



**dataJARltd.**

Apple Device Management Specialists

---

# Notorization

# Overview of Gatekeeper

Apple Introduces Notarization

Xcode Workflow

Non Xcode Workflow

Checking for Notarization

Other Resources



# Gatekeeper

---

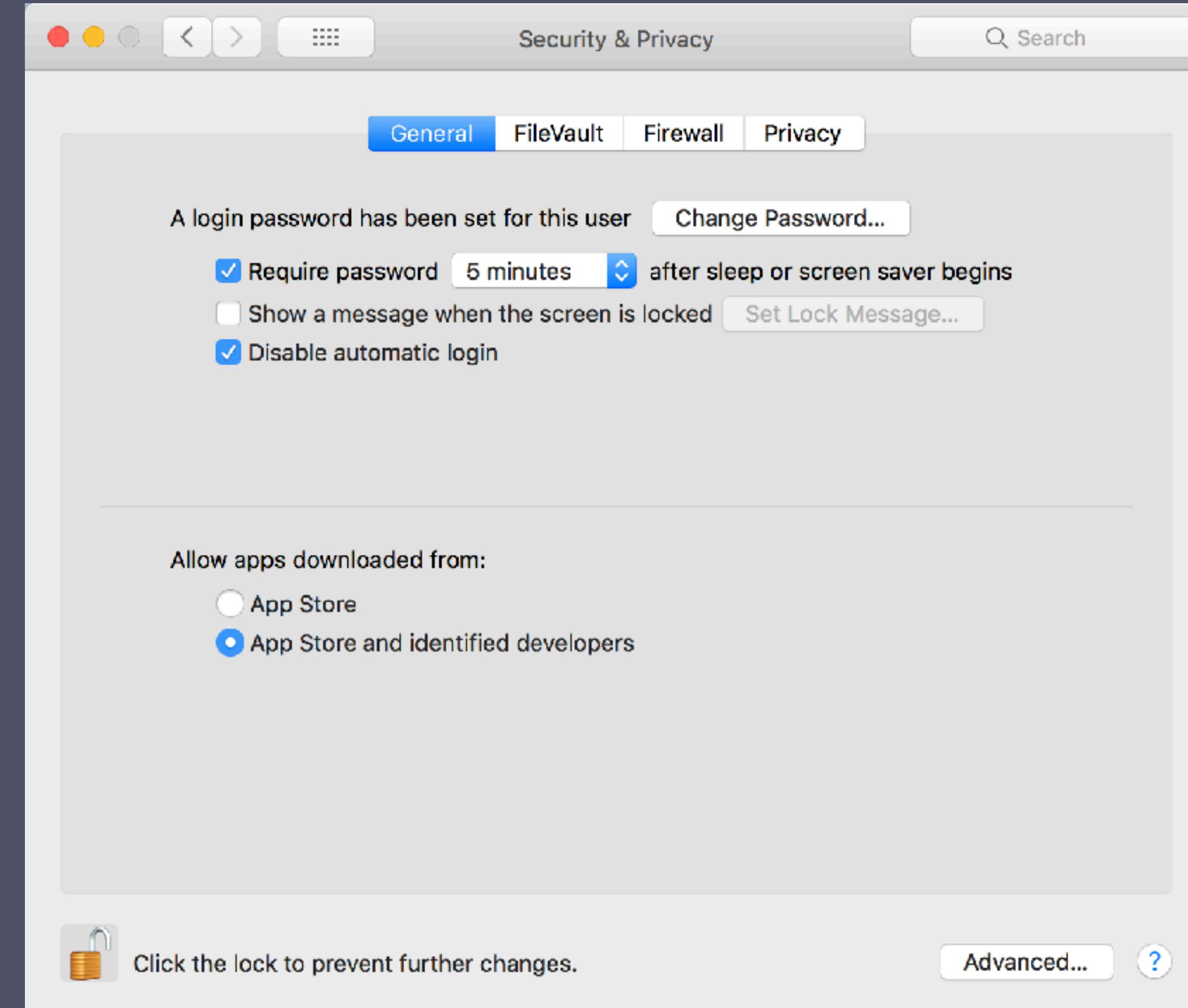


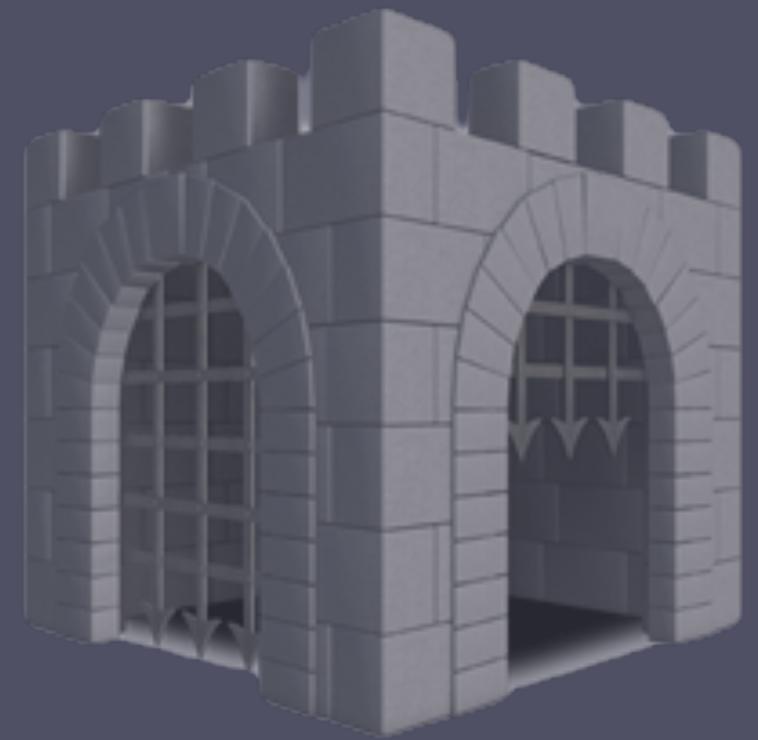
Introduced in macOS 10.7.3

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

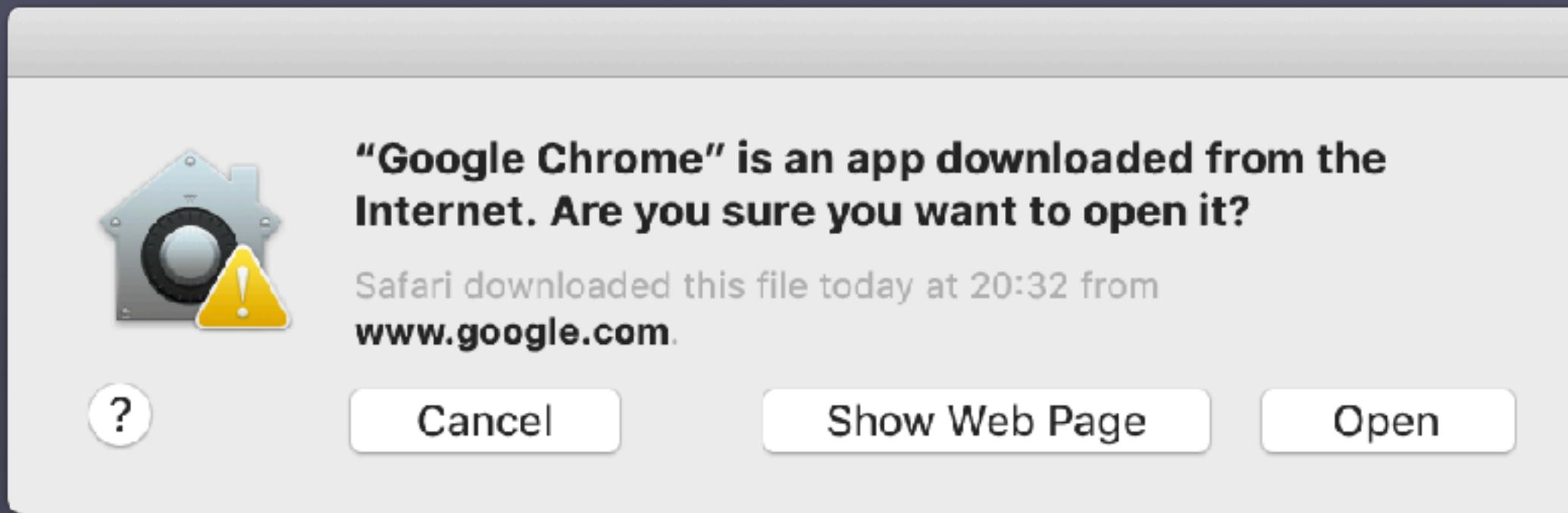
```
xattr Google\ Chrome.app/  
com.apple.quarantine
```

## Remove Quarantine Attribute

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

## Quarantine Attribute set

Valid Developer ID



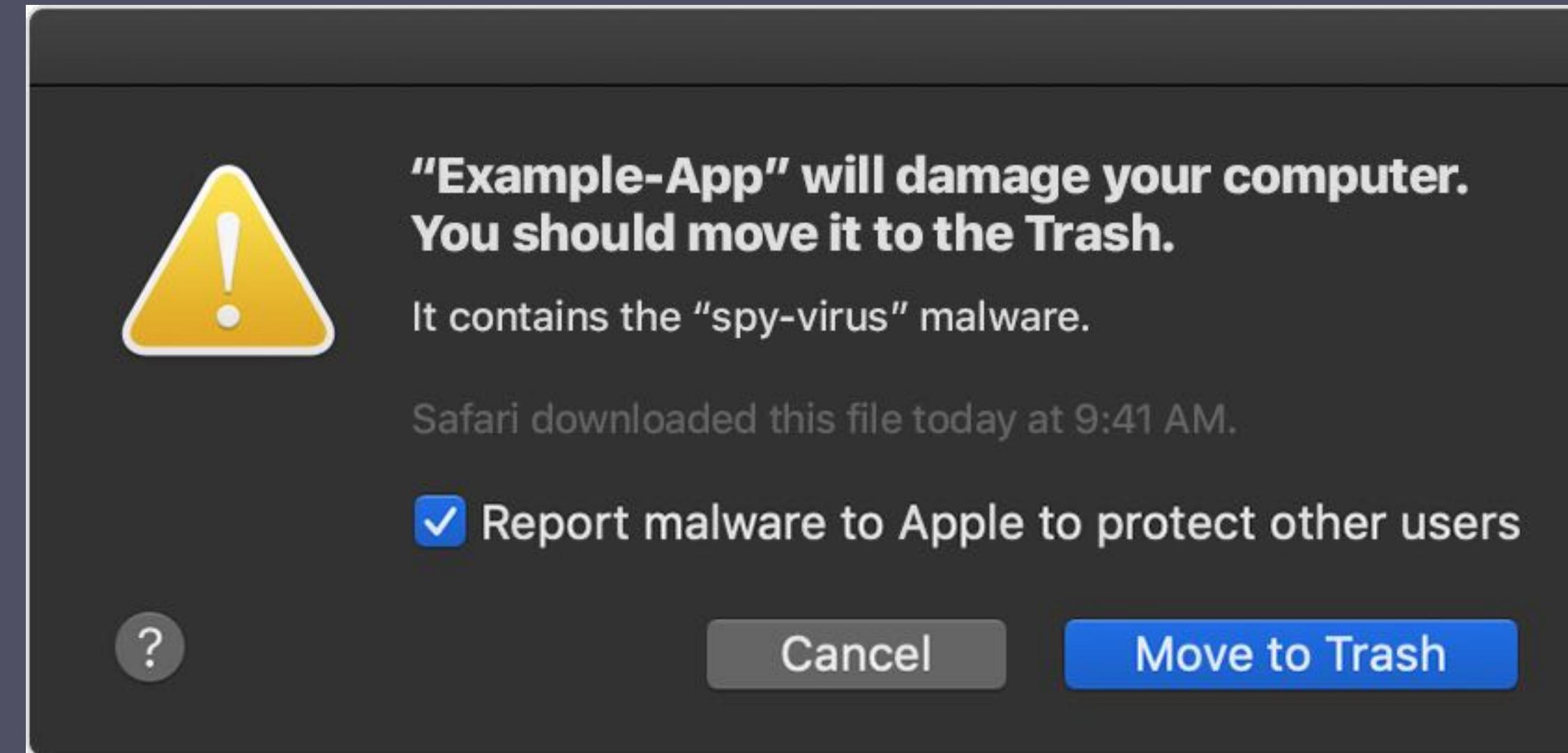
# Quarantine Attribute set

No Developer ID



## 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

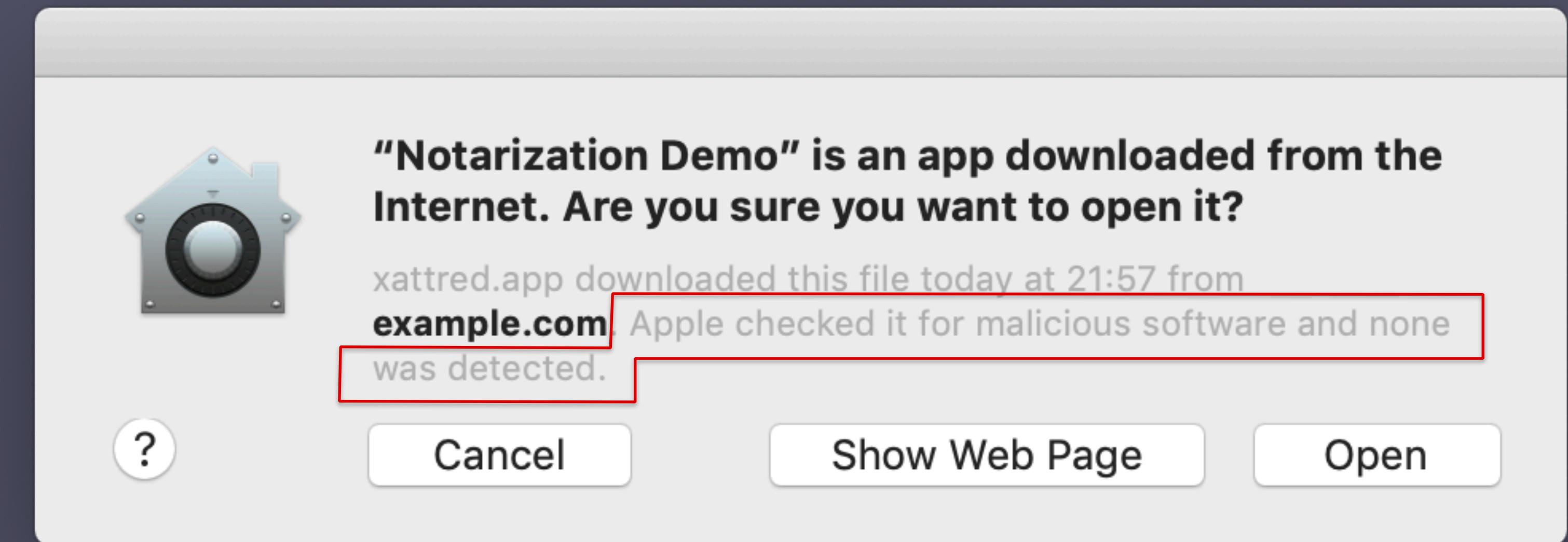
Also publishes the ticket online where  
Gatekeeper can find it.

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

---

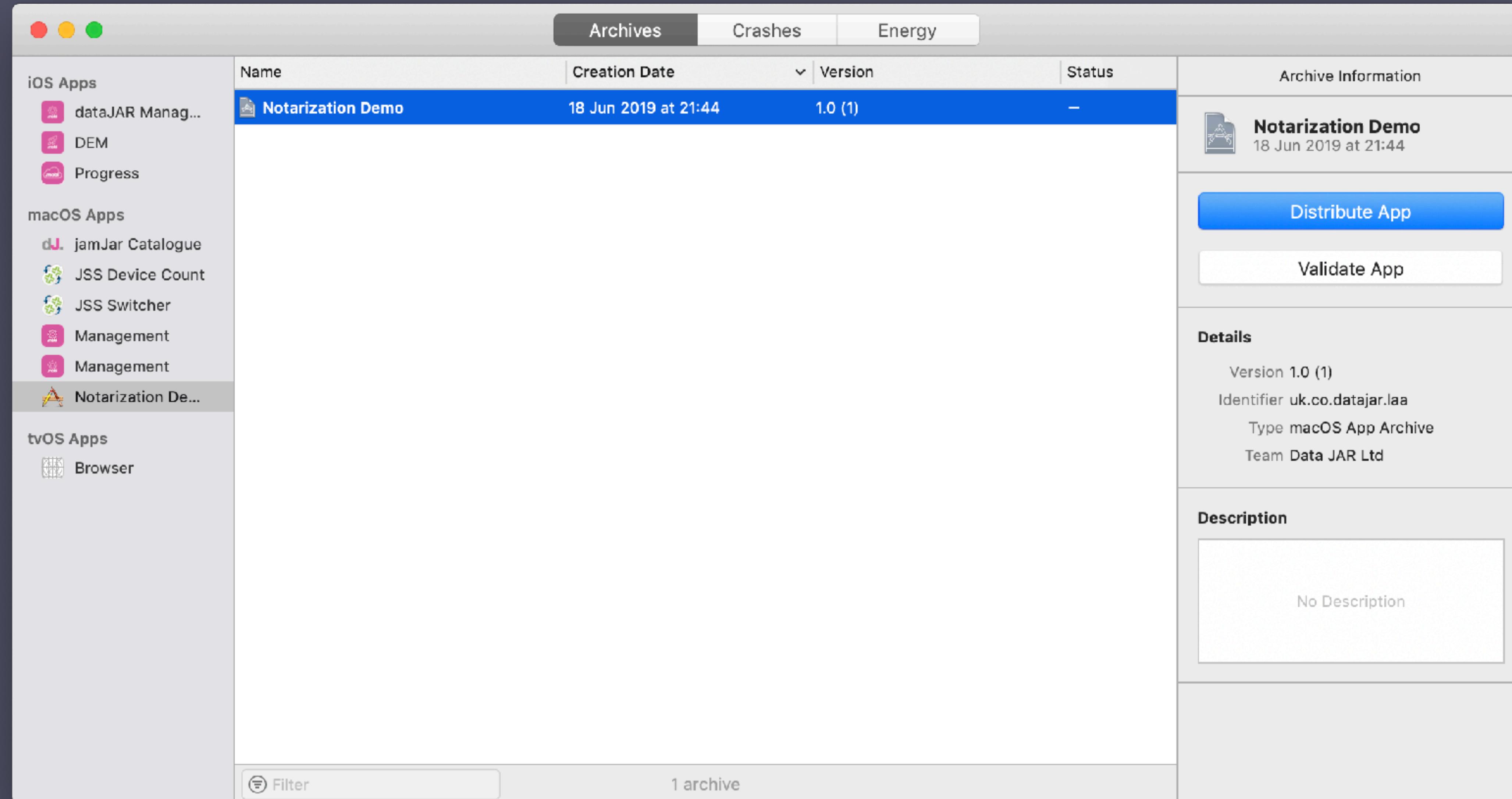


- App Bundles - Developer ID Application Certificate
- Installer Packages - Developer ID Installer Certificate
- Disk Images - Developer ID Application Certificate



# Xcode Workflow

---

The screenshot shows the Xcode Archives tab interface. On the left, a sidebar lists categories: iOS Apps, macOS Apps, and tvOS Apps. Under iOS Apps, there are three entries: "dataJAR Manag...", "DEM", and "Progress". Under macOS Apps, there are six entries: "jamJar Catalogue", "JSS Device Count", "JSS Switcher", "Management", "Management", and "Notarization De...". Under tvOS Apps, there is one entry: "Browser". The main area displays a table with columns: Name, Creation Date, Version, and Status. A single row is selected, corresponding to the "Notarization Demo" entry from the sidebar. The table shows the following data:

Name	Creation Date	Version	Status
Notarization Demo	18 Jun 2019 at 21:44	1.0 (1)	-

On the right side of the interface, there are several sections: "Archive Information" (showing the selected archive's name and creation date), "Distribute App" (a blue button), "Validate App" (a white button), "Details" (listing Version 1.0 (1), Identifier uk.co.datajar.laa, Type macOS App Archive, and Team Data JAR Ltd), and "Description" (a text box containing "No Description"). At the bottom of the main area, there is a "Filter" button and the text "1 archive".

Name	Creation Date	Version	Status
Notarization Demo	18 Jun 2019 at 21:44	1.0 (1)	-

Archive Information

Notarization Demo  
18 Jun 2019 at 21:44

Distribute App

Validate App

Details

Version 1.0 (1)  
Identifier uk.co.datajar.laa  
Type macOS App Archive  
Team Data JAR Ltd

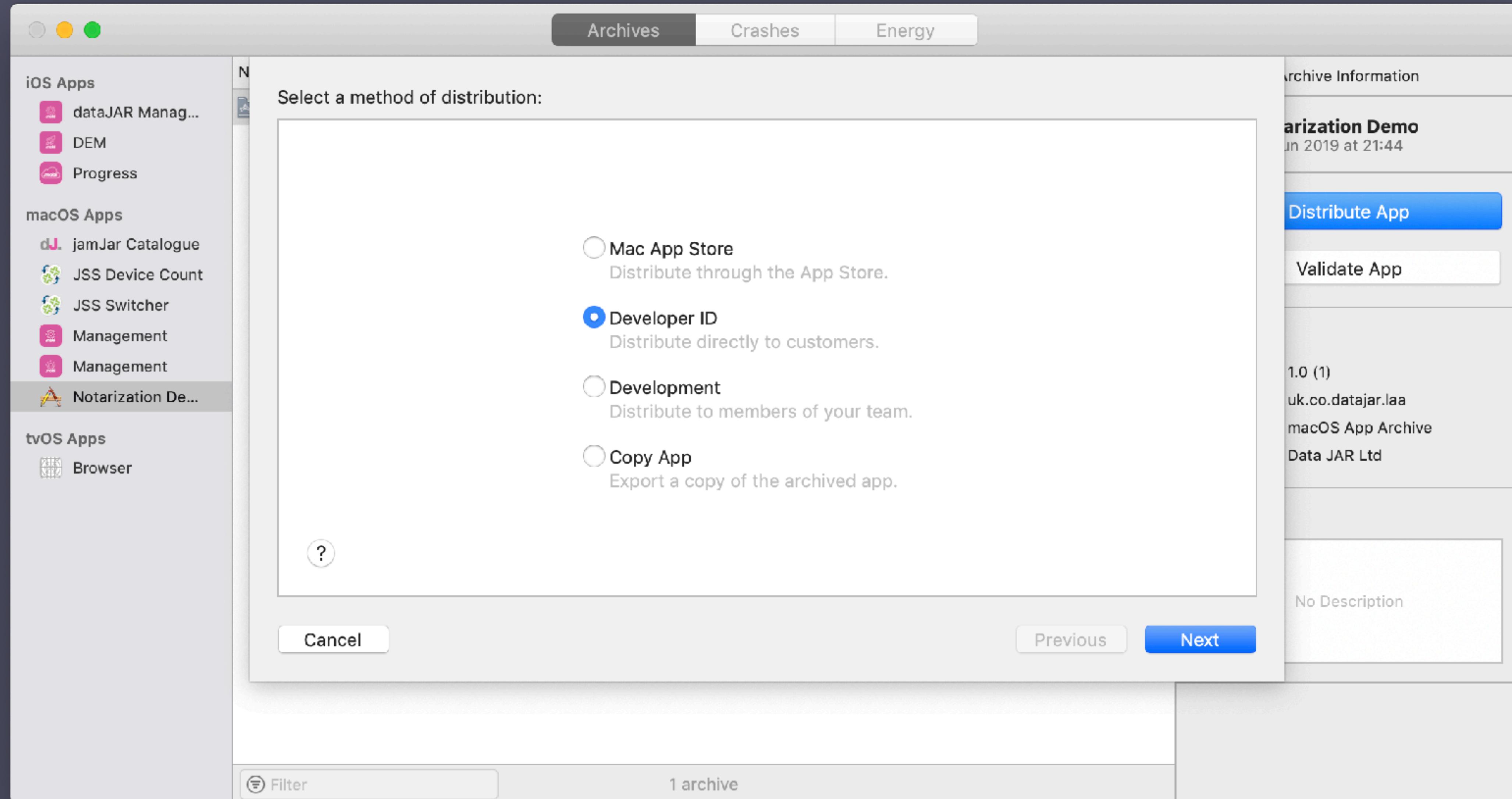
Description

No Description

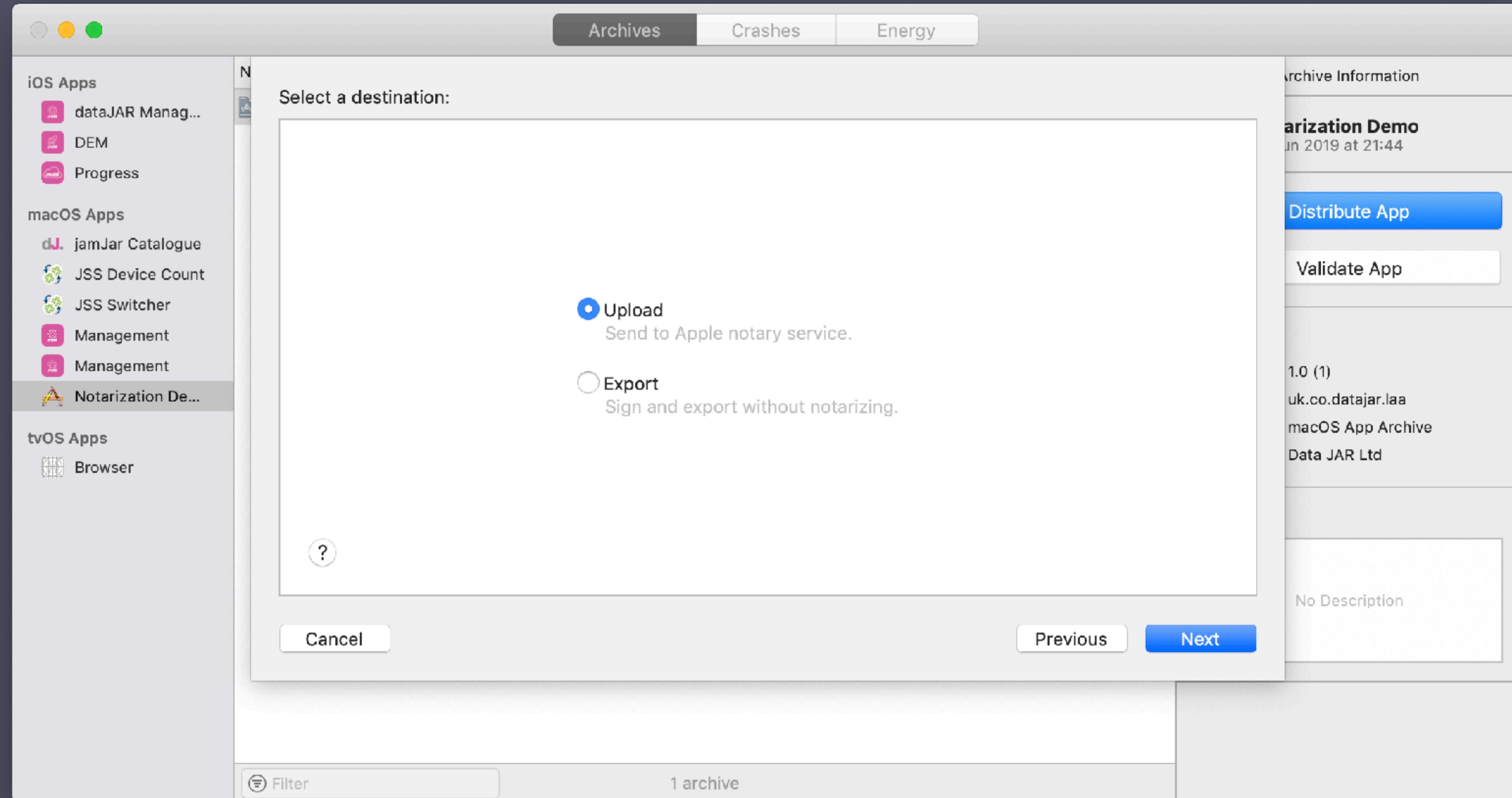
Filter

1 archive

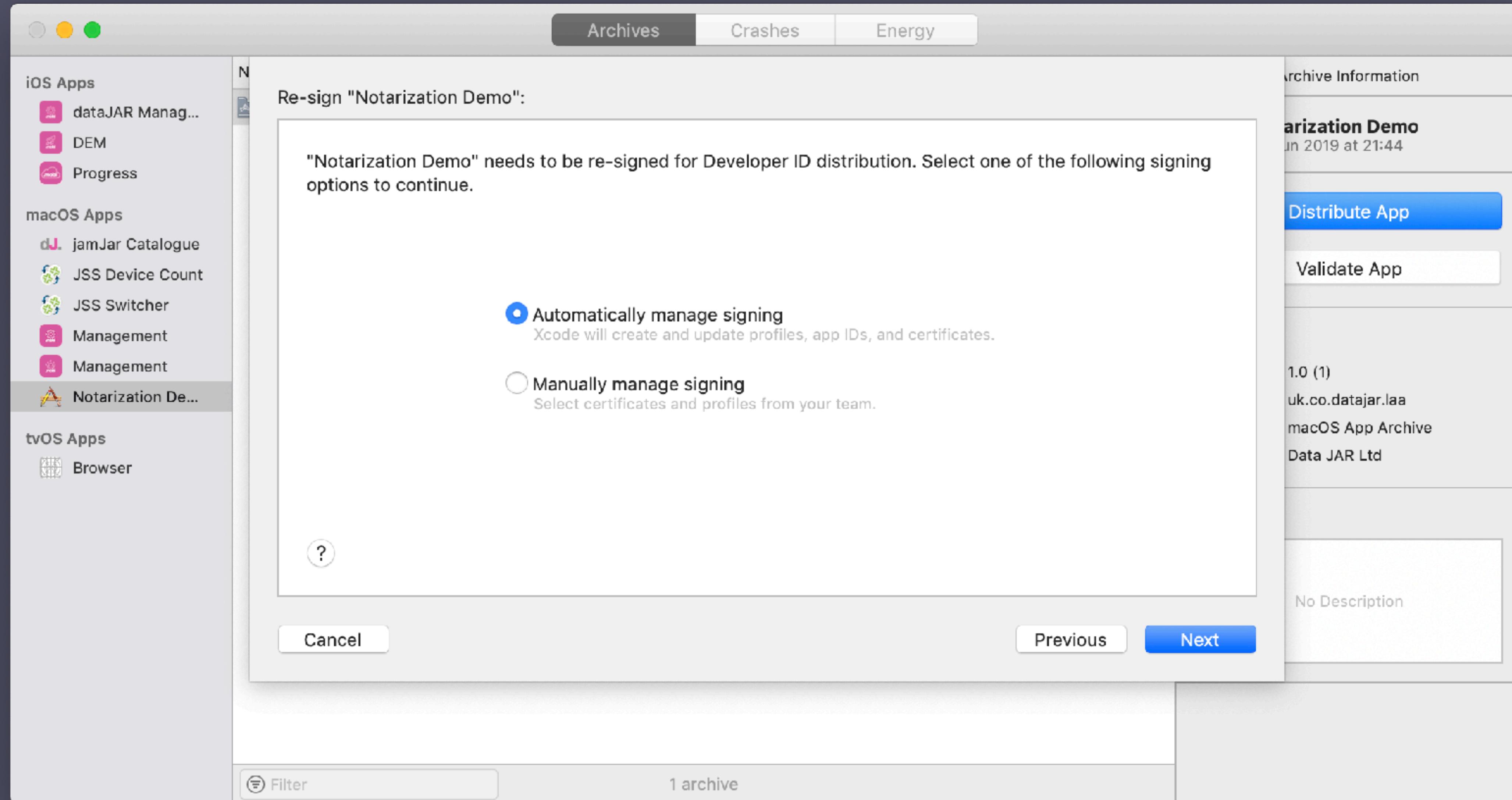
# Archive Workflow



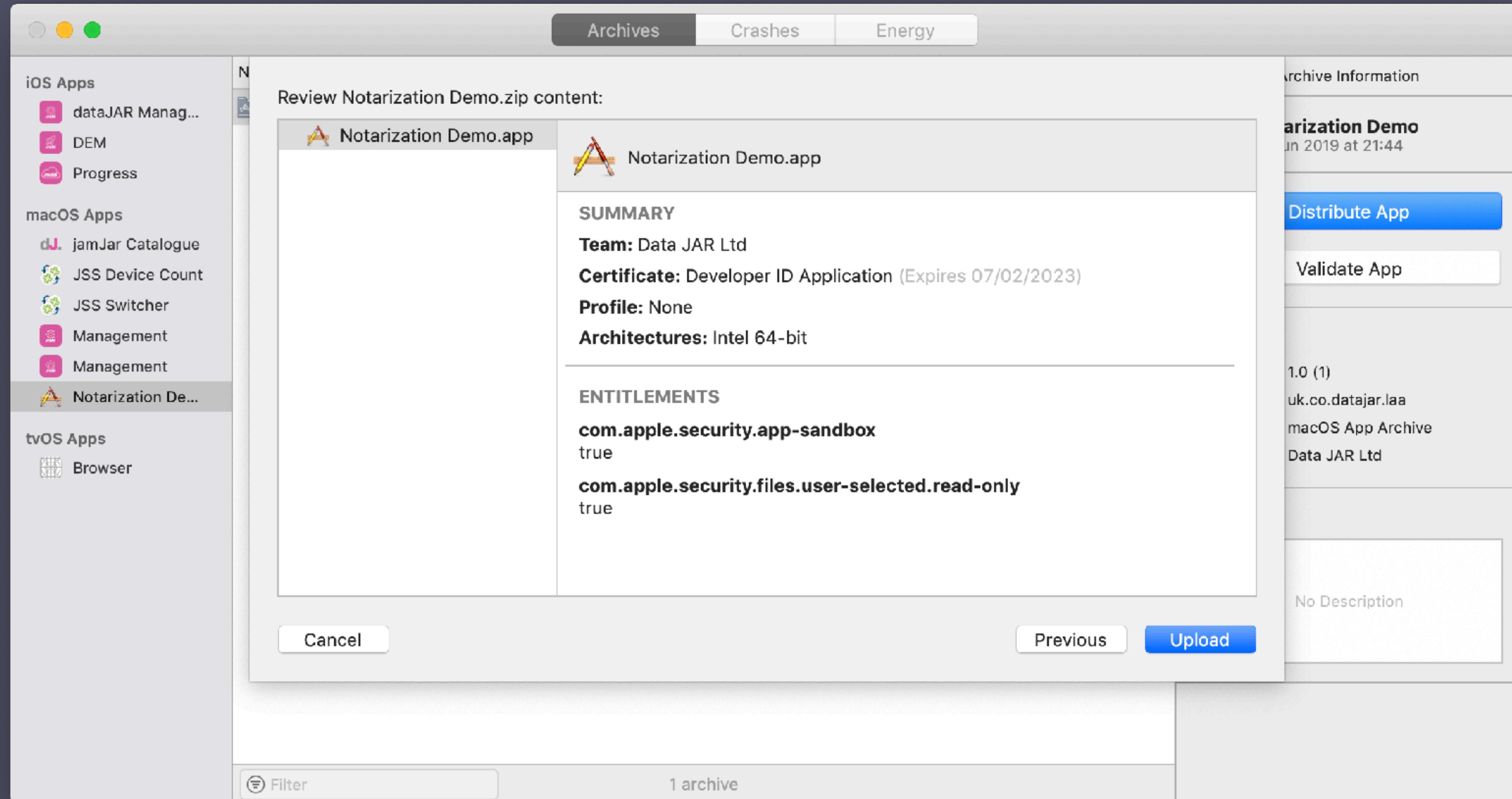
# Distribute using your Developer ID



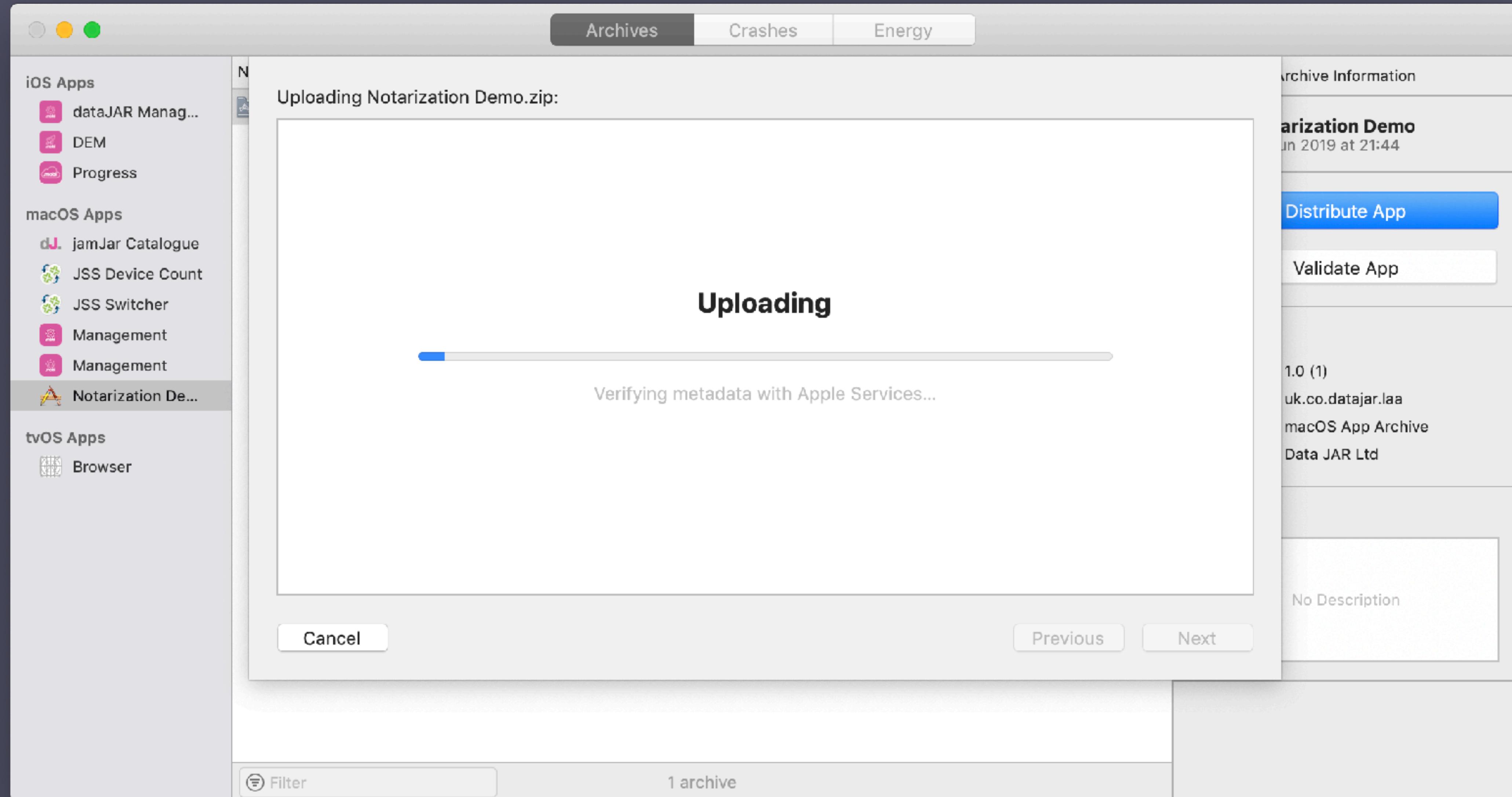
# Upload to the Notary Service



# Sign the App with your Developer ID



Upload the Signed App to Apple



Uploading.....

Archives    Crashes    Energy

iOS Apps

- dataJAR Manag...
- DEM
- Progress

macOS Apps

- jamJar Catalogue
- JSS Device Count
- JSS Switcher
- Management
- Management
- Notarization De...

tvOS Apps

- Browser

Archive upload complete:

Uploaded "Notarization Demo" to Apple notary service.

You will receive a notification when your app is ready for distribution.

Cancel    Export...    Previous    Close

Filter    1 archive

Distribute App

Validate App

1.0 (1)  
uk.co.datajar.laa  
macOS App Archive  
Data JAR Ltd

No Description

Show Status Log

Developer ID

Upload Complete

The screenshot shows the Xcode Archives tab with the following details:

- iOS Apps**:
  - dataJAR Manag...
  - DEM
  - Progress
- macOS Apps**:
  - jamJar Catalogue
  - JSS Device Count
  - JSS Switcher
  - Management
  - Management
  - Notarization De...
- tvOS Apps**:
  - Browser

**Archives** table:

Name	Creation Date	Version	Status
Notarization Demo	18 Jun 2019 at 21:44	1.0 (1)	Processing

**Archive Information** sidebar:

- Notarization Demo** (Icon)
- 18 Jun 2019 at 21:44
- Distribute App** (Large blue button)
- Validate App** (Light gray button)
- Details**
  - Version 1.0 (1)
  - Identifier uk.co.datajar.laa
  - Type macOS App Archive
  - Team Data JAR Ltd
- Description**
  - No Description
- Show Status Log** (Light gray button)
- Developer ID**
  - Status Processing
  - Upload 18 Jun 2019 at 21:50
  - Identifier fea2aab8-cfc0-4114-b4e1-437b3c1709bb
- Export Notarized App** (Light gray button)

# Notary Service processing App

The screenshot shows the Xcode Archives tab interface. On the left, a sidebar lists categories: iOS Apps, macOS Apps, and tvOS Apps. Under iOS Apps, several items are listed, with "Notarization Demo" selected. The main table displays the following information:

Name	Creation Date	Version	Status
Notarization Demo	18 Jun 2019 at 21:44	1.0 (1)	Ready to distribute

To the right of the table, there is a panel titled "Archive Information" containing the following details:

- Notarization Demo** (Icon)
- 18 Jun 2019 at 21:44
- Distribute App** (Large blue button)
- Validate App** (Light gray button)
- Details**
  - Version 1.0 (1)
  - Identifier uk.co.datajar.laa
  - Type macOS App Archive
  - Team Data JAR Ltd
- Description**
  - No Description
- Show Status Log** (Light gray button)
- Developer ID**
  - Status Ready to distribute
  - Upload 18 Jun 2019 at 21:50
  - Identifier fea2aab8-cfc0-4114-b4e1-437b3c1709bb
- Export Notarized App** (Light gray button)

Notary Service passes App, ready for distribution

**Apple Developer**

You can now distribute your Mac software.

To: Richard Mallion

**Developer**

---

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](#)

Inbox - Google 21:52 AD

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/...](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



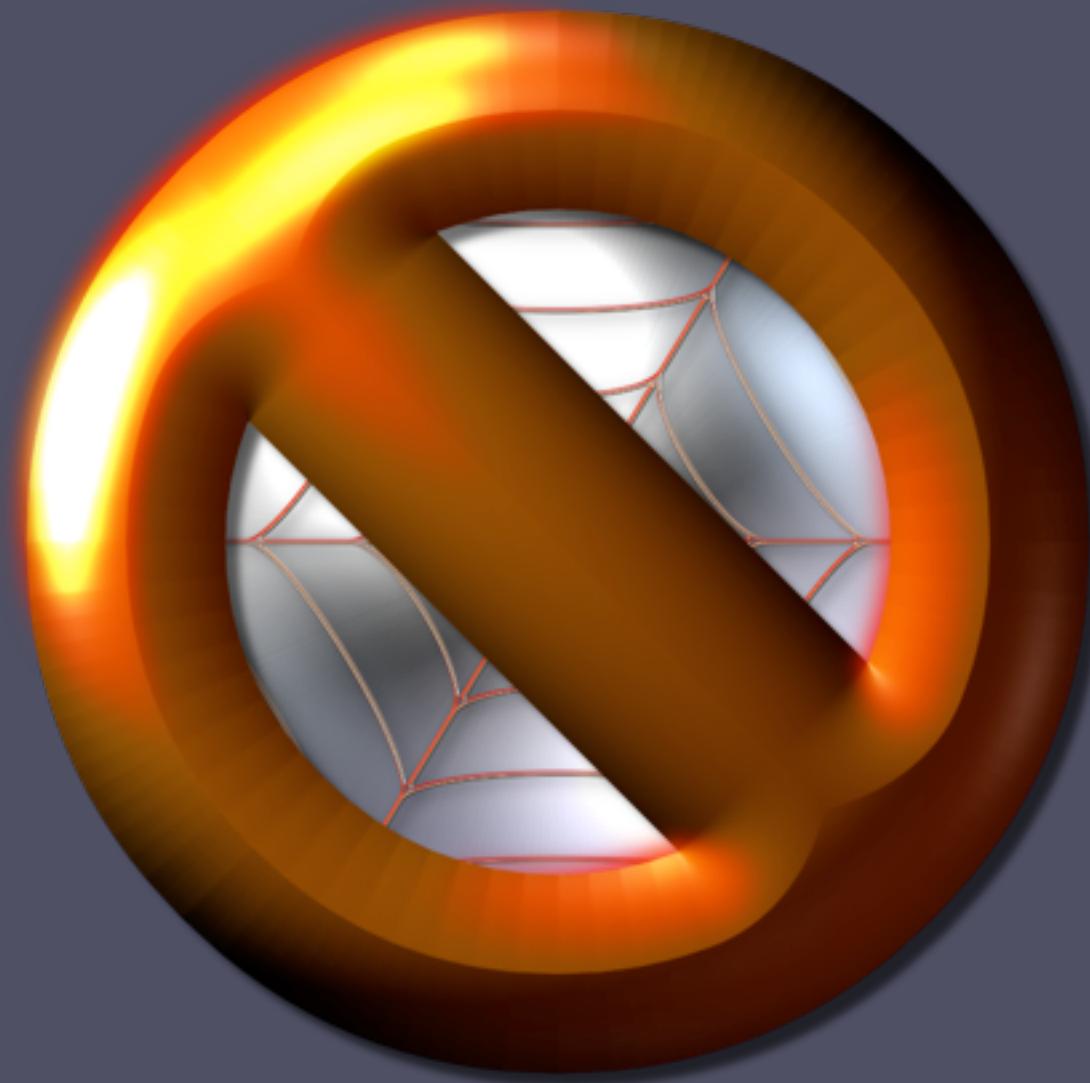
```
spctl --assess --verbose --type open --context  
"context:primary-signature" /path/to/dmg
```

Checking Disk Images

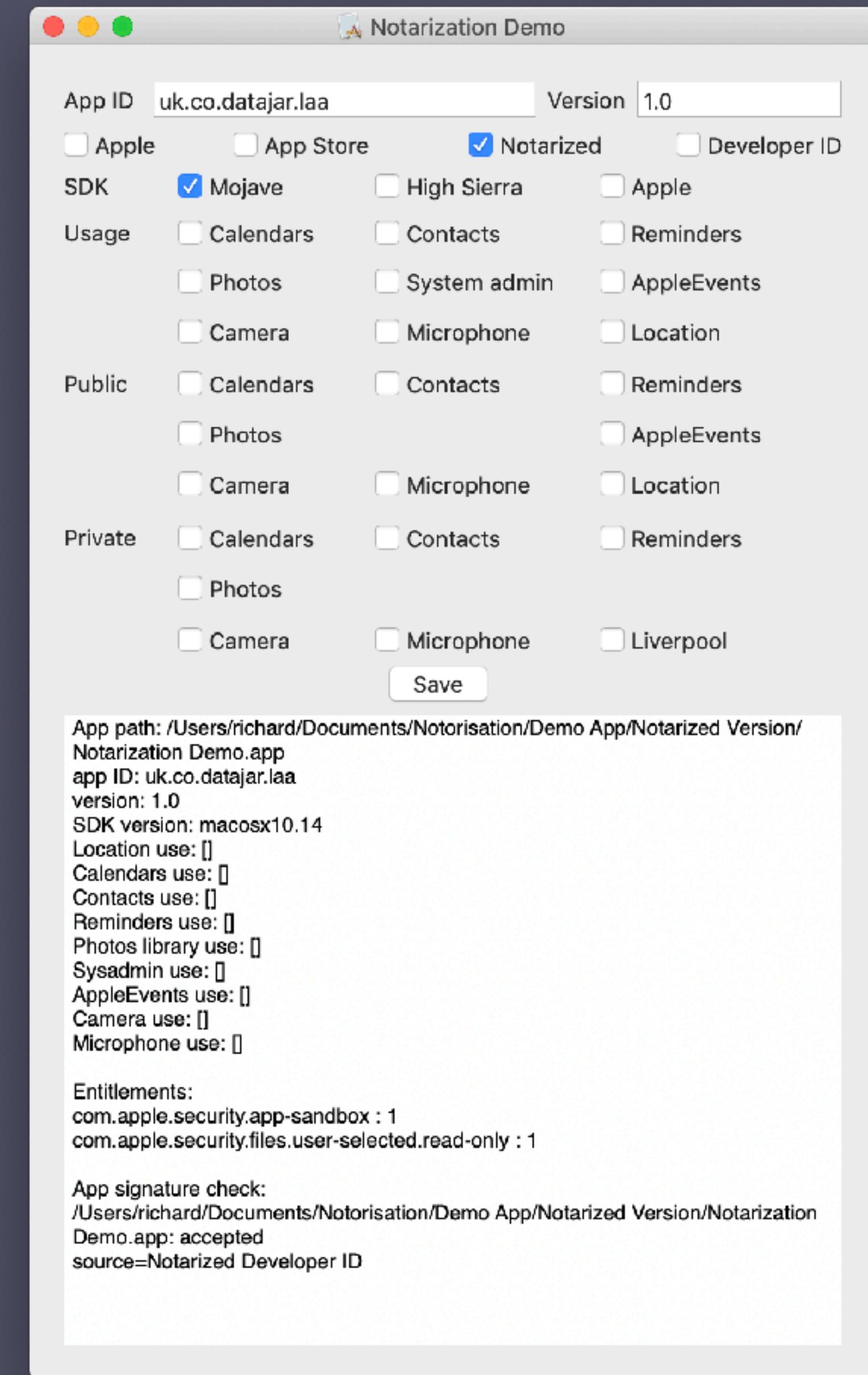


```
codesign --verify --verbose  
--test-requirement="notarized" /path/to/binary
```

Other Binaries



Tacky



<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://developer.apple.com/documentation/security/notarizing_your_app_before_distribution)

<https://eclecticlight.co>

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



# Questions

---

**dataJARltd.**  
Apple Device Management Specialists



dataJARltd.com

01202 555 555

info@dataJARltd.com

123 Main Street

Anytown, USA 12345

www.dataJARltd.com