Developing Digitise apps for Apple iOS Devices

Contents

Overview

This document provides information specific to the development and deployment of Digitise apps for Apple iOS devices resulting from Apple's terms and conditions of use for their devices.

For additional information on using Digitise Apps with Apple devices refer to the Digitise Apps online help.

Digitise Apps works on iPhones, iPads and iPad Minis running iOS 14 or above.

On mobile devices, Digitise apps are managed and run by a *Digitise Apps Client*. The Digitise Apps Client is a mobile app which runs your Digitise apps and communicates with a *Digitise App Server* service, installed on a centrally located server, usually on-premise, to transfer data and to prevent unauthorised access to your Digitise apps. Due to Apple's terms and conditions for running apps on iOS devices, different versions of the Digitise Apps Client are available for developers and users. Developers can use the standard Digitise Apps Client, which allows you to directly download Digitise apps and subsequent updates from within the Client itself. Users, on the other hand, cannot use this version of the Client. For deployment to users' devices, the 'Standalone App' format bundles a copy of the Digitise Apps Client together with one or more Digitise apps into an installable package which can then be downloaded to your devices. Each Standalone App runs its own instance of the Digitise Apps Client which runs the Digitise app(s) contained within the Standalone App. Updates to the app are issued by creating a new version of the Standalone App. You can install as many Standalone Apps on an individual device as you want to run on that device.

The standard Digitise Apps Client and your Standalone Apps have to be individually built for you and require a special code-signing Certificate. These can be built using the automated Digitise Apps Build System. This remote service is hosted by NDL and requires an internet connection. Before you can use the Build System you will need to register through the NDL Technical Support Team using the contact details on the back page of this document. There is no charge to register.

Once built, developer Clients and Standalone Apps can be installed to devices in one of the following ways:

- Over the air from a web site via the device's browser. If you already download other applications from a web site, you can use your existing web site; otherwise you will need to create one. Sample html pages for an IIS web site are included with the Digitise Apps Product Download.
- Over the air using MDM software.
- Connecting the device to a PC with a USB cable and using iTunes.
- Downloading from the Apple App Store (Standalone Apps only).

There are some differences between apps which will be listed on the App Store and those which will be deployed internally. Therefore, in this document, we will refer to apps which will be downloaded to devices via the App Store as '**store**' apps and apps downloaded to devices via internal mechanisms, such as from a web site or using iTunes, as '**enterprise**' apps.

App Studio

The App Studio provides a design and development environment for creating Digitise apps. The Target Platforms available include Apple iOS Platforms and the design process is much the same as for the other supported mobile platforms.

You create a Digitise app for an iOS device as you would for any other device type and then you need to publish it to your Digitise App Server.

In addition, App Studio provides an interface to the Digitise Apps Build System, used to build versions of the standard Digitise Apps Client and Digitise Apps Standalone Apps for your organisation. Your developers can configure a build, submit a request to the Build System and download completed builds all within App Studio. They will need an internet connection to access the Build System.

Within App Studio, when developing your apps there is no distinction between store and enterprise apps. In fact, the same app can be built in both formats, if required, from the same Digitise Apps Project. It's only when you submit a request to the Digitise Apps Build System that you specify whether you want to generate an enterprise or a store app.

Before a developer can use the Digitise Apps Build System they will need to be registered on the System, which they can do by contacting our Technical Support Team using the contact details on the back page of this document.

IMPORTANT: The version of a Digitise app you include within a Standalone App must be exactly the same as the version you publish to the App Server, otherwise the app won't work correctly on users' devices.

If you make any changes to a Digitise app after building a Standalone App, you will need to republish the app to your App Server and rebuild and redeploy your Standalone App to users. We recommend that you always update the app's version number when making changes to prevent issues arising from out-of-sync versions.

For more information about publishing your apps and deploying them to Apple devices, refer to the Digitise Apps' online help, available from within the App Studio and App Manager utilities .

The App Server and App Manager

Both the App Server and App Manager support Apple devices and, as far as possible, work with these devices in the same way that they work with other supported mobile devices. The App Manager identifies Apple devices as either iPads or iPhones together with a randomly-generated alpha-numeric string to identify individual iOS devices within the Digitise Apps environment.

Deploy Digitise apps to iOS Devices

Apple provides two mechanisms for distributing applications to their mobile devices:

1. via their **App Store** –used to distribute approved applications to any device,
2. through the **Apple Developer Enterprise Program** for "Internal Use" or "in-house" applications.

Digitise apps can be distributed using both methods. In this document, we will refer to Digitise apps intended to be deployed via the App Store as '**store**' apps and those to be distributed internally as '**enterprise**' apps.

In order to develop **enterprise apps**, you will need to register with the **Apple Developer Enterprise Program**. At the time of writing, this program costs $299 per year.

In order to develop **store apps**, you will need to register with the **Apple Developer Program**. At the time of writing, this program costs $99 per year.

The following list identifies some significant factors affecting the deployment of "in-house" Apple applications (apps developed for use within your organization only):

- Under Apple's terms and conditions of use, you are not allowed to deploy apps which can download code to the device.

- In-house apps (enterprise Digitise apps) can only be deployed by organisations enrolled in the Apple Developer Enterprise Program. This list summarises some of the main points about this program, but for more details see:

    https://developer.apple.com/business
    https://developer.apple.com/programs
    https://developer.apple.com/programs/enterprise
    https://developer.apple.com/support/compare-memberships

> **Note:**   The organisation must have a Dun and Bradstreet (DUNS) number, see:
>
> What is a D-U-N-S Number? (dnb.co.uk)

- In-house apps can only be deployed to employees of the registered organisation or to customers of the organisation on the organisation's premises or under direct supervision and physical control of the employees in other locations.

- In-house apps must be built with an Enterprise Distribution Certificate issued by Apple and linked to a Provisioning Profile. A Distribution Certificate is valid for three years from date of issue and a Provisioning Profile is valid for one year from date of issue.

- In-house apps will refuse to work after the Provisioning Profile or Distribution Certificate expires.

- The first time an app is opened on an Apple device, it will attempt to verify it is allowed to run by contacting Apple's OCSP server (ocsp.apple.com). Providing your Distribution Certificate is valid and hasn't been revoked, the app is granted permission to run. If your device can't contact the server, this doesn't count as a revocation. The server response is cached on the device for a period of from 3 to 7 days during which time the app will not attempt to re-validate the Certificate. After this period, the next time the device is restarted it will contact the OCSP server again to re-validate. If a revocation is received the app will no longer run. Revoking a Distribution Certificate will cause all apps you have distributed to fail.

- In-house apps can be deployed over the air from a web site, using Mobile Device Management (MDM) software or via a USB connection using iTunes.

- Apple reserves the right to ask for any information pertaining to any in-house app and to reject the right of the organisation to deploy that app to its users.

Similar conditions affect apps for distribution via the App Store (Digitise store apps) but to deploy these apps you need to join the Apple Developer Program and obtain the code-signing Distribution Certificate and Provisioning Profile(s) from this program instead of the Apple Developer Enterprise Program. You will also need to submit each app to the App Store, where it will be reviewed by Apple to determine whether it will be accepted for the Store. Apple reserves the right to reject any app from listing on the Store, if it doesn't conform to their guidelines. For more information about the App Store guidelines, refer to Apple's web site:

https://developer.apple.com/app-store/review/guidelines

To develop and distribute **enterprise** Digitise apps, therefore, you first need to register with the Apple Developer Enterprise Program and obtain a Distribution Certificate and Distribution Provisioning Profile(s).

Note: When creating your Certificate and Profile you need to create 'Distribution' versions of each one and not 'Development' versions. The Development versions are used to install iOS apps on development devices, where each device has to be registered with an Apple Developer Program and hence are not suitable for deploying apps to users.

Likewise, to develop and distribute Digitise **store** apps, you will need to register with the Apple Developer Program and obtain a Distribution Certificate and Provisioning Profile(s) from this program's web site.

If you want to create both enterprise and store apps, you will need to register with both Apple developer programs.

In order to comply with Apple's conditions of use there are two versions of the Digitise Apps Client:

1.   The standard Digitise Apps Client for developers to use during development of your Digitise apps.

     This version of the Client works in a similar way to the standard Client available for other device Platforms. It allows developers to download and upgrade their Digitise apps on their development test devices from the Digitise App Server in the normal way.

     For deployment purposes the Digitise Apps Client is the same as enterprise Digitise apps and requires your Enterprise Program Distribution Certificate and will need its own Provisioning Profile, also obtained from the Apple Developer Enterprise Program web site. You will need to upload your Distribution Certificate and the Provisioning Profile to the remote NDL-hosted Digitise Apps Build System, which can then be used to build and sign a version of the Client specific to your organisation. Digitise Apps' App Studio design utility allows you to upload Certificates and Provisioning Profiles and request a Digitise Apps Client build. The Client will be supplied as an Apple install package which can be downloaded from the Build System to your PC from within App Studio.

2.   A deployment version to be used when deploying Digitise apps to your users.

     To comply with Apple's prohibition on the downloading of code to devices, in order to deploy Digitise apps to your users, the apps have to be converted into Digitise Apps Standalone Apps which can be downloaded and installed to your users' devices over the air, via a USB connection or via the App Store. Users cannot download or update Digitise apps directly from the App Server as you can with the standard Digitise Apps Client.

     Each Standalone App bundles the deployment version of the Digitise Apps Client with one or more Digitise app Models. The deployment Client cannot download Digitise apps nor can it download subsequent updates to the Models contained within a Standalone App.

You can create as many Standalone Apps as you like and download multiple Standalone Apps to a single device.

Each Standalone App has to be signed with an appropriate Distribution Certificate and linked to a Provisioning Profile (see below for more details).

Standalone Apps, both enterprise and store varieties, are generated from within App Studio using the remote NDL-hosted Digitise Apps Build System. As with the standard Digitise Apps Client for iOS devices, before you can create a Standalone App, you will need to upload the appropriate Distribution Certificate(s) and Provisioning Profile(s) to the Build System from App Studio. You can then configure and submit a request for a Standalone App from App Studio. The Standalone App will be provided as an Apple install package which, when completed, can be downloaded in App Studio.

IMPORTANT:	Because of Apple's terms and conditions, you can only use the standard Digitise Apps Client to test your Digitise apps on your development test devices during the development cycle. You must not give this version of the Client to your users, even for them to test your apps whilst in development. Nor can you submit the standard Client to the App Store.

For **enterprise** Standalone Apps, you will need to use a Distribution Certificate obtained from the Apple Developer Enterprise Program and each app will need its own Provisioning Profile linked to this Certificate, generated within the Apple Developer Enterprise Program web site.
For new members of the Apple Developer Enterprise Program, you will need to create a different Provisioning Profile for each Digitise Apps Client or Standalone App that you want to create. Until recently you could create a 'wildcard' Provisioning Profile which allowed you to use a single Provisioning Profile for all your individually developed apps but this facility has now been withdrawn by Apple and you need to create a separate Profile for each application. If you already have a wildcard Provisioning Profile, it appears that, at least for now, when you come to renew your Profile you will be allowed to continue with this Profile.

For **store** Standalone Apps, you will need to use a Distribution Certificate obtained from the Apple Developer Program and a Provisioning Profile linked to this certificate. Unlike the Enterprise Program, the Developer Program still allows you to create wildcard Certificates and Provisioning Profiles, which means you can use the same Certificate and Provisioning Profile pair to sign multiple apps. If you prefer, however, you can create separate Provisioning Profiles for each app.

A Provisioning Profile only lasts a year, and you will need to renew it annually. For enterprise apps, after renewing a Provisioning Profile, you can either provide an update to the complete app or you can simply distribute the new

Profile which will overwrite the existing version. The Profile can be updated over the air from a web site, using MDM software or via email. For store apps, you will need to rebuild your app and upload it to the Apple Store as an update.

Distribution Certificates last for three years (or earlier if you cease to be a member of the relevant Developer Program). At the end of this time apps signed with an expired Certificate will stop working unless you renew the relevant Certificate. Having obtained a new Certificate, you will need to rebuild any Digitise Apps Clients or Standalone Apps using your new Certificate and redistribute them to your developers and users in order for them to continue using Digitise Apps. You can have two Certificates active concurrently allowing you to obtain your new Certificate and upgrade your users before the original Certificate expires.

This document provides further details about obtaining a Distribution Certificate and Provisioning Profiles and provides an introduction to using Digitise Apps on Apple devices. For additional information refer to the Digitise Apps online help, available from within the App Studio and App Manager utilities.

Note: The information and instructions contained in this document are provided for guidance and are based on our understanding of the Apple Developer Enterprise Program at the time of writing. Apple may change this program and their processes at any time. Consequently, the instructions contained below may not always reflect the current situation. For up-to-date information refer to Apple's web site. You can also contact our Technical Support Team for advice using the contact details provided on the back page of this document.

Obtain a Distribution Certificate

A Distribution Certificate is used to sign apps you develop for use on Apple devices. They are provided by Apple through the Apple Developer web site for companies registered in the Apple Developer Enterprise Program or Apple Developer Program. A Distribution Certificate is required in order to distribute your apps to your users.

To create and deploy the standard Digitise Apps Client and **enterprise** Digitise Apps Standalone Apps, you will need a Distribution Certificate from the Apple Developer Enterprise Program. These Certificates only allow distribution of applications to devices used by **employees** of the company.

To create and deploy Digitise Apps **store** Standalone Apps, you will need a Distribution Certificate from the Apple Developer Program. These Certificates allow you to distribute apps via the Apple App Store.

When a Distribution Certificate expires, applications created using it will no longer run. Distribution Certificates are valid for three years from date of issue, or until your Developer Program membership expires, whichever comes first.

Likewise, revoking a Distribution Certificate will cause your apps signed with that certificate to fail on any installed devices. You can create a new Distribution Certificate up to six months before the existing Certificate expires. The overlapping Certificate allows you to upgrade your users before your current Certificate expires.

The following instructions describe how to obtain a Distribution Certificate from the Apple Developer Enterprise Program. A similar process should be followed to obtain a Distribution Certificate from the Apple Developer Program. Make sure you sign-in to the correct program before generating your Certificate.

To obtain a Distribution Certificate, you first need to generate a Certificate Signing Request (CSR) then log in to the Apple Developer web site and use the CSR to create the Certificate. You can then download the Certificate in the form of a *.cer* file. Finally, in order to use the Certificate with Digitise Apps, you will need to convert the *.cer* file to a PKCS#12 format that will contain your Private Key and Certificate in a password protected *.p12* file. You can leave the password blank but you will need to supply the password to the Digitise Apps Build System in order for it to extract the Certificate.

Note: The information and instructions contained in this section are provided for guidance and are based on our understanding of the Apple Developer Enterprise Program and Apple Developer Program at the time of writing. Apple may change this program and their processes at any time. Consequently, the instructions contained below may not always reflect the current situation. For up-to-date information refer to Apple's web site. You can also contact our Technical Support Team using the contact details on the back page of this document.

To generate a Certificate Signing Request (CSR):

Generate a Certificate Signing Request on Mac OS

On Mac OS, you can use the Keychain Access application to generate a Certificate Signing Request. The Keychain Access application is in the *Utilities* subfolder of the *Applications* folder. The following picture provides instructions for generating the Certificate Signing Request as shown on the Apple Developer web site during the Certificate generation process:
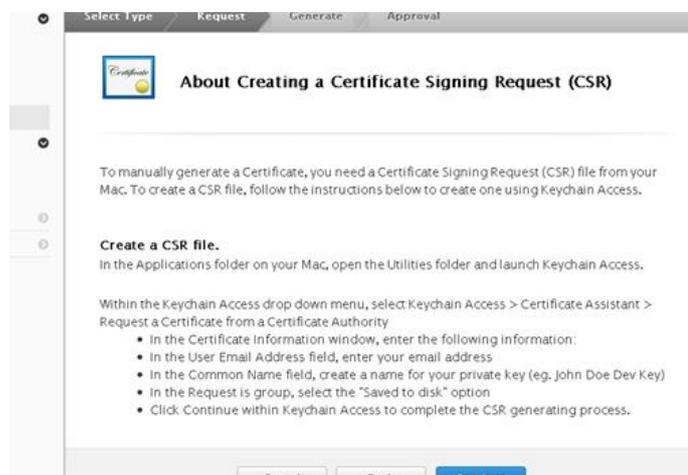
Instructions for Generating a CSR on Apple Mac Computers

Generate a Certificate Signing Request on Windows

For Windows developers, if you don't have access to a Mac computer it is possible to obtain a Certificate on a Windows computer. First, you will need to create the Certificate Signing Request (a CSR file) using OpenSSL:

i.   Install OpenSSL on your Windows computer (from *http://wiki.openssl.org/index.php/Binaries*).

ii.   Open a Windows Command Prompt, and CD to the OpenSSL bin folder (such as *c:\OpenSSL\bin*).

iii. Create a private key by entering the following in the command line:

openssl genrsa -out *mykey***.key 2048**

You can give the key file a name of your choice by substituting *mykey* with the required name. Save the private key file created as you will need to use it later to convert the Certificate file.

When using OpenSSL, do not ignore error messages. If OpenSSL generates an error message, it may still output files. However, those files may not be usable. If you see any errors, check your syntax and run the command again.

> **Note:**   If you get the following error:
>
>   **Warning: can't open config file: /usr/local/ssl/openssl.cnf**
>
> this means that a required configuration file is missing. To resolve the issue, you need to create the missing file. Within your Command Prompt, change back to the OpenSSL bin folder, if you are no longer there, and type:
>
>   **set OPENSSL_CONF=***<bin folder path>***\openssl.cnf**
>
> Then try recreating the private key as before.

iv. Create the CSR file by entering the following in the command line:

openssl req -new -key *mykey***.key -out CertificateSigningRequest.certSigningRequest**
-subj "/emailAddress=*youraddress@example.com* **/CN=***My Company*
/C=GB"

where:

- *mykey***.key** is the name of the private key file you created earlier,
- *youraddress@example.com* should be replaced with the required email address,
- **/CN=***My Company* should indicate the name you want to give to the Certificate. We suggest you replace *My Company* with the same organisational name as used to register on the Apple Developer Enterprise Program

and

- you may also need to change the country parameter, *C=GB*, if you are not within Great Britain, e.g. in the USA substitute **C=US**.

Having generated a CSR, you can then use it to create a Distribution Certificate:

1. Load a browser and open the Apple Developer web site using the following address:

   http://developer.apple.com/

2. Click on the link to the iOS Dev Centre.

3. Log in with the Agent or Admin role.

4. Navigate to *iOS Developer Program -> Certificates, Identifiers & Profiles*:
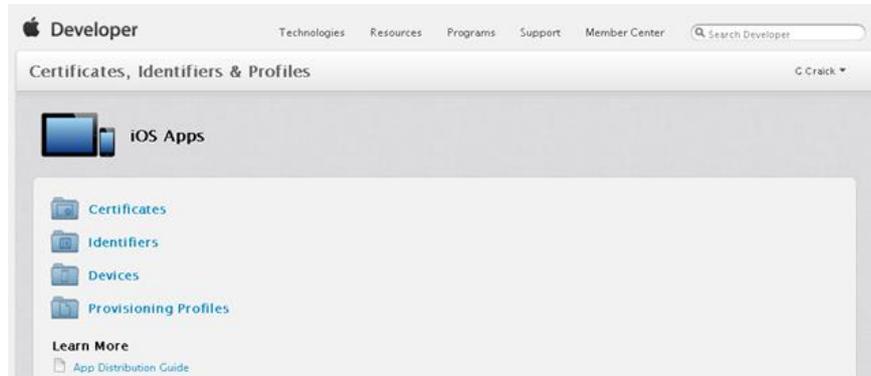
5. Click on *Certificates*.

6. Then in the left-hand panel, click *Certificates -> Production*:

7. To add a new Certificate, click on the ➕ in the top right-hand corner of the page.

    Remember you can only have two Distribution Certificates at any one time. This allows you to create a new Certificate before your current one expires in order to deploy an updated Certificate to your users before their apps stop working.

    Clicking the ➕ button, will display the following page:
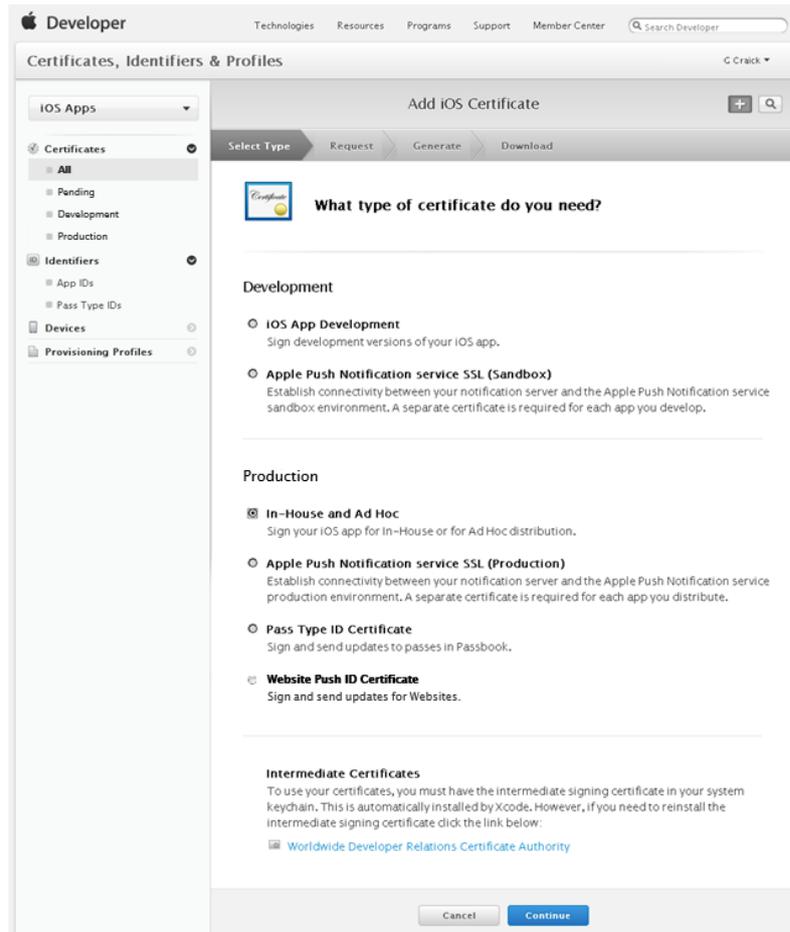
8. Select **In-House and Ad Hoc** in the Production section and then click on the **Continue** button.

9. The following page will be displayed:
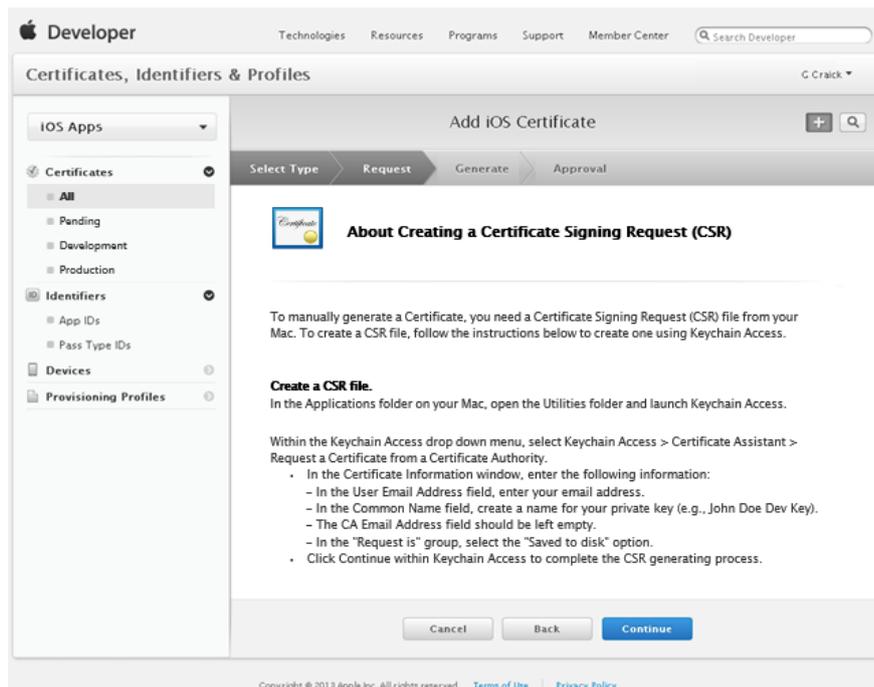
If you are running under Windows simply ignore this page and click **Continue**.

If you are running on a Mac computer, this page provides the information referred to earlier about creating a CSR. If you haven't already created your CSR, do so now. When your CSR file is ready, click **Continue**.

10. The following page will be displayed:
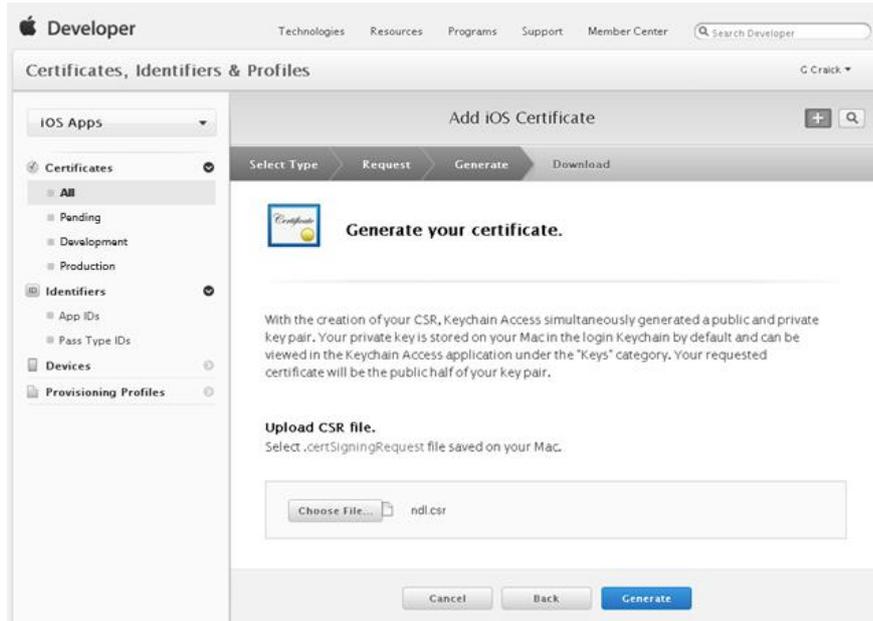
11. Click on **Choose File...** and then navigate to and select the CSR file that you created earlier.

12. Click on **Generate**.

13. Your Certificate will be created.

14. Click on **Certificates -> Production** in the left-hand menu bar to display a list of your Certificates:
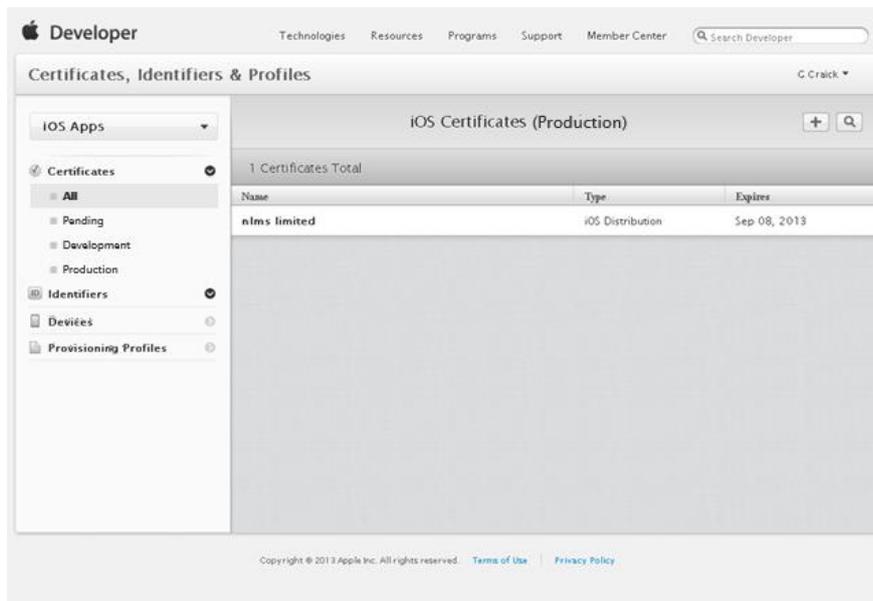
15. Click on the Certificate in the list to expand the entry and display the **Download** button. Choose the **Download** button and save your Distribution Certificate as a *.cer* file to your local machine.

You now need to convert the Certificate *.cer* file to a PKCS#12 format that will contain your Private Key and Certificate in a password protected *.p12* file.

To do this:

Convert a Distribution Certificate to a P12 file on Mac OS

Once you have downloaded the certificate from Apple, you will need to convert it to the P12 keystore format:

i.   Open the Keychain Access application (in the Applications/Utilities folder).

ii.   If you have not already added the Certificate to Keychain, select File -> Import. Then navigate to the Certificate file (the *.cer* file) you obtained from Apple.

iii.   Select the Keys category in Keychain Access.

iv.   Select the private key associated with your Certificate.
       The private key is identified by the iPhone Distribution: <Company Name> public certificate that is paired with it.

v.   Command-click the Certificate and select **Export "iPhone Distribution:** <company name>**"**.

vi.   Save your keystore in the Personal Information Exchange (P12) file format.

vii.   You will be prompted to create a password that is used when you use the keystore to sign applications or transfer the key and Certificate in this keystore to another keystore – make a note of this password, you will need it later.

Convert a Distribution Certificate to a P12 file on Windows

i.   Load a Windows Command Prompt, using **Run As Administrator**.

ii.   Within your Command Prompt, run the following command-line statement from the OpenSSL bin directory to convert the *.cer* file to a *.pem* file:

openssl x509 -in *apple_dist_cert.cer* **-inform DER -out** *apple_dist_cert.pem* **-outform PEM**

Replace *apple_dist_cert* with the name of the Certificate downloaded from the Apple Provisioning Portal.

iii.   You can now generate a P12 file based on the key and the PEM version of the Certificate just created:

openssl pkcs12 -export -inkey *mykey***.key -in** *apple_dist_cert***.pem -out** *apple_dist_cert***.p12**

Replace *mykey***.key** with the name of the private key generated previously and *apple_dist_cert* with the name of the Certificate downloaded from the Apple Provisioning Portal.

iv.   You will be prompted to enter a password during this process – make a note of this password as you will need to supply it to us in order to build your standard Digitise Apps Client and Standalone Apps.

Obtain a
Provisioning Profile

In addition to a Distribution Certificate, you also need Provisioning Profiles to be able to deploy the standard Digitise Apps Client to your test iOS devices and later to distribute your finished Digitise apps to your users' iOS devices.

The Provisioning Profile is obtained from Apple and takes the form of a file with the file extension: **.**_mobileprovision_ A Distribution Provisioning Profile consists of a Name, a Distribution Certificate, and an App ID. You will need to create a separate Provisioning Profile for your Digitise Apps Client and each of your enterprise Digitise Apps Standalone Apps. For Digitise Apps store apps, if you have generated a wildcard Distribution Certificate, you can generate a single Provisioning Profile and use it for all your store apps.

A Provisioning Profile is **only valid for one year** which means that apps built using a Profile have to be renewed each year. 2 months before the Profile expires, any iOS devices which have apps installed on them will display notification that the Profile is due to expire. If the Profile expires the apps will no longer run. Before the Profile expires you will need to create a new Provisioning Profile and update your users.

For the developer Digitise Apps Client and **enterprise** Digitise apps when updating a Provisioning Profile you can either rebuild the Client or enterprise Standalone App and re-download it to users' devices or you can update just the new Provisioning Profile _.mobileprovision_ file. You can download and install a full update using iTunes, MDM software or via a browser from a web site. You can download just the Profile using MDM software, via email or over the air from a web site.

For Digitise Apps **store** apps, when you renew your Provisioning Profile you will need to rebuild your apps and resubmit them to the App Store to upgrade existing users and allow them to continue using the apps.

> **Note:**   The information and instructions contained in this section are provided for guidance and are based on our understanding of the Apple Developer Enterprise Program and Apple Developer Program at the time of writing. Apple may change this program and their processes at any time. Consequently, the instructions contained below may not always reflect the current situation. For up-to-date information refer to Apple's web site. You can also contact our Technical Support Team using the contact details on the back page of this document.

Create a Distribution Provisioning Profile

The following instructions describe how to obtain a Distribution Provisioning Profile from the Apple Developer Enterprise Program. A similar process should be followed to obtain a Provisioning Profile from the Apple Developer Program. Make sure you sign-in to the correct program before generating your Provisioning Profile.

1. If you are already logged in to the Apple iOS Dev Centre on the Apple Developer web site, go straight to the next step.

    If you aren't already logged in, log in with the Agent or Admin role and then navigate to:

    iOS Developer Program -> Certificates, Identifiers & Profiles:
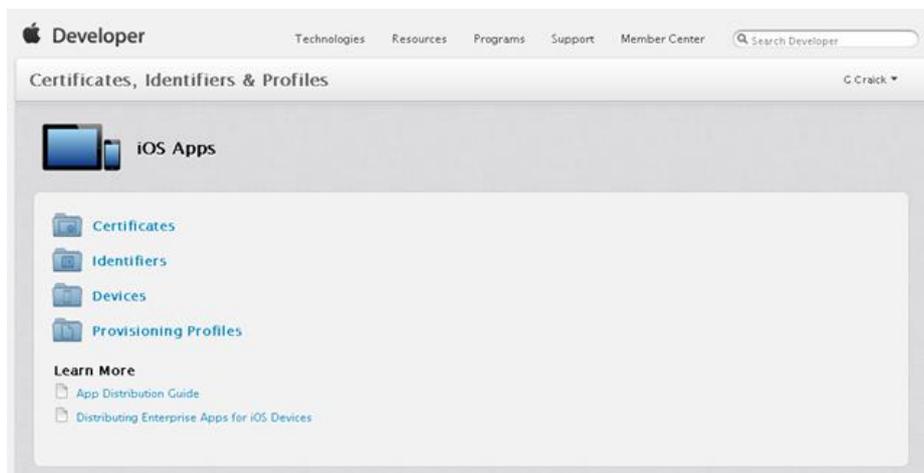
    Before you can create a Distribution Provisioning Profile, you will need to create an App ID for it, so click on ***Identifiers***.

2. On the Certificates, Identifiers and Profiles page, click ***Identifiers -> App IDs*** in the left-hand menu bar. The iOS App IDs list will be displayed:

3. To create a new App ID for your Provisioning Profile, click on the ⊞ in the top right-hand corner of the page.

4. The Register iOS App ID page will be displayed:
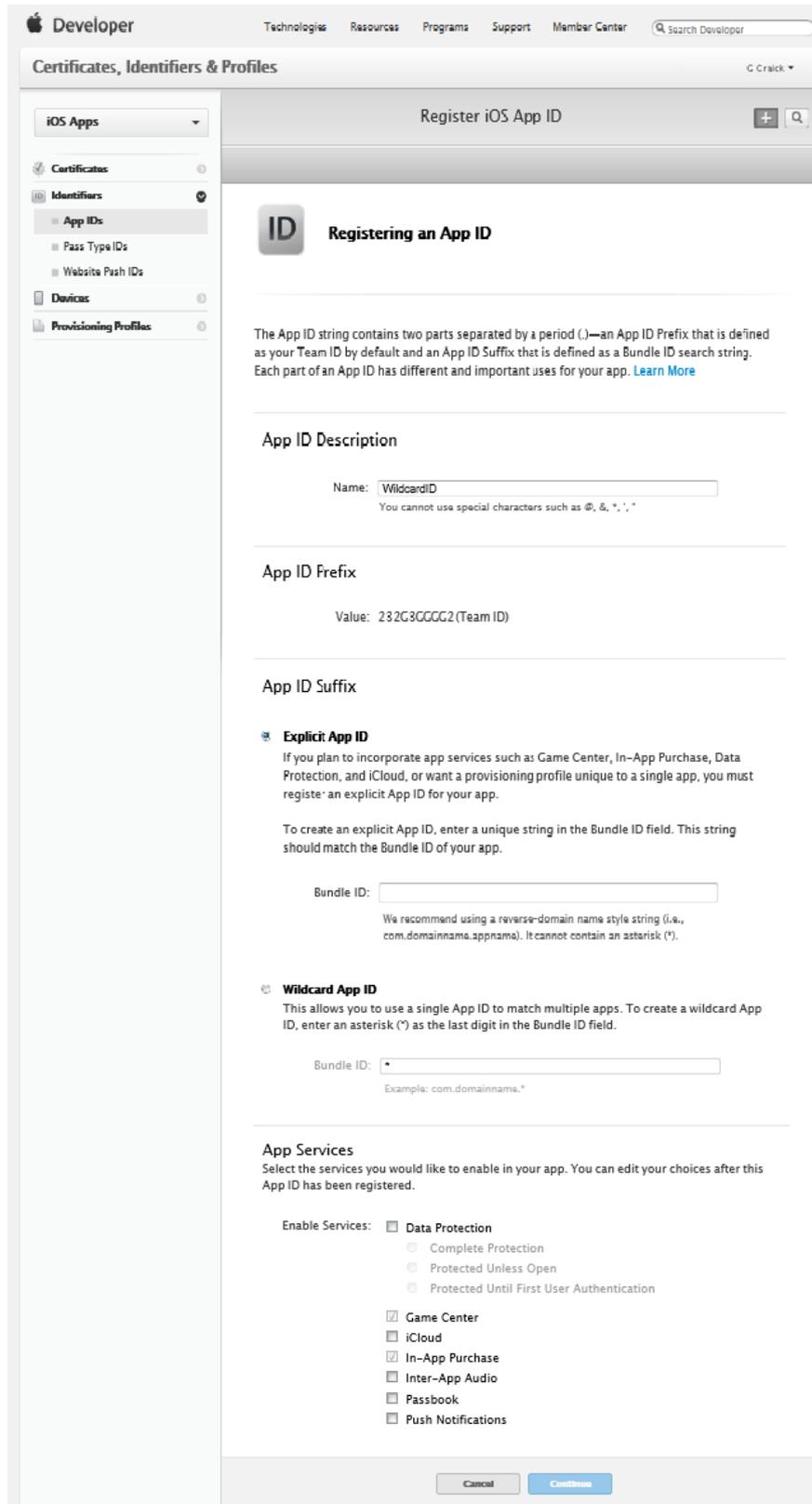
Enter a **Name** of your choice for this ID in the App ID Description section. The name you enter here will appear in the list of App IDs available to use for the Provisioning Profile later in the process, so enter a name here which will enable you to recognize the ID later.

As you need to create a separate Provisioning Profile for each Digitise Apps Client or Standalone App you want to build, select **Explicit App ID** under the **App ID Suffix** section.

5. Next you need to enter a **Bundle ID** for this Profile. This must match the Bundle ID which will be used by the Digitise Apps Build System for your Client or Standalone App Build and hence must take the following form:

App Type	Bundle ID Format
Digitise Apps Client	**ndl‑‑metascybe‑ltd.**customer_ID**.awiMX** where: customer_ID = the name of your organisation as registered with the Build System. Your Build System registration acknowledgement email includes your organisation's name as it is registered on the system. You must remove any spaces and any other none alpha-numeric characters other than '-' and '_'.
Standalone Apps	**ndl‑‑metascybe‑ltd.**customer_ID**.**app_name where: customer_ID = the name of your organisation as it is registered with the Build System. Your Build System registration acknowledgement email includes your organisation's name as it is registered on the system. You must remove any spaces and any other none alpha-numeric characters other than '-' and '_'. app_name = the name of your Standalone App minus any spaces and any other none alpha-numeric characters other than '-' and '_'. This is the name you specify in the Build request dialog box within App Studio for this Standalone App.

6. If you want to include the ability to receive push notifications within your Digitise Apps Client or app, select **Push Notifications** under **App Services**.

> **Note:** If you want to include the ability to receive push notifications within your Digitise apps, you cannot use wildcard Distribution Certificates or Provisioning Profiles and you must obtain separate Provisioning Profiles for each app. The Provisioning Profile must have push notification support included here within the Profile so that the notification service, which will send out the notifications, can identify the exact app to which a message should be sent.

7.   Click **Continue**.

8.   You will then be prompted to confirm the details:
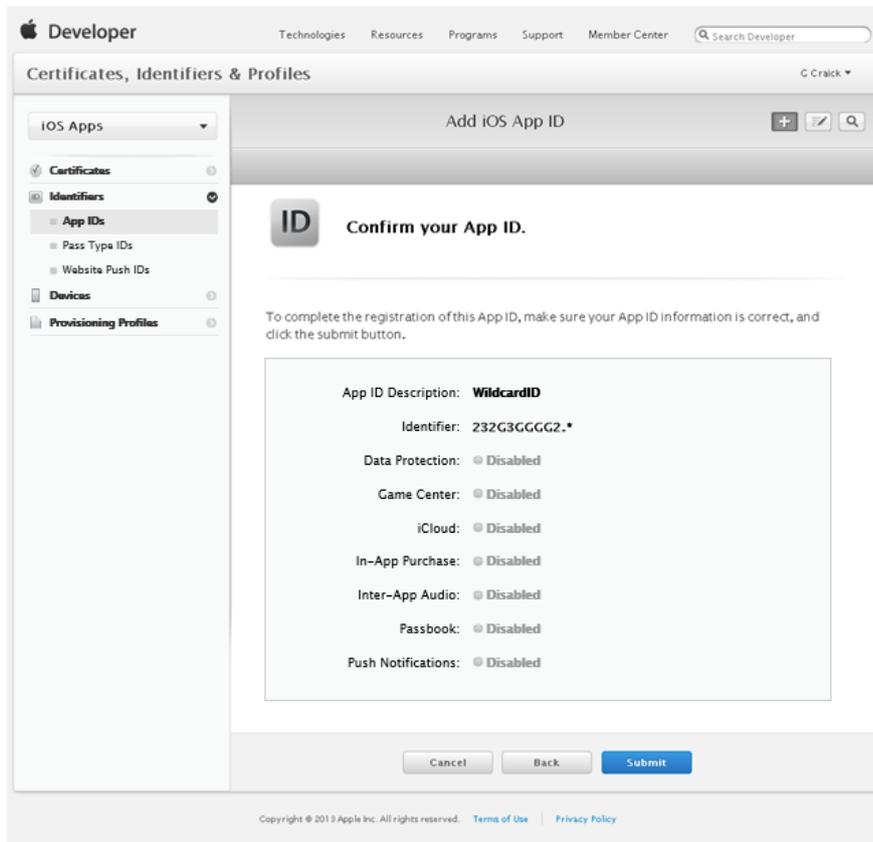
Choose **Submit** to create your App ID.

You can now create your **Distribution Provisioning Profile**.

9.   Click **Provisioning Profiles -> Distribution** in the menu bar on the left of the iOS App IDs page. The iOS Provisioning Profiles (Distribution) page will be displayed:
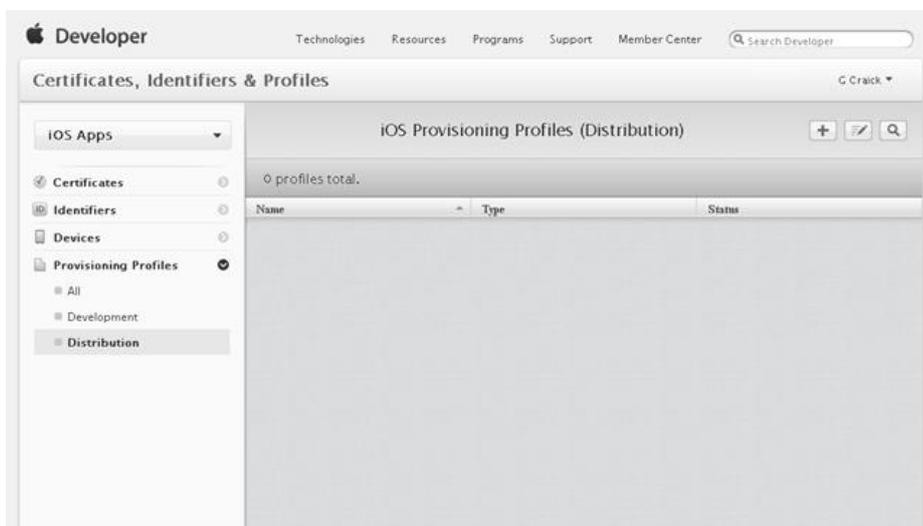
10. Click on [+] to add a new Profile:
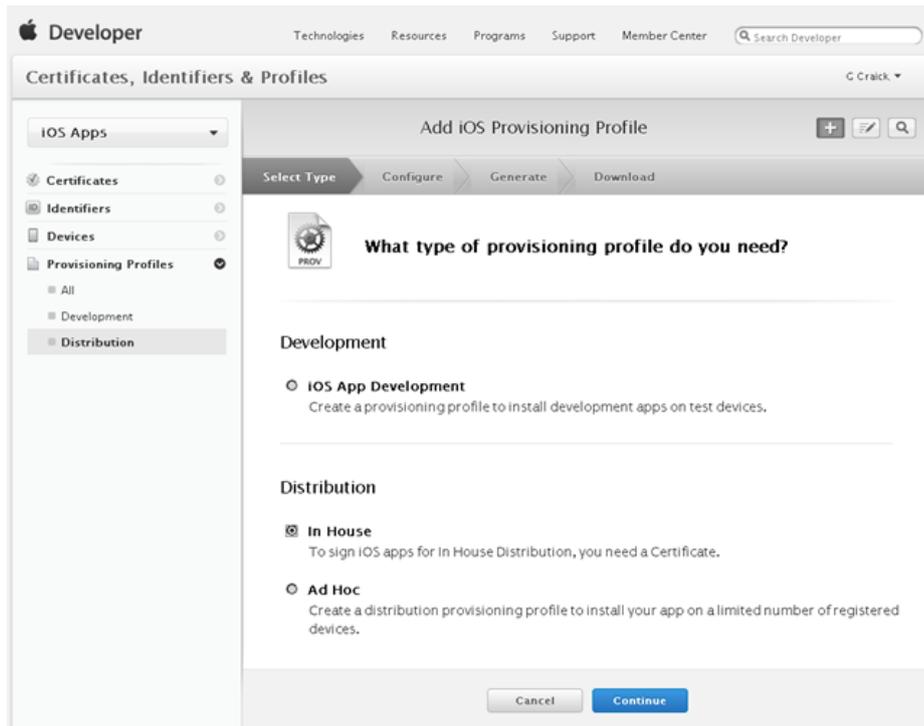
Select **In House** in the **Distribution** section and then click **Continue**.

11. You will now be prompted to select the App ID you created earlier:
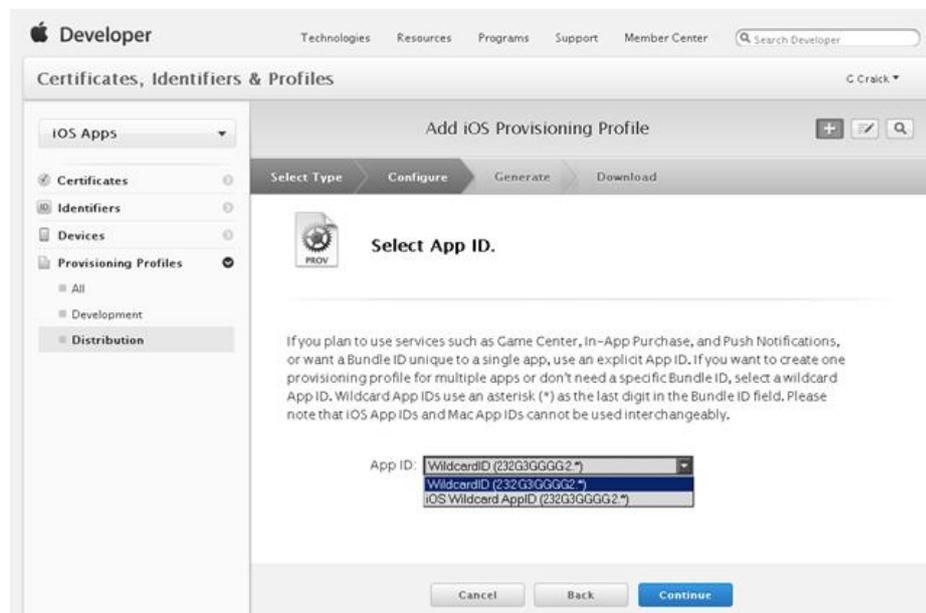
Select your ID from the drop-down list – this is the Name you entered in step 4 above.

Click **Continue**.

12. Next you need to select your Distribution Certificate:
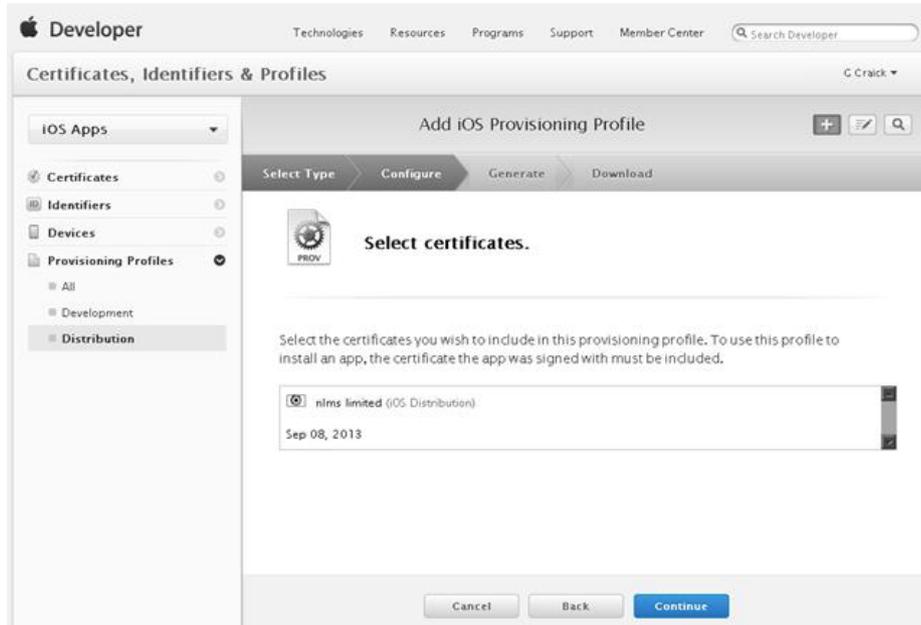
Check that your Certificate is listed and labelled **iOS Distribution**. If it is, select it and then click **Continue**.

13. The next step is to provide a name for your Provisioning Profile.

This name will appear in the Profile on your iOS device when an app that has been provisioned with this Profile has been installed (under Settings -> General -> Profile).

Enter a Profile Name of your choice. We recommend that you choose a name which easily identifies the purpose of this Profile, e.g. the Digitise app with which it will be used, and the date that the Profile will expire.

Click **Generate**.
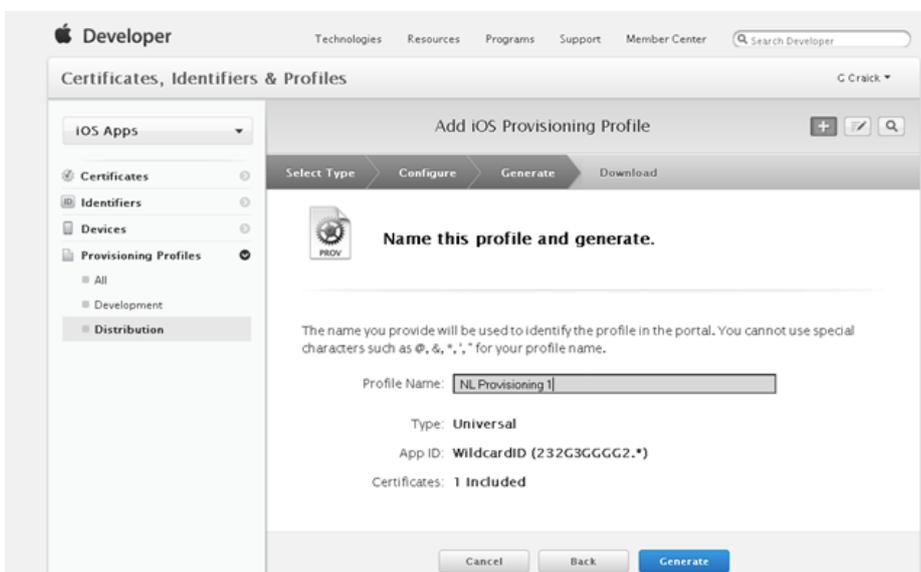
Your new Provisioning Profile will be generated.

14. You can display the list of your current Provisioning Profiles by selecting **Provisioning Profiles ->
Distribution** in the left-hand menu bar.

Clicking on a Provisioning Profile in the list should expand the entry to display more details and various
buttons, including a **Download** button:

15. Click on your Provisioning Profile and then choose the **Download** button to download the Certificate
and save it to a file on your local computer. The file extension should be *.mobileprovision*.

Create a
Development Digitise Apps Client

Developers can use a version of the standard Digitise Apps Client on their test iOS devices, to make developing and testing Digitise apps quicker and easier. The Digitise Apps Client allows you to download Digitise apps from a development test App Server running on a developer's own PC and to update these apps directly from the App Server. This allows your developers to quickly test new apps and updates during development.

You will need to generate your own version of the Client, signed with your Distribution Certificate and linked to a Provisioning Profile you have obtained from the Apple Developer Enterprise Program web site. This can be done from a developer's PC using the automated remote NDL-hosted Digitise Apps Build System.
Consequently, before you can generate a version of the Client you will need to obtain a Distribution Certificate and create a Provisioning Profile from it for use with the Client. You will also need to register to use the Digitise Apps Build System. You can register by contacting our Technical Support Team using the contact details on the back page of this document.

Having obtained the Certificate and Provisioning Profile, as described earlier in this document, you will need to upload these to the Digitise Apps Build System using App Studio, the Digitise Apps app design utility. App Studio includes the facility to build a pre-configured version of the Client, which you can use to generate a version of the Client for your iOS developer devices. App Studio communicates with the remote Build System over a secure SSL Internet connection.
The Build System queues requests for Client builds and will email you when the build starts and completes using the email address supplied when you register to use the Build System. When the Client is ready, you can download it to your PC from within App Studio.

The Client will be supplied as two files, an archive file (*.ipa*) and a manifest file (*.plist*) allowing you to install the Client on your test iOS devices using MDM software, over the air or via a USB connection.

The Provisioning Profile lasts for a year and will need to be renewed annually. You then need to update each device using the Client with the new Profile. You can do this by downloading the new Profile to devices or by creating a new version of the Client and re-installing it. The Profile can be deployed using the same methods as the original Client.

The Distribution Certificate lasts for three years, after which it, too, will need to be renewed. You will then need to rebuild your Client with the new Certificate and re-install it on each device.

Note: Remember the standard Digitise Apps Client can only be used on developer's test devices during development. Under Apple's terms and conditions, you cannot install the Client on user devices even for testing purposes.

Deploy Digitise apps to Users

When you are ready to distribute a Digitise app to your users, you will need to convert it into a Digitise Apps Standalone App which can then be downloaded and installed on users' devices.

A Standalone App combines a version of the Digitise Apps Client with one or more Digitise apps into a single package. The app has to be signed with a Distribution Certificate and linked to a Provisioning Profile created for this app. Standalone Apps can be created using the remote NDL-hosted Digitise Apps Build System.

If you have built a development Digitise Apps Client for your developers, you will already have obtained an Enterprise Distribution Certificate which can also be used to sign any enterprise Digitise apps you want to create and you will already be registered to use the Digitise Apps Build System. If you haven't done this, refer to the previous section for details. If you want to create enterprise Digitise apps, you will also need to generate a separate Provisioning Profile on the Apple Developer Enterprise web site, as described earlier in this document, for each new Standalone App that you want to create (unless you have an existing wildcard Profile).

If you want to create Digitise Apps store apps, you need a different Distribution Certificate than that used to build the developer Digitise Apps Client and enterprise Digitise Apps Standalone Apps. You will need to generate this Distribution Certificate from the Apple Developer Program web site, rather than the Apple Developer Enterprise Program, if you haven't already done so. You will also need to create a Provisioning Profile for your apps. If you create a wildcard Distribution Certificate, you can create a single Provisioning Profile and use the same one for all your apps. If you don't have a wildcard Certificate, you will need to generate a separate Provisioning Profile, linked to your Distribution Certificate, for each store Standalone App. Refer to the earlier sections in this document for information about creating a Distribution Certificate and Provisioning Profile(s).

You will need to upload the relevant Distribution Certificate and associated Provisioning Profile(s) to the Digitise Apps Build System before you can generate a Standalone App. You only need to upload an individual Certificate or Provisioning Profile once, after which it can be used by any Digitise Apps developer registered with the Digitise Apps Build System as a member of your organization.

Your developers can upload Distribution Certificates and Provisioning Profiles and generate Standalone Apps, both enterprise and store versions, from within App Studio, the Digitise Apps app design utility. App Studio communicates with the remote Digitise Apps Build System over a secure SSL Internet connection.

When you request a Standalone App build, you will need to specify whether you want to build an enterprise or store version of the app.

The Build System queues requests for Standalone App builds and will email you when the build starts and completes using the email address supplied when you register to use the Build System. When the Standalone App is ready, you can download it to your PC from within App Studio.

Both types of Standalone App are supplied as two files, an archive file (*.ipa*) and a manifest file (*.plist*). Enterprise apps can be installed on your users' iOS devices using MDM software, over the air or via a USB connection. Store apps need to be uploaded to the Apple App Store, from where they can be downloaded to your users' devices.

The Provisioning Profile lasts for a year and will need to be renewed annually. You then need to update the Profile on each device which runs a Digitise app linked to that Profile. For enterprise Digitise apps, as long as your Distribution Certificate is still valid, you can do this by rebuilding the Standalone App or just updating the Profile. The Profile can be deployed using the same methods as Standalone Apps. For store Digitise apps, you will need to rebuild your apps with the new Profile and re-submit them to the App Store, from where they can be downloaded by your users and re-installed.

The Distribution Certificate lasts for three years, after which it, too, will need to be renewed. You will then need to rebuild your Standalone Apps with the new Certificate and re-install them on each device.

Once on a device, both enterprise and store versions behave the same way. Digitise apps are run by a version of the Digitise Apps Client, just as they are on other platforms. However, as the iOS version of the Client is not allowed to download applications or updates directly from the Digitise App Server it consequently does not have this facility included.

You can create individual Standalone Apps for each of your Digitise apps or you can combine multiple apps into one Standalone App. Users can download and run as many Standalone Apps as required, depending upon the resources available on their device. You can also set up access rights for each Digitise app using the App Manager utility.

> **Note:** You can call one Digitise app from within another Digitise app using the Digitise Apps Scripting facility. In this situation you must include all called apps in the same Standalone App as the calling app; otherwise, the called apps will not run. When you configure the Standalone App before requesting a build, you can specify whether the Digitise Apps contained within the Standalone App should be available to users to run independently or whether they are only required to be called from another app.

If you create a Standalone App for a single Digitise app, when the user runs the Standalone App the Digitise app contained within it will automatically be loaded.

Where multiple Digitise apps are included in a single Standalone App and marked as available to users, the Standalone App's Home screen will list the user-available apps. The user can run an app from the list and return to the list at any time to run another app.

In either case the Standalone App can be configured to automatically log users in anonymously or to require users to login before using the app.

Note: After the first successful login, a user's Login credentials are stored (encrypted) on the device and when a user logs in, the login supplied will be compared against the cached details. If they don't match, and a connection is available, the Standalone App will attempt to authenticate the user with the App Server. Changes to the App Server's configuration, including access rights, are downloaded to a device the next time an app attempts to exchange data with the App Server.

Once you have deployed a Standalone App to your users, if you want to issue an update, you will need to recreate the Standalone App and users can then re-download it.