App Notaris/zation, macOS, and You

Ben Goodstein
Technical Leader (Apple)
EDMS Team
IT Services

App what now?

Have (the signature on a document) attested to by a notary.

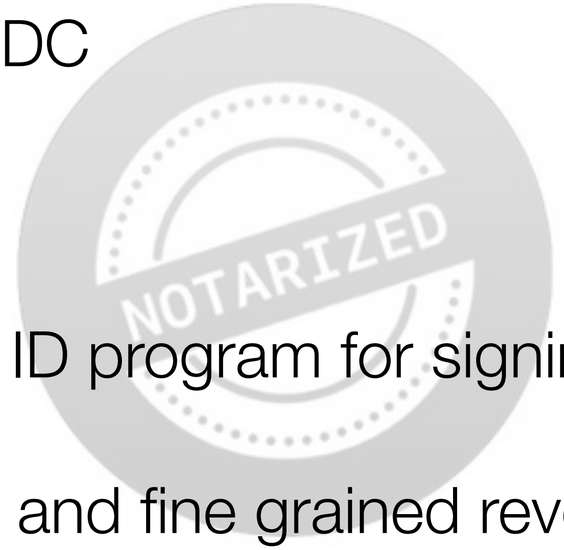
Oxford Dictionaries - notarize (verb)

A person authorized to perform certain legal formalities, especially to draw up or certify contracts, deeds, and other documents for use in other jurisdictions.

Oxford Dictionaries - notary (noun)

Apple App Notarization

- Introduced last year at WWDC
- Available in Xcode 10.1+
- Extension to the Developer ID program for signing apps
- Allows blocking of malware and fine grained revocation of apps

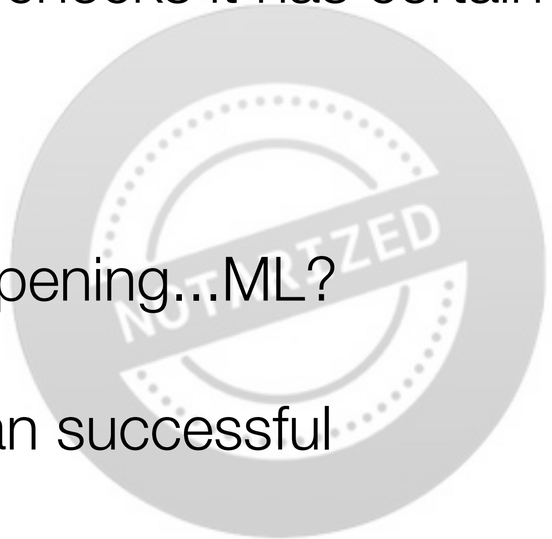


Why Notarize?

- Apps/kexts outside of App Store
- Codesigning only implies:
  - Was signed with a trusted certificate (that is not hard to obtain)
  - Has not been tampered with
  - Is not known to be malware (but it could be)

How do you notarize an app?

- App (or zip, pkg or disk image) is sent to Apple
- Apple scans it for malware & checks it has certain capabilities restricted
  - NOT App Review
  - Other things might be happening...ML?
- Apple creates a "ticket" if scan successful
- Returns this to the signer who "staples" it to the app
- Publishes the ticket so it can be checked



Who checks the ticket?

Gatekeeper

- Front end to `spctl`
- Assesses whether apps pass security policy
- All apps downloaded via a browser are "quarantined" until assessed
- By default only allows App Store/codesigned apps

Gatekeeper

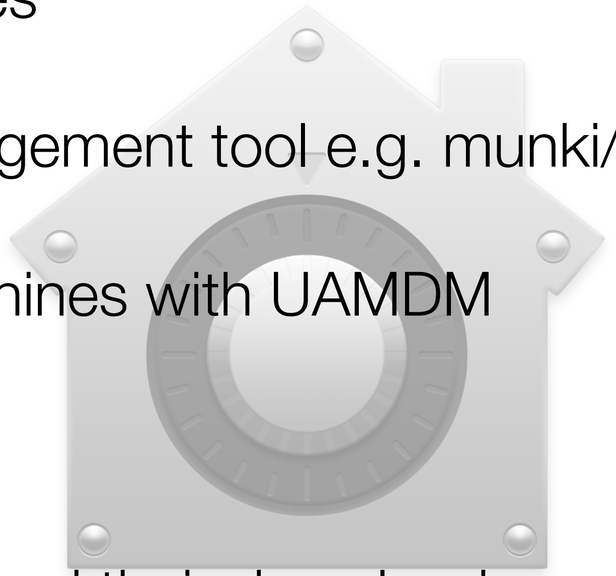
- Is being expanded to check app notarization
- Will allow for single version of app to be blacklisted
- 10.14 - Notarized apps display a line after assessment
- 10.14.5 - New or updated kexts (after March 11th 2019) must be notarized to run
- 10.14.5 - Apps signed by new developers must be notarized to run
- The future: 10.15? - only notarized apps will run?

10.14.5

Is out now!

Gatekeeper

- Won't affect:
  - Existing apps on machines
  - Apps installed by a management tool e.g. munki/Jamf
  - Kexts whitelisted on machines with UAMDM
- Will affect:
  - Self managed machines and their downloads
  - Will be down to software developer



References

- https://developer.apple.com/documentation/security/notarizing_your_app_before_distribution
- https://eclecticlight.co/2019/04/10/macs-move-closer-to-compulsory-notarization/
- https://www.theregister.co.uk/2019/03/20/macos_clampdown_rumors/