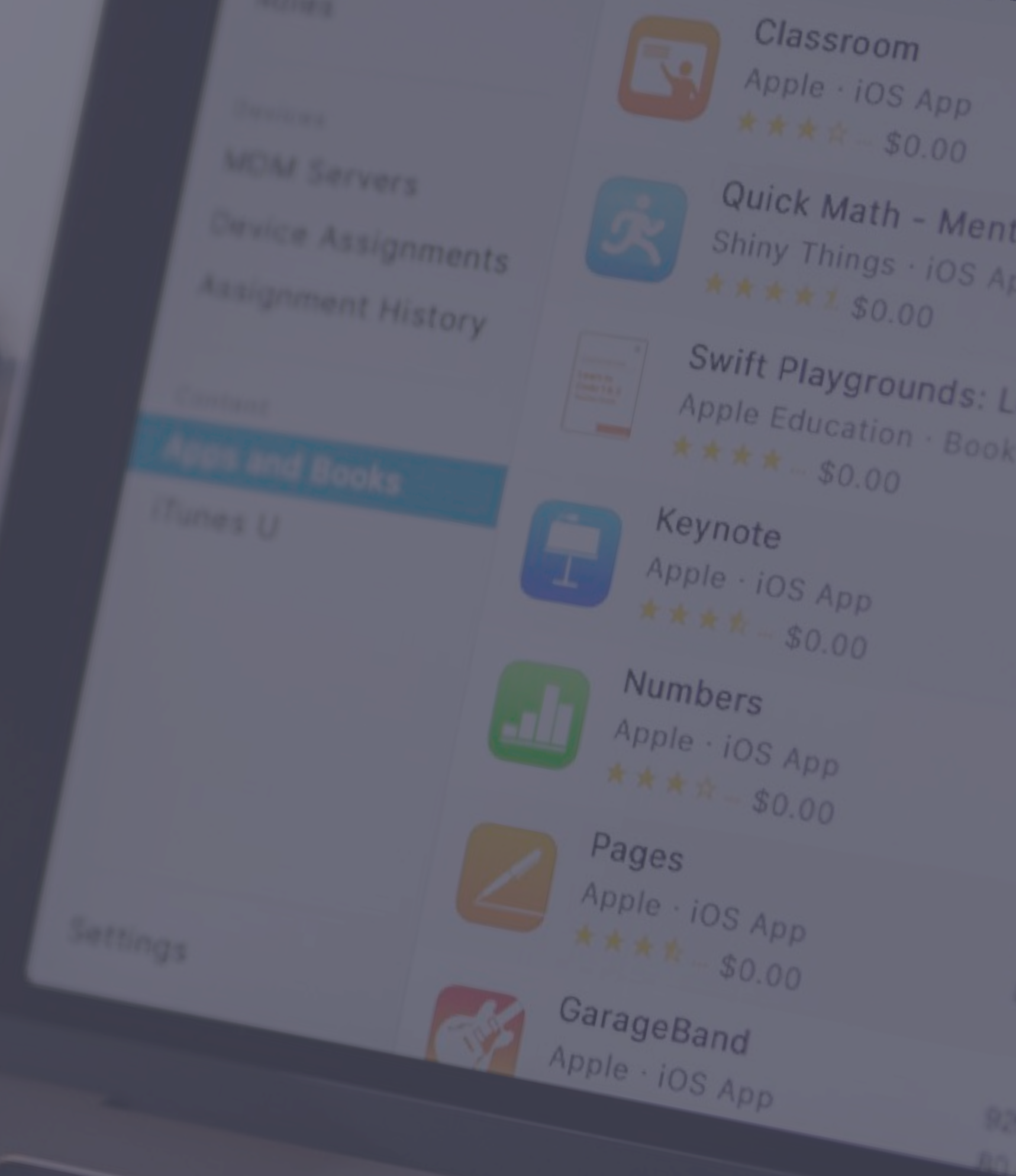


dataJAR Ltd.
Apple Device Management Specialists

Notorization



Overview of Gatekeeper

Apple Introduces Notarization

Xcode Workflow

Non Xcode Workflow

Checking for Notarization

Other Resources



Gatekeeper

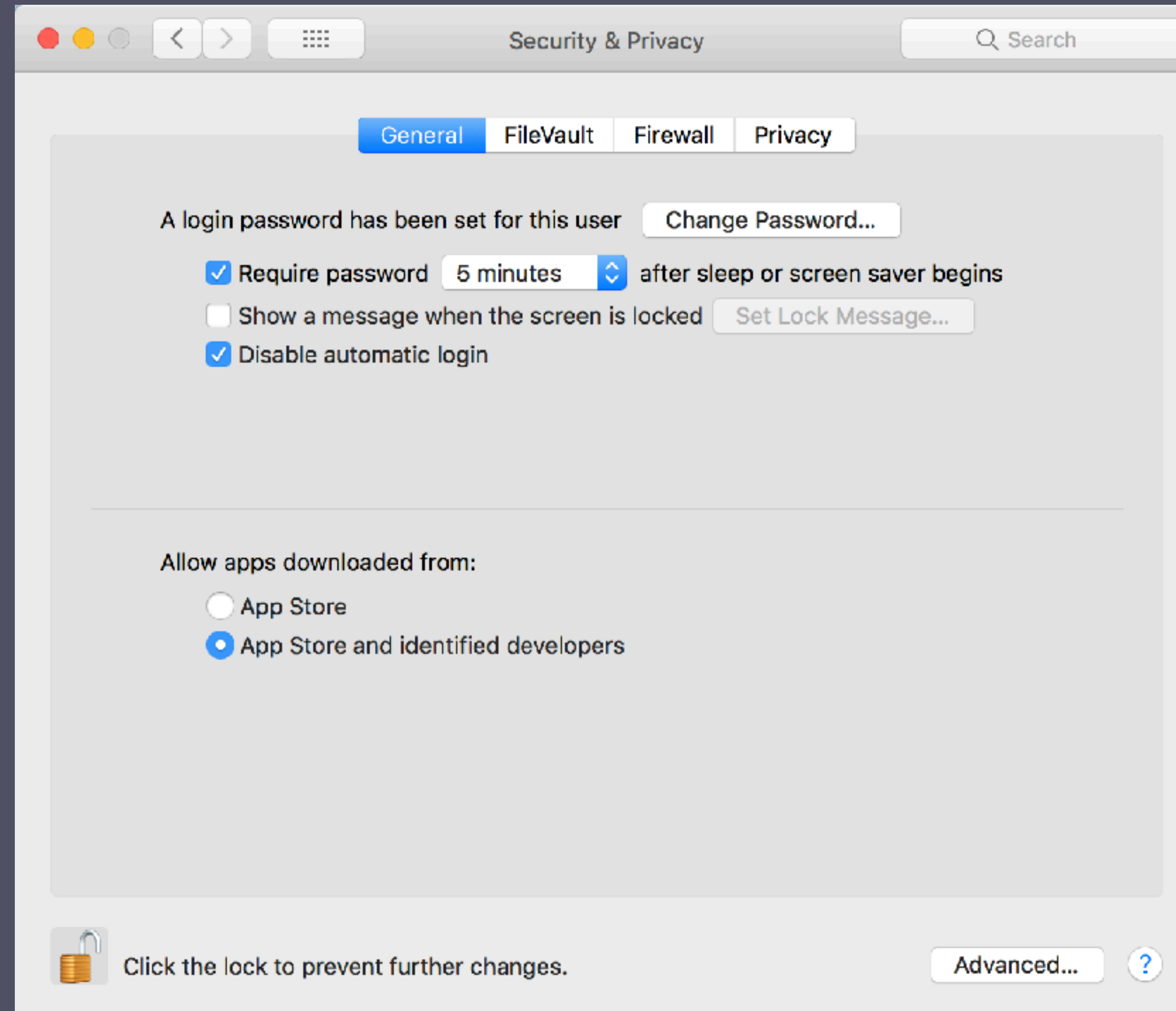


Introduced in macOS 10.7.3

Added to the GUI in macOS 10.7.5

Used to enforce code signing

Verifies downloaded applications before they are run





Relies on the Extended File Quarantine attribute

`com.apple.quarantine`

Extended File Attribute added when
downloaded from the Internet

Safari, Mail, Messages etc



View Quarantine Attribute

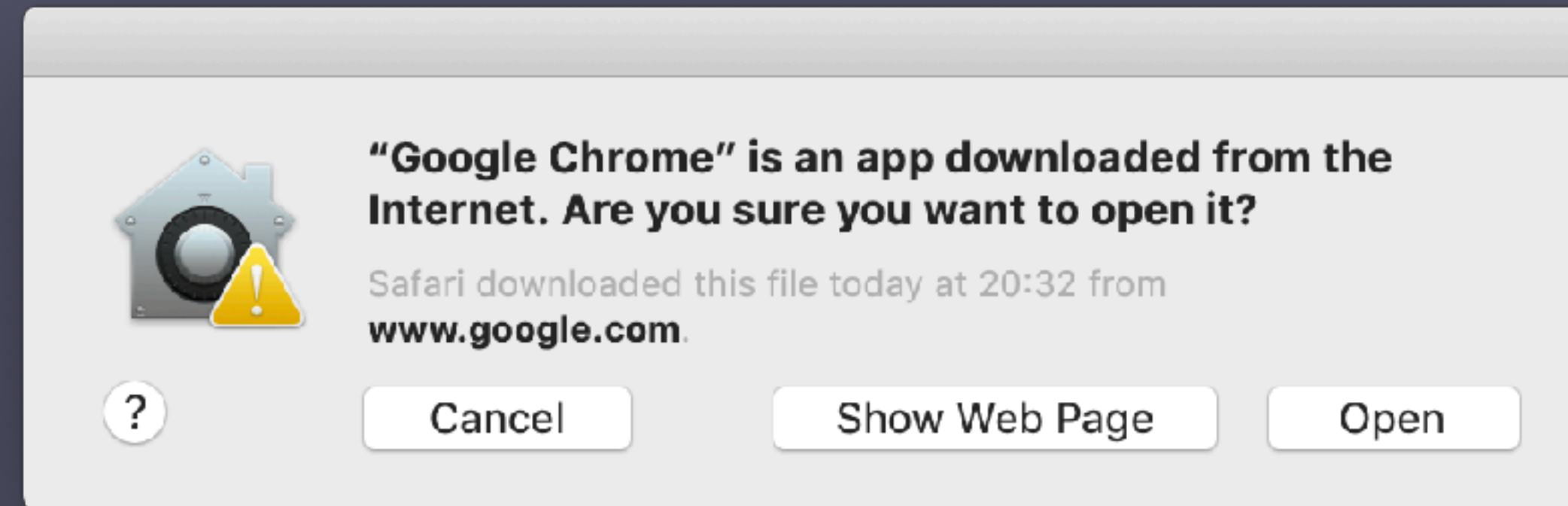
```
xattr Google\ Chrome.app/  
com.apple.quarantine
```

Remove Quarantine Attribute

```
xattr -r -d com.apple.quarantine Google\ Chrome.app/
```


Quarantine Attribute set

Valid Developer ID



Quarantine Attribute set

No Developer ID



"Pirate" can't be opened because it is from an unidentified developer.

Your security preferences allow installation of only apps from the App Store and identified developers.

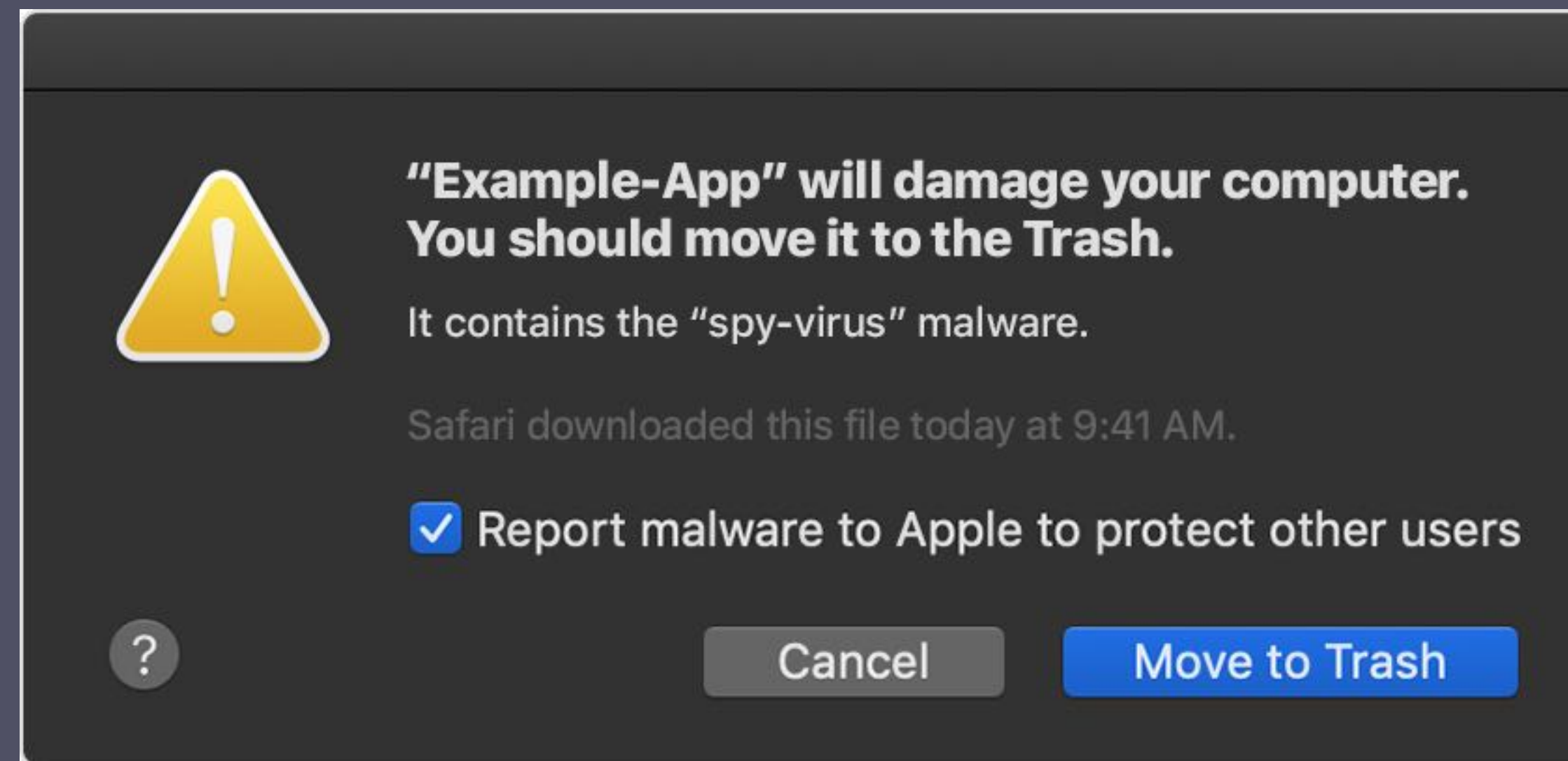
xattred.app downloaded this file today at 20:48 from **example.com**.



OK

Quarantine Attribute set

App modified or malicious content found





spctl

Manages the security assessment policy subsystem

```
spctl --status
```

```
spctl --master-enable
```

```
spctl --master-disable
```



```
spctl --add /path/to/app
```

```
spctl --remove /path/to/app
```

```
spctl --assess /path/to/app
```




Notorization



Announced at WWDC 2018

A new layer of verification on top of Gatekeeper

Identify and block malicious software before distribution



Optional for Developers until:

macOS 10.14.5: New or updated Kernel Extensions or new developers as of April 7th 2019

macOS 10.15: All software must be notarized from June 1st 2019



Identify and block malicious software before distribution

Checks for code-signing issues

Part of the Developer program

Notary service performs automated security checks - Not an APP Review



Before distribution developer submits app to Notary service

If no issues the notary service generates a ticket that is stapled to the app

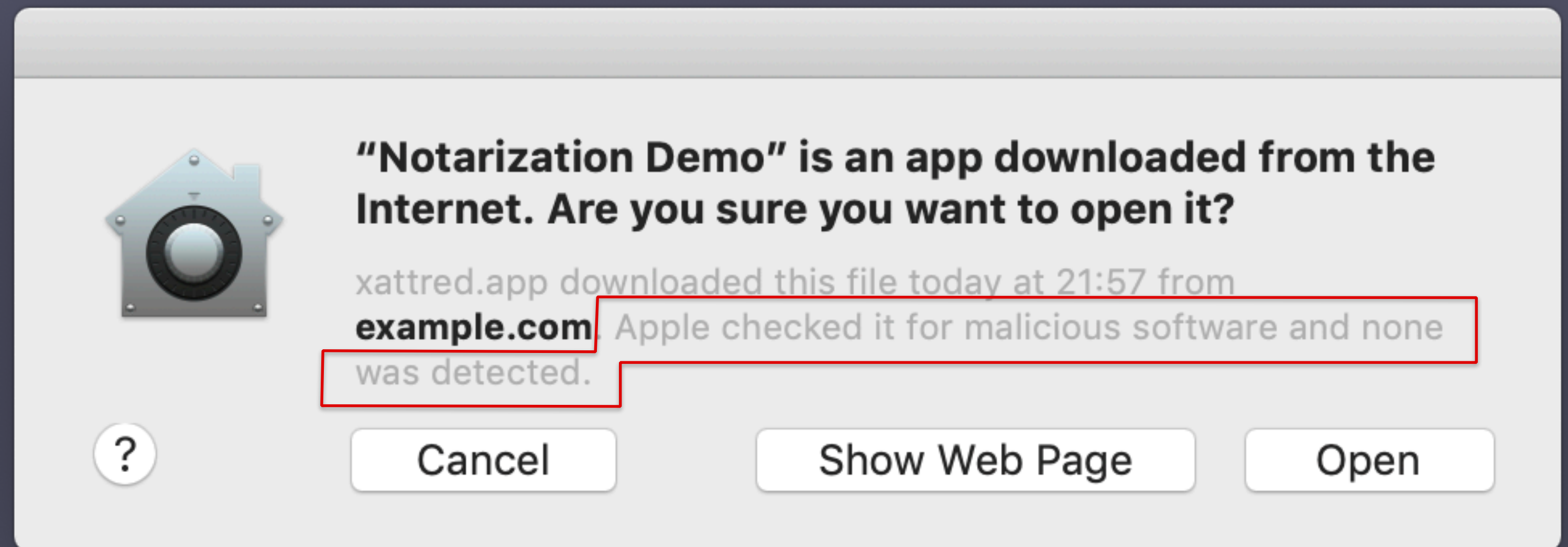
Also publishes the ticket online where Gatekeeper can find it.

Very quick turn around time



The presence of a ticket either online or attached to the app tells Gatekeeper the app has been notarised

Modified Gatekeeper dialogue





The following can be notarised

macOS Apps

Kernel Extensions

Disk Images

Flat Installer Packages

Content of Zip Archives



Benefits

Helps developer stop shipping malicious code

Hardened Runtime is more secure by default

Users can trust these apps more

Audit trail of software notarised by the developer



Correct Signing



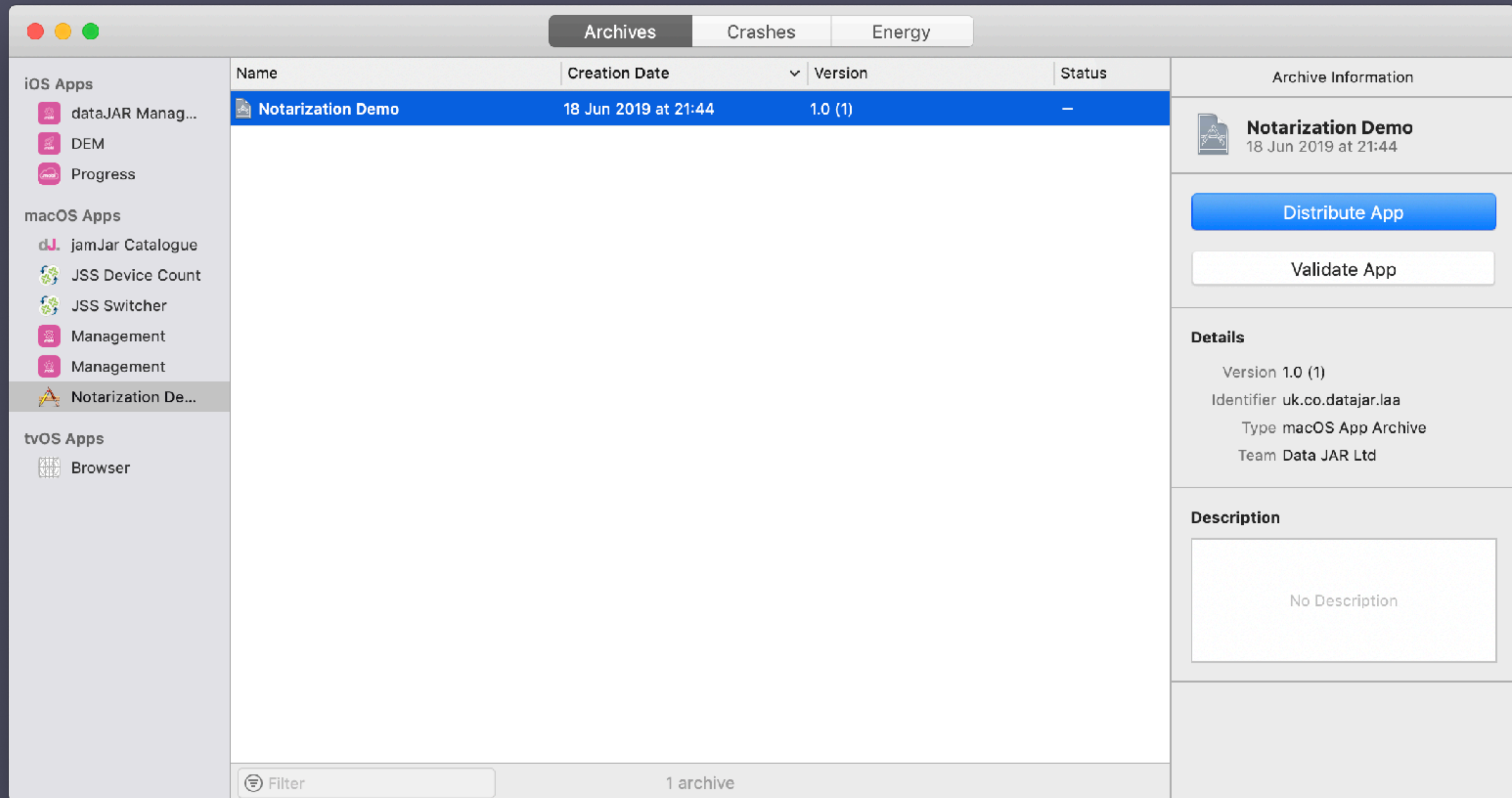
App Bundles - Developer ID Application Certificate

Installer Packages - Developer ID Installer Certificate

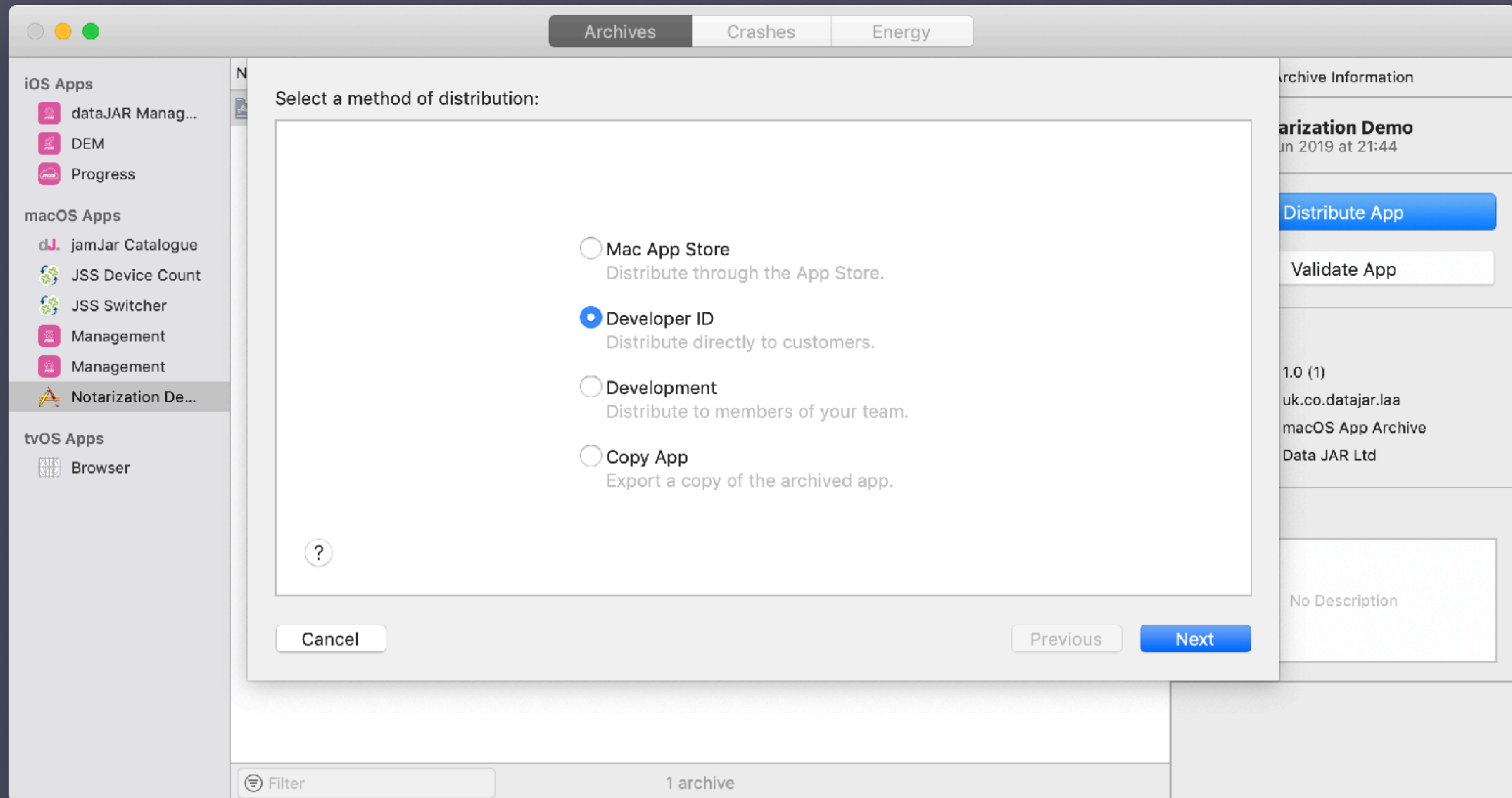
Disk Images - Developer ID Application Certificate



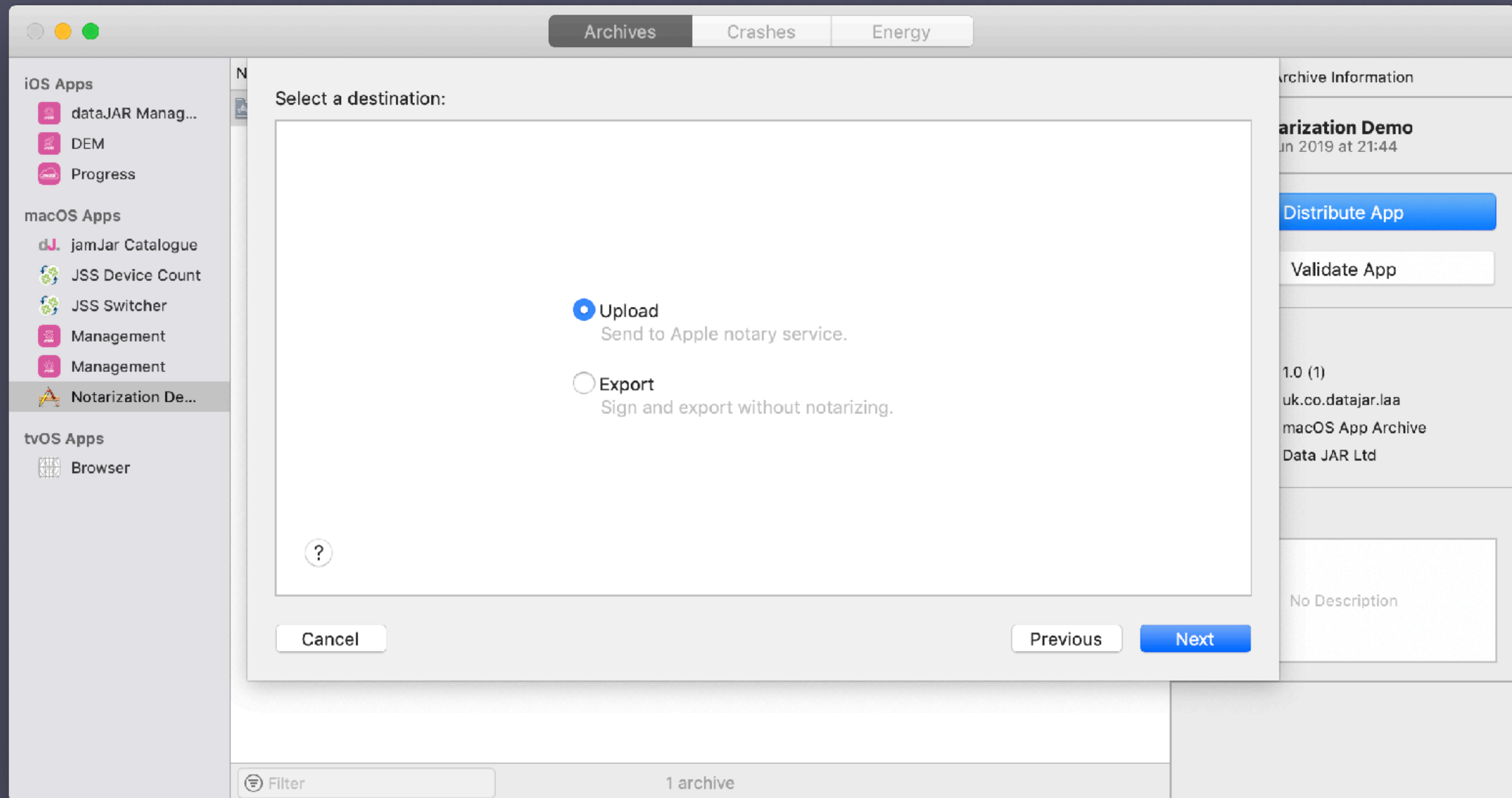
Xcode Workflow



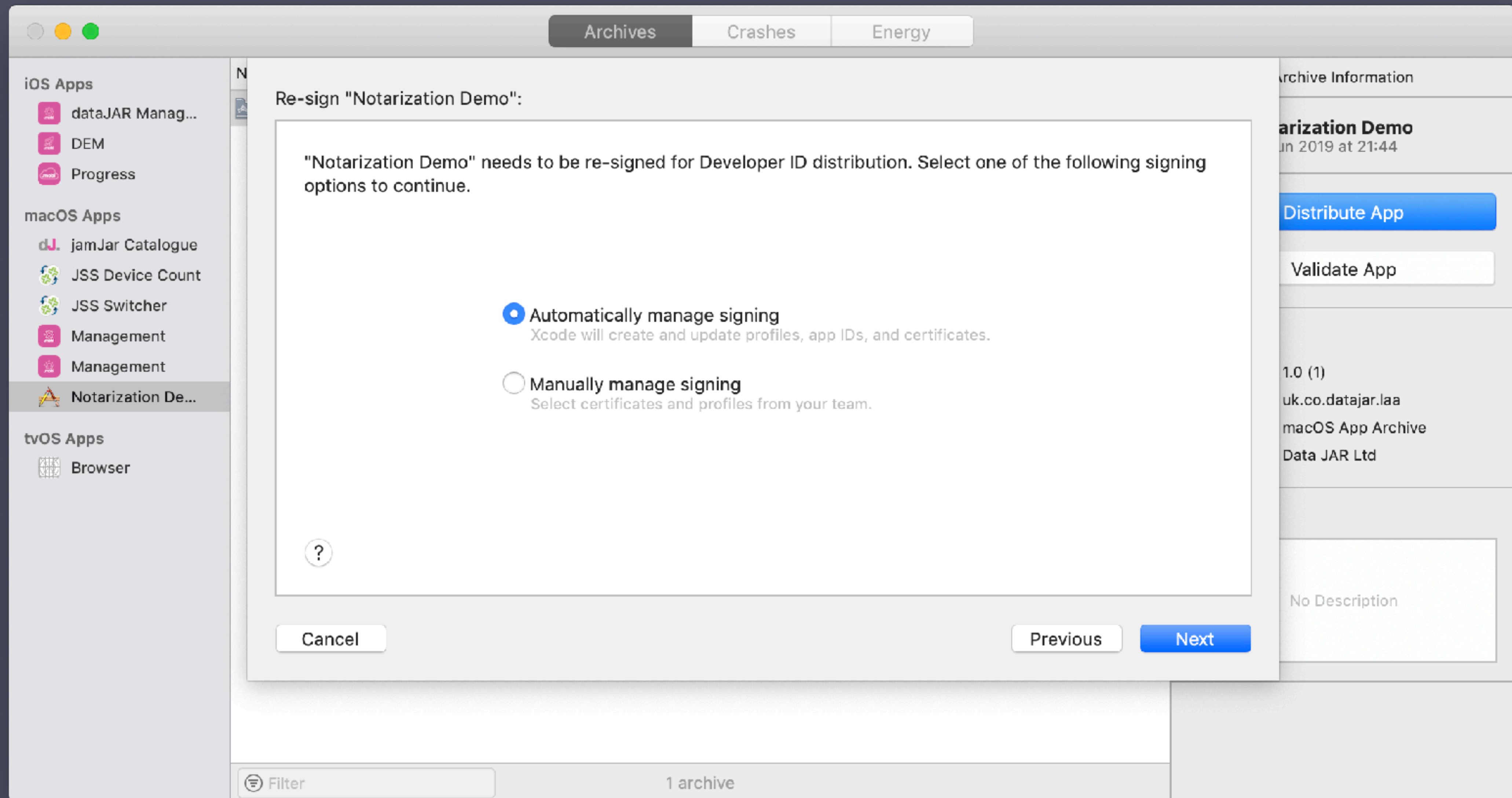
Archive Workflow



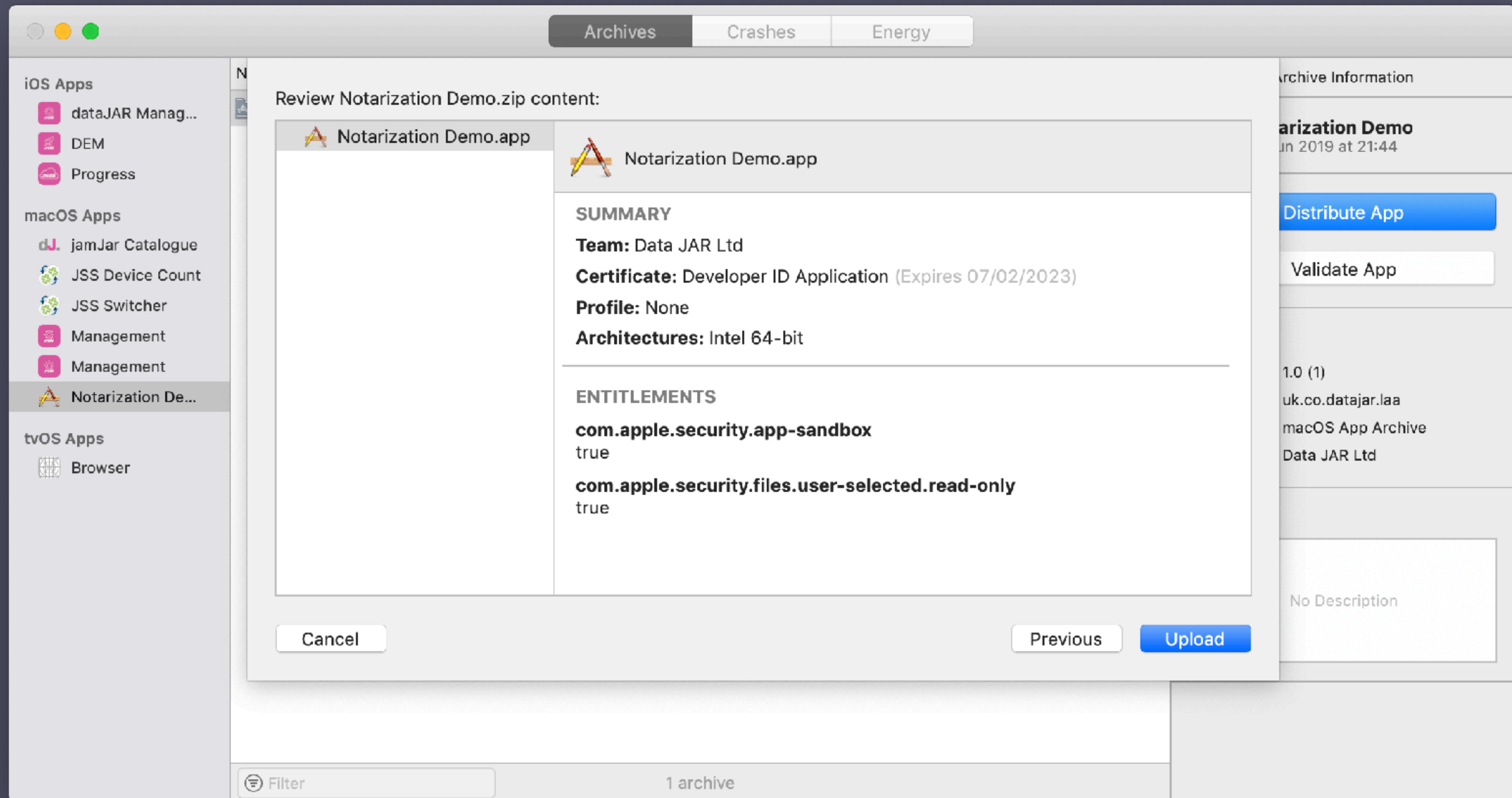
Distribute using your Developer ID



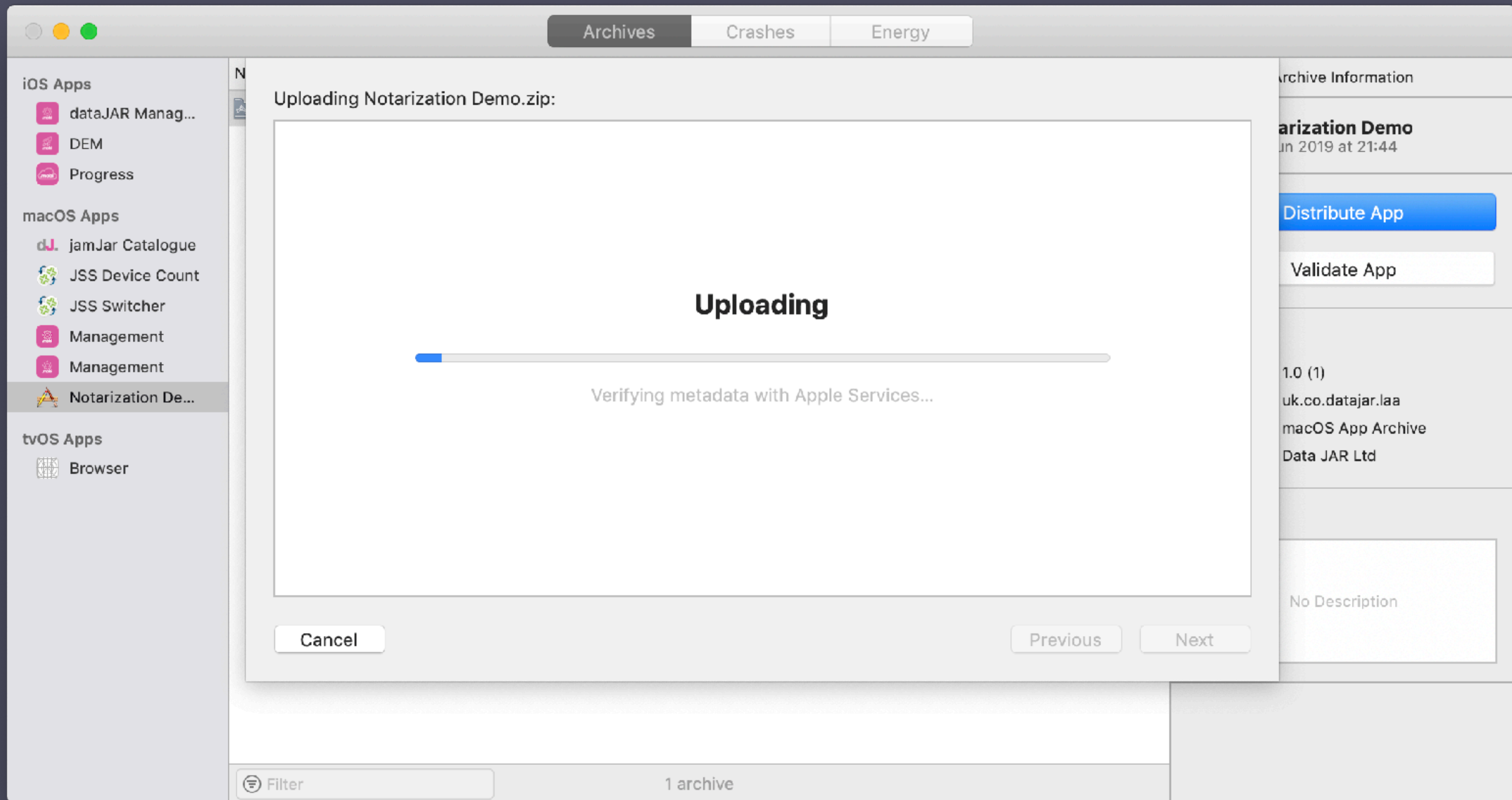
Upload to the Notary Service



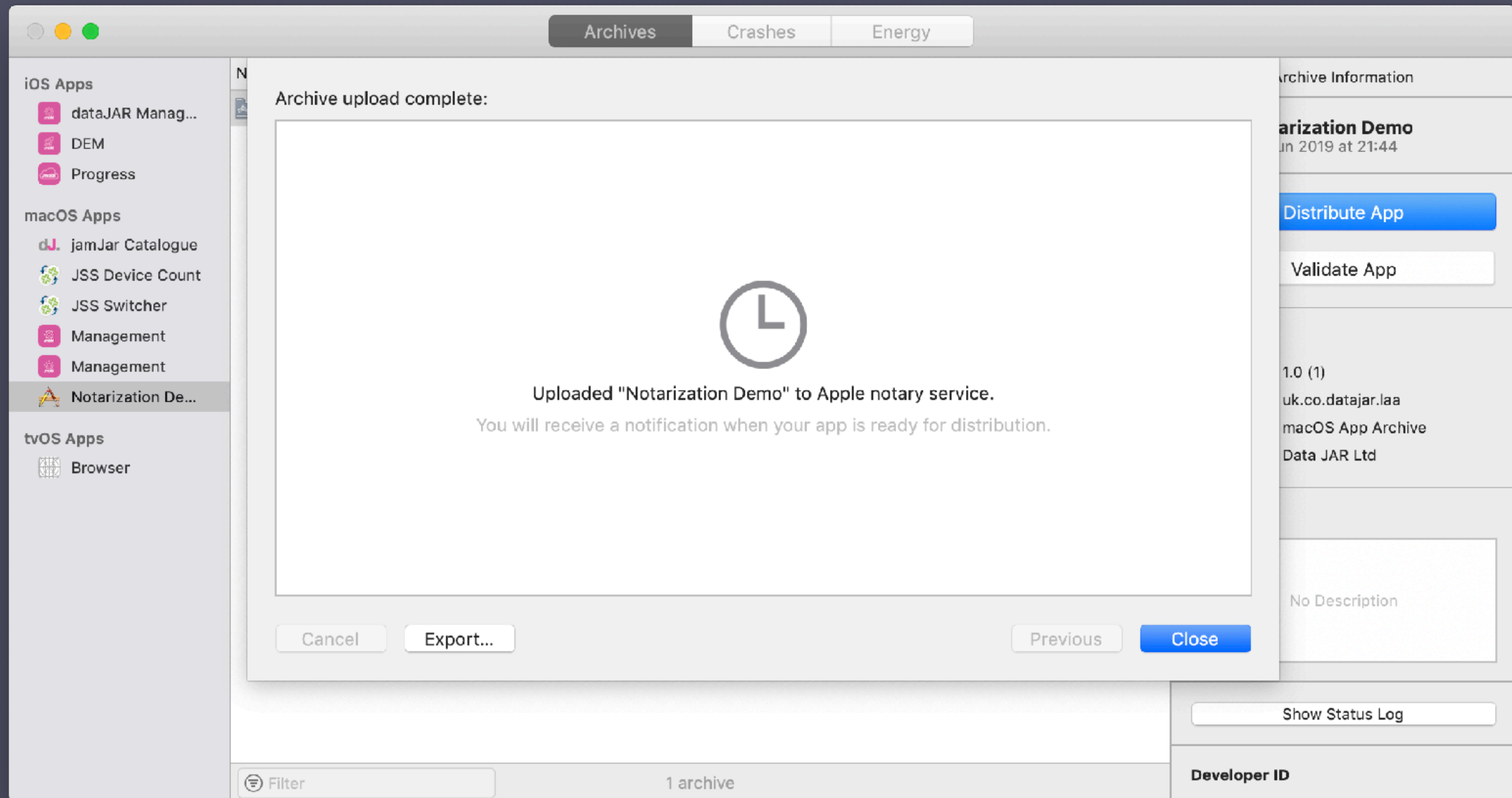
Sign the App with your Developer ID



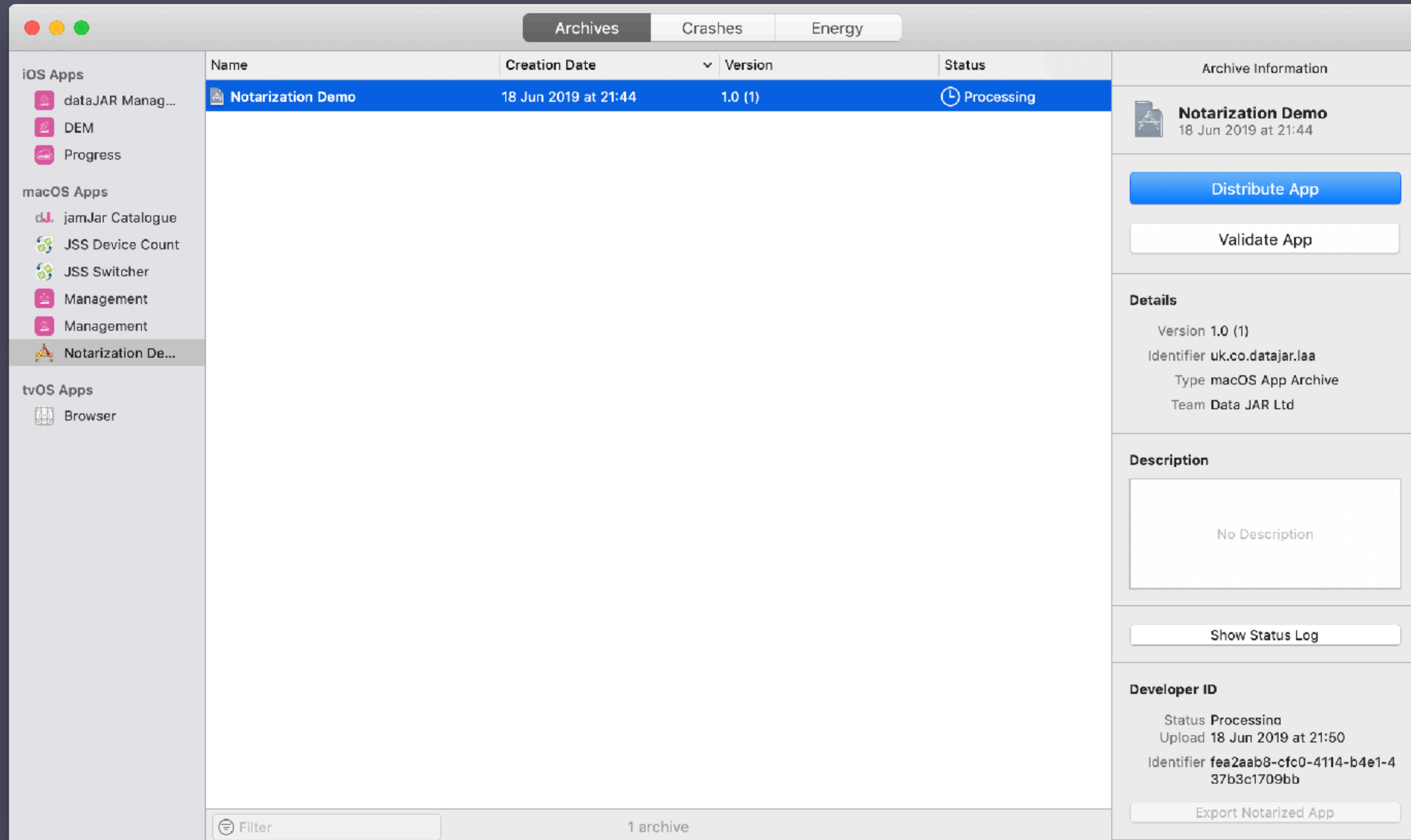
Upload the Signed App to Apple



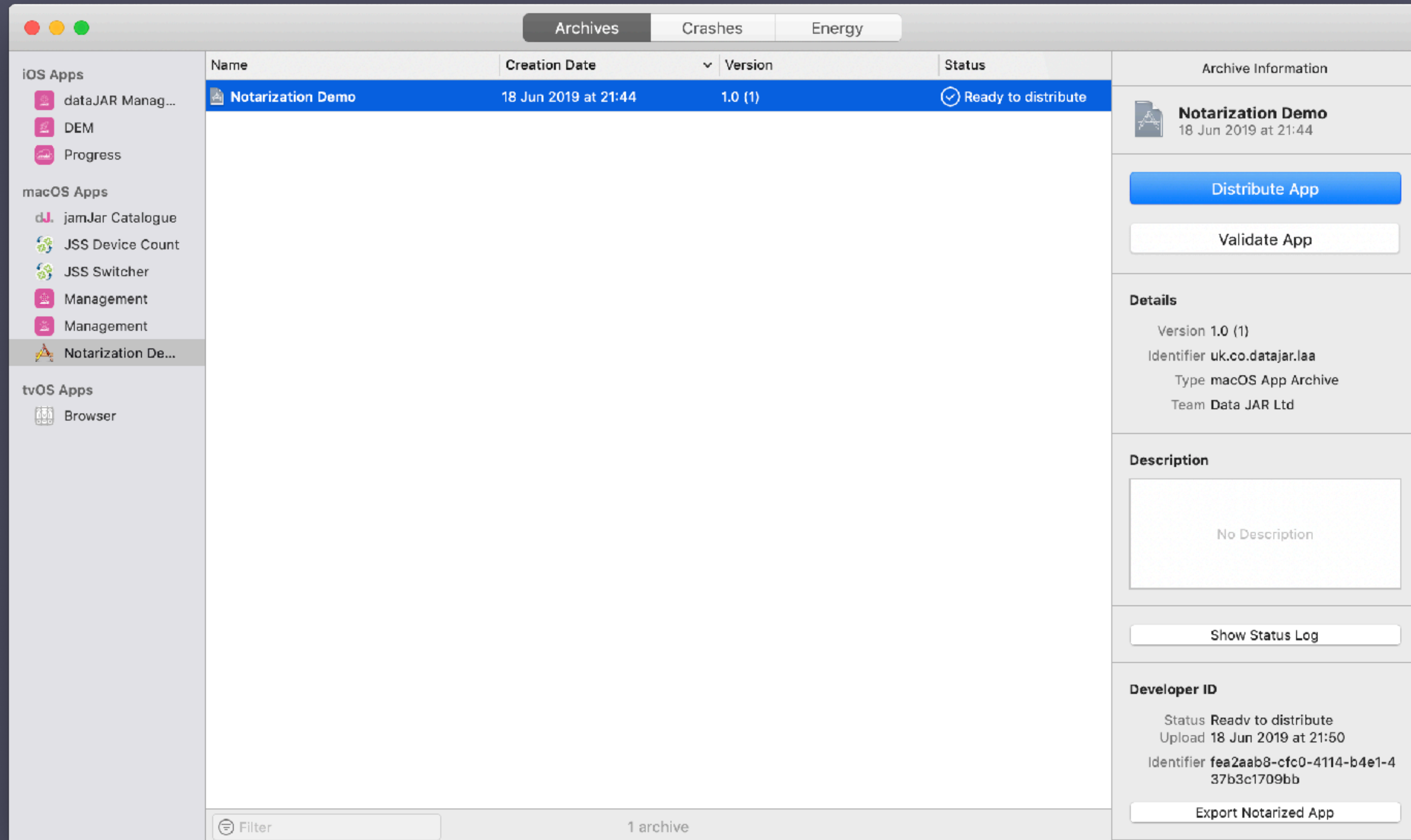
Uploading.....



Upload Complete



Notary Service processing App



Notary Service passes App, ready for distribution

Apple Developer

You can now distribute your Mac software.

To: Richard Mallion

Inbox - Google 21:52

AD



Dear Richard,

Your Mac software has been notarized. You can now export this software and distribute it directly to users.

Bundle Identifier: uk.co.datajar.laa

Request Identifier: fea2aab8-cfc0-4114-b4e1-437b3c1709bb

For details on exporting a notarized app, visit [Xcode Help](#) or the [notarization guide](#).

Best Regards,
Apple Developer Relations

TM and © 2018 Apple Inc.
One Apple Park Way, MS 301-1TEV, Cupertino, CA 95014.

[All Rights Reserved](#) | [Privacy Policy](#) | [Account](#)

Email, push notifications update



Custom Workflow



```
sudo xcode-select -s /Applications/Xcode.app
```

Select your version of Xcode 10+



```
xcrun altool --notarize-app  
--primary-bundle-id "uk.co.datajar.xxx"  
--file "somesoftware.pkg"  
--username "USERNAME"  
--password "@keychain:ITEM_NAME"
```

Result:

```
altool[16765:378423] No errors uploading 'somesoftware.pkg'.  
RequestUUID = 2EFE2717-52EF-43A5-96DC-0797E4CA1041
```

Submit your software



```
xcrun altool --notarization-info 2EFE2717-52EF-43A5-96DC-0797E4CA1041  
--username "USERNAME" --password "@keychain:ITEM_NAME"
```

Status: success

LogFileURL: <https://osxapps-ssl.itunes.apple.com/...>

Status Code: 0

Status Message: Package Approved

Check Status



```
xcrun stapler staple <path-to-item>
```

For zips, unzip, staple content, re-zip

Cannot staple command lines tools

Staple Ticket



```
xcrun stapler validate <path-to-item>
```

Validate



Checking for Notarization



```
spctl --assess --verbose /path/to/app
```

```
source=Notarized Developer ID
```

```
source=Developer ID
```

```
Pirate.app/: rejected
```

Checking Applications



```
spctl --assess --verbose --type install /path/to/package
```

Checking Packages



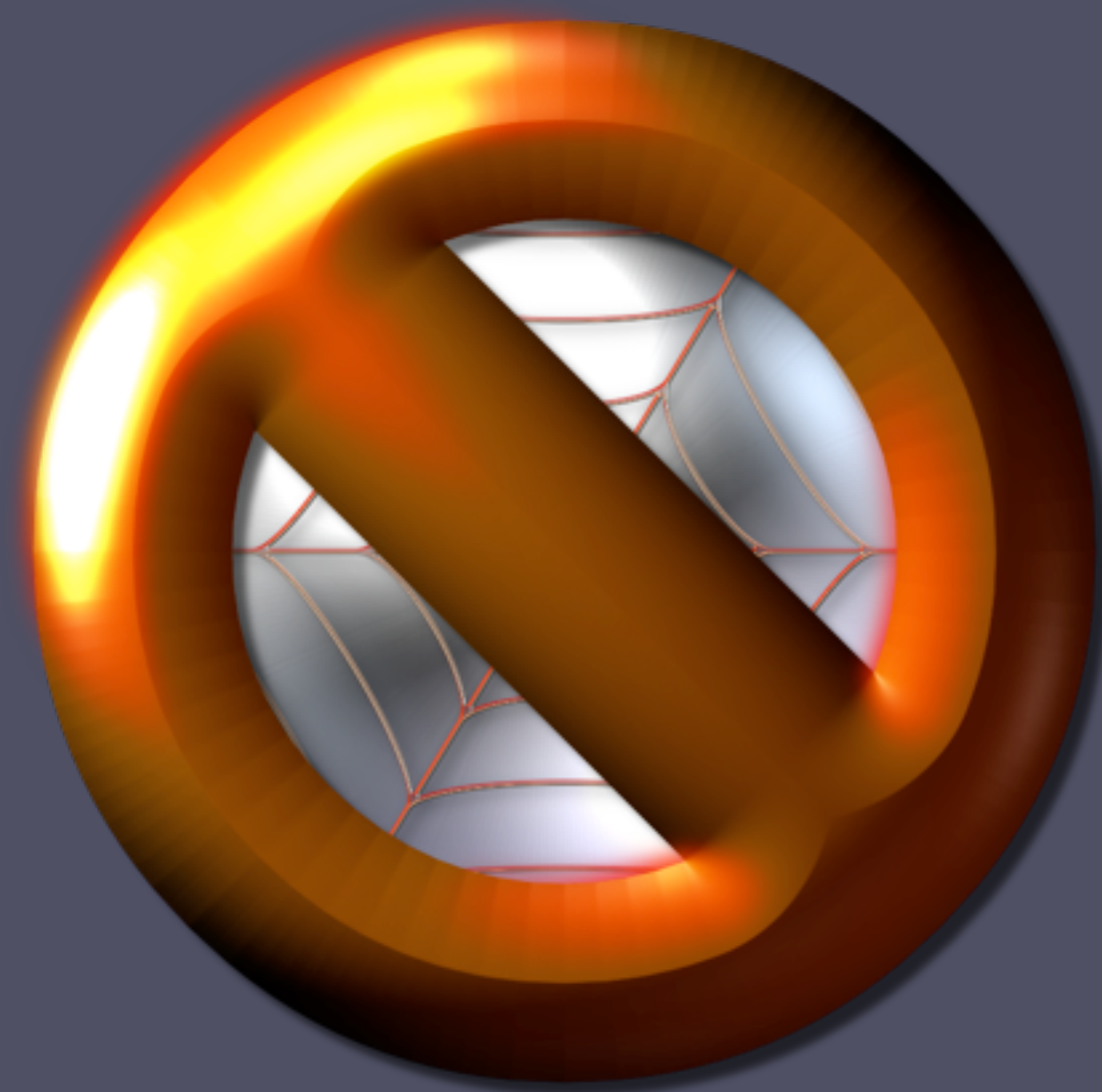
```
spctl --assess --verbose --type open --context  
"context:primary-signature" /path/to/dmg
```

Checking Disk Images



```
codesign --verify --verbose  
--test-requirement="notarized" /path/to/binary
```

Other Binaries



Taccy

Notarization Demo

App ID Version

☐ Apple ☐ App Store ☒ Notarized ☐ Developer ID

SDK ☒ Mojave ☐ High Sierra ☐ Apple

Usage ☐ Calendars ☐ Contacts ☐ Reminders
☐ Photos ☐ System admin ☐ AppleEvents
☐ Camera ☐ Microphone ☐ Location

Public ☐ Calendars ☐ Contacts ☐ Reminders
☐ Photos ☐ AppleEvents
☐ Camera ☐ Microphone ☐ Location

Private ☐ Calendars ☐ Contacts ☐ Reminders
☐ Photos
☐ Camera ☐ Microphone ☐ Liverpool

App path: /Users/richard/Documents/Notorisation/Demo App/Notarized Version/Notarization Demo.app
app ID: uk.co.datajar.laa
version: 1.0
SDK version: macosx10.14
Location use: []
Calendars use: []
Contacts use: []
Reminders use: []
Photos library use: []
Sysadmin use: []
AppleEvents use: []
Camera use: []
Microphone use: []

Entitlements:
com.apple.security.app-sandbox : 1
com.apple.security.files.user-selected.read-only : 1

App signature check:
/Users/richard/Documents/Notorisation/Demo App/Notarized Version/Notarization Demo.app: accepted
source=Notarized Developer ID

<https://eclecticlight.co>



```
xcrun altool --notarization-history -u "USERNAME"  
-p "@keychain:ITEM_NAME"
```

Notary Service History



Other Resources

WWDC 2019 - All About Notarization

https://developer.apple.com/documentation/security/notarizing_your_app_before_distribution

<https://eclecticlight.co>

<https://derflounder.wordpress.com/2019/04/10/notarizing-automator-applications/>



Questions

dataJAR Ltd.
Apple Device Management Specialists

