Oracle Banking Digital Experience

Mobile Application Builder Guide – iOS
Release 18.1.0.0.0

Part No. E92727-01

January 2018

ORACLE®

Mobile Application Builder Guide – iOS

January 2018

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax:+91 22 6718 3001
www.oracle.com/financialservices/

Table of Contents

1. Preface 4

1.1 Intended Audience 4

1.2 Documentation Accessibility 4

1.3 Access to Oracle Support 4

1.4 Structure 4

1.5 Related Information Sources 4

2. OBDX Servicing Application 5

2.1 Pre requisite 5

2.2 Create Project 5

2.3 Adding UI to workspace. 5

2.4 Open project in Xcode 6

2.5 Generating Certificates for Development, Production and Push Notifications 6

3. Archive and Export 11

4. OBDX Authenticator Application 14

4.1 Building Authenticator UI 14

4.2 Authenticator Application Workspace Setup 16

4.3 Building Authenticator Application 18

5. Application Security Configuration 20

1. Preface

1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=accandid=docacc.

1.3 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=accandid=info or visit

http://www.oracle.com/pls/topic/lookup?ctx=accandid=trs if you are hearing impaired.

1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

The subsequent chapters describes following details:

- Configuration / Installation.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 18.1.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide

2. OBDX Servicing Application

2.1 Pre requisite

- Download and Install node js as it is required to run npm and cordova commands.
- XCode 10 to be download from Mac App Store

2.2 Create Project

1. Extract iOS workspace from installer and place in a folder.
2. The workspace by default contains framework for running on devices. Hence to run the application on simulator, delete and copy the 3 frameworks (OBDXExtensions.framework, OBDXFramework.framework and Cordova.framework) from installer/simulator to zigbank\platforms\ios directory.

2.3 Adding UI to workspace.

Use any 1 option below

a. Building un built UI (required in case of customizations)

Extract unbuilt UI and traverse to **OBDX_Installer/installables/ui/channel/_build** folder and perform below steps

Windows –

```
npm install -g grunt-cli
npm install
set IS_GRUNT=true
node render-requirejs/render-requirejs.js mobile
grunt --max_old_space_size=5120 iosbuild --platform=ios
```

Linux -

```
sudo npm install -g grunt-cli
sudo npm install
export IS_GRUNT=true
node render-requirejs/render-requirejs.js mobile
grunt --max_old_space_size=5120 iosbuild --platform=ios
```

Copy folders (build.fingerprint,components,corporate,extensions,framework,images,index,index.html, manifest.json,pages,partials,resources,retail,sw.js) from newly created dist folder into workspace (platforms/ios/www/)

b. Using built UI (out of box shipped with installer)

i. Unzip dist.tar.gz for android from installer and copy folders(build.fingerprint,components,corporate,extensions,framework,images,index,index.html,manifest.json,pages,partials,resources,retail,sw.js) to workspace (platforms/ios/www/)

2.4 Open project in Xcode

Open Xcode by clicking ZigBank.xcodeproj at zigbank/platforms/ios/

1. Adding URLs to app.plist (ZigBank/Resources)

   a. FOR NONOAM (DB Authenticator setup)

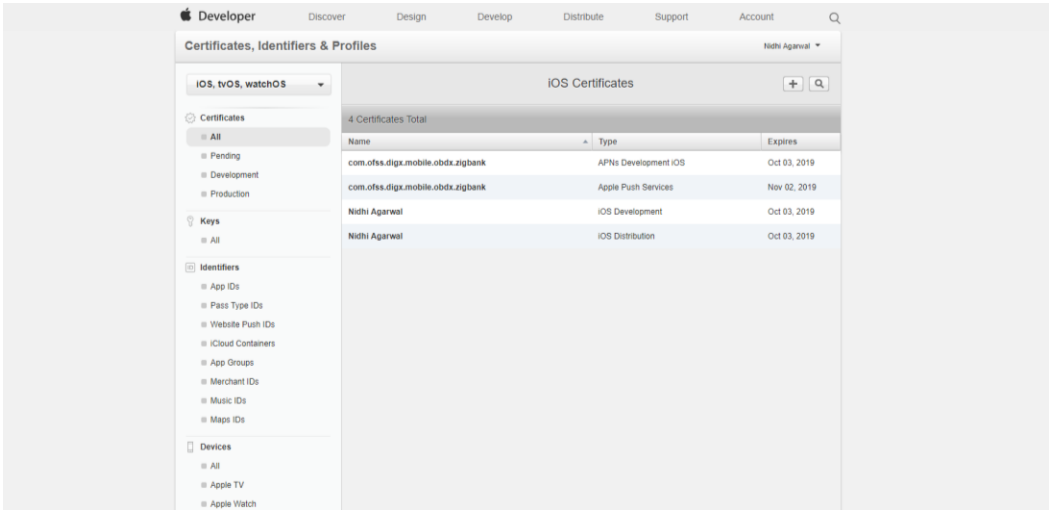
LoginController	**NONOAM**
KEY_SERVER_URL	Eg http://mum00cag.in.oracle.com:7780

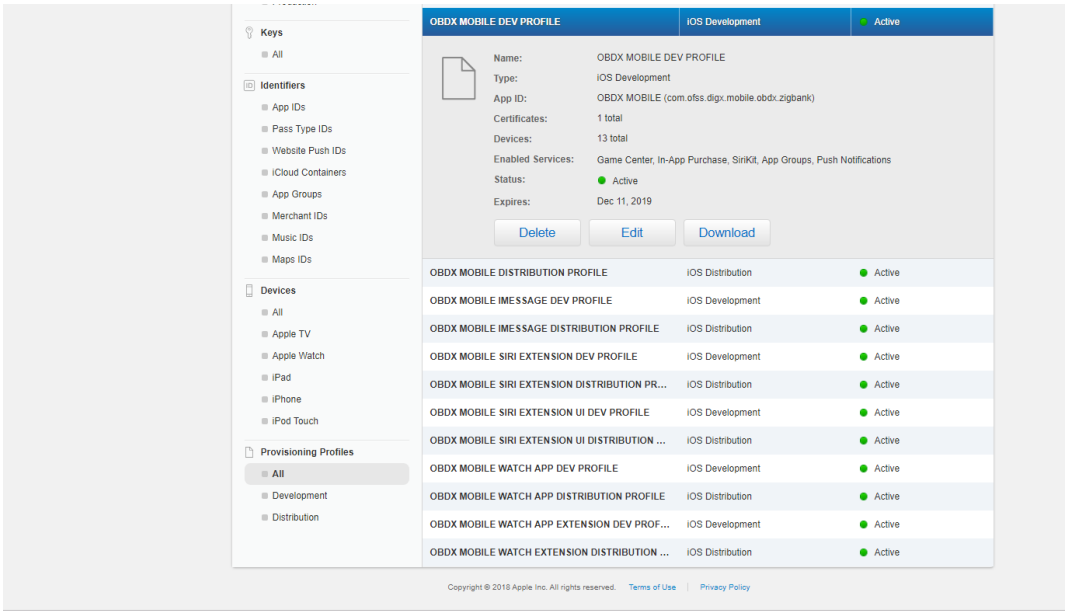
   b. OAM Setup (Refer to installer pre requisite documents for OAuth configurations)

LoginController	**OAM**
KEY_OAM_URL	Eg. http://mum00aoo.in.oracle.com:14100 (This URL must be of OHS without webgate)
KEY_SERVER_URL	Eg.http://mum00cag.in.oracle.com:7780

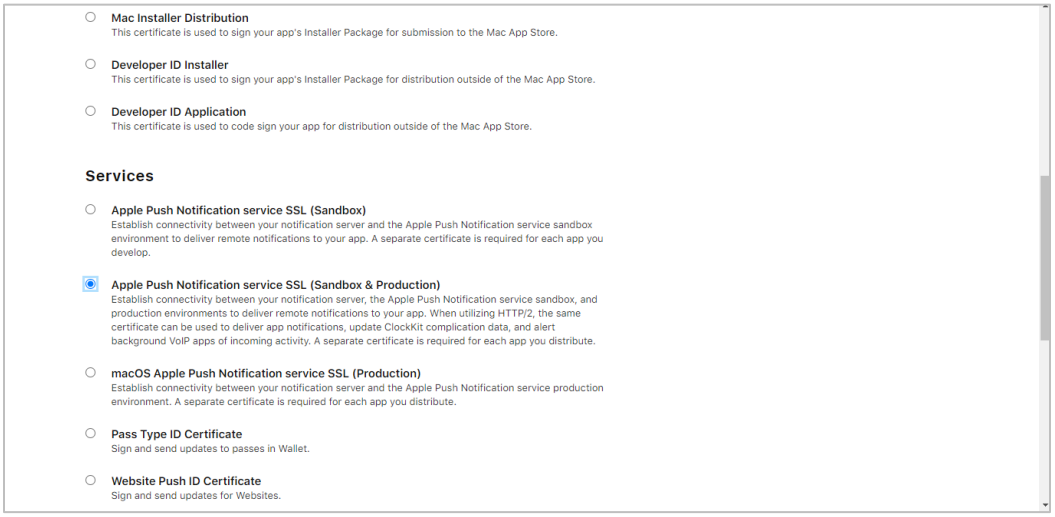
2.5 Generating Certificates for Development, Production and Push Notifications

Create all certificates (by uploading CSR for keychain utility), provisioning profiles and push certificates as shown below by login in developer console. For development add device UUIDs and add same to provisioning profiles. Add capabilities as shown below and ensure the bundle identifier matches the one of the application in Xcode

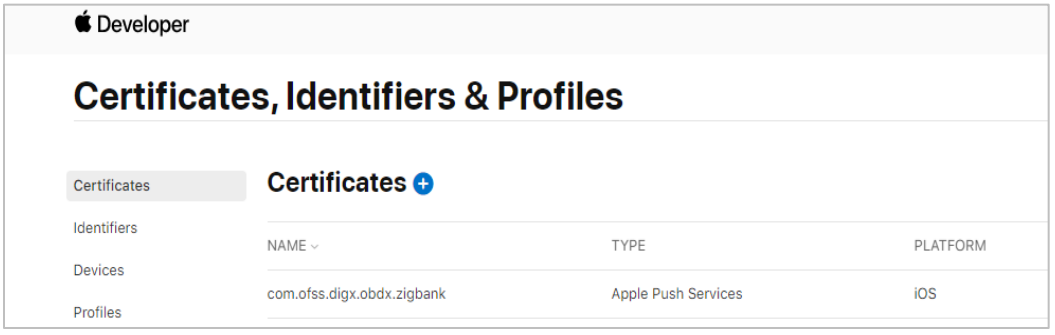




Ensure AppGroups capability is added to all profiles and for mobile profile SiriKit, App Groups, Push Notifications must by added.



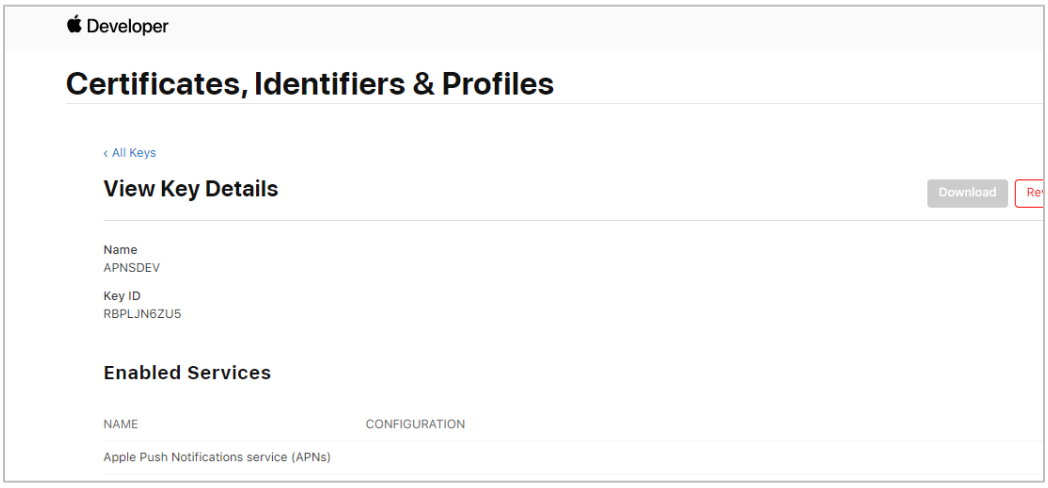
Note the certificate/bundle name



Note the Team ID from top right corner

Navigate to the “Keys” section and create APNS key

Note APNS key and download the .p8 file. Copy the .p8 to config/resources\mobile

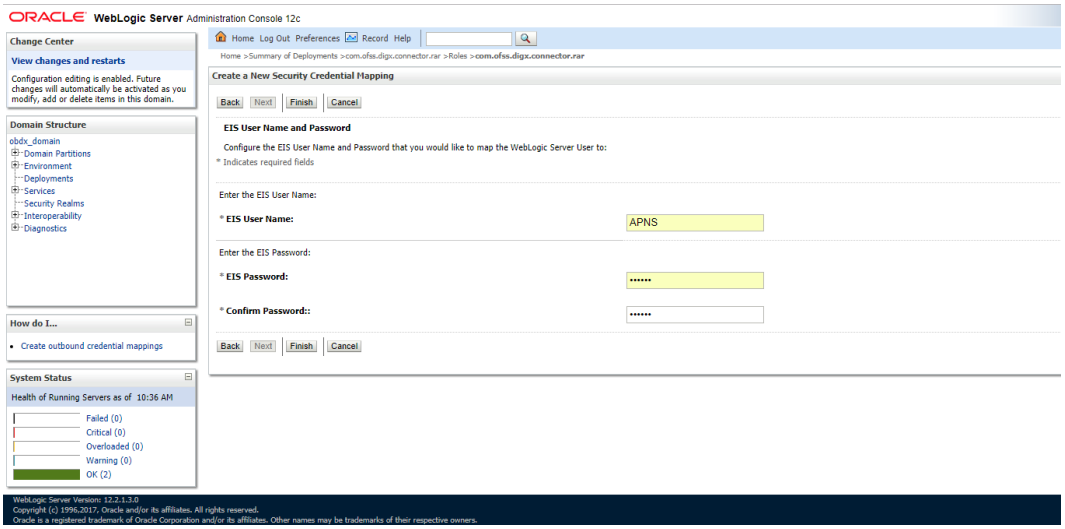


Update the password as shown below –

Sr. No.	Table	PROP_ID	CATEGORY_ID	PROP_VALUE	Purpose
1	DIGX_FW_CONFIG_ALL_B	ios_cert_path	DispatchDetails	resources/mobile/AuthKey_RBPLJN6ZU5.p8	Update the certificate path/name if required. Should be relative to config directory
2	DIGX_FW_CONFIG_ALL_B	APNS	DispatchDetails	<Password> Eg - RBPLJN6ZU5	Provides id of .p8 certificate
3	DIGX_FW_CONFIG_ALL_B	APNSKeyStore	DispatchDetails	DATABASE or CONNECTOR	Specifies whether to pick certificate password from database or from connector. Default DB (No change)
4	DIGX_FW_CONFIG_ALL_B	Proxy	DispatchDetails	<protocol,proxy_address>	Provides proxy address, if any, to be provided while connecting to APNS server.

Sr. No.	Table	PROP_ID	CATEGORY_ID	PROP_VALUE	Purpose
					Delete row if proxy not required. Example: HTTP,148.50.60,80
5	DIGX_FW_CONFIG_ALL_B	CERT_TYPE	DispatchDetails	For dev push certs add row with value ‘dev’	For prod push certificates this row is not required
6	DIGX_FW_CONFIG_ALL_B	APNS_BUNDLE	DispatchDetails	Eg. com.ofss.digx.obdx.zigbank	Bundle Name
7	DIGX_FW_CONFIG_ALL_B	APNS_TEAMID	DispatchDetails	Eg. 3NX1974C93	Team ID of Apple developer account

If CONNECTOR is selected in Step 2 update certificate id as below

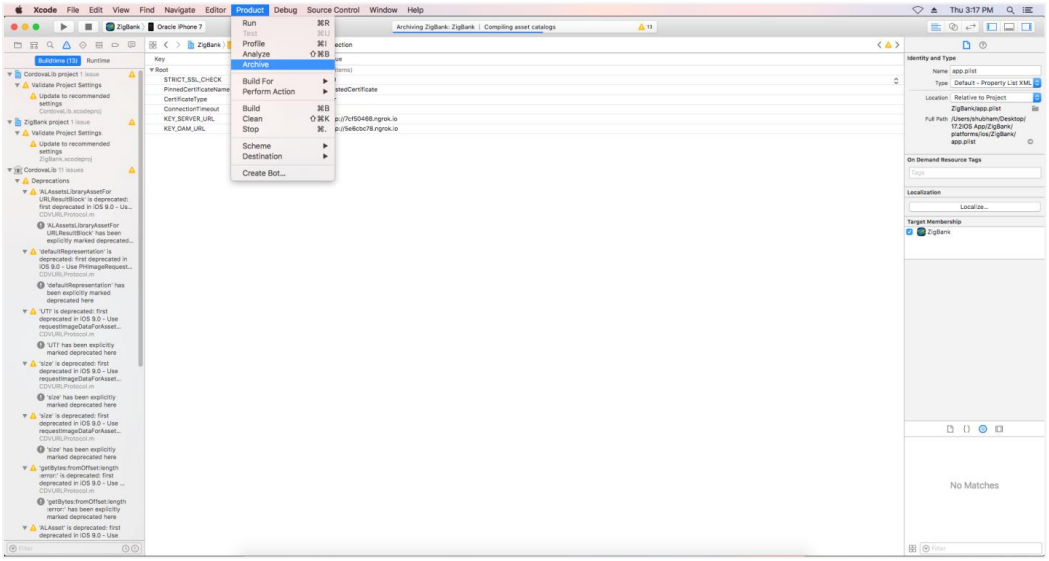


Properties for tokens to be configured as –

Sr. No.	Table	PROP_ID	CATEGORY_ID	PROP_VALUE (Default Value)	Purpose
1	DIGX_FW_CONFIG_ALL_B	MOBILEJWT_EXPIRYTIME	dayoneconfig	864000	Time in secs after which user will have to reregister for alternate login in mobile app

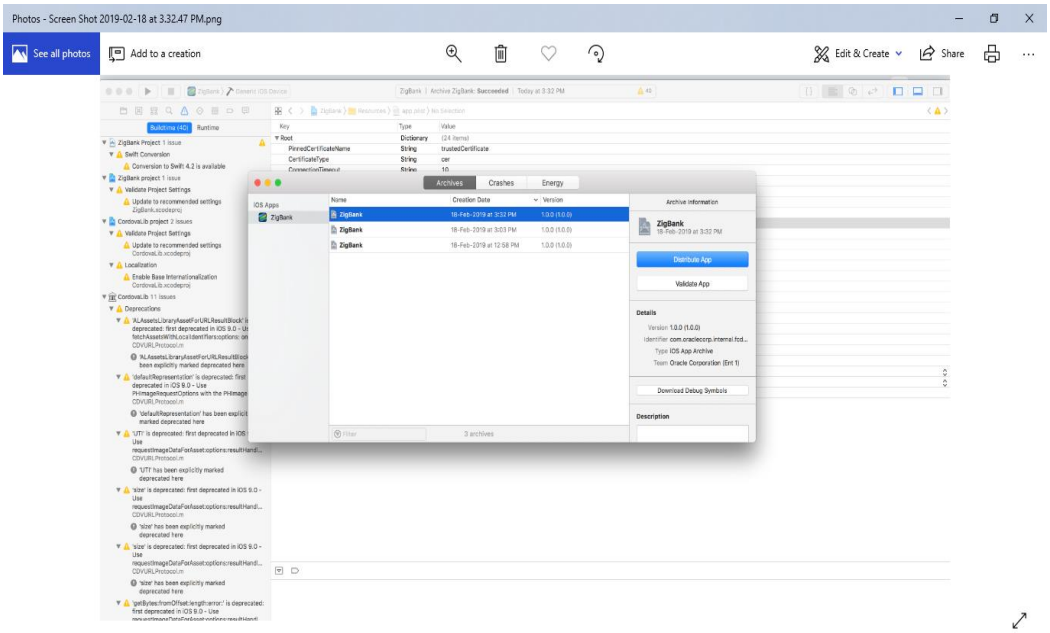
3. Archive and Export

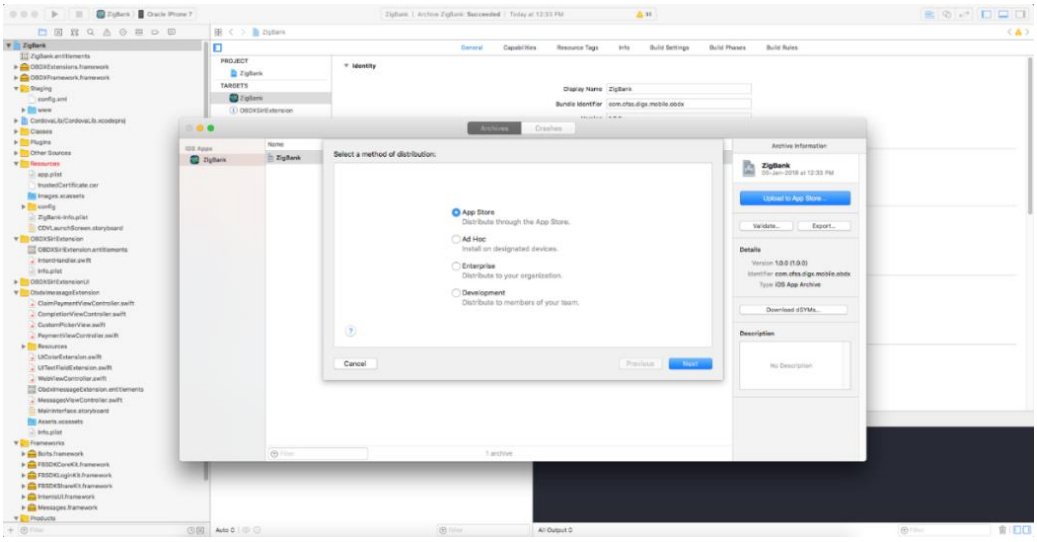
a. In the Menu bar click on **Product -> Archive (Select Generic iOS Device)**

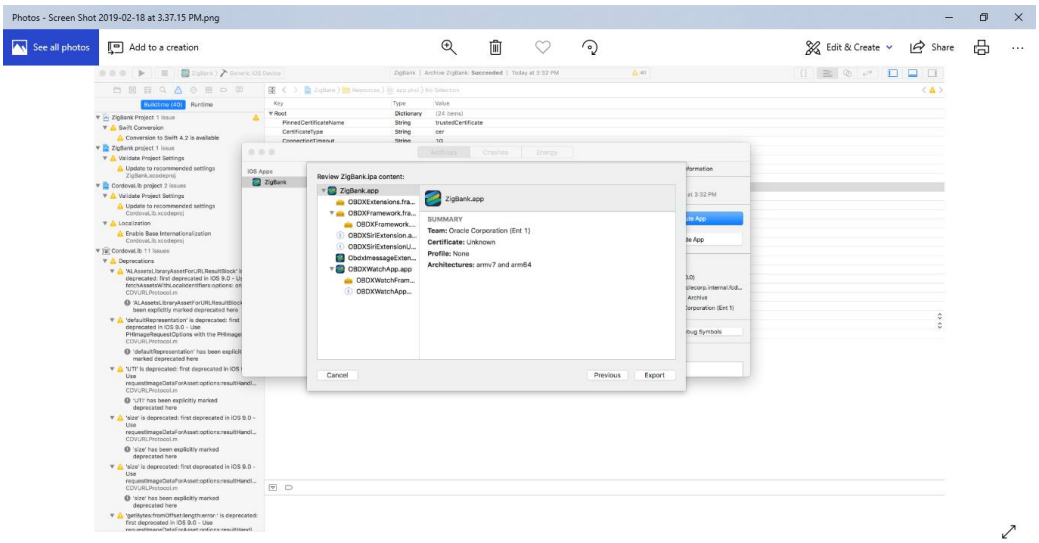


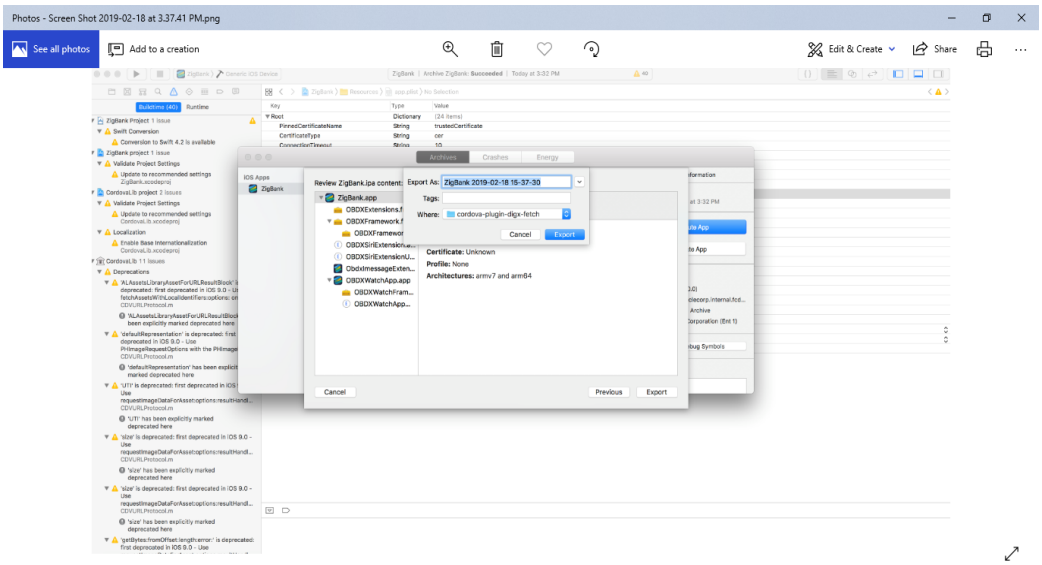
b. After archiving has successfully completed. Following popup will appear

c. Click on Export in the right pane of the popup -> **Distribute App -> Select method of distribution -> Choose Provisioning Profile ->** select **Export one app for all Compatible Devices -> Next -> Next and generate the ipa**.




Select a method of distribution:
App Store
Distribute through the App Store.
Ad Hoc
Install on designated devices.
Enterprise
Distribute to your organization.
Development
Distribute to members of your team.
Cancel
Next

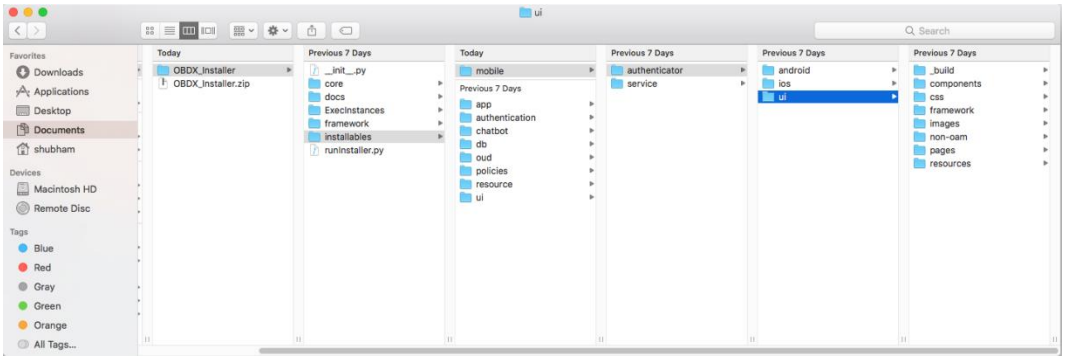

Photos - Screen Shot 2019-02-18 at 3.37.15 PM.png
See all photos
Add to a creation
Edit & Create
Share
Review ZigBank.ipa content:
ZigBank.app
SUMMARY
Team: Oracle Corporation (Ent 1)
Certificate: Unknown
Profile: None
Architectures: armv7 and arm64
Cancel
Previous
Export


Photos - Screen Shot 2019-02-18 at 3.37.41 PM.png
See all photos
Add to a creation
Edit & Create
Share
Export As: ZigBank 2019-02-18 15-37-30
Tags:
Where: cordova-plugin-dlgx-fetch
Cancel
Export
Certificate: Unknown
Profile: None
Architectures: armv7 and arm64
Cancel
Previous
Export

4. OBDX Authenticator Application

4.1 Building Authenticator UI

1. Extract OBDX_Installer.zip. It contains **OBDX_Installer/installables/mobile/authenticator/ui** folder. The folder structure is as shown :



(a) OAM based Authentication

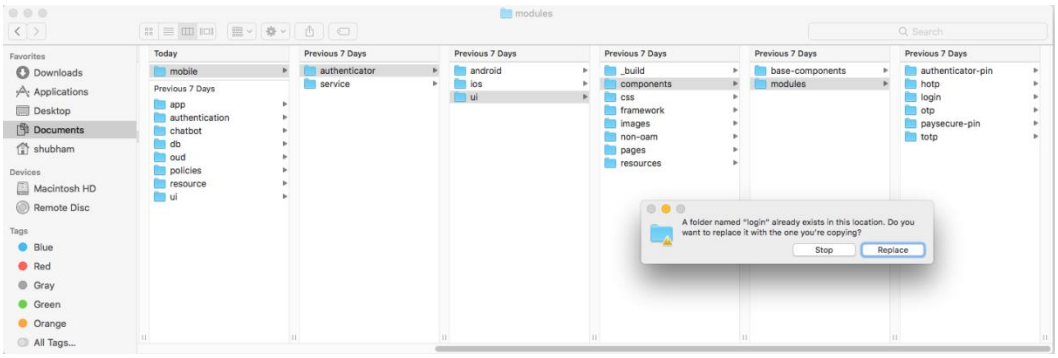
2. Open Terminal at *"_build"* level.
3. Run following command :

```
sudo npm install -g grunt-cli

sudo npm install

node render-requirejs/render-requirejs.js

grunt authenticator --verbose
```

4. After running above commands and getting result as "*Done, without errors.*" a new folder will be created at "_build" level with name as "dist".

(b) NON-OAM Based Authentication

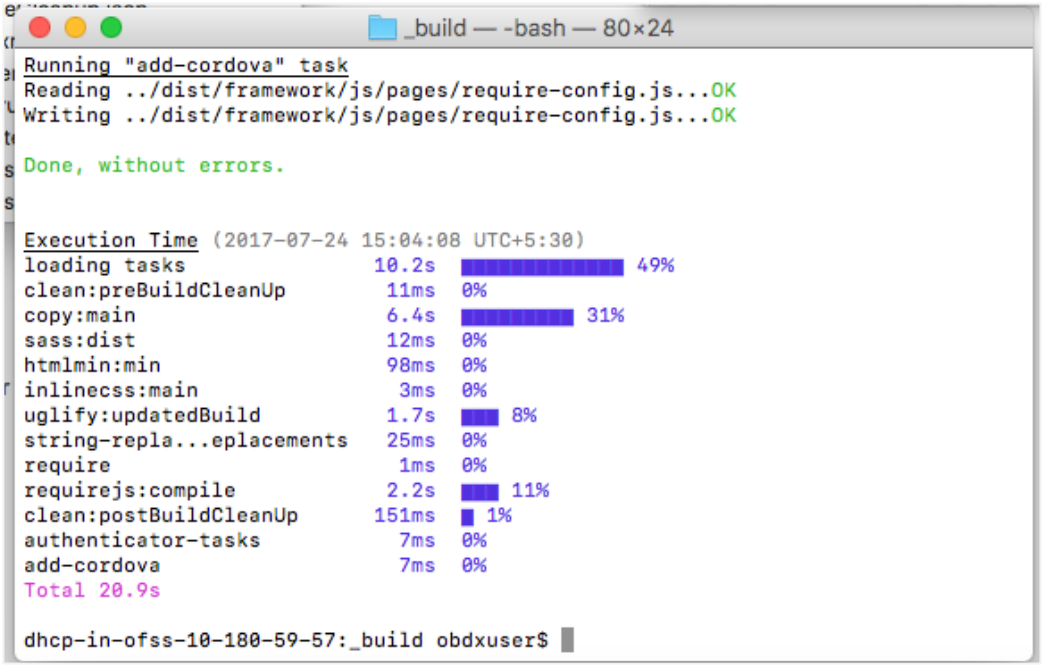
1. Copy "*non-oam/login"* folder and Replace it at location "*components/modules/" [in ui folder]* location. This will replace existing "*login*" folder.

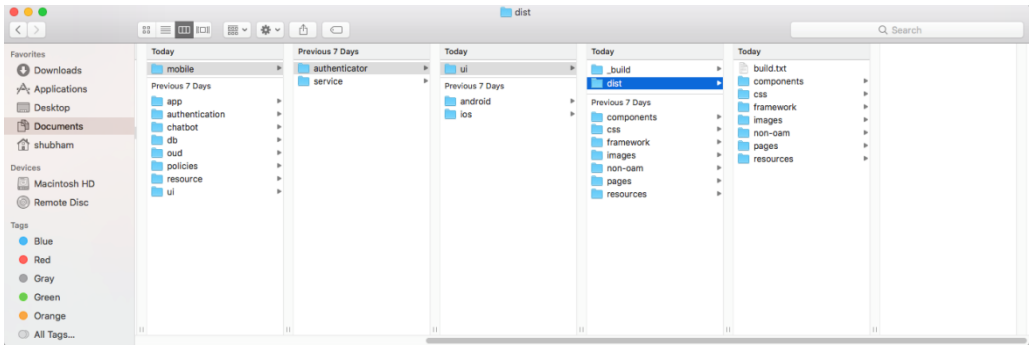


2. Open Terminal at “_build” level.
3. Run following command :

```
sudo npm install -g grunt-cli

sudo npm install

node render-requirejs/render-requirejs.js

grunt authenticator --verbose
```

4. After running above commands and getting result as “*Done, without errors.*” a new folder will be created at “_build” folder level with name as “dist”.

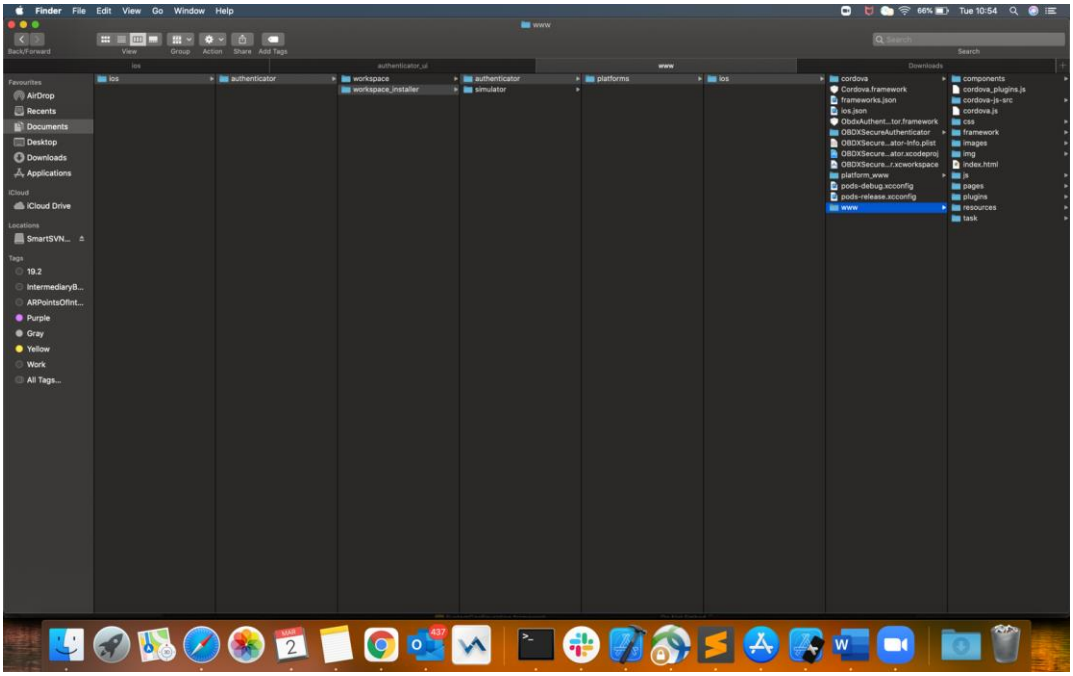




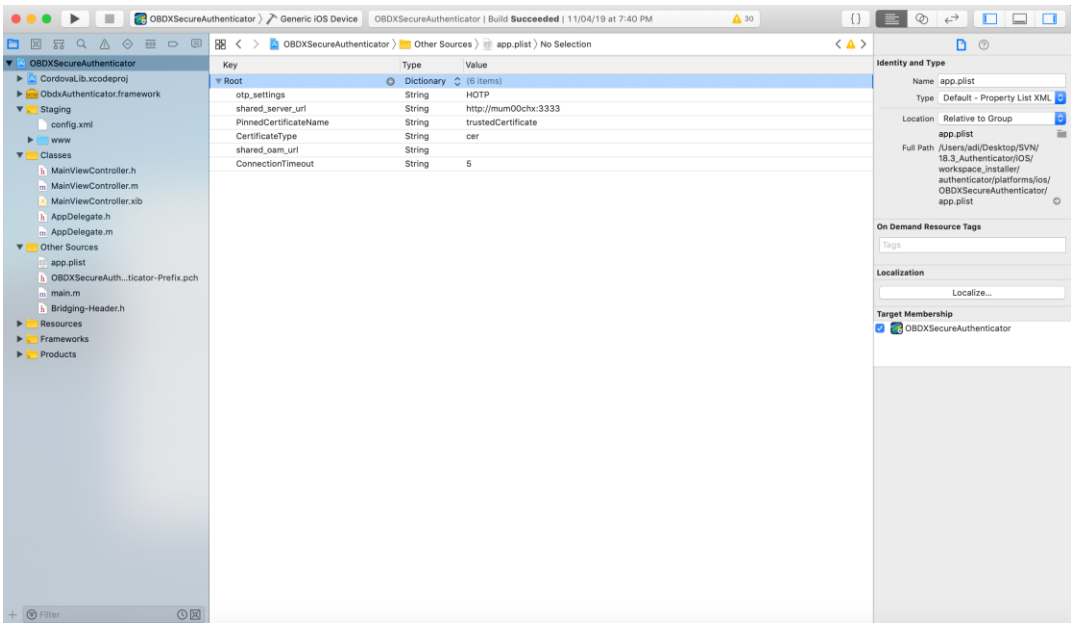
4.2 Authenticator Application Workspace Setup

1. Unzip and navigate to iOS workspace as shipped in installer.
2. Open the "**OBDX_Installer/installables/mobile/authenticator/ui/ios/www**" folder in the finder and paste and replace the following generated UI files from "*ui/dist*" folder :
    - components
    - css
    - framework
    - images
    - pages
    - resources

Finally the **Installer/installables/mobile/authenticator/ui/ios/www** folder must look like:



3. Double click on **OBDXSecureAuthenticator.xccodeproj** to open the project in Xcode



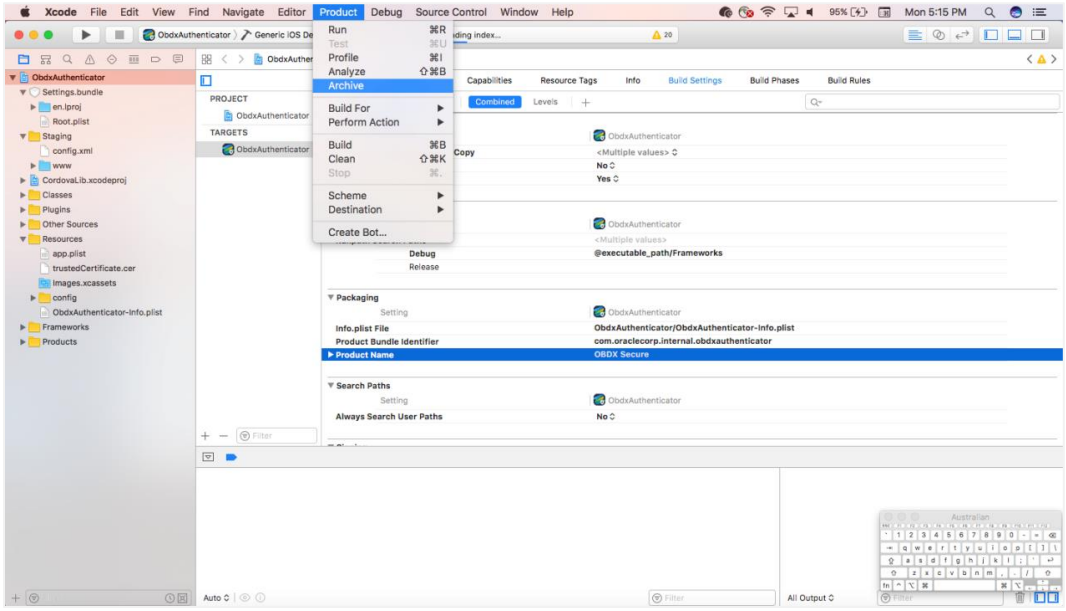
Update HOTP or TOTP in above screenshots and update the server URL.

4. The application can be archived using steps in Section 4.3 for running on device

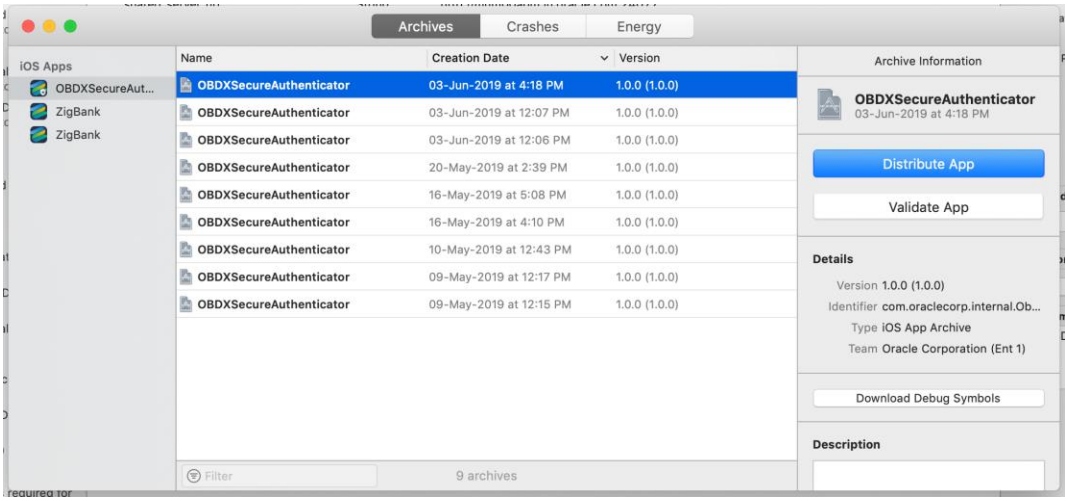
5. To run the application on simulator, copy & replace the framework from simulator/ObdxAuthenticator.framework to /authenticator/platforms/ios/

4.3 Building Authenticator Application

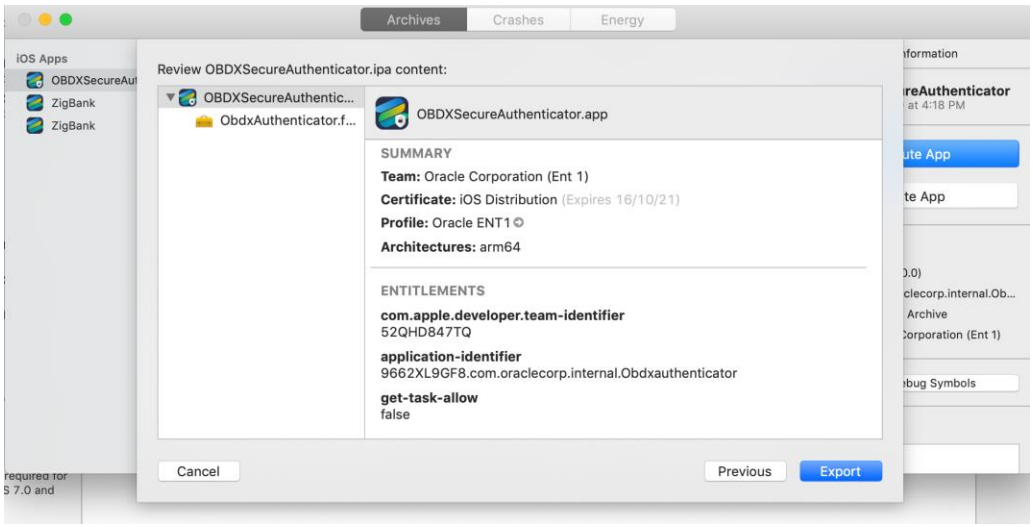
1. Set the simulator to *Generic iOS* device. Then go to *Product -> Archive*.



2. Choose your Archive. Click Distribute App as shown below and select appropriate profiles.



3. Click export to save the .ipa


Archives
Crashes
Energy
iOS Apps
OBDXSecureAu
ZigBank
ZigBank
Review OBDXSecureAuthenticator.ipa content:
OBDXSecureAuthentic...
ObdxAuthenticator.f...
OBDXSecureAuthenticator.app
SUMMARY
Team: Oracle Corporation (Ent 1)
Certificate: iOS Distribution (Expires 16/10/21)
Profile: Oracle ENT1
Architectures: arm64
ENTITLEMENTS
com.apple.developer.team-identifier
52QHD847TQ
application-identifier
9662XL9GF8.com.oraclecorp.internal.Obdxauthenticator
get-task-allow
false
Cancel
Previous
Export

5. Application Security Configuration

OBDX supports single and multiple certificate pinning as part of application security. This can be achieved by maintaining below key values in app.plist

1. PinnedCertificateName - OHS Server Certificate Name
2. PinnedCertificateOAMName - OAM Server Certificate Name
3. KEY_SERVER_URL = OHS Server URL
4. KEY_OAM_URL = OAM Server URL

LoginController needs to be changed to OAM if BANK is on OAM

Make sure the type of certificates should be "cer" and respective certificates need to be imported in xcode project. This can be achieved as below.

1. Right click on Project (eg. OBDX) in Project Navigator
2. Add Files to Project (OBDX)
3. Navigate to certificates and Add. [Copy items if needed should be selected]

Clean Build