Building Apps for Enterprise and Education

Session 704
Dave Rahardja
iOS Software Engineer

Alexander Botkin
iOS Software Engineer
Enterprise and Education Apps

Solves a problem
Well-designed
A pleasure to use
Enterprise and Education Apps

Solves a problem
Well-designed
A pleasure to use
Some unique requirements
  • Mobile Device Management
  • Supervised
  • Use cases
Enterprise and Education Apps

Solves a problem
Well-designed
A pleasure to use
Some unique requirements
• Mobile Device Management
• Supervised
• Use cases

Watch for tips and tricks
Mobile Device Management
Mobile Device Management
Mobile Device Management

Remote management
Install network access
Install accounts
Install books (New)
Single Sign-on—now with certificates (New)
Install and configure apps
Mobile Device Management

Remote management
Install network access
Install accounts
Install books (New)
Single Sign-on—now with certificates (New)
Install and configure apps

Allow MDM to configure your apps
Managed Apps and Accounts
Managed Apps and Accounts

MDM-installed = “Managed”

• Apps
• Accounts
• Third-party keyboards (New)
• Document Providers (New)
Managed Apps and Accounts

MDM-installed = “Managed”

• Apps
• Accounts
• Third-party keyboards (New)
• Document Providers (New)

User-installed = “Not managed”
Managed Apps and Accounts

MDM-installed = “Managed”
• Apps
• Accounts
• Third-party keyboards (New)
• Document Providers (New)

User-installed = “Not managed”

Restricts data flow
Managed Apps and Accounts

MDM-installed = “Managed”
• Apps
• Accounts
• Third-party keyboards (New)
• Document Providers (New)

User-installed = “Not managed”

Restricts data flow
Per-App VPN
Managed Apps and Accounts

MDM-installed = “Managed”
- Apps
- Accounts
- Third-party keyboards (New)
- Document Providers (New)

User-installed = “Not managed”

Restricts data flow
Per-App VPN

Rely on iOS to manage data flow between apps and accounts
Supervised Devices
Supervised Devices
Supervised Devices

Indicates enterprise ownership (vs BYOD)
Can only be set at activation

• Device Enrollment Program
• Apple Configurator
Supervised Devices
Supervised Devices

Additional restrictions and controls

- Always-On VPN (New)
- Global HTTP proxy
- Third-party content filter (New)
- Single App Mode (MDM-driven and autonomous)
- Prevent Erase All Contents and Settings (New)
- Prevent enabling restrictions (New)
- Many more
Supervised Devices

Additional restrictions and controls

• Always-On VPN (New)
• Global HTTP proxy
• Third-party content filter (New)
• Single App Mode (MDM-driven and autonomous)
• Prevent Erase All Contents and Settings (New)
• Prevent enabling restrictions (New)
• Many more

Supervise your enterprise-owned devices
Three Example Apps

Document Access

Point of Sale

Assessment
App 1—Secure Document Access
CONFIDENTIAL

Strategic Plan 2015

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut vitae fringilla nisi. Nam hendrerit lectus vel libero tincidunt, non lobortis risus congue. Ut odio dolor, cursus tempus lectus ut, accumsan porta turpis. Sed at tristique erat.

Fusce interdum, odio nec mattis feugiat, nisi felis imperdiet erat, at ultrices dolor erat eget massa. Phasellus suscipit, justo et aliquet tempor, diam arcu pretium lorem, ac ullamcorper ipsum risus in. Nunc consectetur imperdiet lorem porta venenatis. Ut commodo euismod felis, pretium consequat tristique augue sit amet adipiscing.


Sed vitae urna ac tortor adipiscing ultricies. Curabitur nibh libero, molestie id suscipit ac, cursus non metus. Integer ornare tortor eget mauris ultricies, eget congue leo gravida. Nunc eu luctus magnis. Ut orci nibh, consequat et purus eu, porttitor malesuada quam.
MDM App Configuration

Special NSUserDefaults key: `@“com.apple.configuration.managed”`

Respond to configuration changes

Define your keys

- URL for document
- Server root certificate
Using Single Sign-on

Use HTTP or HTTPS

Don’t do any user authentication—rely on MDM

Your app may provide alternate authentication
Downloading to Secure File

All files already get `NSFileProtectionCompleteUntilFirstUserAuthentication`
Download to `NSFileProtectionComplete`
Use `NSURLSession` data task
Don’t back up
HTTPS Certificate Pinning

Require HTTPS
Specify trusted root certificates during HTTPS authentication
Prevents man-in-the-middle attacks
Use certificate pinning instead of SSID detection
What We Learned

MDM app configuration
Single Sign-on (do nothing)
Downloading files securely
HTTPS certificate pinning
App 2—Point of Sale
<table>
<thead>
<tr>
<th>Baby Outfits</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Baby Blue</td>
<td>$12.99</td>
</tr>
<tr>
<td>Flower Child</td>
<td>$11.99</td>
</tr>
<tr>
<td>Flower Princess</td>
<td>$11.99</td>
</tr>
<tr>
<td>Little Brother</td>
<td>$9.99</td>
</tr>
<tr>
<td>Little Sister</td>
<td>$9.99</td>
</tr>
<tr>
<td>Thumbs Up</td>
<td>$10.99</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Baby Headbands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Black Bow</td>
<td>$1.99</td>
</tr>
<tr>
<td>Grey Flower</td>
<td>$1.99</td>
</tr>
<tr>
<td>Pink Flower</td>
<td>$2.99</td>
</tr>
</tbody>
</table>
Single App Mode

MDM-controlled
iBeacon

Provide context

Verify device location

Use in conjunction with Core Location

Use iBeacon to verify location-sensitive operation
Network Reachability

Detect if a server is reachable

Use the `SCNetworkReachability` API

Use Network Reachability to provide intelligent offline behavior
Summary

MDM-managed Single App Mode
iBeacon
Network reachability
App 3—Assessment
Final Exam Spring 2014

1. In two two three sentences, please define the following terms:
   - variable
   - class
   - selector
   - object
   - self
   - id
   - category
   - protocol
   - thread

2. Describe what a concurrent dispatch queue is, and how they can be useful.

3. Describe how ARC works, and its advantages and disadvantages compared to manual memory management and garbage collectors.
Document Providers

Allows document exchange between apps
Install an app = add network access
Use `UIDocumentPickerViewController` to access Document Providers
Use Document Providers to get access to enterprise network resources
Autonomous Single App Mode

Put your own app into Single App Mode
Supervised only

Use Autonomous Single App Mode to lock the user to your app
Use Autonomous Single App Mode sparingly
Summary

Document Providers
Autonomous Single App Mode
Summary

Assume MDM will be used to manage your apps and devices
Assume enterprise-owned devices will be supervised
Rely on iOS for system-wide services
  • Single Sign-on
  • VPN and global proxy
  • Managed data flow
  • Single App Mode
  • Document Providers
  • iBeacon, Core Location
Reinvent your enterprise with iOS.

iOS 8 is more advanced than ever for every line of business. Get the latest content from WWDC14 geared to IT and enterprise developers. Learn about key technologies in iOS including how to deploy devices, secure corporate data, and build breakthrough custom apps.
More Information

Paul Danbold
Core OS Technologies Evangelist
danbold@apple.com

Documentation
iOS Developer Program
http://developer.apple.com/enterprise

Apple Developer Forums
http://devforums.apple.com
## Related Sessions

<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Apple Devices</td>
<td>Pacific Heights</td>
<td>Tuesday 9:00AM</td>
</tr>
<tr>
<td>Distributing Enterprise Apps</td>
<td>Pacific Heights</td>
<td>Tuesday 11:30AM</td>
</tr>
<tr>
<td>Building a Document-based App</td>
<td>Marina</td>
<td>Thursday 11:30AM</td>
</tr>
</tbody>
</table>
# Labs

<table>
<thead>
<tr>
<th>Laboratory</th>
<th>Location</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing Apps for Enterprise and Education Lab</td>
<td>Core OS Lab A</td>
<td>Wednesday 2:00PM</td>
</tr>
<tr>
<td>Managing Apple Devices Lab</td>
<td>Core OS Lab B</td>
<td>Thursday 9:00AM</td>
</tr>
</tbody>
</table>