Managing Apple Devices

What’s new in iOS 7 and OS X Mavericks

Session 300

Todd Fernandez
Senior Manager - Device Management

MacBook Air
Finder File Edit View Go Window Help
Mon 9:41 AM
iPad
9:41 AM
Messages
FaceTime
Photos
Camera
Maps
Clock
Photo Booth
Calendar
Notes
Reminders
Newsstand
App Store
Game Center
Settings
Mail
Videos
Music
Weather
Passbook
Stocks
iTunes
Phone
Safari

MacBook Air

MacBook Air

MacBook Air

Agenda

- MDM protocol and Configuration Profile updates
- App Store volume purchasing and license management
- Streamlined device enrollment

MDM and Configuration Profiles

Apple Device Management

- MDM protocol
  - Get info
  - Lock or wipe
  - Install managed apps
  - Install configuration profiles
- Configuration profiles
  - Accounts
  - Restrictions
  - Service access
  - MDM enrollment

New MDM queries

AirPrint destinations

Manage Apple TVs

Wi-Fi Hotspot 2.0

Managed app configuration

Per-app VPN

Fonts

Web content filtering

Managed Open In

New restrictions

AirPlay mirroring destinations

FileVault

Single sign on

Full Exchange Web Services support

Accessibility options for single app mode

New MDM commands

What’s New?

What’s New?

- Managed App Enhancements
- Single Sign On
- Per-app VPN
- FileVault
- AirPlay Mirroring
- And Much More

Managed Apps

Today

- Installed via MDM
- Delete app
- Prevent iCloud backup

Managed Apps

New in iOS 7

- Silent installation 👤
- App configuration
- App feedback
- Managed Open In

Single Sign On

- Generalize use of credentials across system
    - Stored in one place
    - Used for multiple apps
- Credentials
- Matching URL prefixes
- Allowed app identifiers

Per-App VPN

- Individual apps can establish VPN to remote services
- More focused than system-wide VPN
  - Secure data always goes through your network
  - End user data does not go through your network
- Managed apps configured during installation

FileVault

- Prevent users from disabling FileVault
- Individual recovery key escrow
  - https:// URL destination for recovery key
  - PKCS1 certificate payload to encrypt recovery key
  - Must be in a system profile
  - Only one payload per system
- Institutional recovery key rotation

AirPlay Mirroring

- Command
  - Begin mirroring to a destination
- Payload
  - Destination whitelist 👤
  - Destination passwords

Apple TV

- Enroll and manage via MDM
- Query and set language and locale
- Configure Network 802.1X payload

And Much, Much More

- Install fonts
- Wi-Fi Hotspot 2.0

iOS X

- AirPrint destinations
- Accessibility options for single app mode 👤
- Web content filtering 👤

iOS

- Exchange Web Services now supports all account types
- Passcode now has parity with iOS

X

New Restrictions

- Account changes 👤
- Find My Friends changes 👤
- Apps using cellular data 👤
- Host pairing 👤
- Wallpaper changes 👤
- Define service for text selections 👤
- Limit ad tracking
- iCloud Keychain sync
- Over-the-air PKI updates
- Lock screen Wi-Fi and Airplane mode buttons

MDM Protocol

- Mobile Hotspot enabled
- Do Not Disturb enabled
- Find My iPhone enabled
- iTunes account signed in

?

- Set custom lock screen
- Put device in lost mode
- Disable personal hotspot

!

Demo

Managed app enhancements

Chris Skogen
Engineering Manager

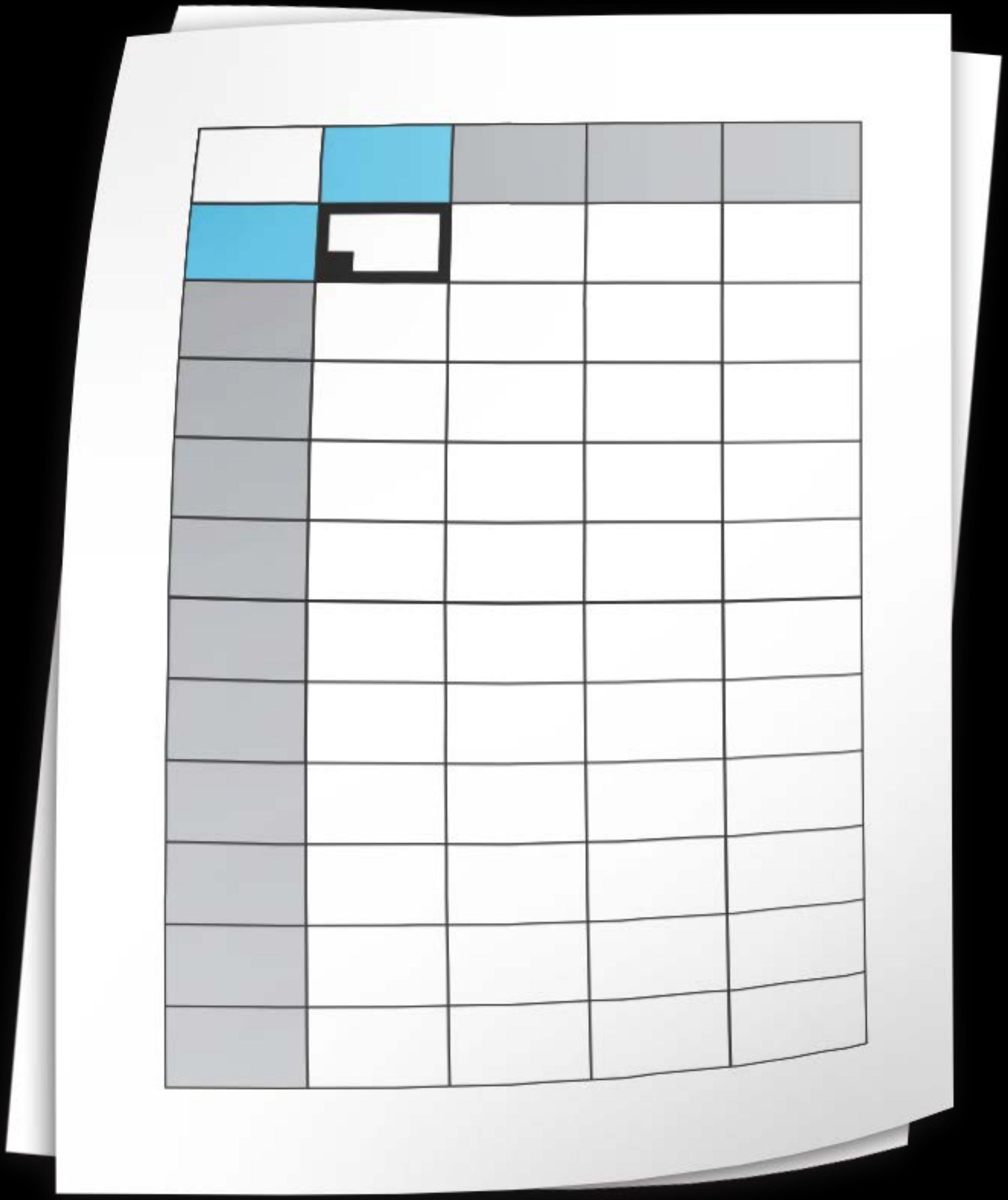
Jussi-Pekka Mantere
Engineering Manager

App Store Volume Purchase Program

App Store Volume Purchase Program

Today

- Purchase app and book codes in bulk
  - App Store or B2B Store
- Code management and distribution integrated into MDM solutions



App Store Volume Purchase Program

What's new

- Licenses instead of codes
- iOS and Mac apps
- Books for enterprise
- APIs for integration into MDM solutions

App Store Volume Purchase Program

What's new

- Licenses instead of codes
- iOS and Mac apps
- Books for enterprise
- APIs for integration into MDM solutions

App Store Volume Purchase Program

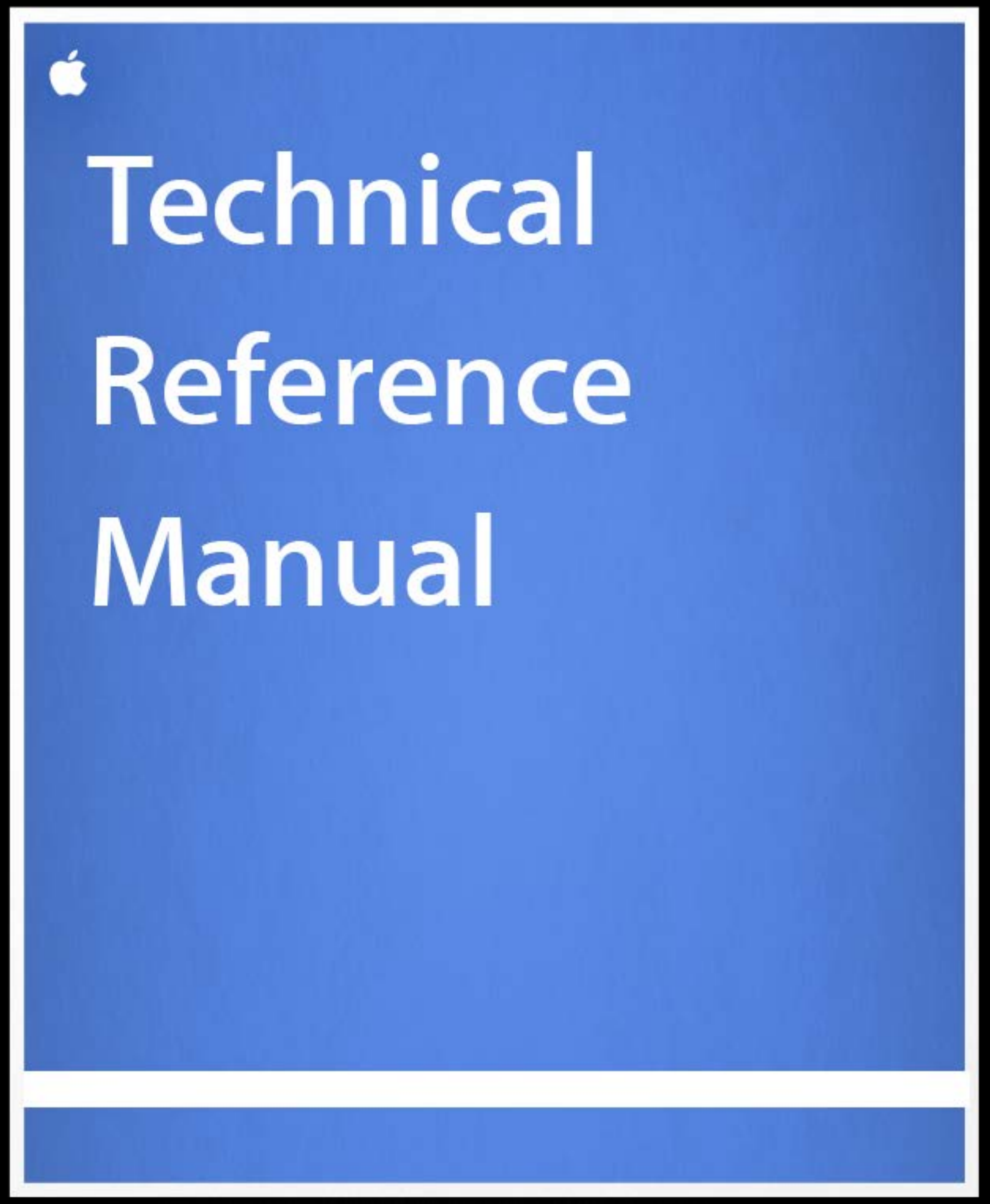
What’s new

- Licenses instead of codes
- iOS and Mac apps

App Store Volume Purchase Program

What's new

- Licenses instead of codes
- iOS and Mac apps
- Books for enterprise


Technical Reference Manual

App Store Volume Purchase Program

What's new

- Licenses instead of codes
- iOS and Mac apps
- Books for enterprise
- APIs for integration into MDM solutions

App Store Volume Purchase Program

End user experience

- Assigned apps available in Purchased list
- Apps may be installed via MDM command
    - Apps will be managed iOS
- Revoked apps
    - No longer appear in Purchased
    - Notify user of revocation and prompt to buy
    - Will not launch after 30-day grace period iOS
    - Will not launch on OS X if developer checks receipts and quits on launch with an expired receipt X

MDM Server Enhancements

Overview

- Account authentication
- User invitations
- Assignments and revocations

Account Authentication

- Allow organization admin to enter secure token
- Don’t have to store your customer’s credentials
- Token expires after a year

User Invitations

- Preserve user privacy
- Users do not have to reveal Apple ID
- One-time invitation to link Apple ID to organization in iTunes Store
- Get an individual URL for user

Assignments and Revocations

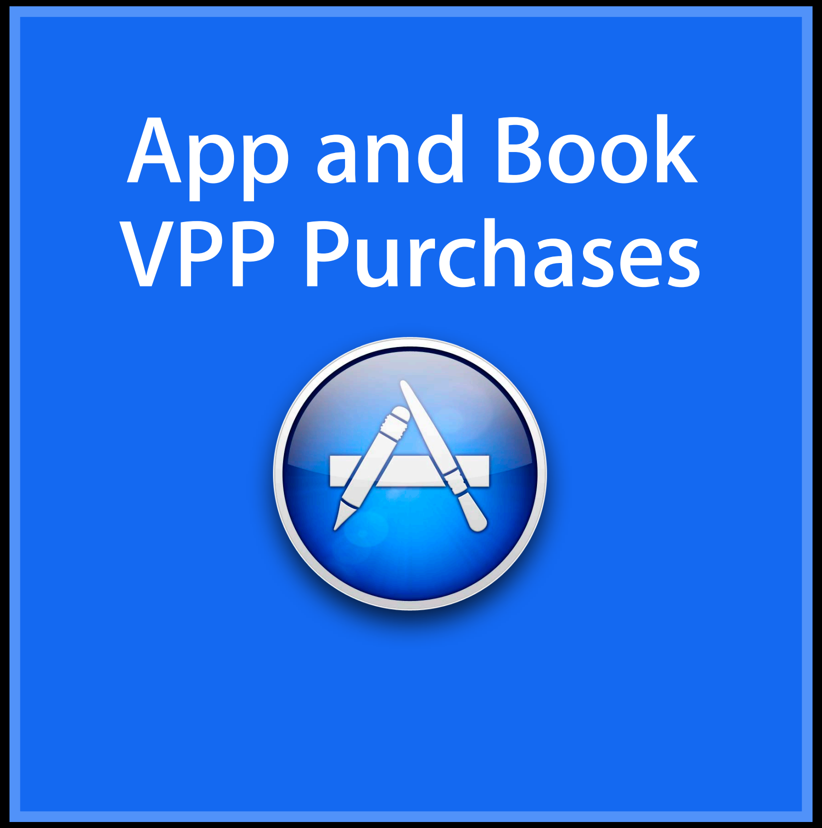
Assignments

- Get list of VPP app and book purchases
- Assign apps and books to users
- Tell device to install app with MDM command

Revocations

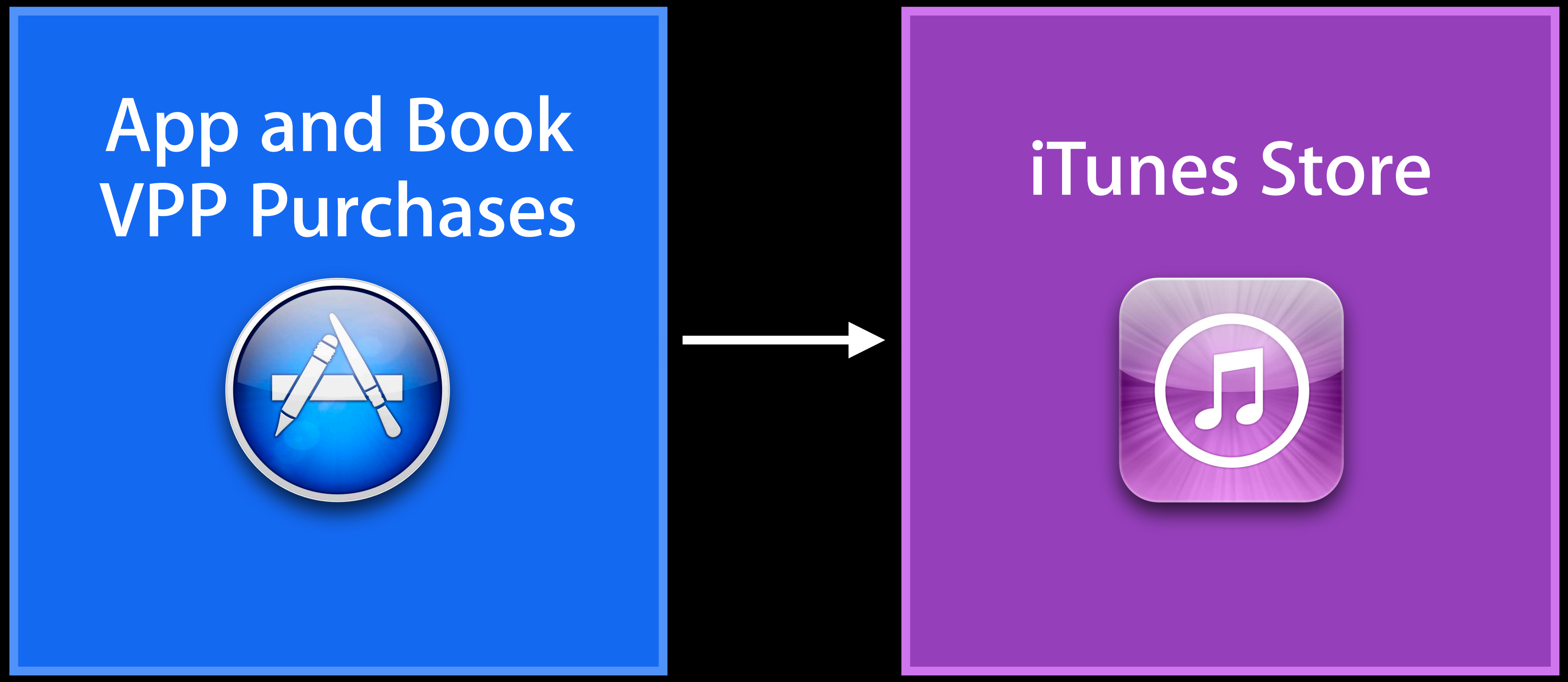
- Apps can be revoked and reassigned to another user
- Book assignments are permanent

Architecture



App and Book VPP Purchases

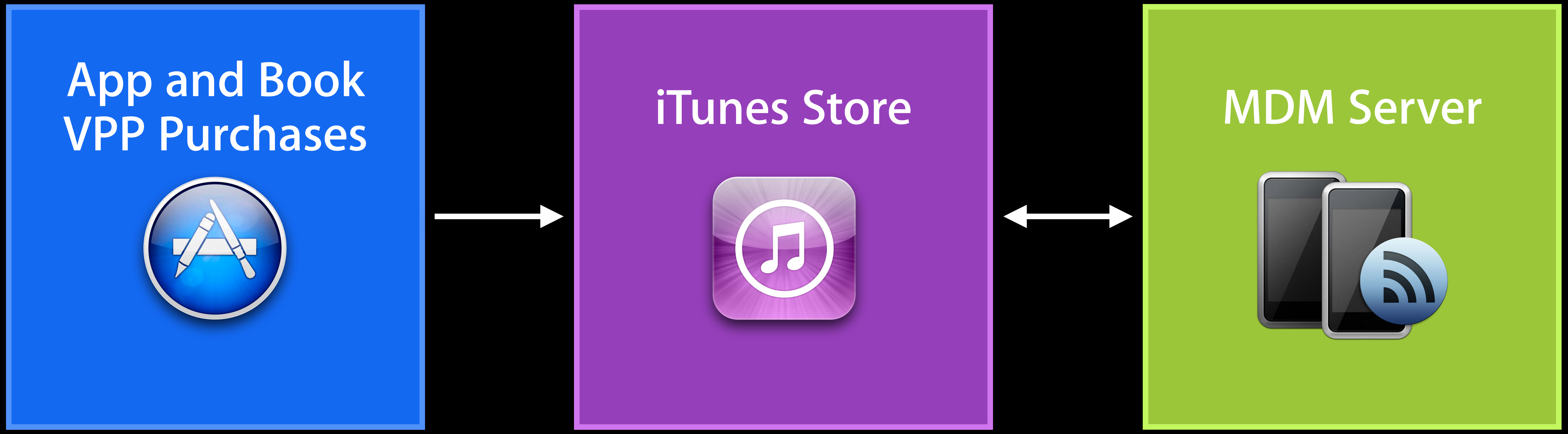
Architecture



App and Book VPP Purchases

iTunes Store

Architecture

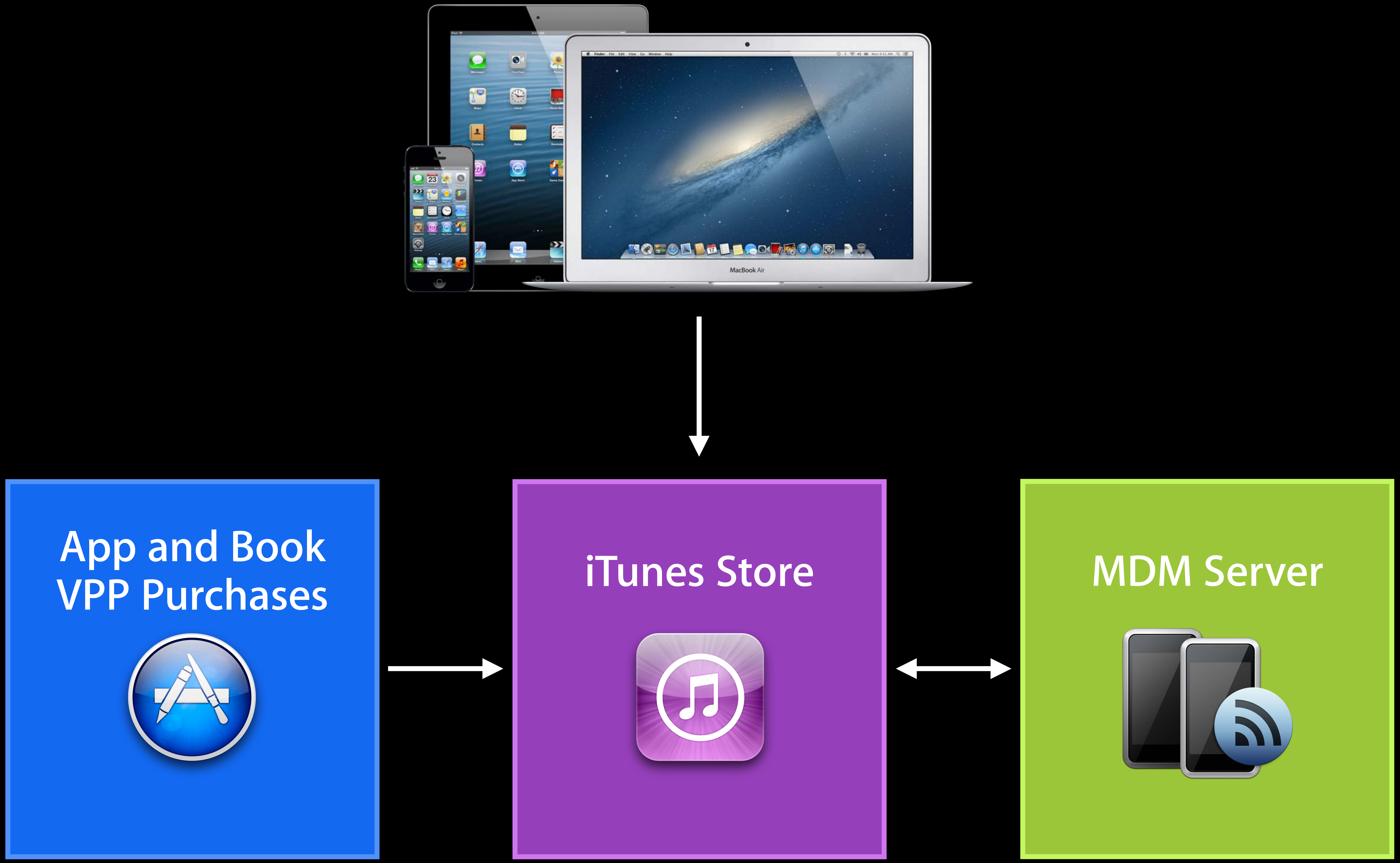


App and Book VPP Purchases

iTunes Store

MDM Server

Architecture

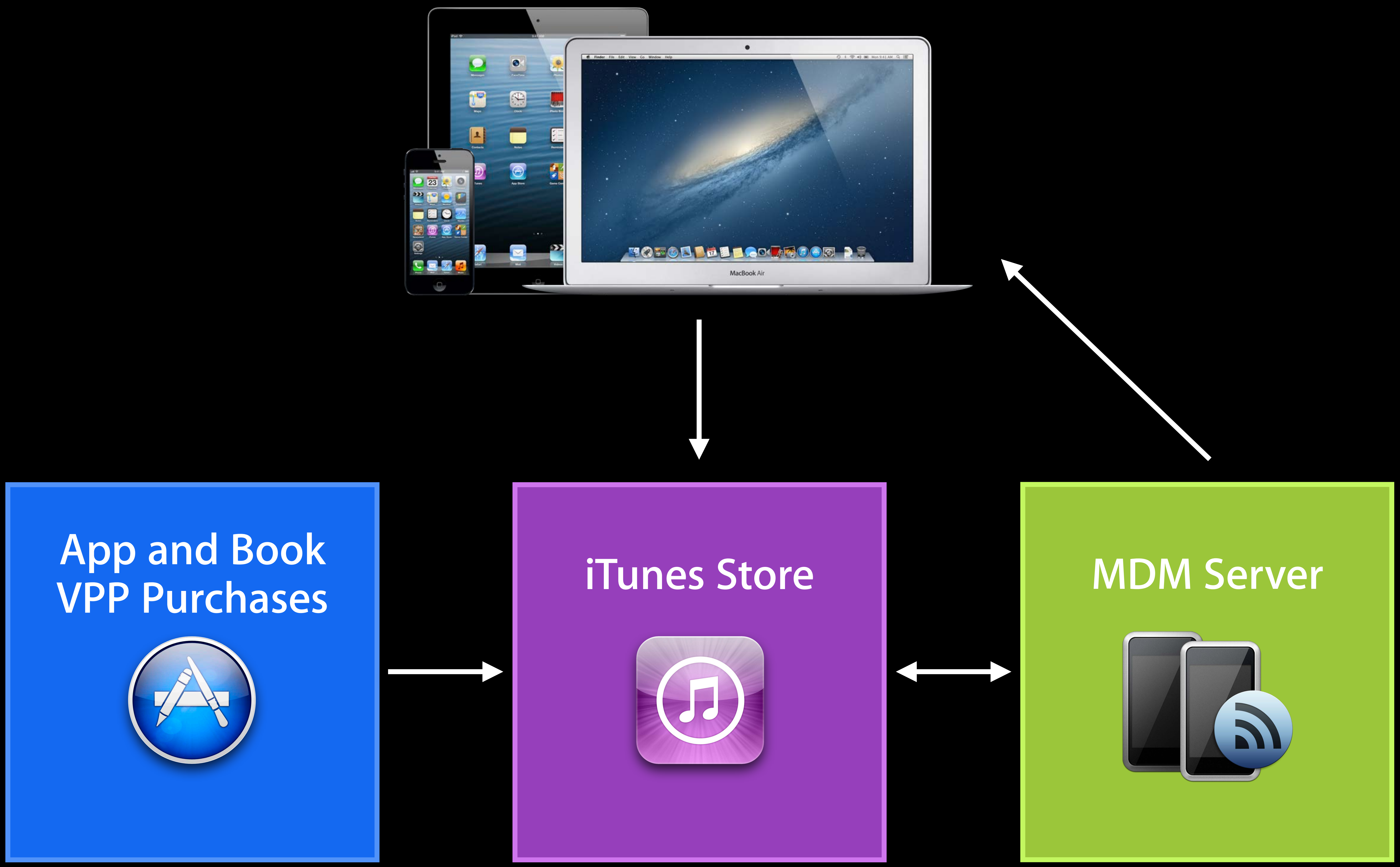


App and Book VPP Purchases

iTunes Store

MDM Server

Architecture



VPP APIs

Usage

- Call service URL

  `https://vpp.itunes.apple.com/<servicePath>`

- Obtain service URLs using `VPPServiceConfigSrv` ✓
  - Don’t hard code—URLs subject to change ✗
- Provide parameters as JSON strings (`application/json`)
- Include `sToken` with all service requests

VPP APIs

Service response

- JSON format
- Fields with null values not included
- Error results in ErrorNumber and ErrorMessage
    - ErrorMessage maps to single ErrorNumber
    - ErrorNumber can represent multiple ErrorMessages

VPP APIs

Error numbers

ErrorNumber	Meaning
9600	Missing required argument(s)
9601	Token verification failed
9602	Invalid argument
…	…
9607	License is irrevocable
…	…

VPP APIs

associateVPPLicenseWithVPPUserSrv Example

- associate_license.json

```
{“userId”:2,”licenseId”:4,”sToken”:”db21Nfjrh…1449b10eee”}
```

- curl command

```
curl https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/
associateVPPLicenseWithVPPUserSrv -d @associate_license.json
```

VPP APIs

associateVPPLicenseWithVPPUserSrv Example

```
{
    “status”:0,
    “license”:{
        “licenseId”:4,
        “adamID”:497799835,
        “productTypeId”:7,
        “pricingParam”:”STDQ”,
        “productTypeName”:”Software”,
        “isIrrevocable”:false,
        “status”:”Associated”
    },
    “user”:{
        “userId”:2
        “email”:”user2@test.com”,
        “clientUserIdStr”:”810C9B91-DF83-41DA-80A1-408AD7F081A8”,
        “status”:”Associated”,
        “itsIdHash”:"C2Wwd8LcIaE2v6f2/mvu82Gs/Lc="
    }
```

VPP APIs

associateVPPLicenseWithVPPUserSrv Example

```
        “licenseId”:4,
        “adamID”:497799835,
        “productTypeId”:7,
        “pricingParam”:”STDQ”,
        “productTypeName”:”Software”,
        “isIrrevocable”:false,
        “status”:”Associated”
    },
    “user”:{
        “userId”:2
        “email”:”user2@test.com”,
        “clientUserIdStr”:”810C9B91-DF83-41DA-80A1-408AD7F081A8”,
        “status”:”Associated”,
        “itsIdHash”:"C2Wwd8LcIaE2v6f2/mvu82Gs/Lc="
    }
}
```

VPP APIs

Getting started and sending invitations

- `VPPServiceConfigSrv`
- `registerVPPUserSrv`

VPP APIs

Assignment and revocation

- `getVPPUserSrv`
  - Returns user and any assigned licenses
- `getVPPUsersSrv`
  - Returns list of all users in the organization
  - Supports getting all users modified since last time list was requested
- `getVPPLicensesSrv`
  - Returns list of purchased licenses including assigned user
- `associateVPPLicenseWithVPPUserSrv`
- `disassociateVPPLicenseFromVPPUserSrv`

VPP APIs

Housekeeping

- `editVPPUserSrv`—update user info
- `VPPClientConfigSrv`—store organization info on server
- `retireVPPUserSrv`—disassociate VPP user from iTunes account and revoke any revocable licenses assigned to that user
    - Retired VPP user can be reinvited by calling `registerVPPUserSrv` with user’s `clientUserIdStr`

VPP APIs

Three kinds of users

MDM user account

`clientUserIdStr`

VPP user account

`userId`

End user’s Apple ID

`itsIdHash`

VPP APIs

Two key forms

- Single long—`userId`
- Tuple of strings—`{ clientUserIdStr, itsIdHash }`
- One-to-one association at any given time, but not immutable link
- Relationship between the two can change

VPP APIs

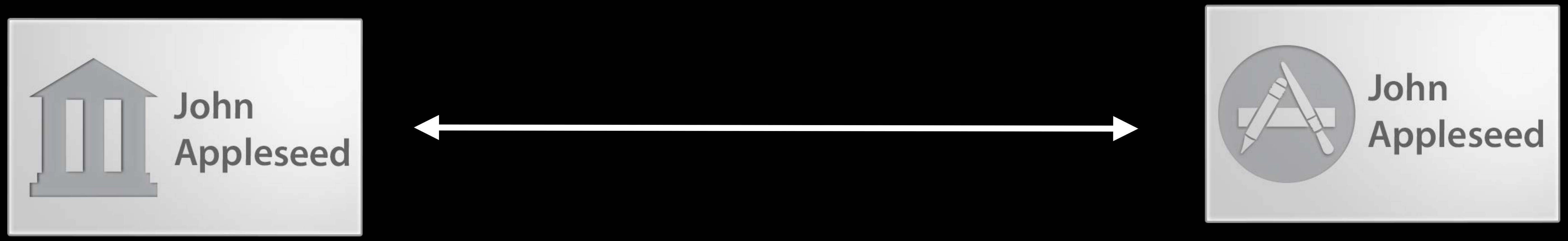
`userId` key form

- Simple to track
- Not tied one-to-one to single `clientUserIdStr`
- Always refers to exactly one `clientUserIdStr`
  - Converse not true: one `clientUserIdStr` can refer to multiple `userId` values over time
- `userId` associated with active `clientUserIdStr` may change when end user accepts invitation

VPP APIs

`userId` key form

clientUserIdStr = “directoryuserid”

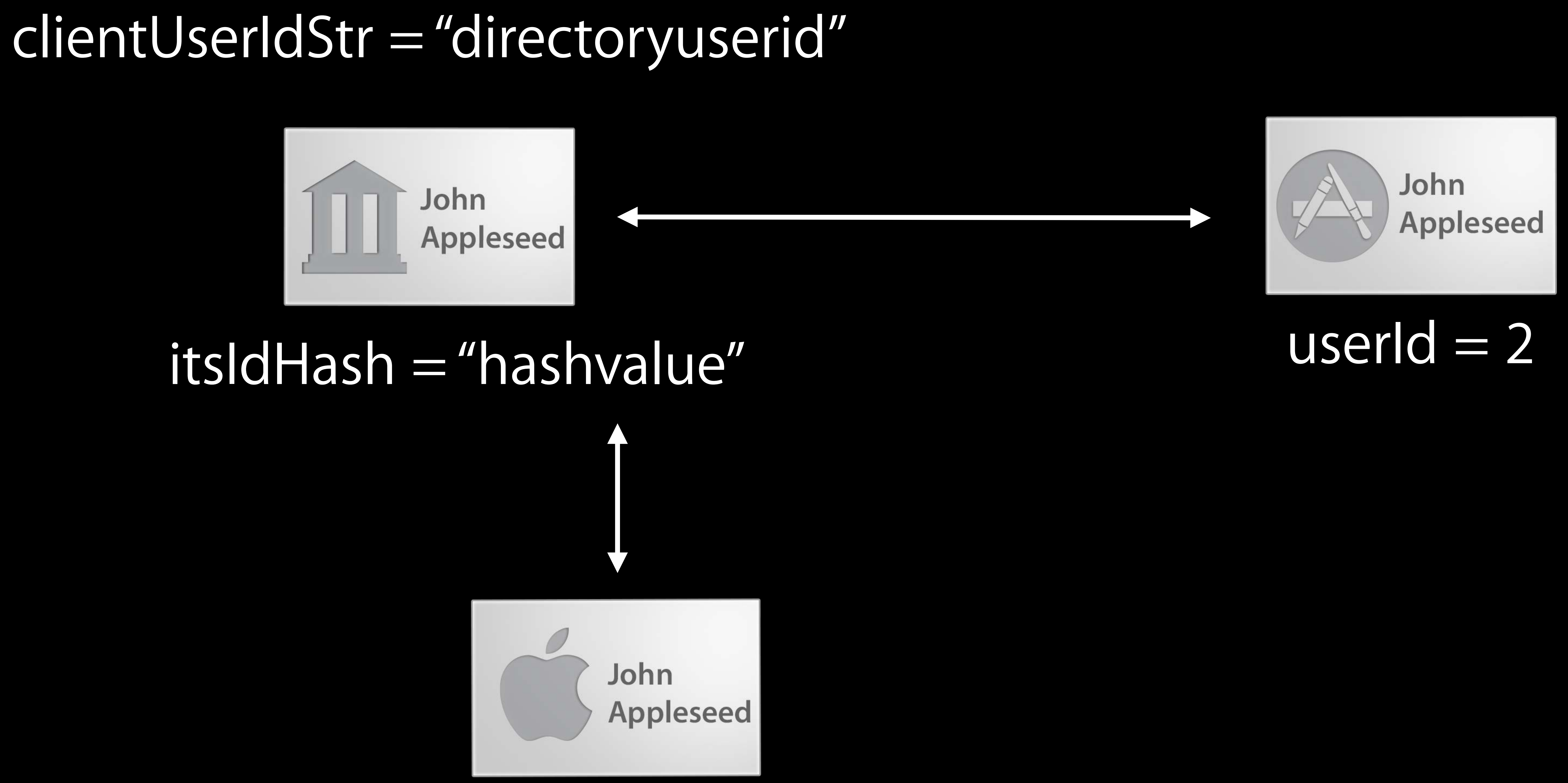


itsIdHash

userId = 2

VPP APIs

`userId` key form



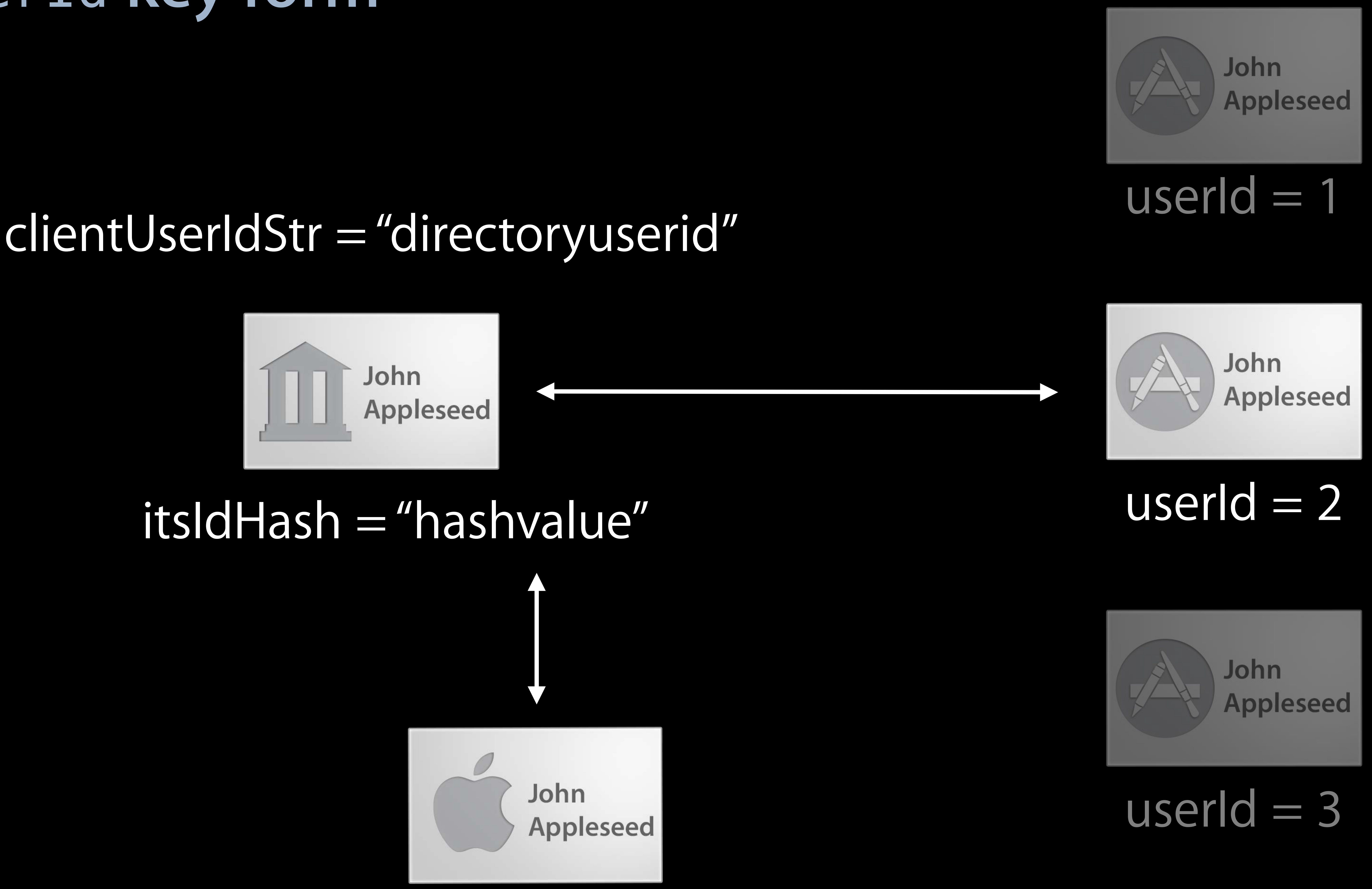
clientUserIdStr = “directoryuserid”

itsIdHash = “hashvalue”

userId = 2

VPP APIs

`userId` key form



clientUserIdStr = “directoryuserid”

itsIdHash = “hashvalue”

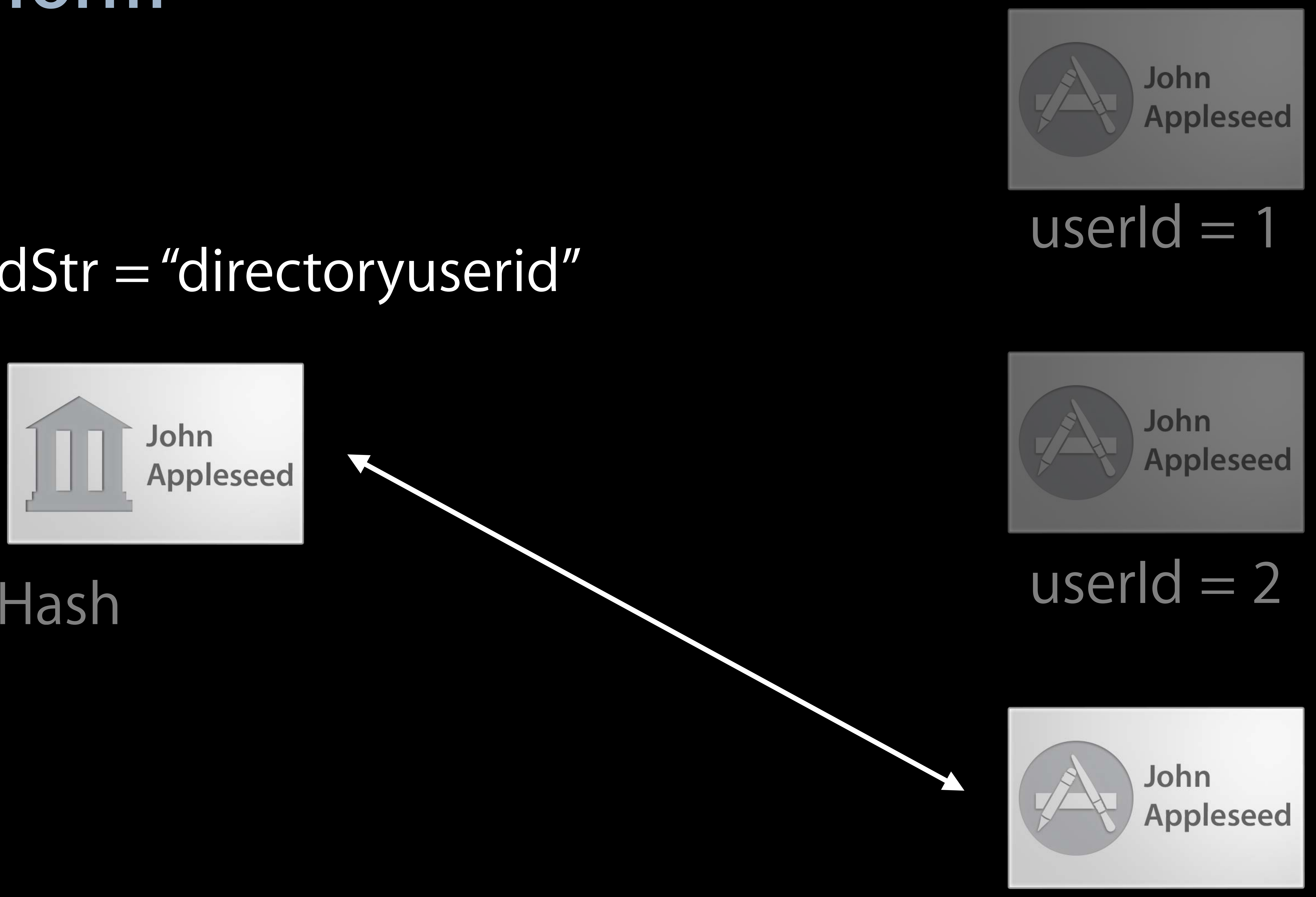
userId = 1

userId = 2

userId = 3

VPP APIs

`userId` key form



clientUserIdStr = “directoryuserid”

itsIdHash

userId = 1

userId = 2

userId = 3

VPP APIs

`{ clientUserIdStr, itsIdHash }` key form

- More directly maps association to end user's Apple ID
  - Possible to retire VPP user and then re-invite the same MDM user, who may or may not use the same Apple ID
- `itsIdHash` is NULL when end user has not accepted invitation
- `itsIdHash` uniquely (and opaquely) refers to end user's Apple ID
- Two MDM users (distinct `clientUserIdStr` values) can have the same itsIdHash if they both accepted invitation with the same Apple ID
  - Can't prevent this from happening, but may want to alert admin

VPP APIs

`{ clientUserIdStr, itsIdHash }` key form

clientUserIdStr = “directoryuserid_1”

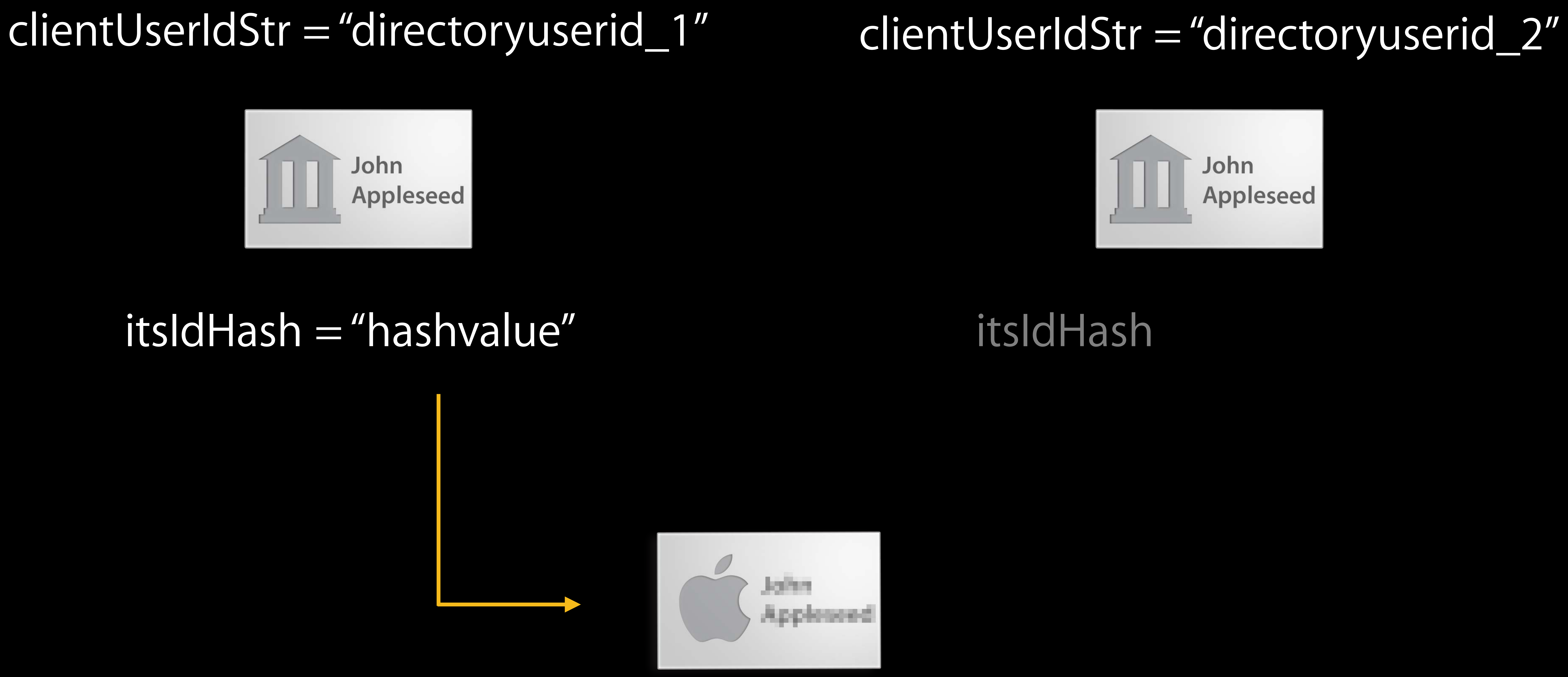
itsIdHash

clientUserIdStr = “directoryuserid_2”

itsIdHash

VPP APIs

`{ clientUserIdStr, itsIdHash }` key form



clientUserIdStr = “directoryuserid_1”

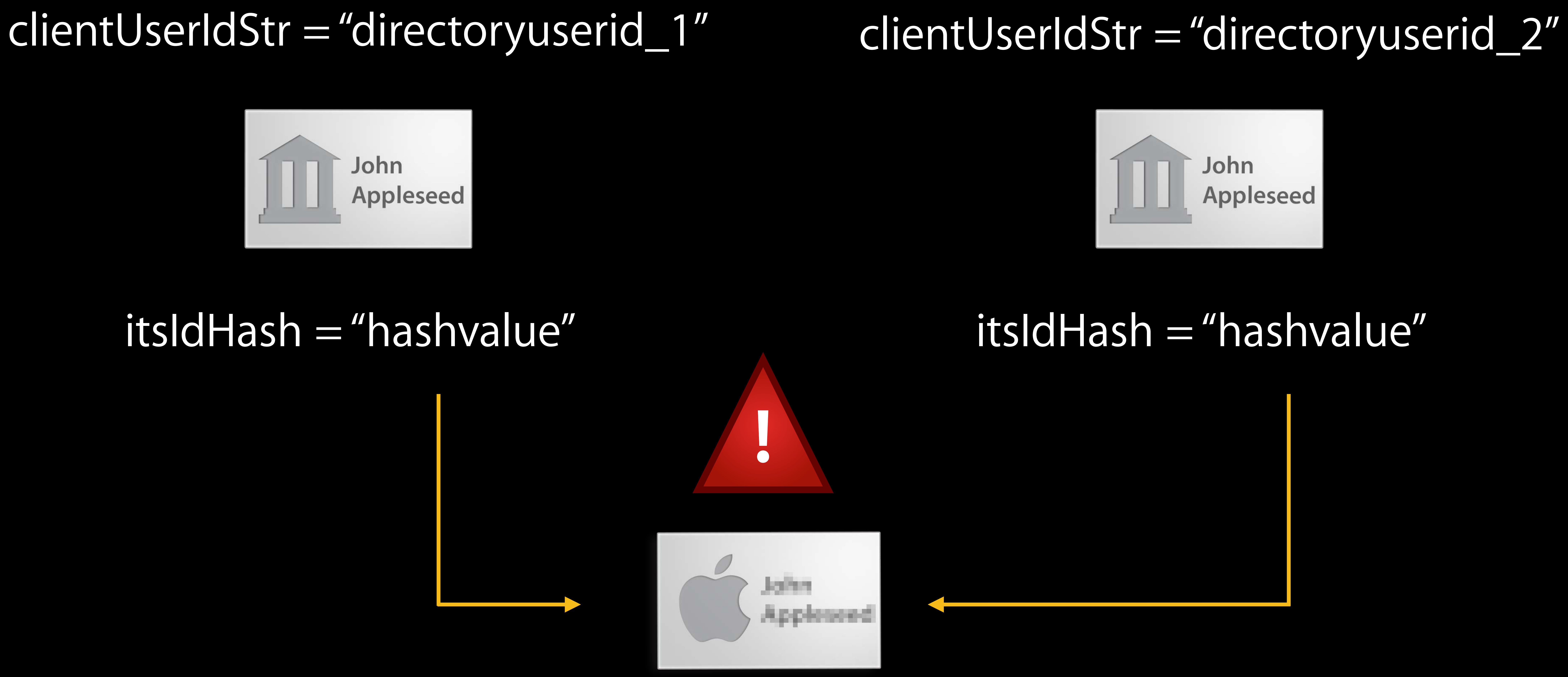
clientUserIdStr = “directoryuserid_2”

itsIdHash = “hashvalue”

itsIdHash

VPP APIs

`{ clientUserIdStr, itsIdHash }` key form



clientUserIdStr = “directoryuserid_1”

clientUserIdStr = “directoryuserid_2”

itsIdHash = “hashvalue”

itsIdHash = “hashvalue”

VPP APIs

`{ clientUserIdStr, itsIdHash }` key form

- Only one active VPP user account for any given `clientUserIdStr`
  - All requests only use `clientUserIdStr` to identify VPP user account
  - Include `itsIdHash` to fetch a retired user using `getVPPUserSrv`

VPP APIs

Which key form to choose

- Recommend you choose one of the two key forms and always use that ✓
- Don’t mix key forms unless you keep strictly in sync ✗

John Appleseed
VS
John Appleseed
John Appleseed

App Store Volume Purchase Program

Tips and tricks—users

- Choose a `clientUserIdStr` that will never change ✓
  - Do not choose a username or email address ✗
- Can make MDM user accounts the truth
  - Must handle retired VPP user accounts, which cannot be removed from the service
  - Retired accounts can be returned by `getVPPUsersSrv`
  - Handle VPP accounts retired by external means, e.g. user breaks link
  - Can reregister and send new invitation which may link to new Apple ID
- Retired VPP users interesting if they were assigned irrevocable licenses

App Store Volume Purchase Program

Tips and tricks—licenses

- Use `isIrrevocable` to determine if a license can be revoked ✓
  - Do not assume a particular license type can or cannot be revoked ✗
- Licenses may be assigned to VPP user account before invitation accepted and associated with Apple ID, but that allocates a license to that account
  - May want to wait until 'status' = "Associated" and itsIdHash is not NULL
- Can make MDM server the truth for revocable license assignments
- Do not have to track unassigned licenseIds
  - `associateVPPLicenseWithVPPUserSrv` will identify one for you
  - Track assigned revocable licenseIds so they can be revoked ✓

App Store Volume Purchase Program

Tips and tricks—installing apps

- Separate assignment from install command ✓
  - May be a delay in notification of device of assignment
  - Command will fail if iTunes account not signed in

App Store Volume Purchase Program

Summary

- Revocable app assignments
- Permanent book assignments
- Tell device to install assigned apps
- Fully integrated with iOS managed apps
- OS X Server caching server minimizes bandwidth usage

App Store Volume Purchase Program

Summary

- Revocable app assignments
- Permanent book assignments
- Tell device to install assigned apps
- Fully integrated with iOS managed apps
- OS X Server caching server minimizes bandwidth usage

Streamlined Device Enrollment

Easy

Streamlined Device Enrollment

- New enrollment method for devices purchased by an organization
  - Organization provides enrollment settings to new Apple service
  - Enrollment integrated into normal out-of-box Apple device experience

Streamlined Device Enrollment

Organization workflow

Streamlined Device Enrollment

Organization workflow

Orders Devices

Streamlined Device Enrollment

Organization workflow

Orders Devices

Assigns Devices to Service

Streamlined Device Enrollment

Organization workflow

Orders Devices

Assigns Devices to Service

Specifies Service Settings

Streamlined Device Enrollment

Organization workflow

Orders Devices

Assigns Devices to Service

Specifies Service Settings

Receives Devices

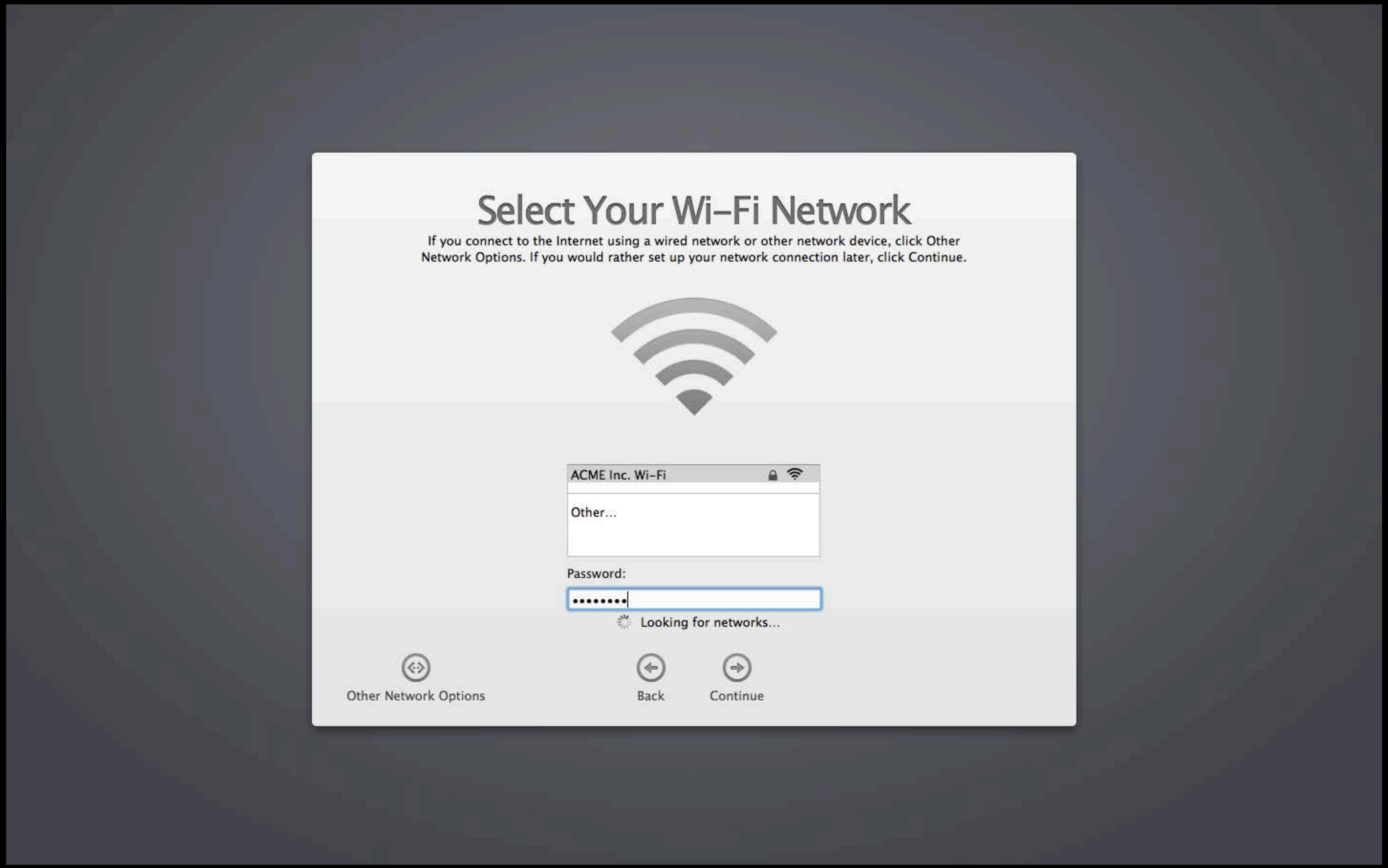
Streamlined Device Enrollment

Organization workflow

- Orders Devices
- Assigns Devices to Service
- Specifies Service Settings
- Receives Devices
- Hands Devices (in box!) to End Users

Streamlined Device Enrollment

End User workflow



Select Your Wi-Fi Network

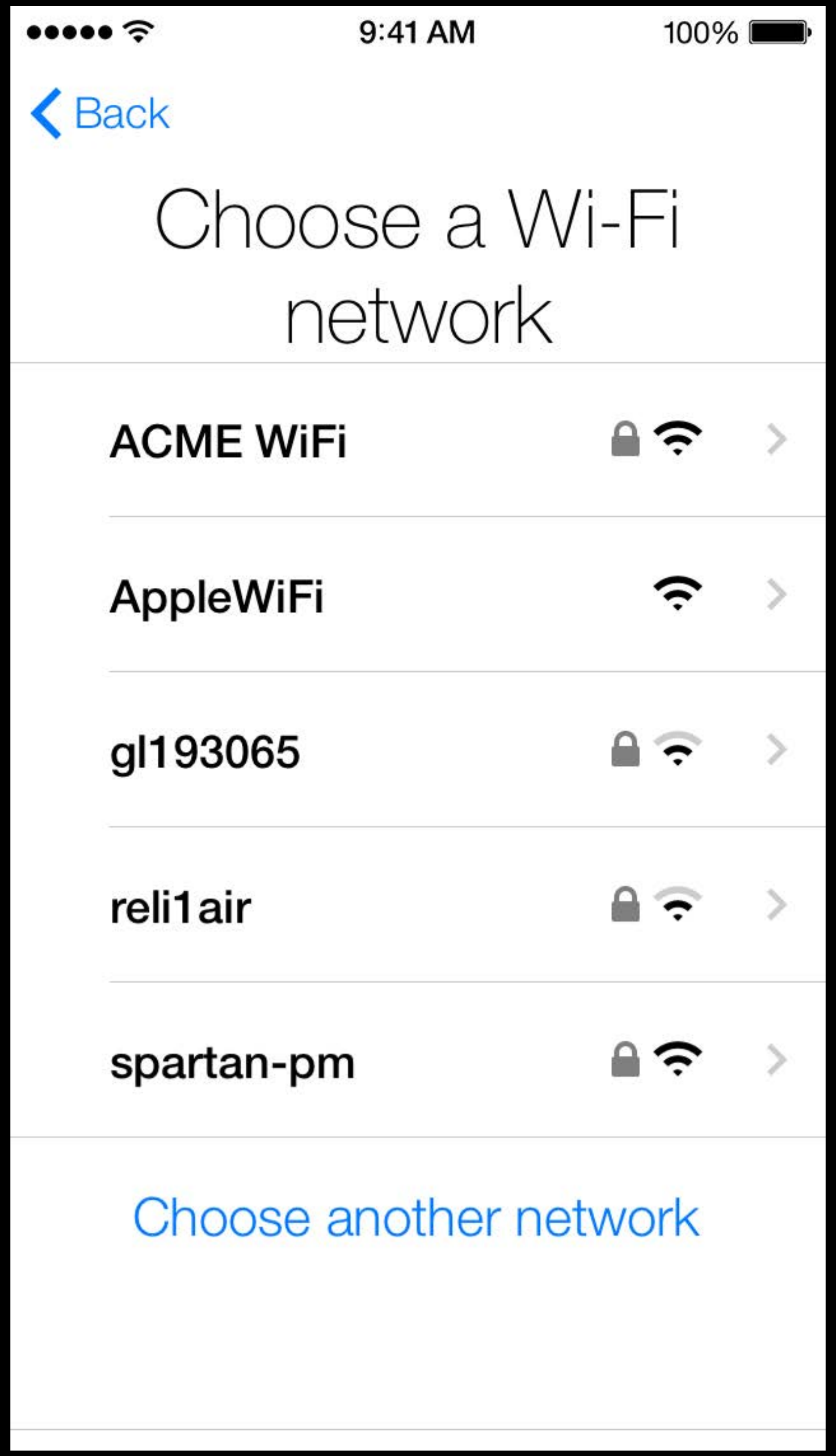
If you connect to the Internet using a wired network or other network device, click Other Network Options. If you would rather set up your network connection later, click Continue.

ACME Inc. Wi-Fi

Other...

Password: ••••••••

Looking for networks...



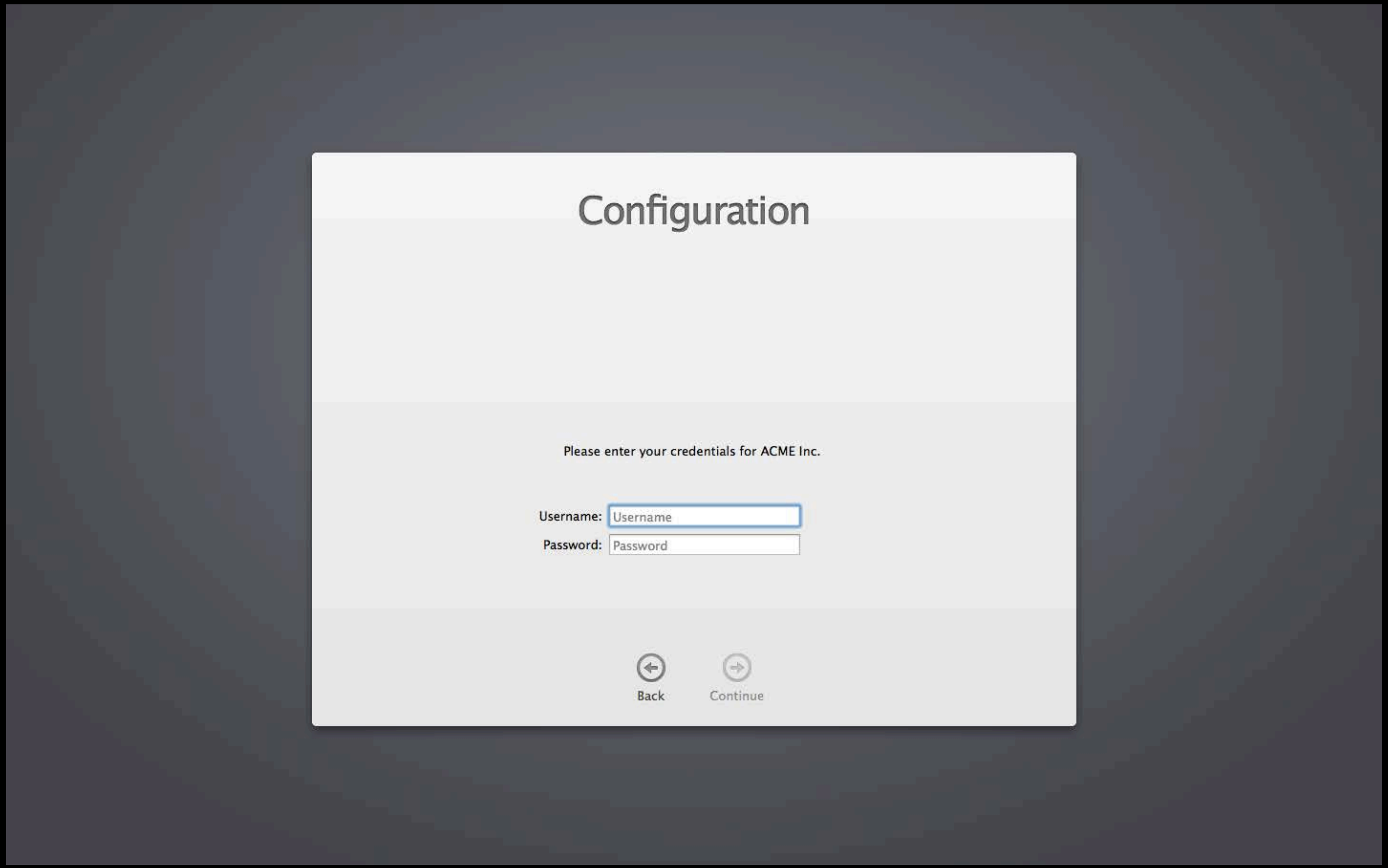
Choose a Wi-Fi network

- ACME WiFi
- AppleWiFi
- gl193065
- reli1air
- spartan-pm

Choose another network

Streamlined Device Enrollment

End User workflow

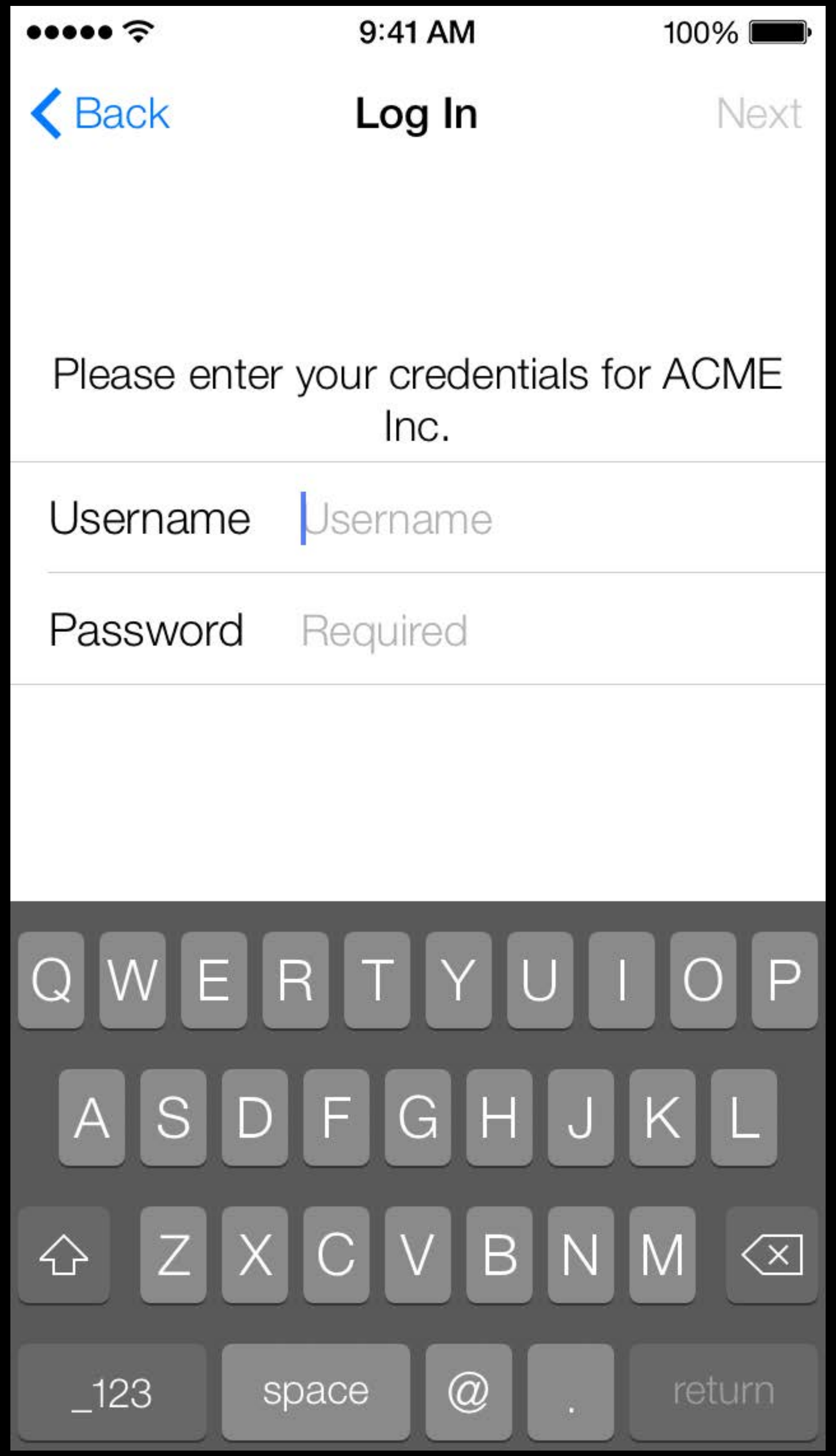


Configuration

Please enter your credentials for ACME Inc.

Username: Username

Password: Password



Please enter your credentials for ACME Inc.

Username Username

Password Required

Streamlined Device Enrollment

Service settings

- URL to enroll in organization's MDM server
- Prevent user from skipping enrollment
- Supervise device
  - Allow device to pair with any Mac
  - Prevent removal of MDM enrollment
- Setup assistant panes to skip

MDM Server Enhancements

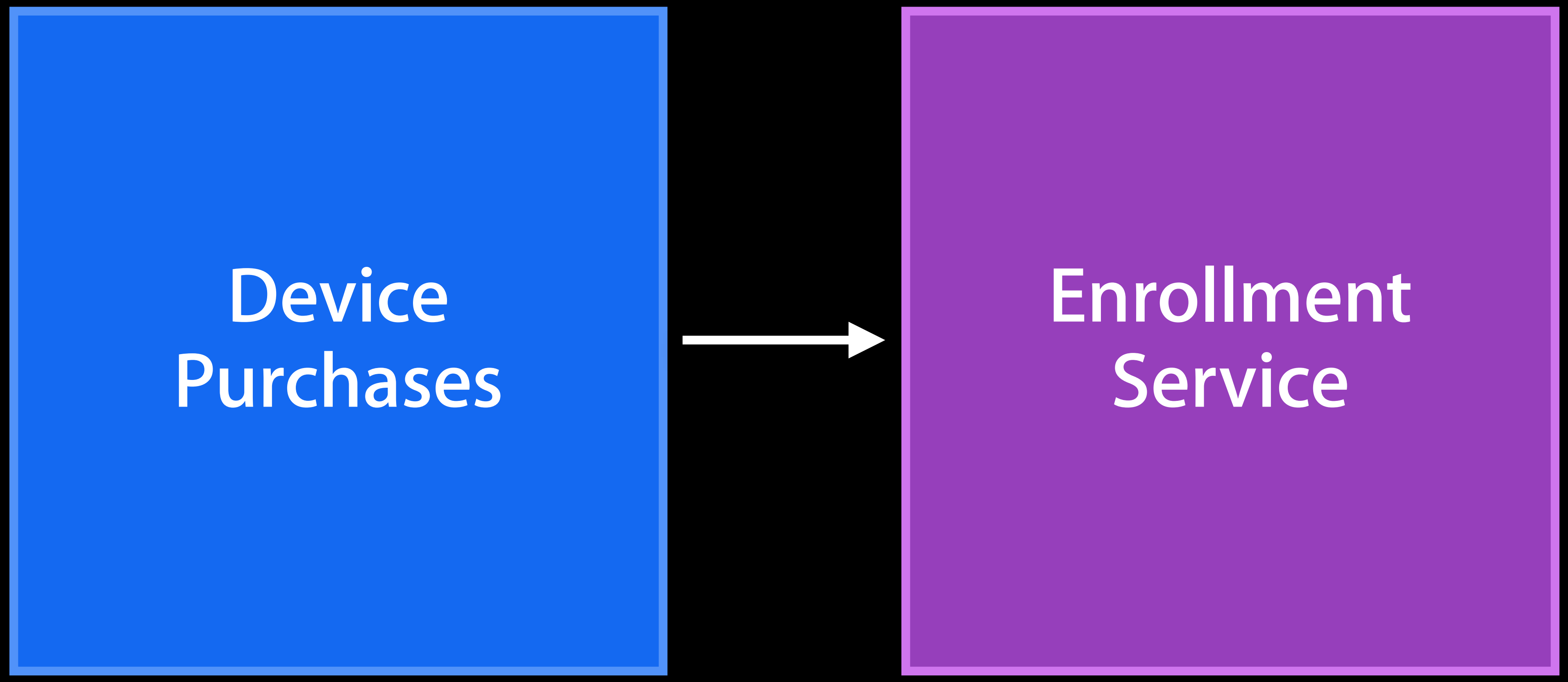
Overview

- Account authentication
- Settings editor
- Assign settings to devices

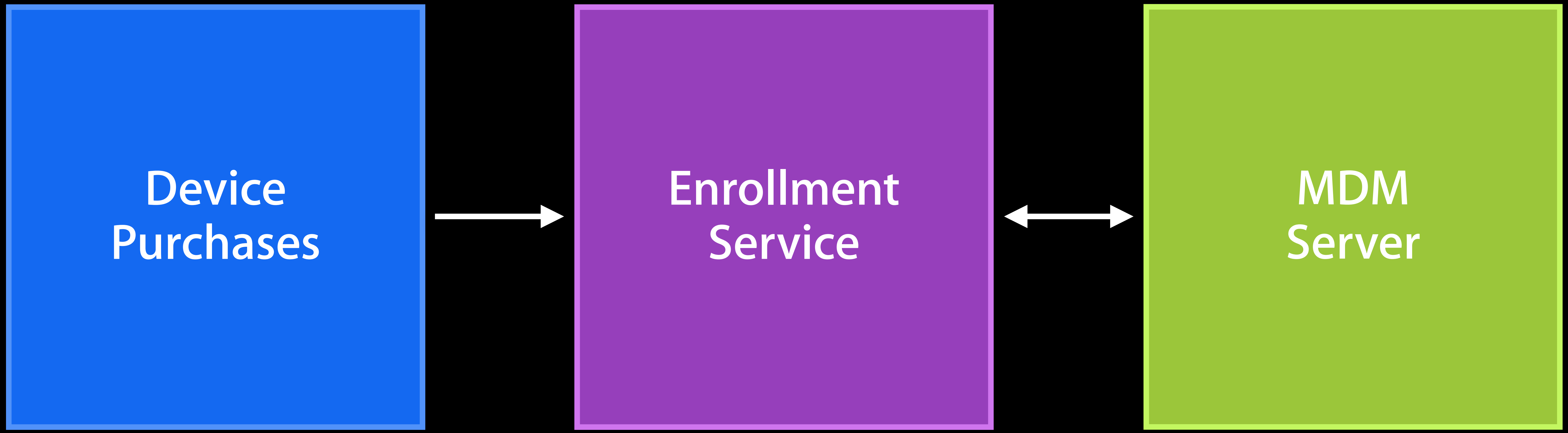
Architecture

Device Purchases

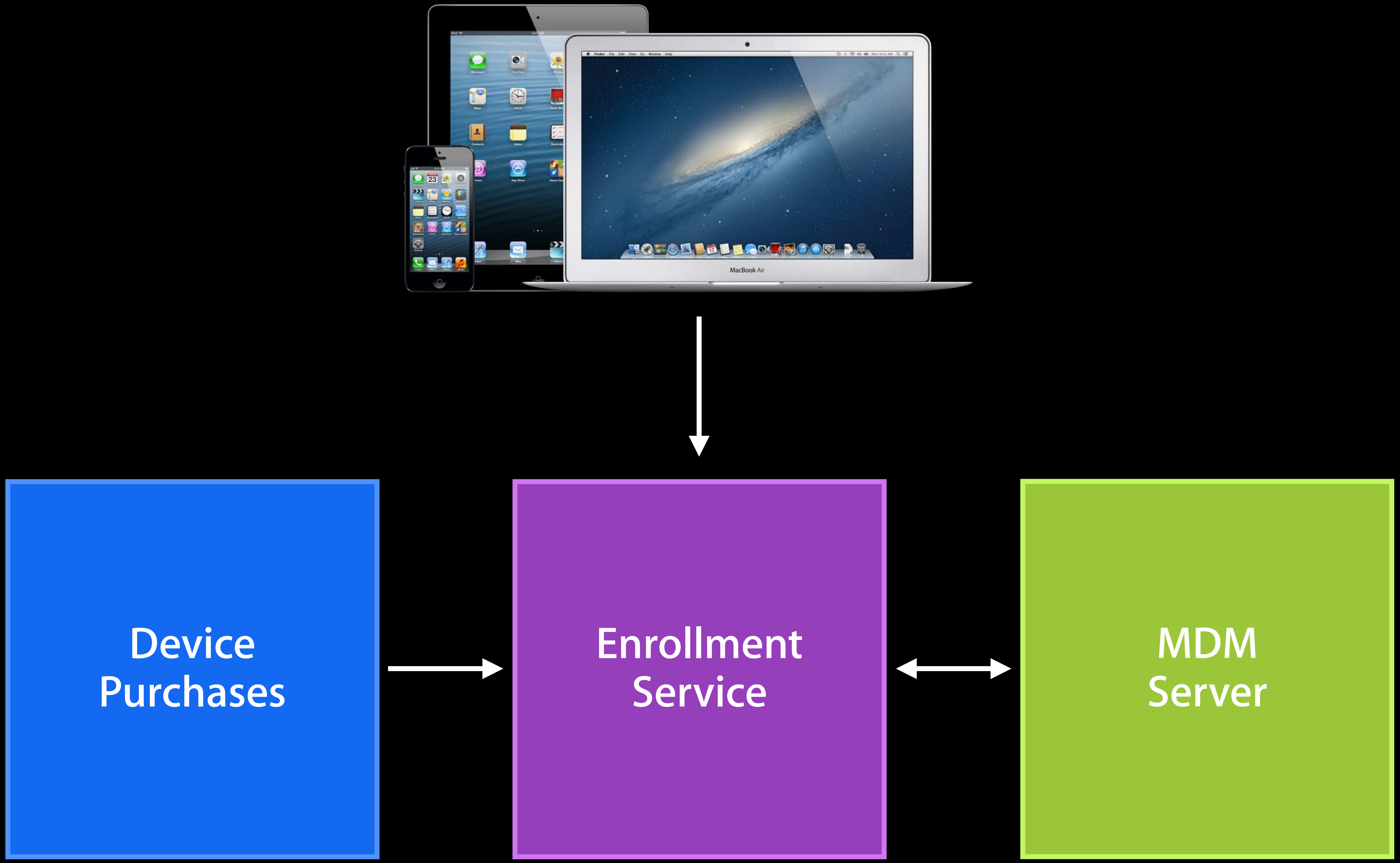
Architecture



Architecture



Architecture

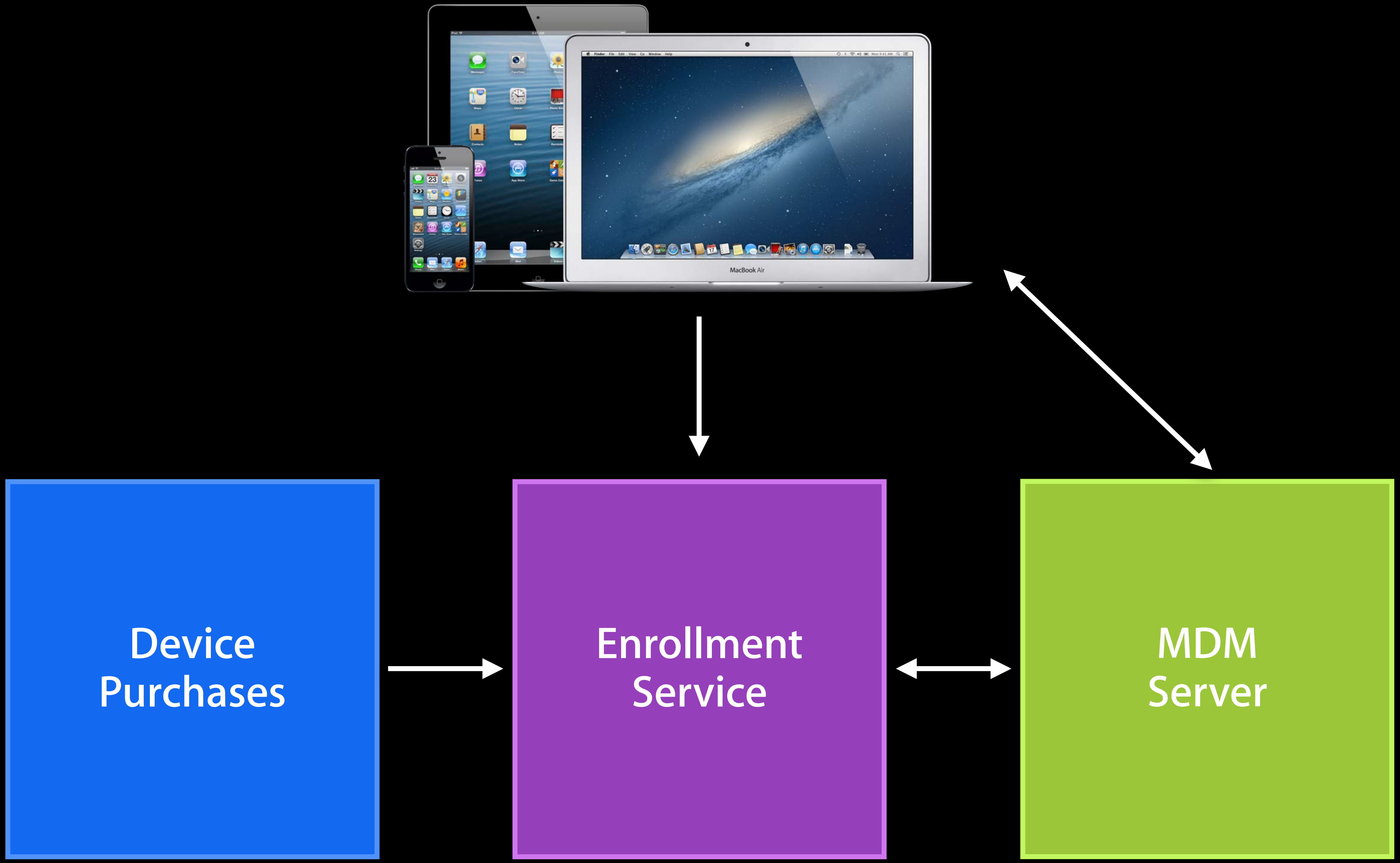


Device
Purchases

Enrollment
Service

MDM
Server

Architecture



Enrollment APIs

Getting started

- Account Details
- Fetch Devices

Enrollment APIs

Assigning settings to devices

- Define Settings
- Assign Settings
- Fetch Settings

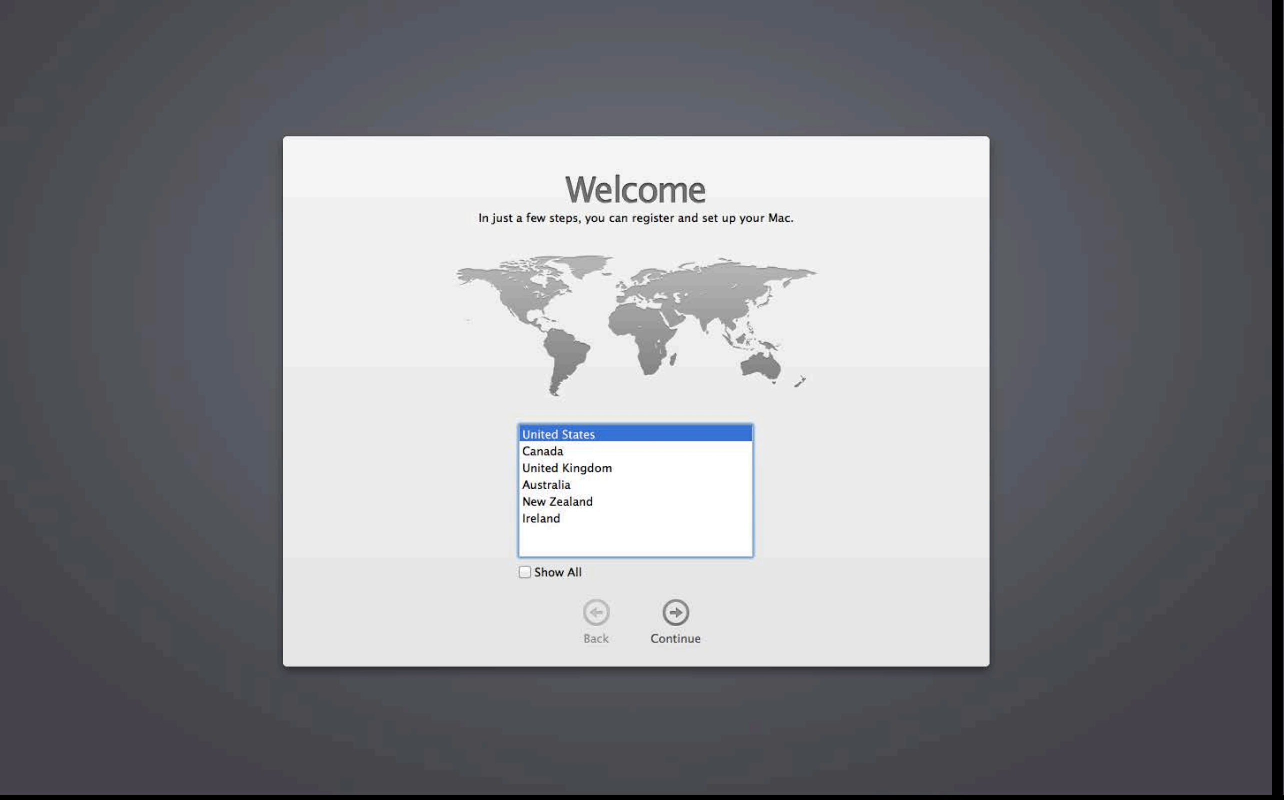
Enrollment APIs

Housekeeping

- Sync Devices
- Device Details
- Disown Devices
- Remove Settings

OS X Setup Experience

Today

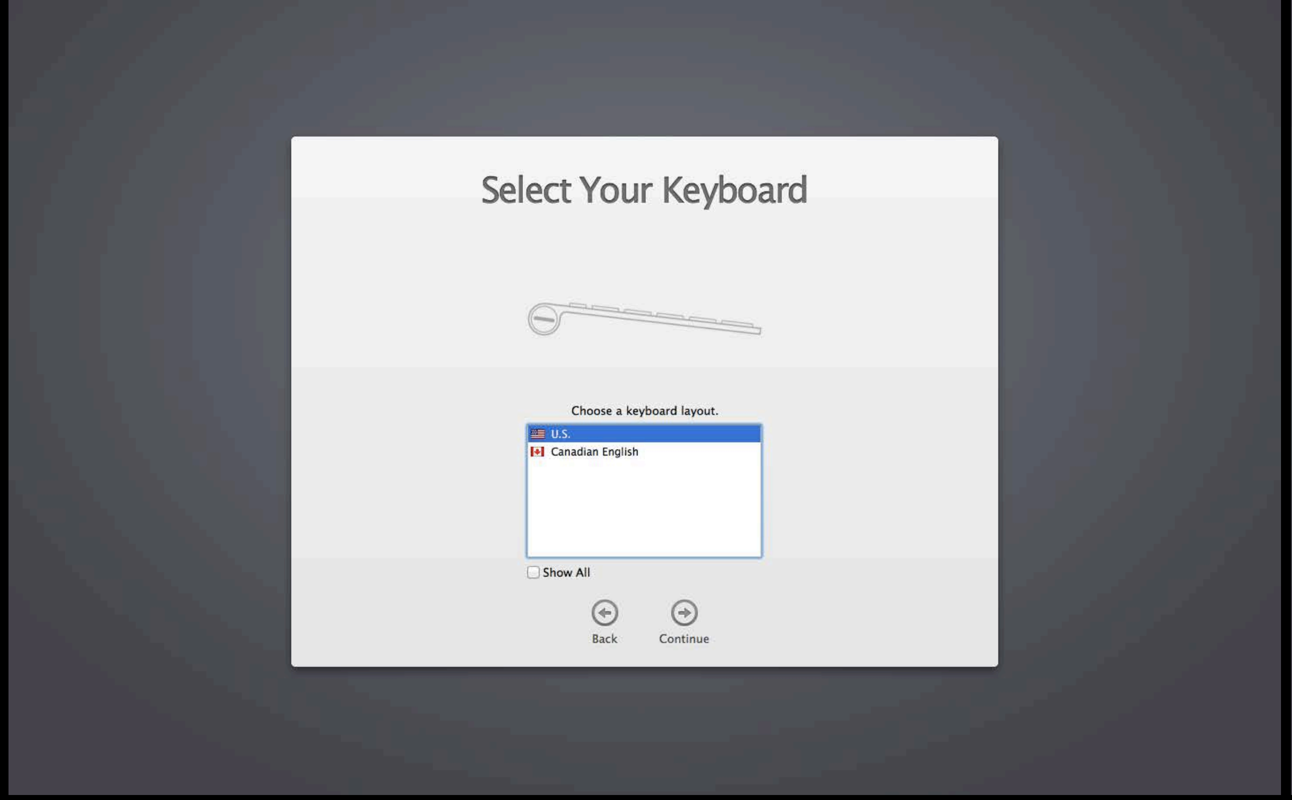


Welcome

In just a few steps, you can register and set up your Mac.

- United States
- Canada
- United Kingdom
- Australia
- New Zealand
- Ireland

☐ Show All

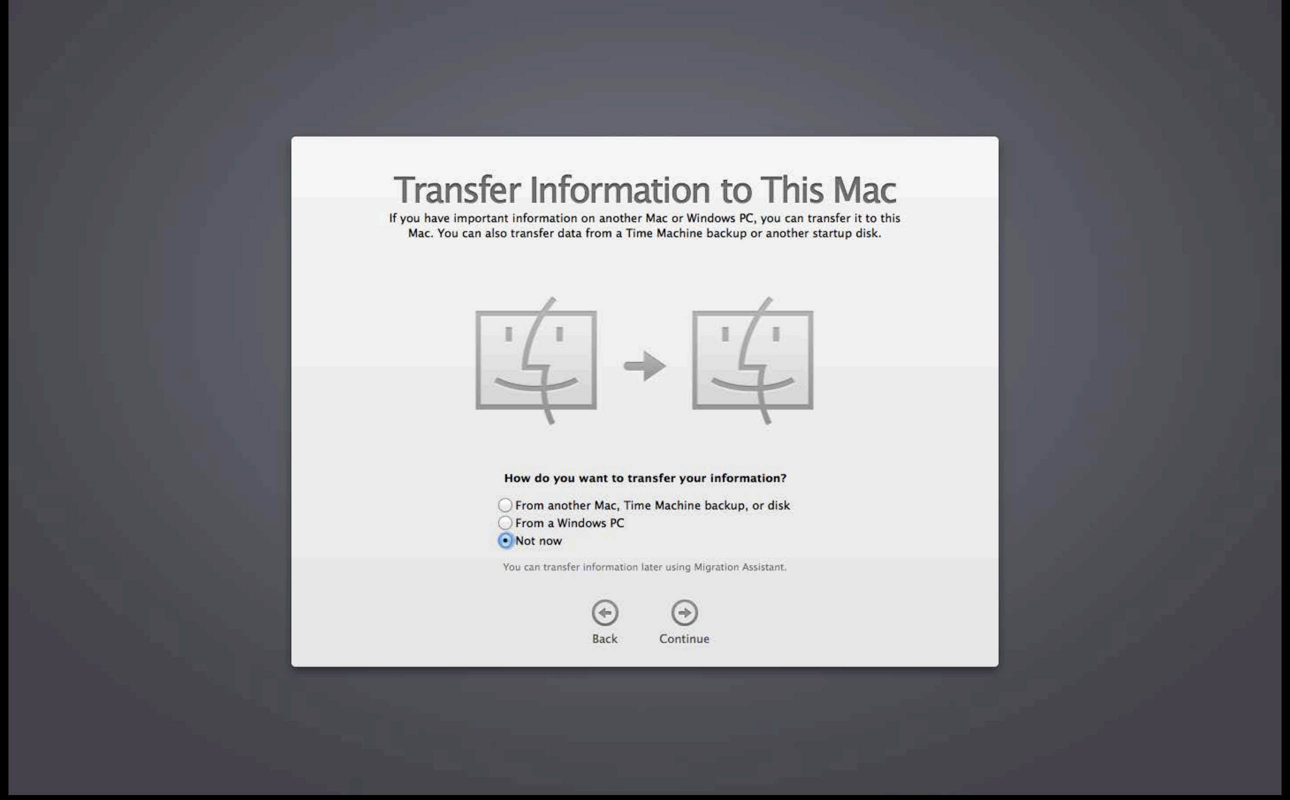


Select Your Keyboard

Choose a keyboard layout.

- U.S.
- Canadian English

☐ Show All



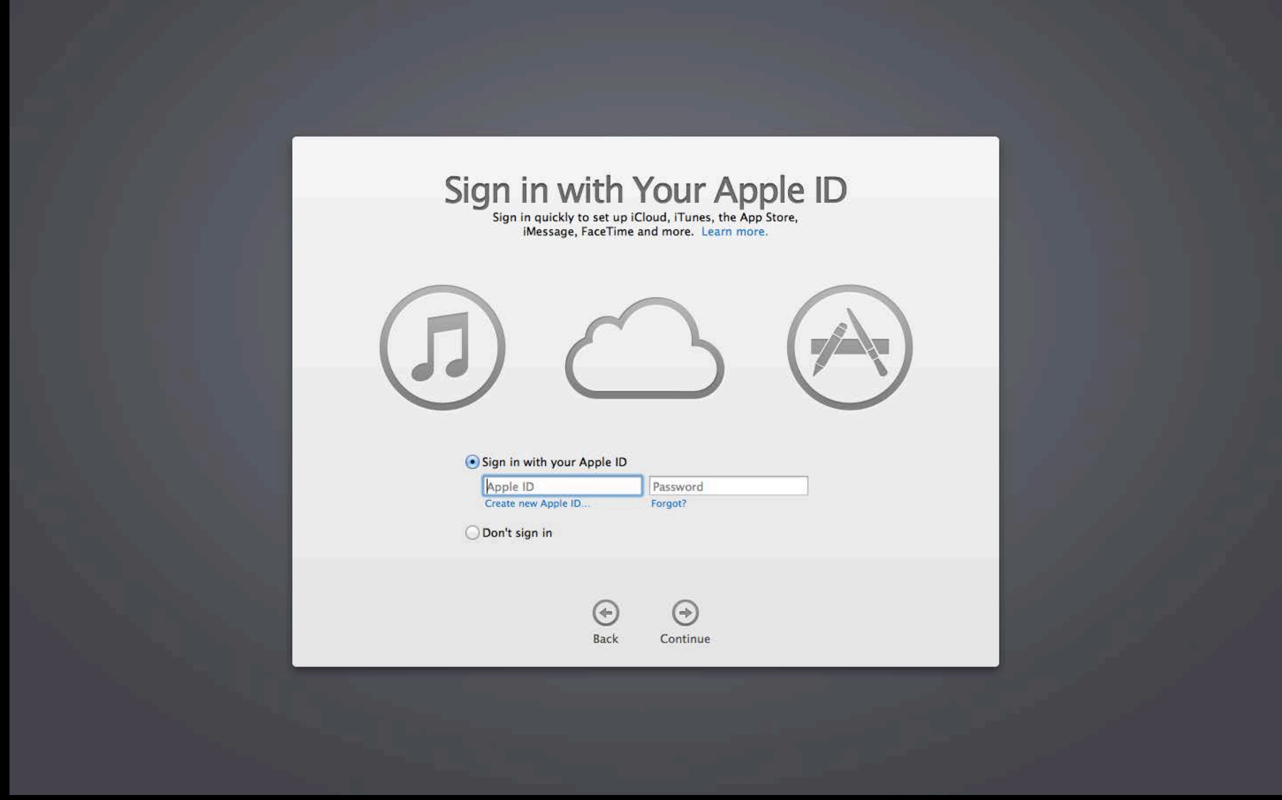
Transfer Information to This Mac

If you have important information on another Mac or Windows PC, you can transfer it to this Mac. You can also transfer data from a Time Machine backup or another startup disk.

How do you want to transfer your information?

○ From another Mac, Time Machine backup, or disk
○ From a Windows PC
● Not now

You can transfer information later using Migration Assistant.

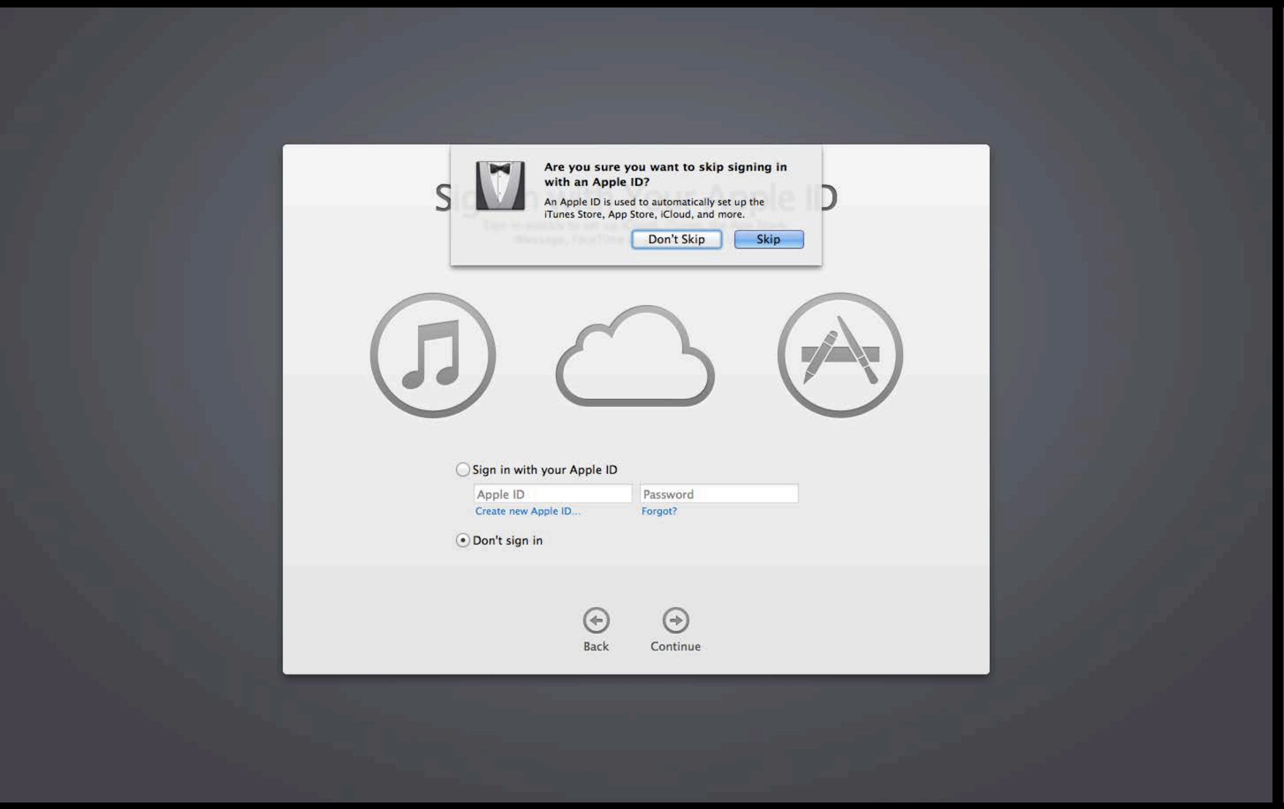


Sign in with Your Apple ID

Sign in quickly to set up iCloud, iTunes, the App Store, iMessage, FaceTime and more. Learn more.

● Sign in with your Apple ID
Apple ID | Password
Create new Apple ID... | Forgot?

○ Don't sign in

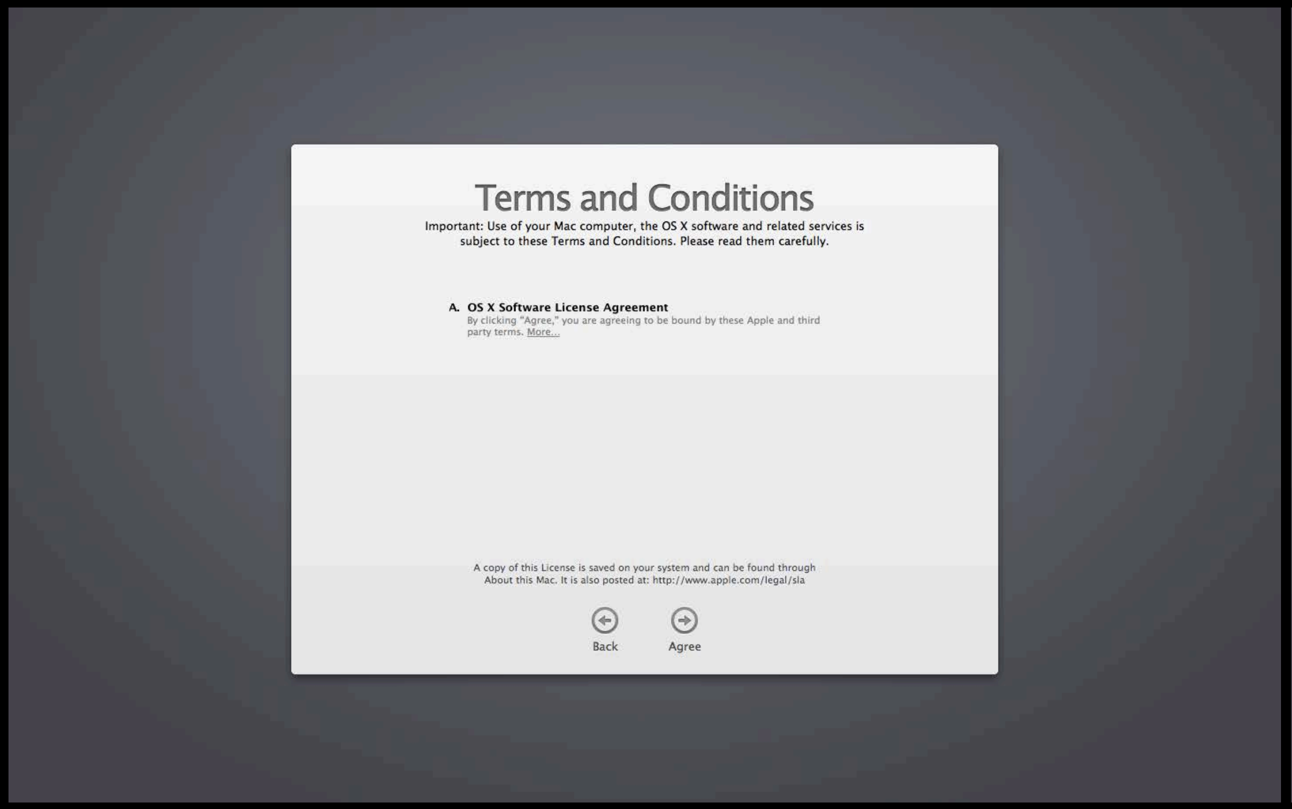


Are you sure you want to skip signing in with an Apple ID?

An Apple ID is used to automatically set up the iTunes Store, App Store, iCloud, and more.

○ Sign in with your Apple ID
Apple ID | Password
Create new Apple ID... | Forgot?

● Don't sign in

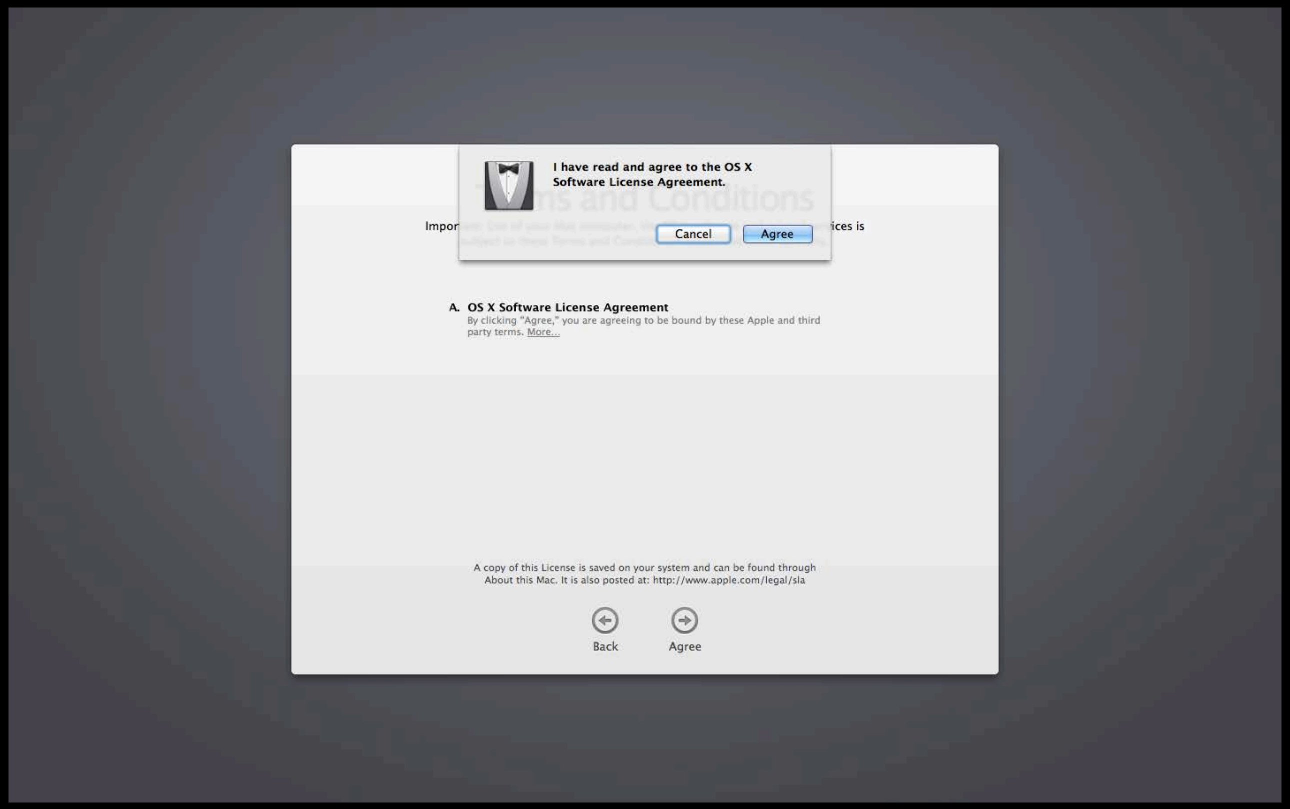


Terms and Conditions

Important: Use of your Mac computer, the OS X software and related services is subject to these Terms and Conditions. Please read them carefully.

A. **OS X Software License Agreement**
By clicking "Agree," you are agreeing to be bound by these Apple and third party terms. More...

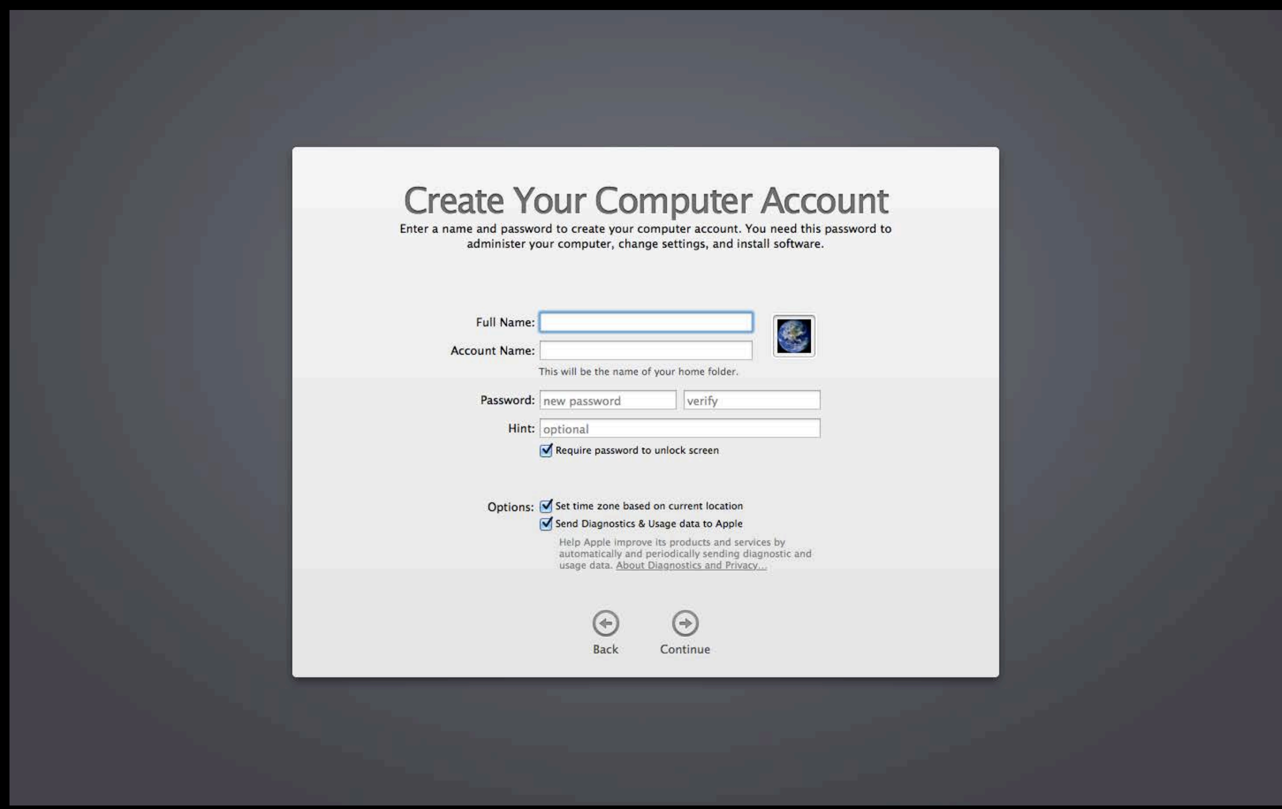
A copy of this License is saved on your system and can be found through About this Mac. It is also posted at: http://www.apple.com/legal/sla



I have read and agree to the OS X Software License Agreement.

A. **OS X Software License Agreement**
By clicking "Agree," you are agreeing to be bound by these Apple and third party terms. More...

A copy of this License is saved on your system and can be found through About this Mac. It is also posted at: http://www.apple.com/legal/sla

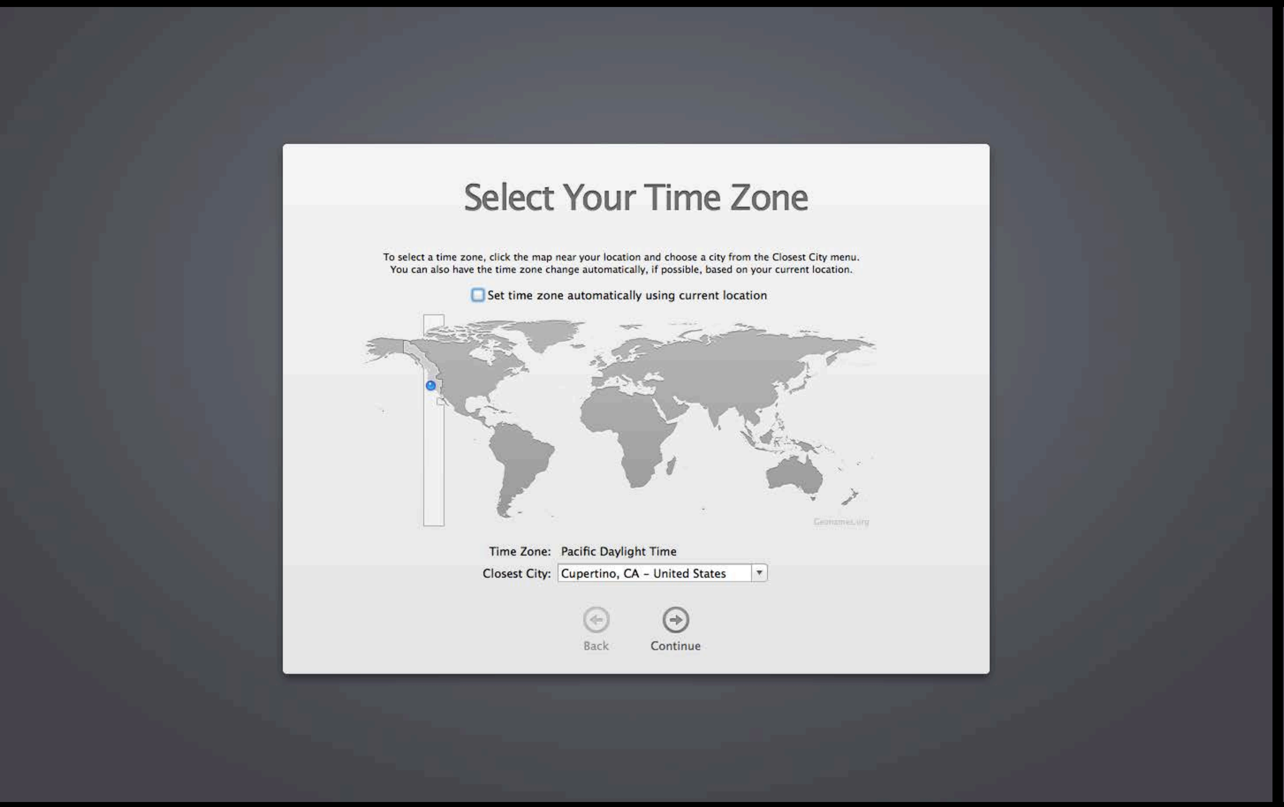


Create Your Computer Account

Enter a name and password to create your computer account. You need this password to administer your computer, change settings, and install software.

Full Name:
Account Name:
This will be the name of your home folder.
Password: new password | verify
Hint: optional
☑ Require password to unlock screen

Options: ☑ Set time zone based on current location
☑ Send Diagnostics & Usage data to Apple
Help Apple improve its products and services by automatically and periodically sending diagnostic and usage data. About Diagnostics and Privacy...

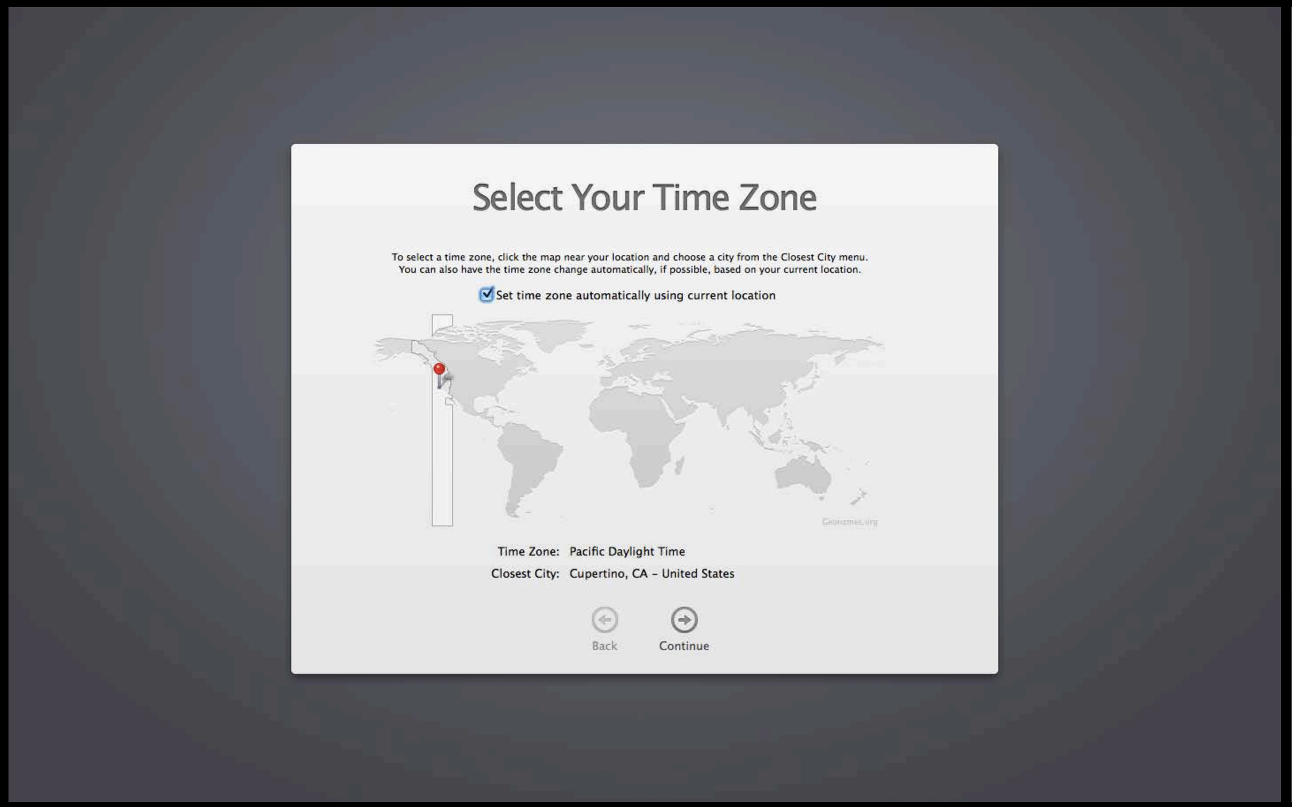


Select Your Time Zone

To select a time zone, click the map near your location and choose a city from the Closest City menu. You can also have the time zone change automatically, if possible, based on your current location.

☐ Set time zone automatically using current location

Time Zone: Pacific Daylight Time
Closest City: Cupertino, CA – United States

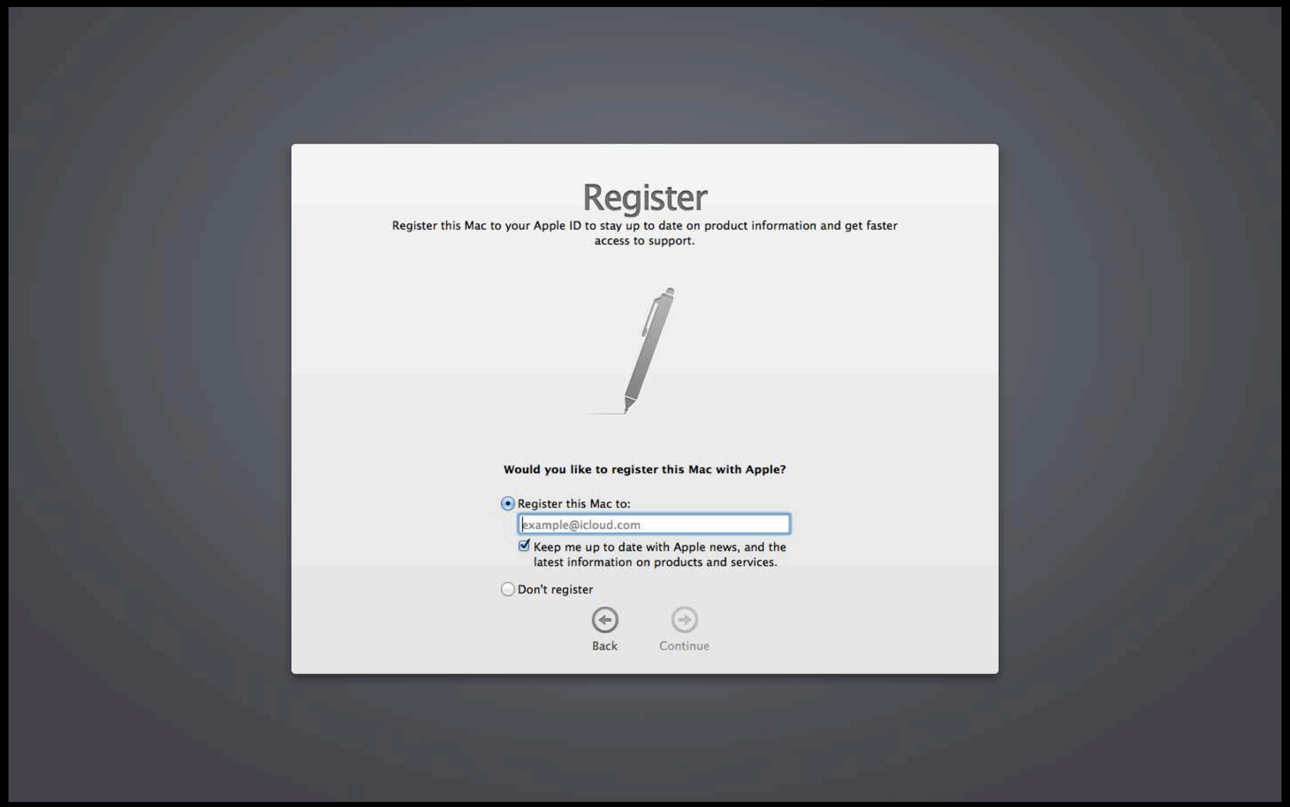


Select Your Time Zone

To select a time zone, click the map near your location and choose a city from the Closest City menu. You can also have the time zone change automatically, if possible, based on your current location.

☑ Set time zone automatically using current location

Time Zone: Pacific Daylight Time
Closest City: Cupertino, CA – United States



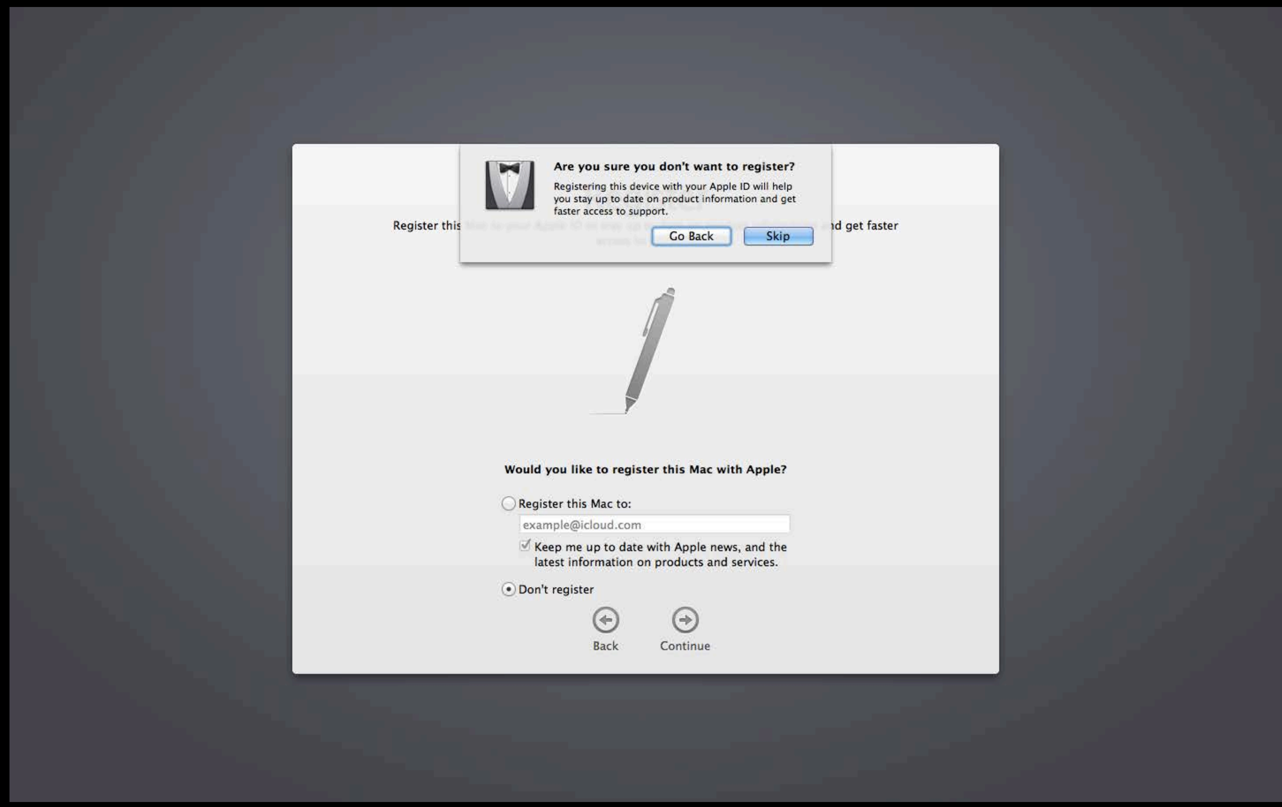
Register

Register this Mac to your Apple ID to stay up to date on product information and get faster access to support.

Would you like to register this Mac with Apple?

● Register this Mac to:
example@icloud.com
☑ Keep me up to date with Apple news, and the latest information on products and services.

○ Don't register



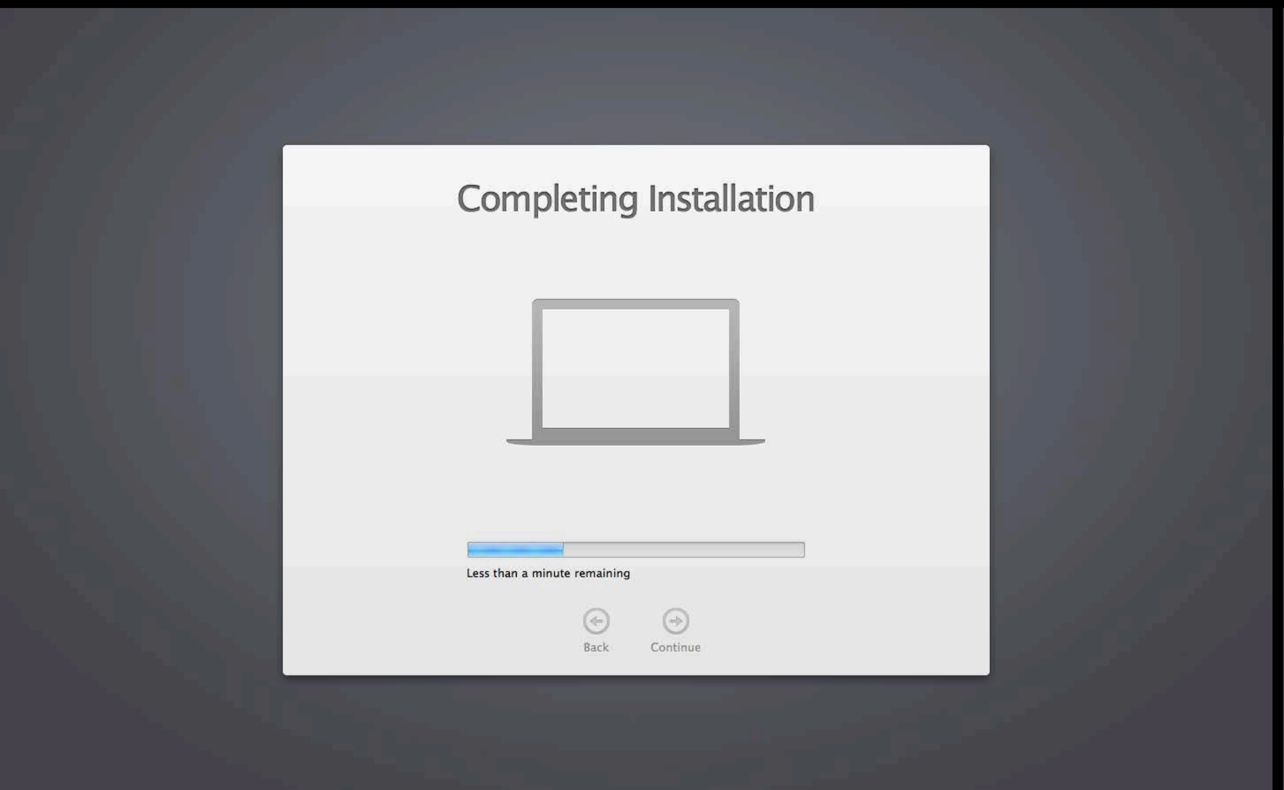
Are you sure you don't want to register?

Registering this device with your Apple ID will help you stay up to date on product information and get faster access to support.

Would you like to register this Mac with Apple?

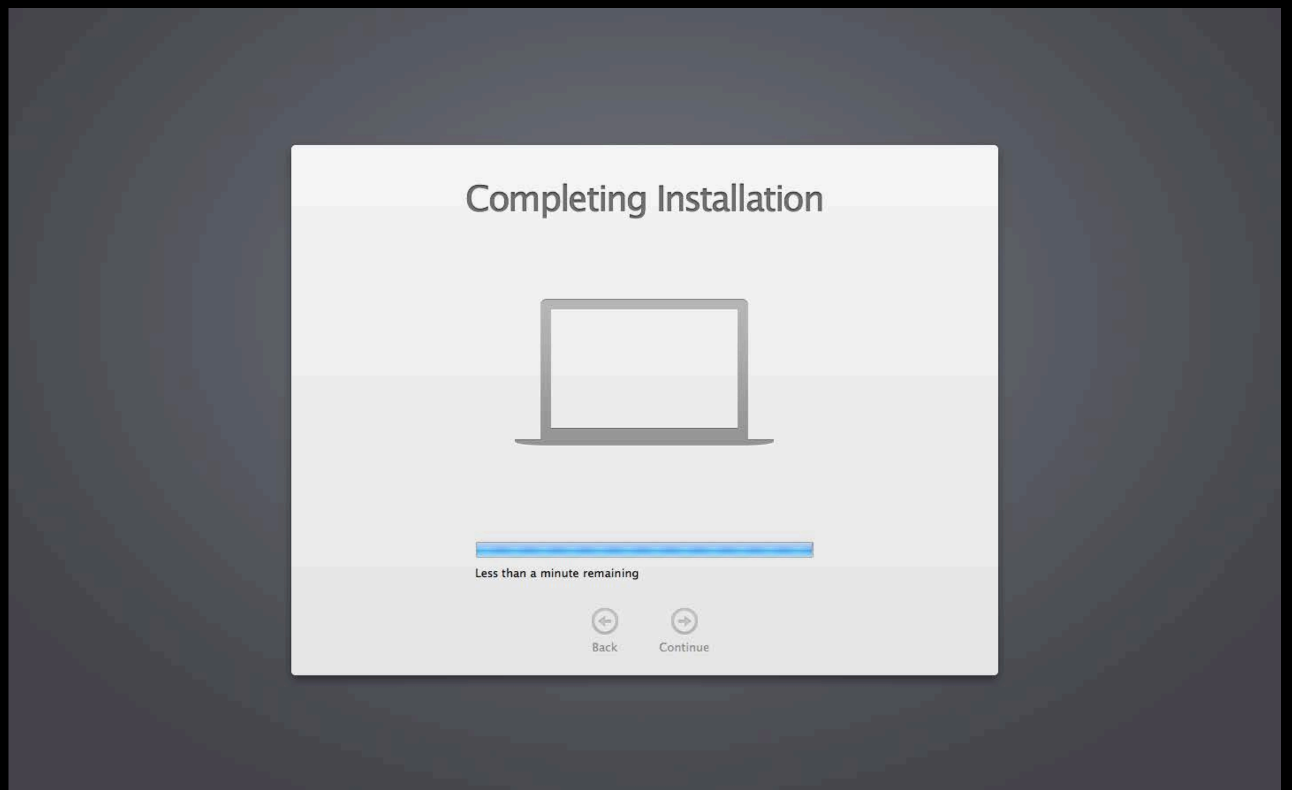
○ Register this Mac to:
example@icloud.com
☑ Keep me up to date with Apple news, and the latest information on products and services.

● Don't register



Completing Installation

Less than a minute remaining



Completing Installation

Less than a minute remaining

Thank You

Your Mac is set up and ready to use.

Start using your Mac

Welcome
Select Your Keyboard
Transfer Information to This Mac
Sign in with Your Apple ID
Create Your Computer Account
Select Your Time Zone
Completing Installation
Completing Installation

OS X Setup Experience

With streamlined device enrollment

Demo

Putting it all together

Chris Skogen
Engineering Manager

Jussi-Pekka Mantere
Engineering Manager

Summary

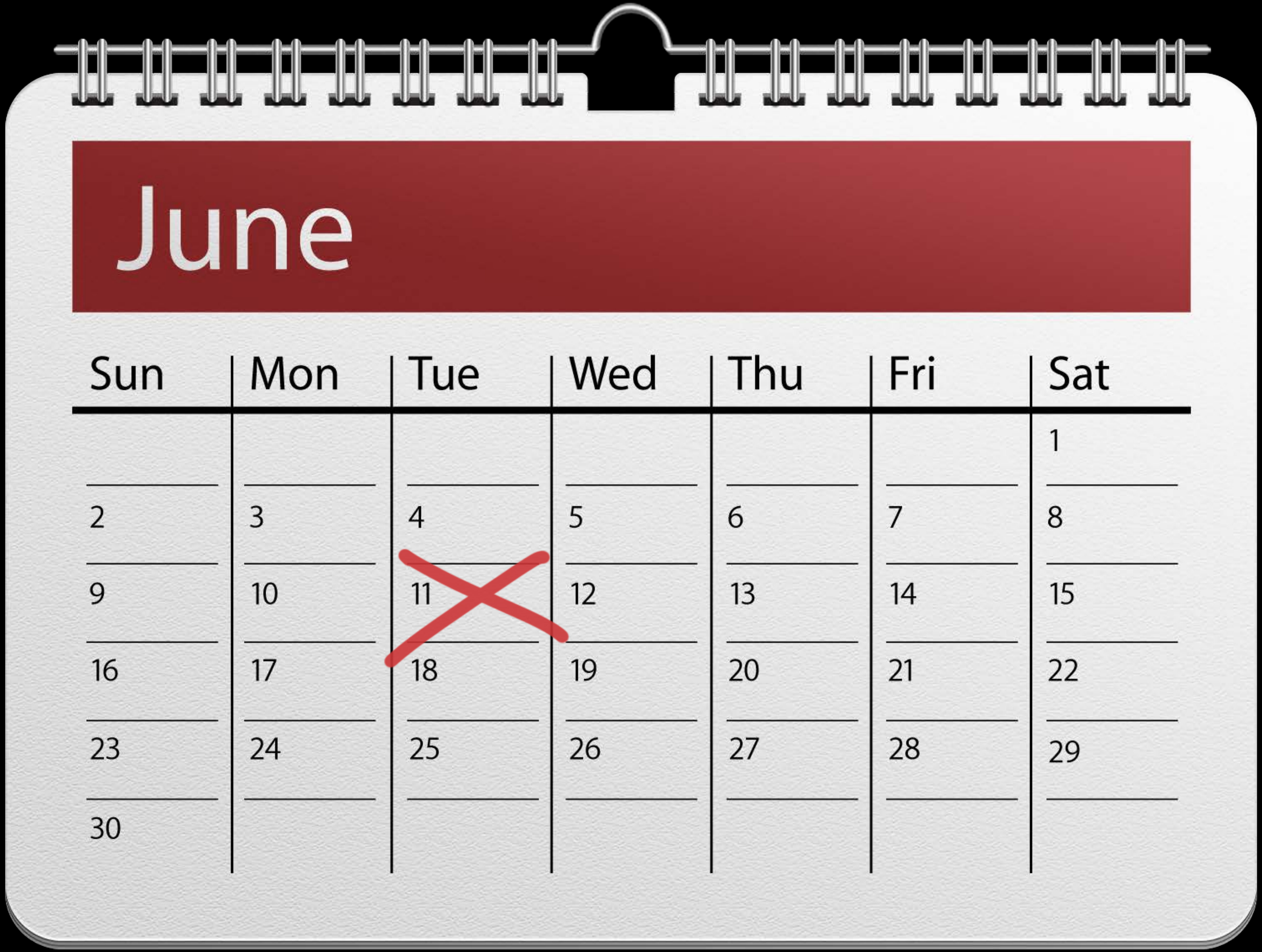
- Enhanced configuration profiles and MDM protocol
- App and book assignments
- Streamlined device enrollments
- Integrate into your MDM products

Schedule

June

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Schedule



June

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Schedule

July

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

More Information

Paul Marcos
App Services Evangelist
pmarcos@apple.com

Documentation
Apple MDM Protocol
https://developer.apple.com/account/ios/certificate/certificateCreate.action

Configuration Profile Reference
https://developer.apple.com/library/ios/#featuredarticles/iPhoneConfigurationProfileRef

Developer Forum
Apple MDM Protocol
http://devforums.apple.com/thread/187061?tstart=0

Related Sessions

Extending Your Apps for Enterprise and Education Use	Nob Hill Tuesday 3:15PM	🟩
What's New in Foundation Networking	Mission Wednesday 9:00AM	🟦
Using Store Kit for In-App Purchases	Mission Thursday 10:15AM	🟩
Using Receipts to Protect Your Digital Sales	Presidio Thursday 2:00PM	🟩

Labs

Managing Apple Devices	Services Lab B Tuesday 12:45PM	🟦
Apps for Enterprise and Education Lab	Services Lab B Tuesday 4:30PM	🟩

WWDC2013