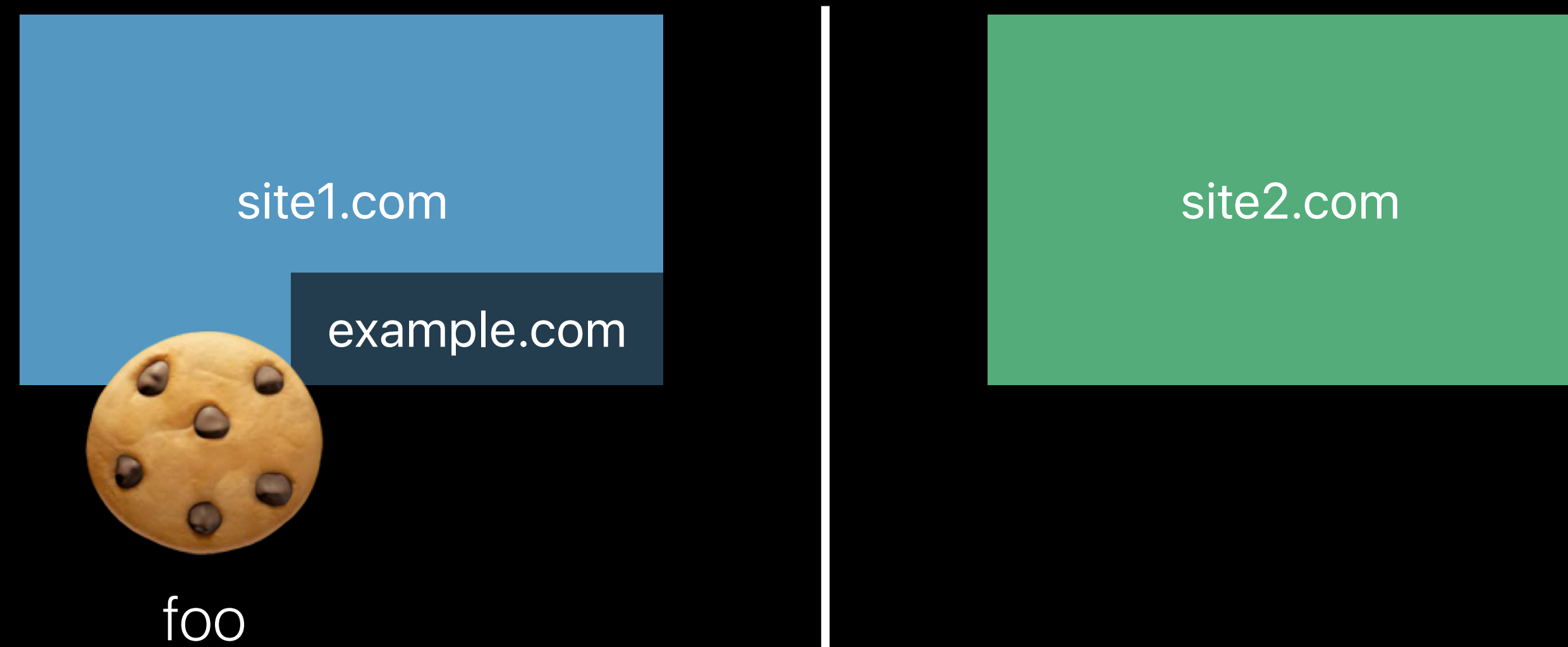
Cookie Partitioning

Cookies from example.com are partitioned by each domain that embeds



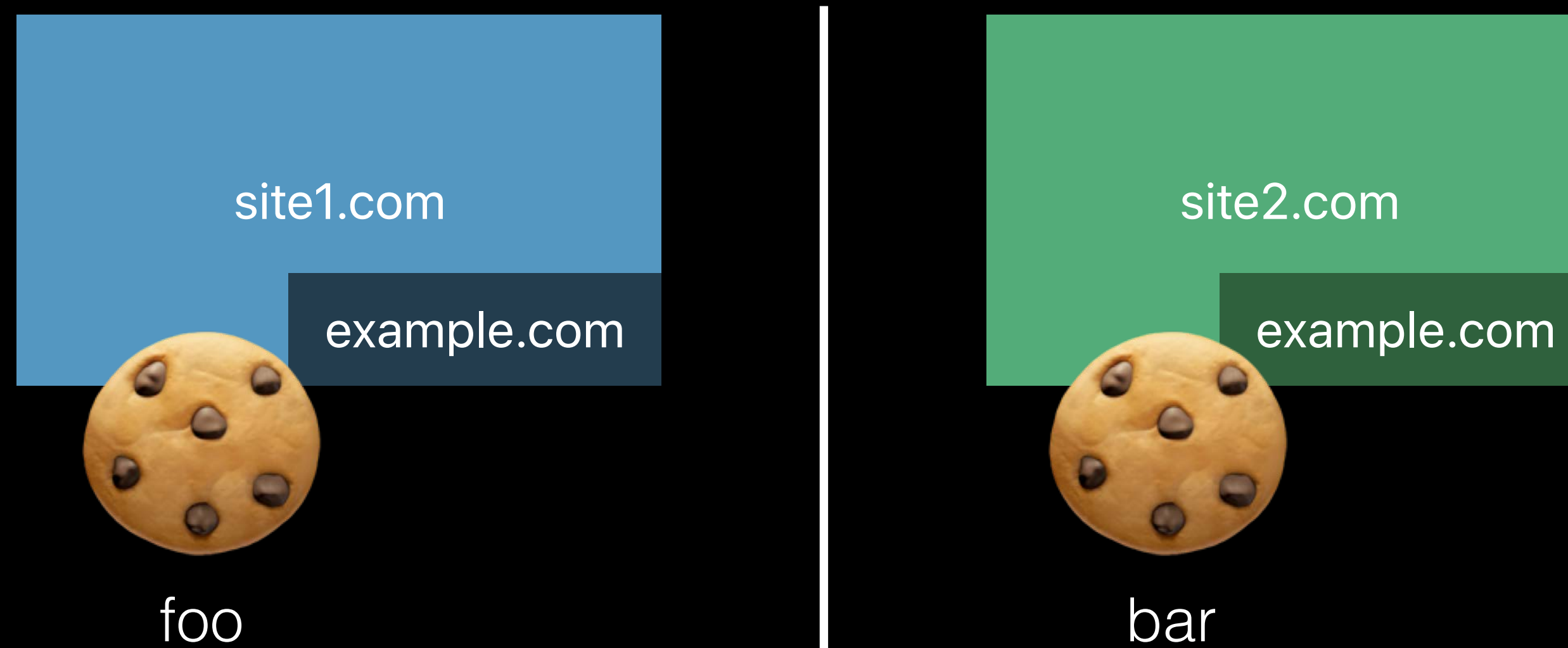
Cookie Partitioning

Cookies from example.com are partitioned by each domain that embeds



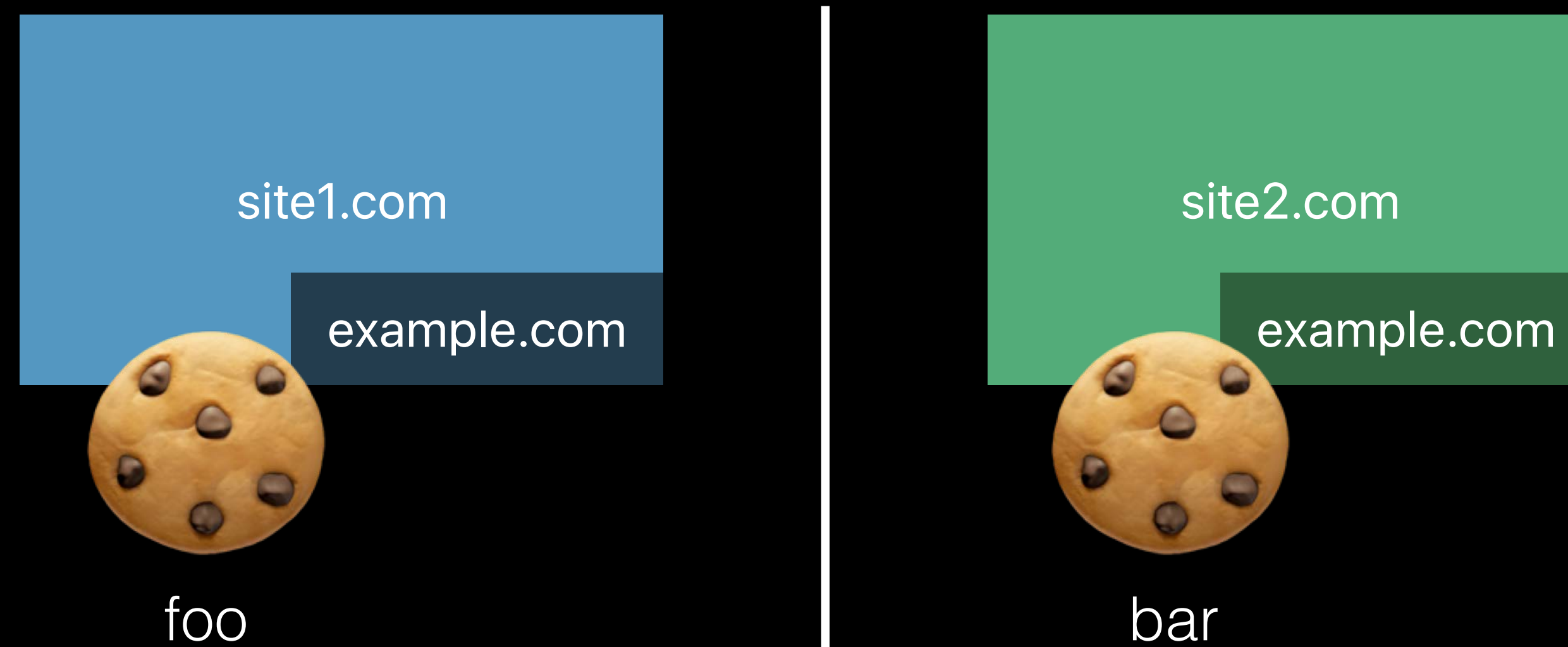
Cookie Partitioning

Cookies from example.com are partitioned by each domain that embeds



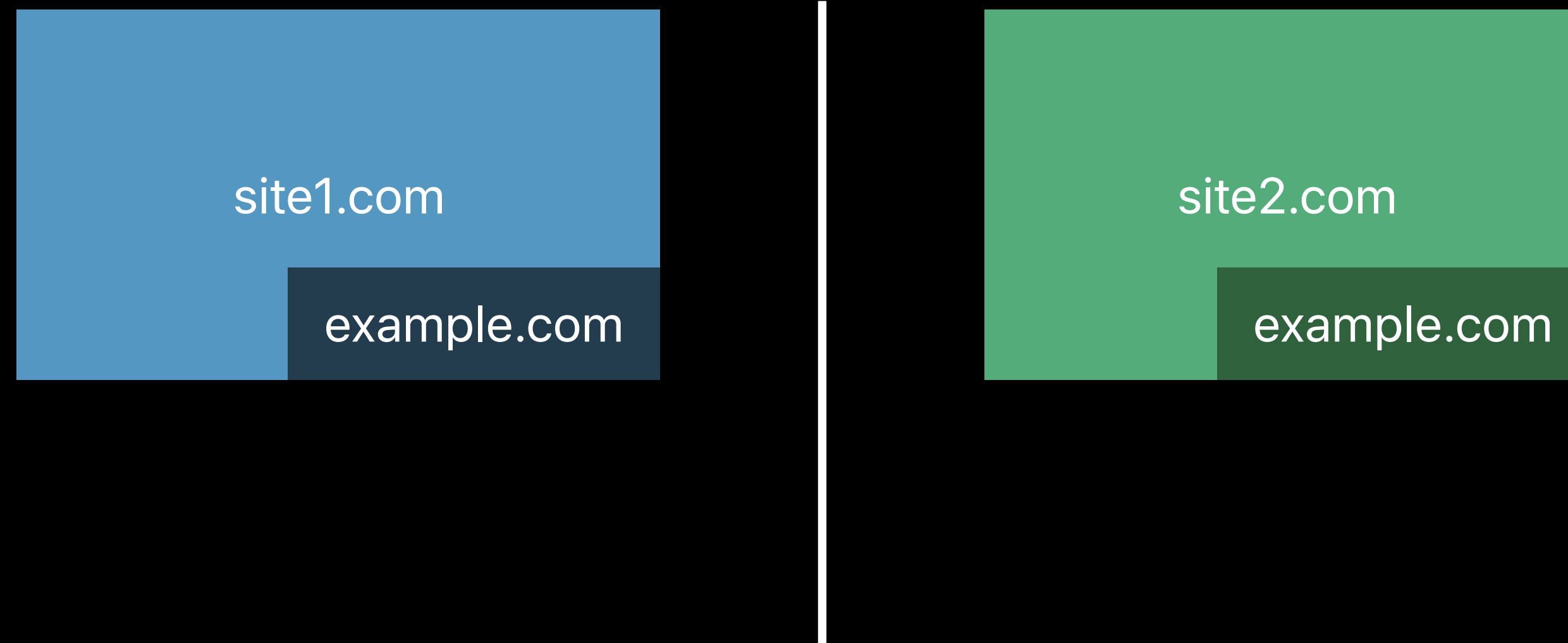
Cookie Purging

Cookies from example.com are purged on a regular basis



Cookie Purging

Cookies from example.com are purged on a regular basis



Intelligent Tracking Prevention

User interaction

Safari will not delete cookies and website data from example.com

- If example.com is a first party site
- If the user taps, clicks, or fills out a form

Do not rely on storage if a user does not interact with your site

Ensure your analytics package does not rely on third party cookies

Differential Privacy

Differential Privacy

Launched on iOS, macOS

Millions of donations per day

Building better products with privacy

New uses

Differential Privacy

New use cases

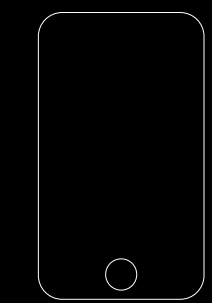


NEW

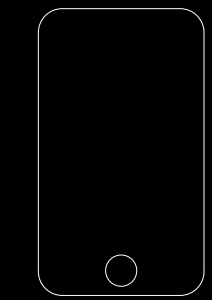
Learn commonly used Health data types

- Learn 'steps' not 10,678 steps

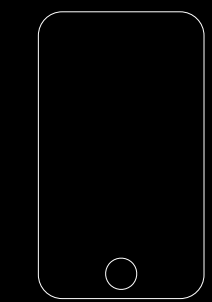
Learning Popular Health Data Type



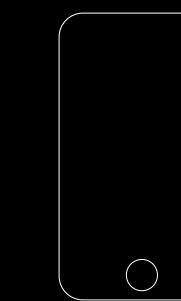
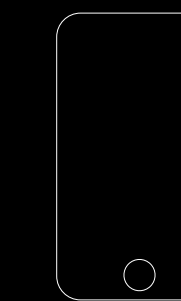
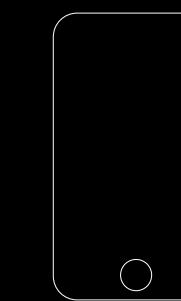
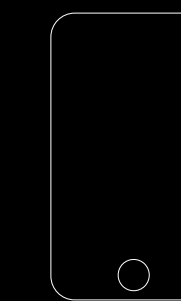
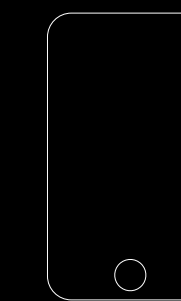
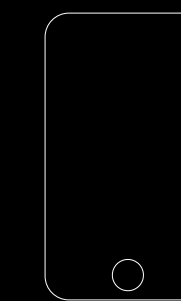
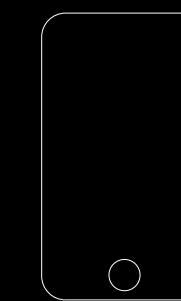
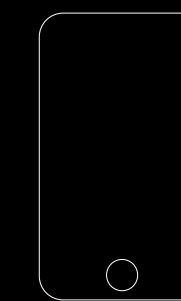
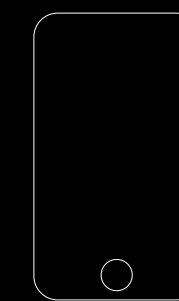
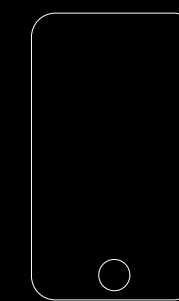
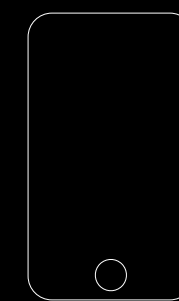
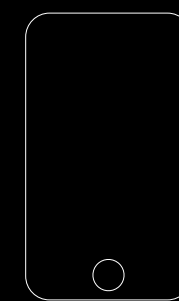
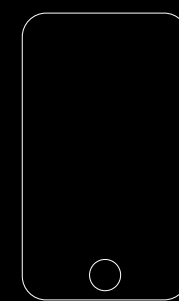
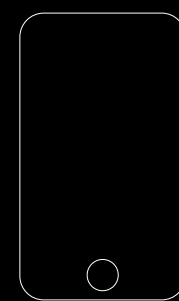
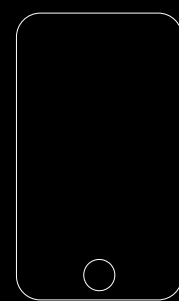
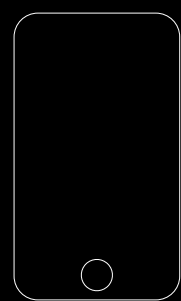
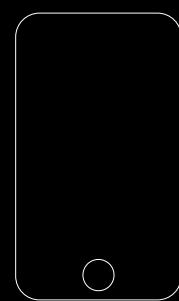
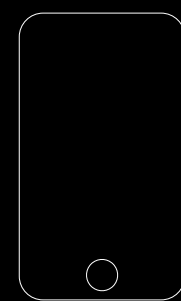
Julien



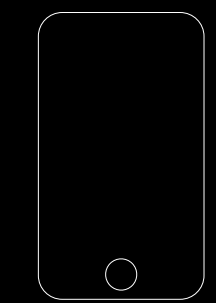
Jessie



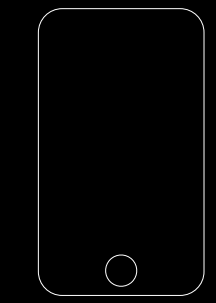
Timmy



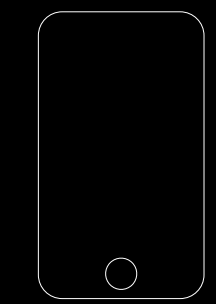
Learning Popular Health Data Type



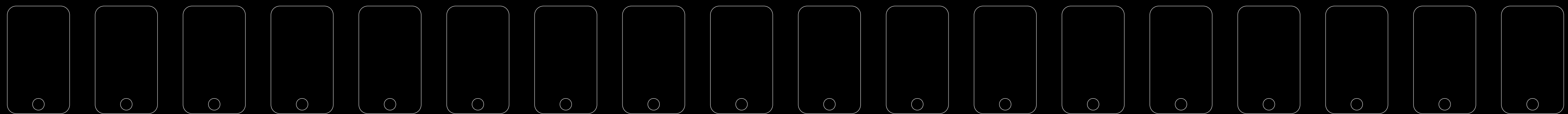
Julien



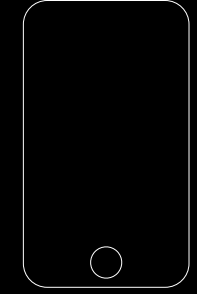
Jessie



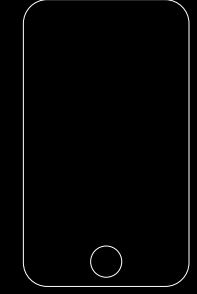
Timmy



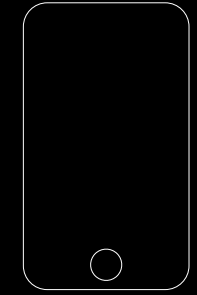
Learning Popular Health Data Type



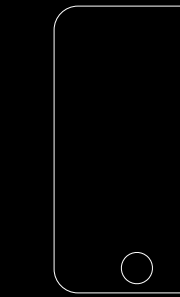
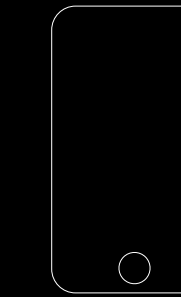
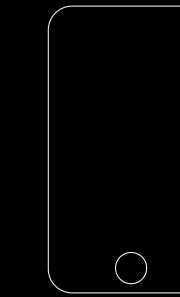
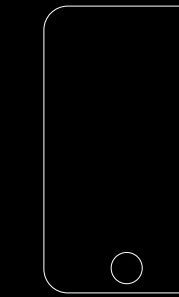
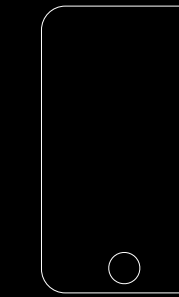
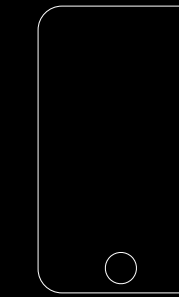
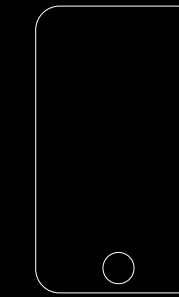
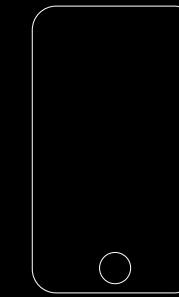
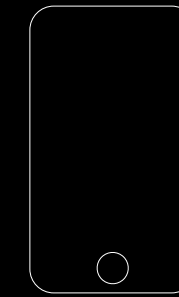
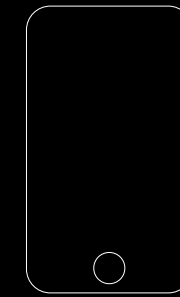
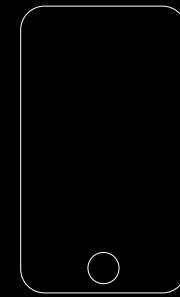
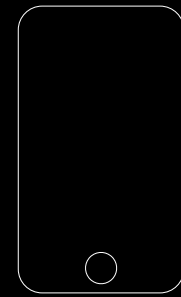
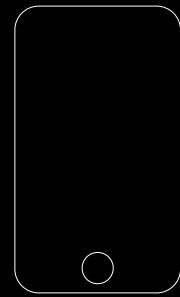
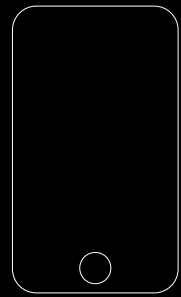
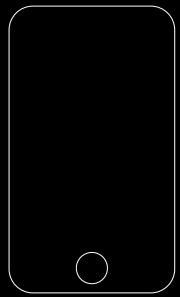
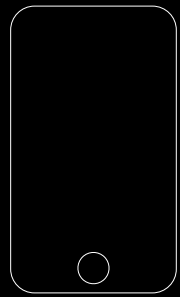
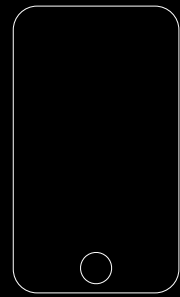
Julien



Jessie



Timmy



Differential Privacy

New use cases



Learn web domains that cause performance issues

Reach out to developers

Build great features

Build great features + respect user privacy

More Information

<https://developer.apple.com/wwdc17/702>

Related Sessions

Introducing Core ML

Hall 3

Tuesday 3:10PM

Introducing MusicKit

Grand Ballroom B

Tuesday 3:10 PM

Introducing ARKit: Augmented Reality for iOS

Hall 3

Tuesday 5:10 PM

Natural Language Processing and your Apps

Hall 3

Wednesday 9:00AM

What's New in Photo APIs

Hall 2

Wednesday 1:50PM

Vision Framework: Building on Core ML

Hall 2

Wednesday 3:10PM

What's New in Location Technologies

Grand Ballroom B

Thursday 3:10PM

Introducing Core NFC

WWDC 2017 Video

Labs

Security & Privacy Lab

Technology Lab D

Tue 1:50PM–3:50PM

iCloud Photo Library & PhotoKit Lab

Technology Lab G

Wed 9:00AM–11:00AM

Location and Mapping Technologies Lab

Technology Lab B

Wed 11:00AM–1:00PM

Security & Privacy Lab

Technology Lab J

Wed 1:00PM–4:20PM

Core ML and Natural Language Processing Lab

Technology Lab D

Thu 11:00AM–3:30PM

