Developing UWP Digitise apps for Windows PCs and Tablets

Document Number: DevUWPAppsDA108-003
Issue 4 Effective: 11th September 2023

Contents

Overview

Note: The information and instructions contained in this document are provided for guidance and are based on our understanding at the time of writing of the requirements for deploying Universal Windows Platform apps to Windows PCs, laptops or tablets. These requirements and the processes we describe to fulfil them may change at any time for reasons over which we have no control. Consequently, the instructions contained below may not always reflect the current situation. For up-to-date information refer to Microsoft's web site. You can also contact our Technical Support Team using the contact details on the back page of this document.

Digitise Apps includes support for versions of its Client and Standalone Apps which target Microsoft's Universal Windows Platform (UWP). This document provides information specific to the development and deployment of Digitise apps targeting this platform.

For additional information about using Digitise Apps refer to the Digitise online help.

UWP versions of the Digitise Apps Client and Standalone Apps run under Windows 10 and Windows 11 and can be installed either by sideloading them to your devices, i.e. they are downloaded and installed directly to the device, or via the Microsoft app Store. In this document, we will refer to apps which will be sideloaded to devices as '**enterprise**' apps and those which will be downloaded from Microsoft's Store as '**store**' apps.

Note that if you want to upload apps to the Microsoft app Store, you will need a Windows Developer Account, for which Microsoft charge a nominal fee.

UWP apps must be code signed with a security Certificate, which validates them as coming from a known publisher. This means that the Digitise Apps Windows Universal Client and Digitise Apps Windows Universal Standalone Apps have to be code signed with an appropriate Certificate. If you will be downloading Digitise apps from within the standard Digitise Apps Universal Client, you do not need to code sign the apps; only the Digitise Apps Client needs to be signed.

For signing Digitise Apps Universal Clients and **enterprise** Digitise Apps Universal Standalone Apps you can use either a self-signed Certificate or obtain a trusted Certificate from one of the commercial or non-profit Certificate Authorities, such as GoDaddy or CACert. You will also need to install the Certificate on each device that will run a Digitise Apps Client or app signed with that Certificate.

For **store** Universal Standalone Apps, you can just use a self-signed certificate, you don't need a trusted certificate from one of the Certificate Authorities, and you don't need to install the Certificate on individual devices.

Digitise Apps is supplied with a default Certificate, self-signed by NDL, and a version of the Universal Client signed with this Certificate. You can use the supplied Universal Client to distribute the standard Client to your developers and users and use the Certificate to produce your own pre-configured versions of the Universal Client and to create enterprise Universal Standalone Apps.

Alternatively, instead of using our Certificate, you may prefer to create or obtain your own Certificate. Once you have a Certificate you can use it to sign both the standard Universal Client and enterprise Universal Standalone Apps.

For store Digitise apps, we recommend you create your own self-signed Certificate, which is slightly different to the self-signed Certificate you can use to sign enterprise apps, and use that to sign all your store apps.

A Certificate has a life span specified when the Certificate is created. When the Certificate expires, you will need to renew it, to continue signing with it. Apps which were signed with your expiring Certificate and which have already been installed will continue to run when the Certificate expires but for installations the Certificate must be valid at the time of installing. If your certificate expires you will need to rebuild any Digitise Apps Universal Clients and Digitise Apps Universal Standalone Apps signed with the expiring Certificate, if you will want to install or re-install them after the expiry date.

The supplied NDL Certificate has a life span of approximately 100 years and so is unlikely to need renewing. If you create your own self-signed Certificate, you can choose when you want it to expire. Certificates obtained from a Certificate Authority generally have a much shorter life.

If you want to sign a standard Universal Client or enterprise Universal Standalone App with your own Certificate or with the NDL Certificate, you can build a Client or app from within App Studio.

Likewise, when creating store apps, you can build the app and sign it with a specified Certificate from within App Studio.

Building Clients and Standalone Apps in App Studio uses a remote automated Build System hosted by NDL and requires an Internet connection on the development PC running App Studio. Files are sent to and from the Digitise Apps Build System using a secure SSL connection.

When you request a build of a Client or Standalone App in App Studio, App Studio will send the required files to the remote Build System. Once your Client or app has been built, the Build System will notify you by email and you can download the completed installation package from within App Studio.

If you have your own Certificate, one member of your organisation uploads it to the Build System from where it will be available to other members of your organisation, so you don't have to submit it every time you request a build. The NDL Certificate will be available to all Digitise Apps users by default and so if you don't want to use your own Certificate you can always use the NDL Certificate instead. You can use the same Certificate to sign all your Digitise Apps Clients and enterprise Standalone Apps, you don't need to create a separate Certificate for each one.

If you use your own Certificate you will need to obtain a new Certificate before your current one expires and update the Build System with the new Certificate. App Studio will show you the date on which your current Certificate expires.

Signed versions of the Client and enterprise Standalone Apps can be downloaded to devices in a variety of ways, e.g. you can copy the install file directly to the device, use a Mobile Device Management system (MDM), download from an internal web site, deploy by e-mail or download from a Company Hub app.

Signed versions of store apps are downloaded to devices from the Microsoft app Store.

Create a Self-signed Code Signing Certificate

This section provides information about creating your own self-signed code signing Certificate that you can use to sign the Digitise Apps Universal Client and Digitise Apps Universal Standalone Apps.

To create a self-signed certificate:

1. If you are generating a Certificate to sign **enterprise** apps, ignore this step and move to step 2.

   If you are generating a Certificate to sign **store** apps, before you can create your Certificate, you will need to create at least one app in the Microsoft Windows Partner Center Dashboard and reserve a name for the app. This will allow you to obtain your publisher identity, which you will need to include within the Certificate. This identity is linked to the Microsoft account you use to login to the Windows Partner Center and if you add all your apps to the Store using the same account, will be the same for all your apps. This means that you can use the same Certificate to code sign all your store Digitise Apps Windows Universal Standalone Apps.

   To obtain your publisher identity from the Windows Partner Center:

   i. Load a browser and navigate to the Windows Partner Center Dashboard.

   ii. Select the app you previously registered on the Partner Center.

   iii. Choose **App management -> App identity** from the left-hand menu.

   iv. Locate the value for **Package/Identity/Publisher**. This will be a GUID in the form:

   CN= XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

   You will need to include this GUID in the Subject field when requesting your Certificate.

2. Run Windows Powershell as Administrator (i.e. with elevated privileges).

3. Enter the following command (as a single line):

For enterprise apps:

```
New-SelfSignedCertificate -Type CodeSigningCert
          -Subject "CN=<companyname>"   -Confirm
          -NotAfter (Get-Date).AddYears(<years>) -KeyUsage "None"
          -TextExtension @("2.5.29.19={text}")
```

where <*companyname*> should be replaced by the name of your organisation as you want it to appear within the Certificate and <*years*> is the number of years you want the certificate to be valid for e.g. for a 10 year Certificate you might enter the following command:

```
New-SelfSignedCertificate -Type CodeSigningCert
          -Subject "CN=MyCompany Ltd." -Confirm
          -NotAfter (Get-Date).AddYears(10) -KeyUsage "None"
          -TextExtension @("2.5.29.19={text}")
```

For store apps:

```
New-SelfSignedCertificate -Type CodeSigningCert
          -Subject "CN=<publisheridentityGUID>" -Confirm
          -NotAfter (Get-Date).AddYears(<years>) -KeyUsage "None"
          -TextExtension @("2.5.29.19={text}")
```

where <*publisheridentityGUID*> should be replaced by the GUID you obtained from the Windows Partner Center in the previous step, and <*years*> is the number of years you want the certificate to be valid for e.g. for a 10 year Certificate you might enter the following command:

```
New-SelfSignedCertificate -Type CodeSigningCert
          -Subject "CN= 11111111-2222-3333-4444-555555555555" -Confirm
          -NotAfter (Get-Date).AddYears(10) -KeyUsage "None"
          -TextExtension @("2.5.29.19={text}")
```

4. Type 'Y' when asked to confirm you want to create the certificate.
5. Your new certificate will be generated and added into the Local Computer Certificate store.
6. You now need to extract the Certificate from the Certificate store:
   i. Hit **Windows Key + R** to display a Windows run-box.
   ii. Enter: `mmc`

   and then click **OK**, to open the Microsoft Management Console.

   Click **Yes** if asked whether you want to allow the app to make changes to your device.
   iii. Choose **File -> Add/Remove Snap-in...** from the mmc console menus.

iv. Select **Certificates** from the **Available snap-ins** list on the left and then click **Add**.

v. When prompted, select **Computer account** and then click **Next**.

vi. Select **Local Computer** in the next dialog and then click **Finish**.

vii. Click **OK** in the **Add or Remove Snap-ins** dialog.

viii. In the tree on the left hand side of the MMC console, navigate to **Certificates -> Personal -> Certificates**.

ix. In the list on the right, locate and select the Certificate that you just created.

x. Right-click on the Certificate and then choose **All Tasks -> Export...** from the context menu displayed.

xi. Click **Next** in the Welcome dialog.

xii. Select **Yes, export the private key** in the Export Private Key dialog and click **Next**.

xiii. Ensure the **Export File Format** is set to **Personal Information Exchange (PFX)** and the **Include all certificates in the certification path is possible** is checked. Click **Next**.

xiv. The Security dialog will be displayed. Enter a password and confirm it – make a note of the password, you will need it when you add this Certificate to the Digitise Apps Build System. Click **Next**.

xv. Specify a filename for the certificate – make a note of the filename and the folder in which the file will be saved. Click **Next**.

xvi. Click **Finish**.

7. Once you have the '*.pfx*' file you will need to upload this to the Digitise Apps Build System in order to use it to create pre-configured Universal Clients and/or sign your Universal Standalone Apps. For details of how to do this refer to the Digitise Apps online help.

8. On devices which will run a Digitise Apps Client or **enterprise** Digitise Apps Standalone App, you will need to install the Certificate used to sign them before you can install the Client or app(s). If you have used the same Certificate to sign more than one Client and/or app, you only need to install the Certificate once on each device. After building a pre-configured Universal Client or enterprise Universal Standalone App, you can download the build from the Build System within App Studio. The download will include a copy of the Certificate with a '*.cer*' file extension. You can use this file to install the Certificate to Windows devices.

   On devices which will only download Digitise apps from the Microsoft Store, providing you have signed the apps with a self-signed Certificate, you do not need to install the Certificate separately on these devices.

Obtain a Trusted Code Signing Certificate

As an alternative to using an untrusted self-signed Certificate, you can obtain a trusted code signing Certificate from one of the Certificate Authorities, such as GoDaddy or CACert.

To do this:

1. Visit the Certificate Authority's web site and specify that you require a code signing certificate.
2. Enter the name of your organisation for the Subject field.
3. In addition, Microsoft also requires that the Certificate has the following attributes:
    i. The "Basic Constraints" extension must be either **Subject Type=End Entity** or unspecified.
    ii. The "Enhanced Key Usage" property must contain **Code Signing** and may also contain **Lifetime Signing**. Any other EKUs are prohibited.
    iii. The "KeyUsage" (KU) property must be either **Unset** or **DigitalSignature**.
4. Follow the instructions provided by the Certificate Authority to obtain your Certificate and, if necessary, create a '*.pfx*' file version.
5. Once you have the '*.pfx*' file you will need to upload this to the Digitise Apps Build System in order to use it to create pre-configured Universal Clients and/or sign your Universal Standalone Apps. For details of how to do this refer to the Digitise Apps online help.
6. When using a trusted code signing Certificate, you do not need to install the Certificate separately to your devices before you install your Digitise Apps Clients or Standalone Apps.

Install Digitise Apps Clients and Standalone Apps on Windows Devices

On Windows desktops and tablets, the Digitise Apps Universal Client and **enterprise** Universal Standalone Apps are 'sideloaded' to your devices, i.e. they are downloaded and installed directly to the device and not via the Windows app Store. They can be presented to your devices by copying them directly to the device, using a mobile device management system (MDM), via a secure web site, via e-mail or via a Company Hub app.

Before you can install a Universal Client or enterprise Standalone App on a device, you will need to configure the device to allow sideloading of apps. You may also need to install a copy of the Certificate, used to code sign the Client or Standalone Apps, to the device. After which you can then download and install your Client and Standalone Apps.

Store apps, on the other hand, are downloaded to a Windows desktop or tablet from the Microsoft app Store in the usual manner.

For more information about installing the Digitise Apps Universal Client and Universal Standalone Apps, refer to the Digitise Apps online help.

The Haybarn at Parkhill Walton Road Wetherby West Yorkshire LS22 5DZ

01937 543 500

Support: **01937 543 510**

support@ndl.co.uk