Notarization and your CI system

Philippe Casgrain, BackToMac 2020

Agenda

- Build a Mac application with Developer ID

- Notarization overview in Xcode

- Build script with Developer ID

- Introduction to `altool`

- Notarization on the command-line

- Notarization script

- Tips and tricks

Introducing « Camera On Top »

Camera On Top

Sample Mac application for this presentation

Camera On Top is a tiny Mac application that displays your main FaceTime camera's feed in a resizable window that floats above all other windows.

Notarization overview

Notarization is…

- Suggested in macOS 10.14 Mojave

- Almost mandatory in macOS 10.15 and later

- Applicable to individual apps and disk images (quarantine)

- NOT APP REVIEW

  - Essentially a fancy malware scanner run by Apple

- Automated

- Reliable like code-signing

Build script

Continuous Integration

- Runs scripts using an interpreter

  - Shell like bash or zsh

  - Sometimes Ruby or Python

- Usually runs scripts in sequence

- Halts and reports errors on non-zero exit code

altool

xcrun altool – Validate and Upload apps for the App Store, or Notarize apps for distribution outside of the Mac App Store

`man altool`

notarize.sh

Things to watch out for

- Have a unique build number for each version

- Use an API key

  - `https://appstoreconnect.apple.com/access/api`

  - Store passwords in keychain if you must

- Always log progress and errors

- Hardened runtime

  - Exceptions exist for most cases