

PayNow_ApplePay 串接文件

V1.0.5(2020/07/01)

目錄

1. 介接準備說明	3
2. ApplePay 開發者前置作	4
2.1 建立商務帳號 (Create Merchant ID)	4
2.2 建立交易憑證 (Apple Pay Payment Processing Certificate)	7
2.3 建立商家憑證 (Apple Pay Merchant Identity Certificate)	9
2.4 商家 Domains (Merchant Domains)	11
3. ApplePay 信用卡串接說明	13
3.1 交易流程圖	13
3.2 商家頁面 ApplePay 串接	14
3.3 PayNow 商家驗證	20
4. APPLE 開發者帳號申請說明	21
4.1 ApplePay 開發者帳號註冊需求	21
4.2 開發者帳號申請流程	23
附錄 1. 商家驗證(後端)檢查碼	33
1.1 說明:	33
1.2 POST 時檢查碼組成:	33
1.3 回傳時檢查碼組成(僅成功呼叫, 失敗呼叫將以原 POST 值回傳)	34
附錄 2. SHA-256 C#範例	35
2.1 範例	35
附錄 3. 信用卡授權	36
3.1 說明	36
3.2 參數說明	36
附錄 4. 檢核碼系統串接	38
4.1 說明:	38
4.2 取得隨機檢查碼/取得加密金鑰(參數說明)	38
檢核碼使用的 AES256 加密(註 1 及註 2)key 及 IV 固定為下:	39
註 1、AES256 加密;	40
註 2、AES256 解密:	41
註 3、PassCode 產生範例:	42
註 4、TimeStr 時間戳格式:	42
註 5、加權檢核碼產生規則:	43
註 6、SHA256 雜湊加密字串:	45
註 7、SHA256 雜湊加密字串:	45

1. 介接準備說明

1.1 商店需有 APPLE 的開發者帳號(個人/公司)

1.2 使用開發者帳號完成開發者前置準備

1.3 將以下資料寄件至 service@paynow.com.tw 信箱

(1) PayNow 統編

(2) Apple Pay 的 MerchantID(merchant.xxx.xxx)

(3) 2-2 建立憑證開始需電洽 PayNow 02-2521-5088

1.4 商家需自行串接 三段程式

(1) APPLE PAY 的付款交易(Apple Pay JS)

(2) PayNow 商家驗證

(3) PayNow 金流授權

1.5 付款頁面，UI 設計需遵守 APPLE PAY 規範

1.6 Apple Pay 交易環境必須支援 TLS 1.2

1.7 Apple Pay 僅接受實體商品業者

2. ApplePay 開發者前置作

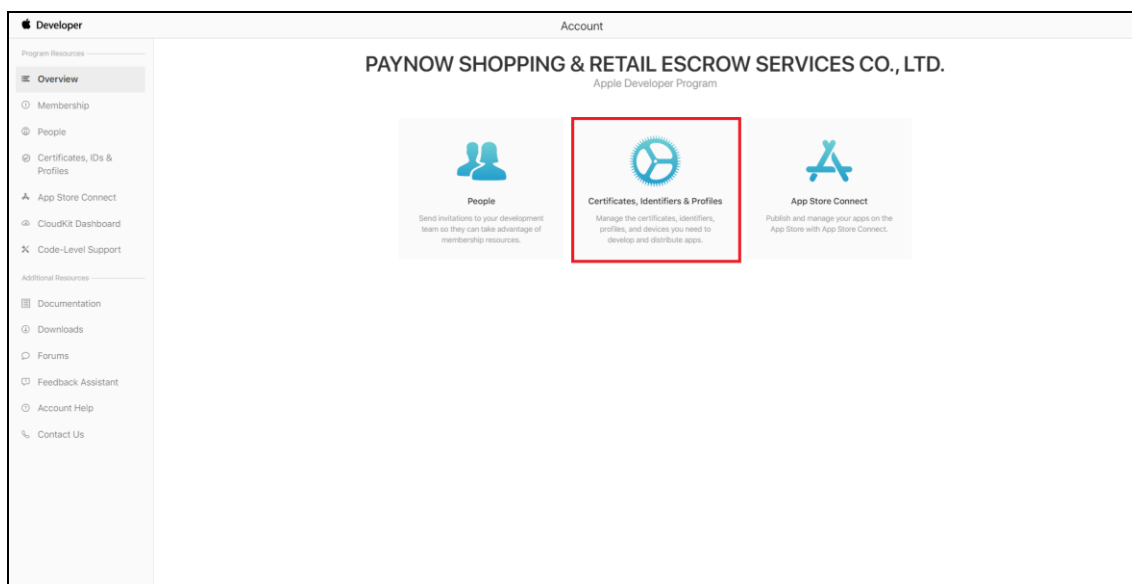
2.1 建立商務帳號 (Create Merchant ID)

(1) 登入至您的 Apple

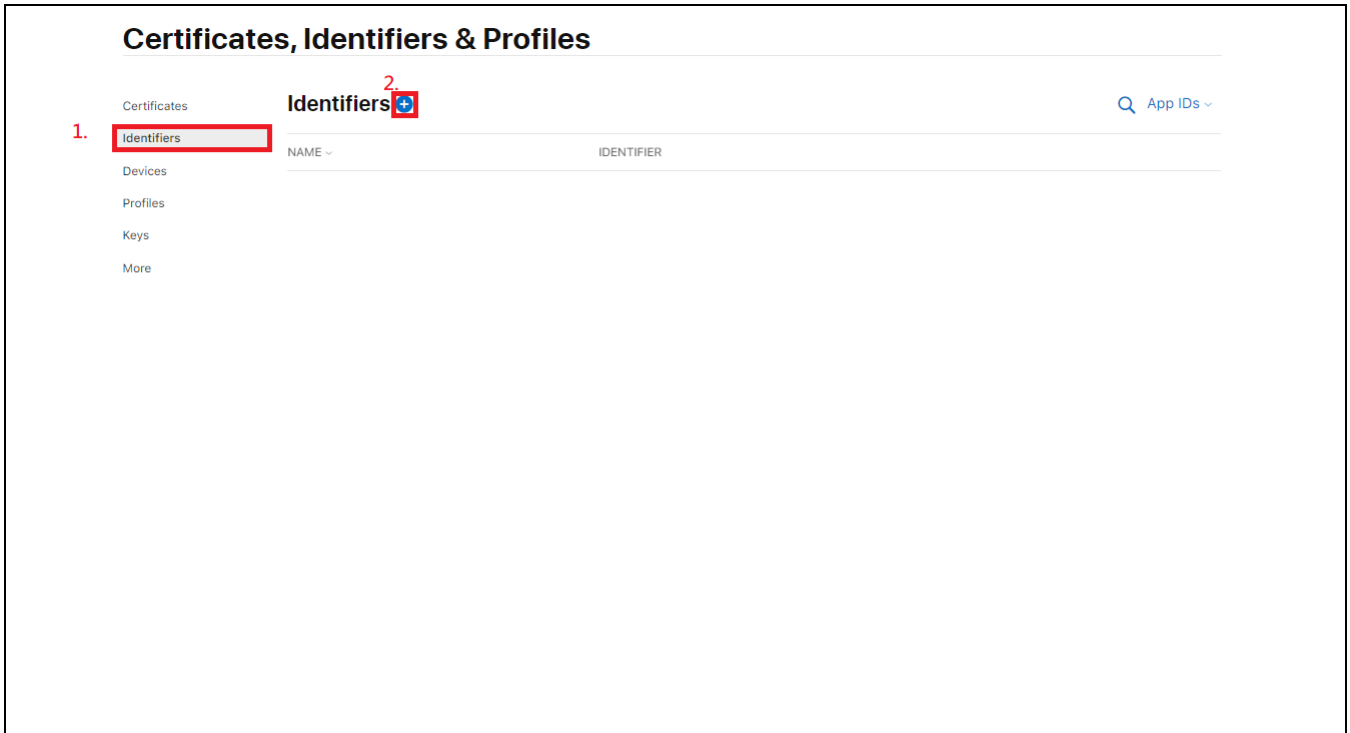
登入網址: <https://developer.apple.com/account/>



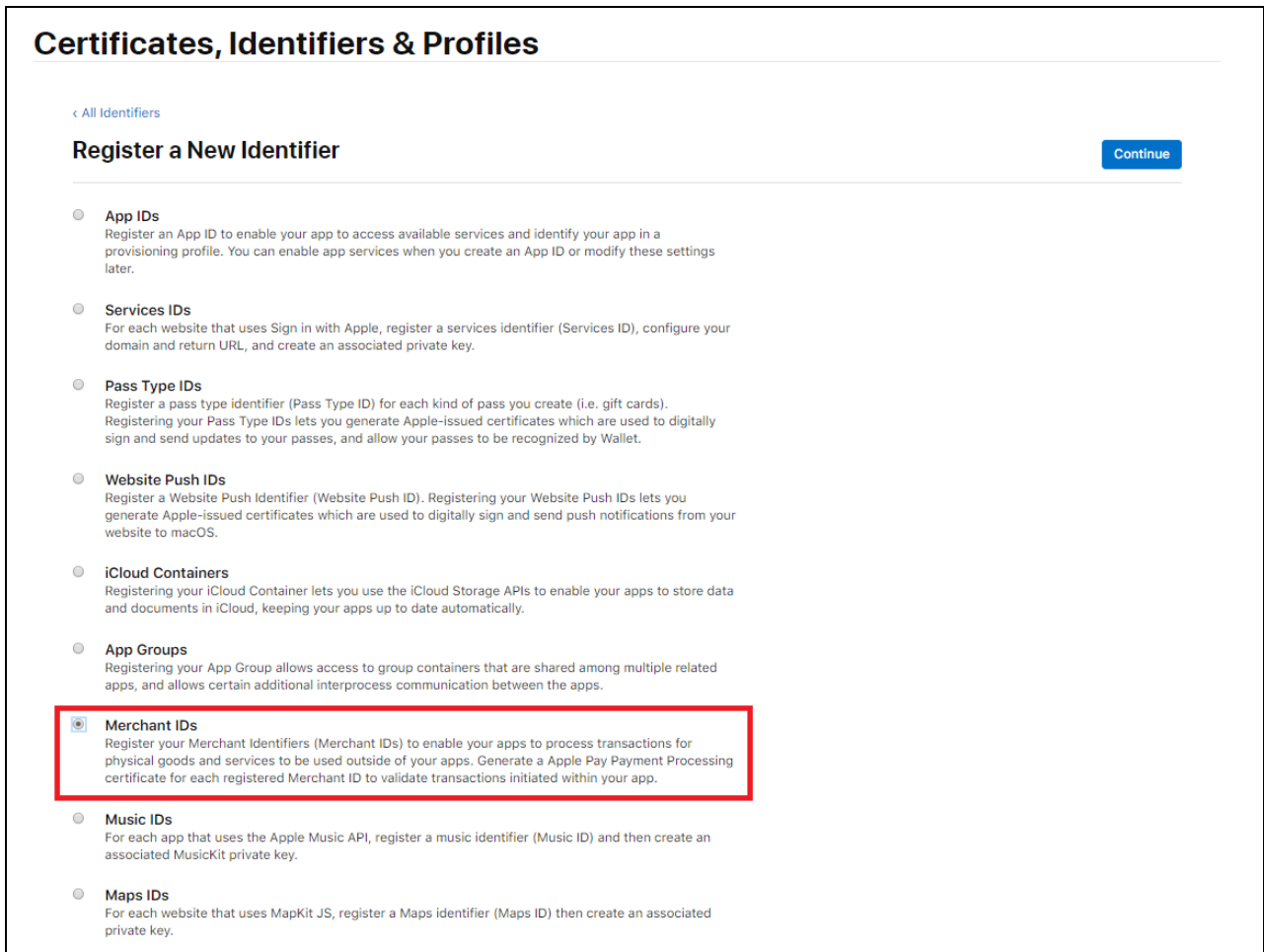
(2) 選擇 「Certificates, Identifiers & Profiles」



(3) 點選「Identifiers」並點選「+」號新增



(4) 點選「Merchant IDs」註冊商務資料



(5) 填入「Description」及「Identifiers」

Ps. 「Identifiers」建議填入 反序的 Domain，前面自動出現的「merchant.」為正常情況

Certificates, Identifiers & Profiles

< All Identifiers

Register a Merchant ID Back Continue

Description	Identifier
<input type="text" value="PayNow"/>	<input type="text" value="merchant.tw.com.paynow.mpay"/>

You cannot use special characters such as @, &, *, '."

We recommend using a reverse-domain name style string (i.e., com.domainname.appname).

(6) 點選 Register 完成註冊

Certificates, Identifiers & Profiles

< All Identifiers

Register a Merchant ID Back Register

Description	Identifier
PayNow	merchant.tw.com.paynow.mpay

以下步驟需聯絡 PayNow 客服 02-2521-5088，並將以下資料寄件至 service@paynow.com.tw 信箱

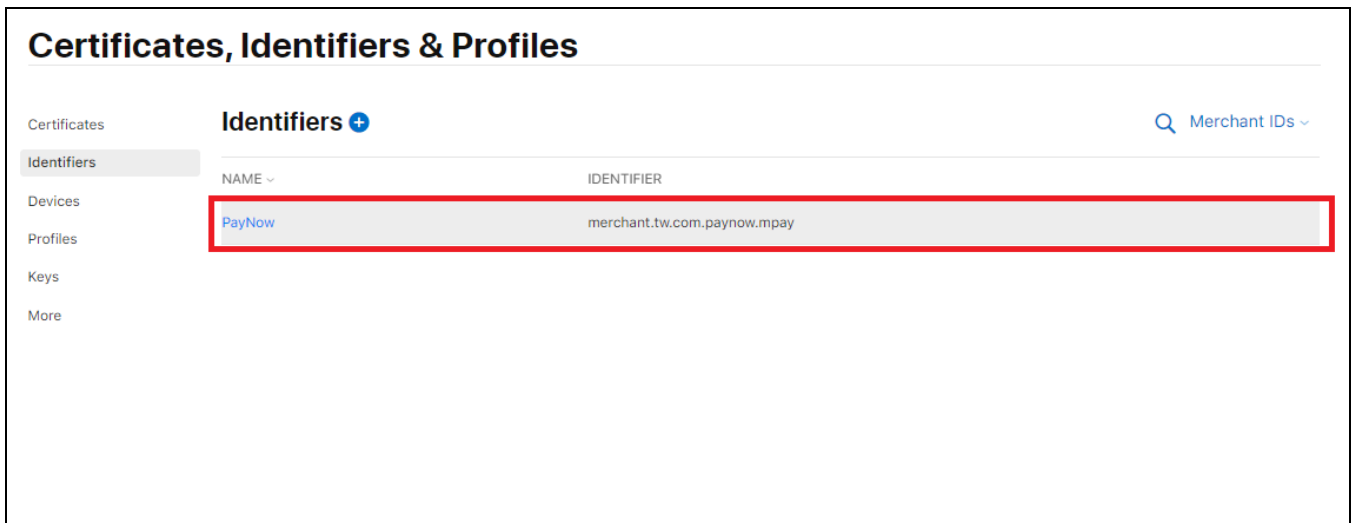
(1) PayNow 統編

(2) Apple Pay 的 MerchantID(merchant.xxx.xxx)

客服將給予一個檔案供商家建立交易憑證

2.2 建立交易憑證 (Apple Pay Payment Processing Certificate)

(1) 點選剛註冊好的 Merchant IDs

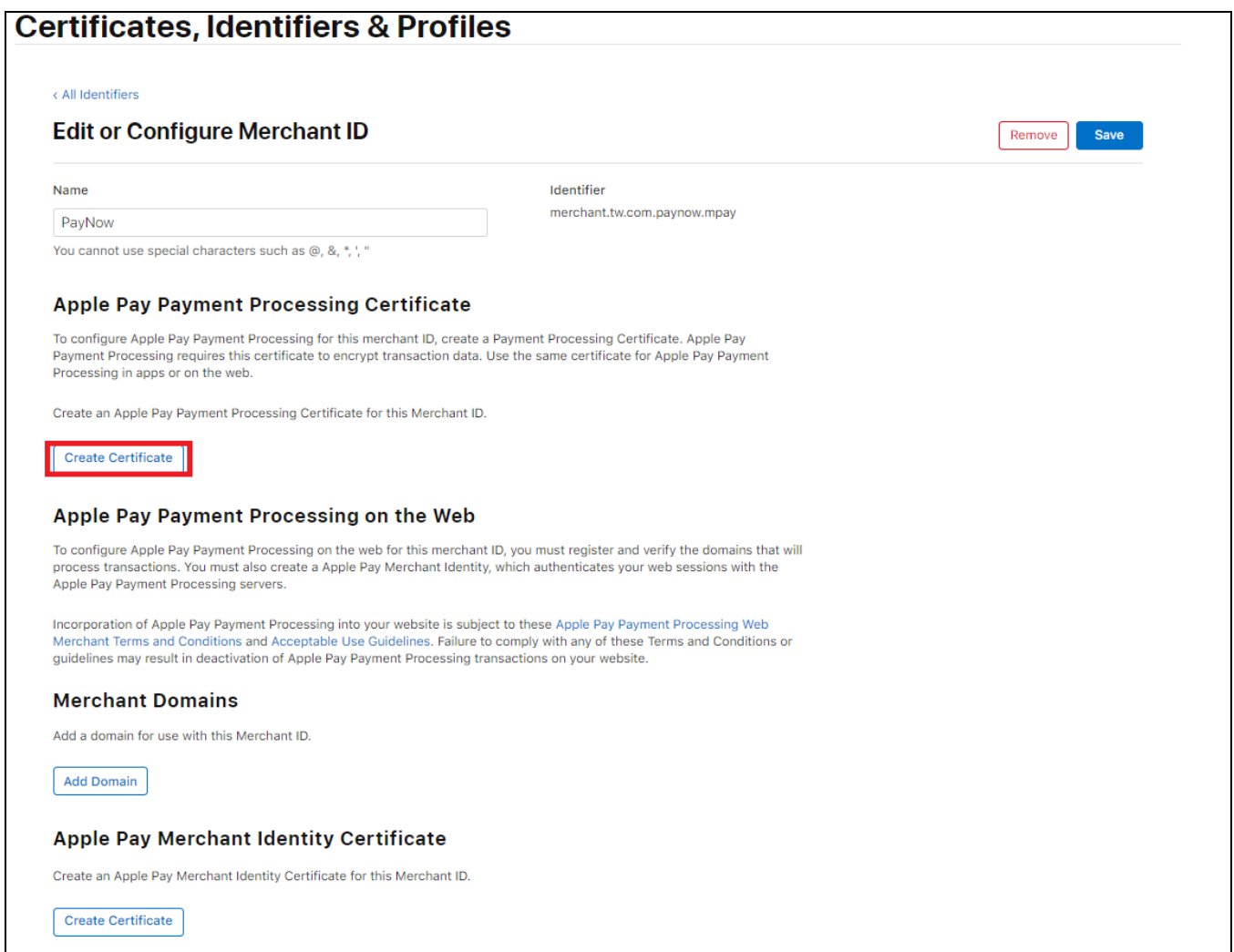


Certificates, Identifiers & Profiles

Certificates Identifiers + Merchant IDs

NAME	IDENTIFIER
PayNow	merchant.tw.com.paynow.mpay

(2) 點選 Apple Pay Payment Processing Certificate 下的「Create Certificate」按鈕



Certificates, Identifiers & Profiles

[< All Identifiers](#)

Edit or Configure Merchant ID

Remove Save

Name: Identifier: merchant.tw.com.paynow.mpay

You cannot use special characters such as @, &, *, ', "

Apple Pay Payment Processing Certificate

To configure Apple Pay Payment Processing for this merchant ID, create a Payment Processing Certificate. Apple Pay Payment Processing requires this certificate to encrypt transaction data. Use the same certificate for Apple Pay Payment Processing in apps or on the web.

Create an Apple Pay Payment Processing Certificate for this Merchant ID.

Create Certificate

Apple Pay Payment Processing on the Web

To configure Apple Pay Payment Processing on the web for this merchant ID, you must register and verify the domains that will process transactions. You must also create an Apple Pay Merchant Identity, which authenticates your web sessions with the Apple Pay Payment Processing servers.

Incorporation of Apple Pay Payment Processing into your website is subject to these [Apple Pay Payment Processing Web Merchant Terms and Conditions](#) and [Acceptable Use Guidelines](#). Failure to comply with any of these Terms and Conditions or guidelines may result in deactivation of Apple Pay Payment Processing transactions on your website.

Merchant Domains

Add a domain for use with this Merchant ID.

Add Domain

Apple Pay Merchant Identity Certificate

Create an Apple Pay Merchant Identity Certificate for this Merchant ID.

Create Certificate

(3) 回答問題，選擇「No」並點選「Continue」繼續

Certificates, Identifiers & Profiles

< All Identifiers

Edit or Configure Merchant ID Remove **Continue**

Name	Identifier
PayNow	merchant.tw.com.paynow.mpay

Will payments associated with this Merchant ID be processed exclusively in China?

No Yes

(4) 上傳 PayNow 提供之檔案(檔案名稱為「apple_payment_processing_certificate_商家統編」)

Certificates, Identifiers & Profiles

< All Certificates

Create a New Certificate Back Continue

Certificate Type
Apple Pay Payment Processing Certificate

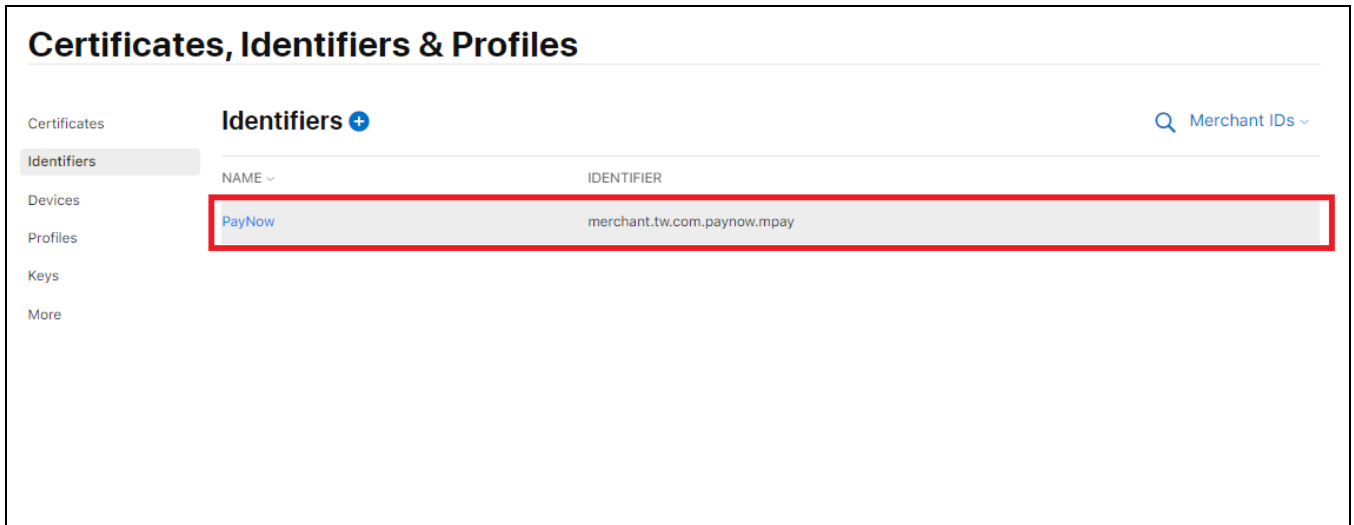
Upload a Certificate Signing Request
To manually generate a Certificate, you need a Certificate Signing Request (CSR) file from your Mac.
[Learn more >](#)

Choose File

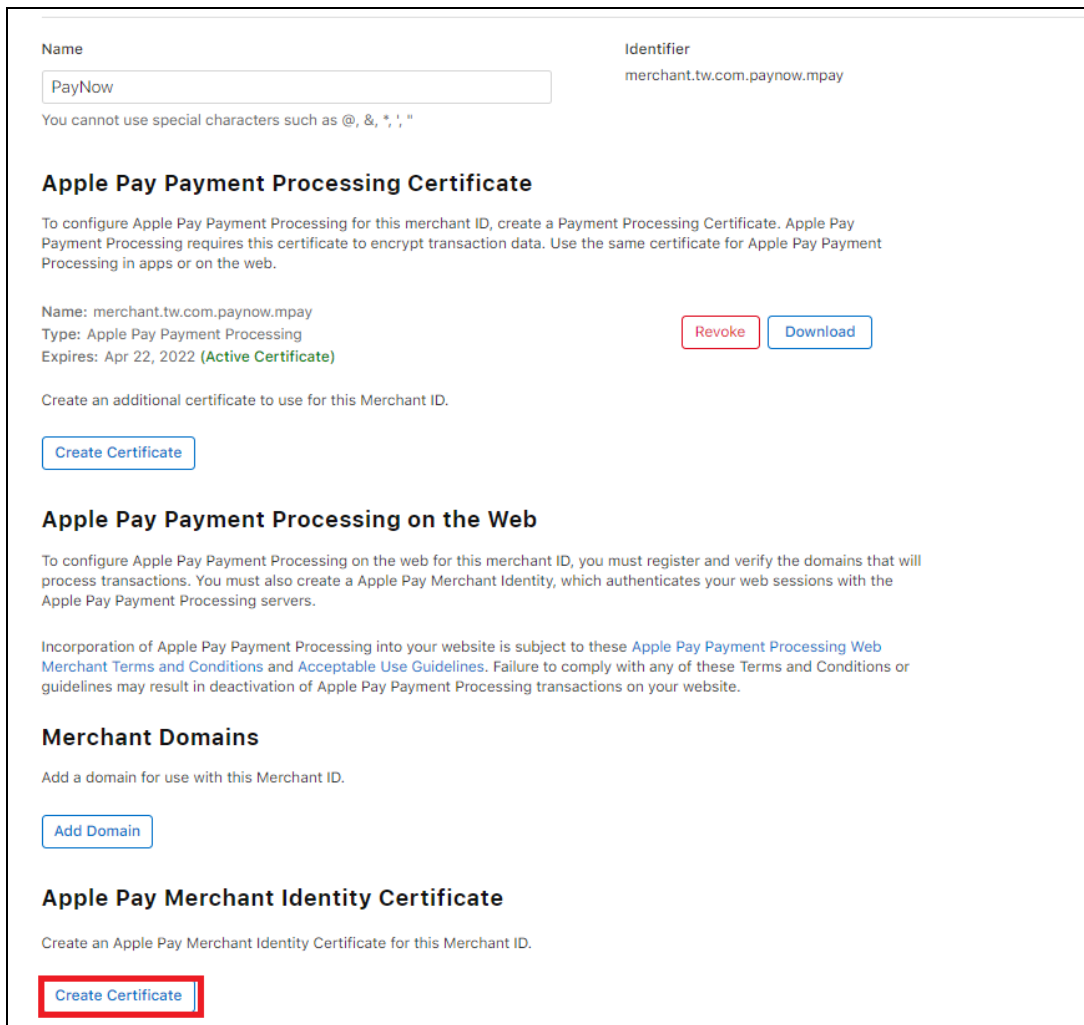
(5) 下載檔案傳送給 PayNow，將再次給予另一個檔案供商家建立商家憑證

2.3 建立商家憑證 (Apple Pay Merchant Identity Certificate)

(1) 點選剛註冊好的 Merchant IDs



(2) 點選 Apple Pay Merchant Identity Certificate 下的「Create Certificate」按鈕



(3) 上傳 PayNow 提供之檔案(檔案名稱為「apple_merchant_identity_certificate_商家統編」)

Certificates, Identifiers & Profiles

[< All Certificates](#)

Create a New Certificate

[Back](#) [Continue](#)

Certificate Type
Apple Pay Merchant Identity Certificate

Upload a Certificate Signing Request
To manually generate a Certificate, you need a Certificate Signing Request (CSR) file from your Mac.
[Learn more >](#)

[Choose File](#)

(4) 將檔案下載並傳送給 PayNow

2.4 商家 Domains (Merchant Domains)

(1) 點選 Merchant Domains 下的 Add Domain 按鈕

PayNow merchant.tw.com.paynow.mpay

You cannot use special characters such as @, &, *, ', "

Apple Pay Payment Processing Certificate

To configure Apple Pay Payment Processing for this merchant ID, create a Payment Processing Certificate. Apple Pay Payment Processing requires this certificate to encrypt transaction data. Use the same certificate for Apple Pay Payment Processing in apps or on the web.

Name: merchant.tw.com.paynow.mpay
Type: Apple Pay Payment Processing
Expires: Apr 22, 2022 (Active Certificate)

[Revoke](#) [Download](#)

Create an additional certificate to use for this Merchant ID.

[Create Certificate](#)

Apple Pay Payment Processing on the Web

To configure Apple Pay Payment Processing on the web for this merchant ID, you must register and verify the domains that will process transactions. You must also create a Apple Pay Merchant Identity, which authenticates your web sessions with the Apple Pay Payment Processing servers.

Incorporation of Apple Pay Payment Processing into your website is subject to these [Apple Pay Payment Processing Web Merchant Terms and Conditions](#) and [Acceptable Use Guidelines](#). Failure to comply with any of these Terms and Conditions or guidelines may result in deactivation of Apple Pay Payment Processing transactions on your website.

Merchant Domains

Add a domain for use with this Merchant ID.

[Add Domain](#)

Apple Pay Merchant Identity Certificate

Name: merchant.tw.com.paynow.mpay
Type: Apple Pay Merchant Identity
Expires: Apr 22, 2022

[Revoke](#) [Download](#)

Create an additional certificate to use for this Merchant ID.

[Create Certificate](#)

(2) 輸入付款頁面網站的 Domain

Certificates, Identifiers & Profiles

[< View Identifier](#)

Register Save

To use Apple Pay Payment Processing on the web you must register and verify your fully qualified domain name. To begin enter your domain below.

Enter the domain you wish to register

https://

(3) 下載指定檔案，並於該 Domain 下新增名為「.well-known」資料夾，

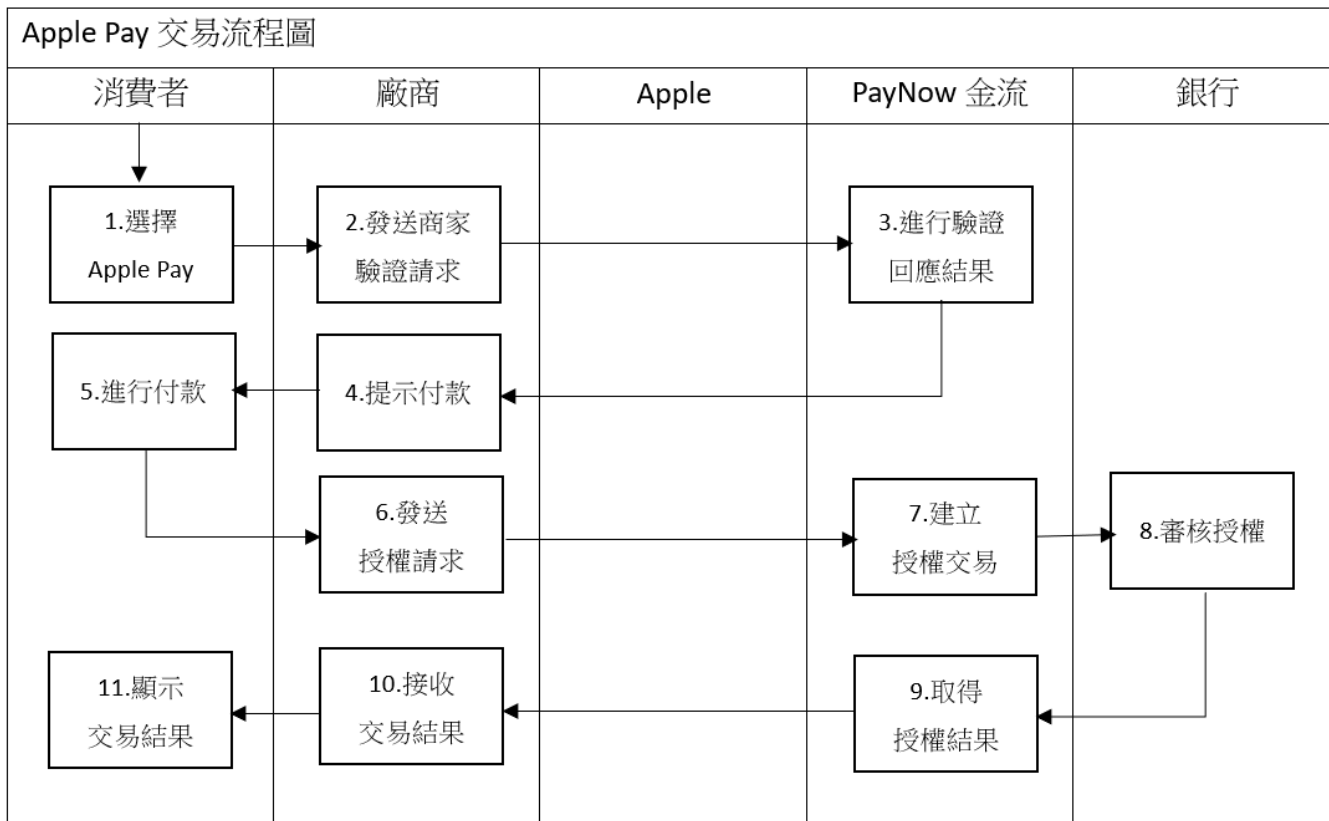
放入剛下載的「apple-developer-merchantid-domain-association.txt」再點選「Verify」

參考資料: https://developer.apple.com/documentation/apple_pay_on_the_web/setting_up_your_server

The screenshot shows the 'Certificates, Identifiers & Profiles' section of the Apple Developer portal. The page title is 'Verify'. There are two buttons: 'Download' and 'Verify'. The 'Download' button is highlighted with a red box and labeled '1.'. The 'Verify' button is highlighted with a red box and labeled '3.'. Below the buttons, there is a section titled 'Instructions and Information' with the text: 'To verify ownership of your domain download the file and place it at the location listed below. After uploading your file continue with the verification step.' Below this, there is a section titled 'We'll look for your file at the following location:' with a red box around the URL: 'https://mpay.paynow.com.tw/well-known/apple-developer-merchantid-domain-association.txt'. This URL is labeled '2.'.

3. ApplePay 信用卡串接說明

3.1 交易流程圖



3.2 商家頁面 ApplePay 串接

(1) 功能流程：

1. [Apple Pay 付款檢查](#)
2. [建立 Apple Pay Session 物件](#)
3. 消費者按下按鈕，進行[商店驗證（前端）](#)
4. 傳送資訊至後端呼叫「[PayNow 商家驗證](#)」商家驗證（後端）
5. 將「[PayNow商家驗證](#)」回傳值pass給ApplePaySession的「completeMerchantValidation」
6. 消費者進行指紋驗證授權交易，傳送資訊至後端呼叫「[信用卡授權](#)」
付款授權（後端）
7. 將「[信用卡授權](#)」回傳值，進行[付款授權（前端）](#)

(2) 付款頁面設計

1. Apple Pay 營銷準則

參考網址：

<https://developer.apple.com/apple-pay/marketing/>

2. 付款按鈕樣式規範

參考網址：

<https://developer.apple.com/design/human-interface-guidelines/apple-pay/overview/buttons-and-marks/>

範例：

```
<div id="btnApplePay" class="apple-pay-button apple-pay-button-black" style="-webkit-appearance: -apple-pay-button; -apple-pay-button-type: buy; width: 200px; height: 64px;"></div>
```

3. 付款按鈕 CSS 樣式

參考網址：

https://developer.apple.com/documentation/apple_pay_on_the_web/displaying_apple_pay_buttons

範例：

```
/* CSS */
@supports (-webkit-appearance: -apple-pay-button) {
  .apple-pay-button {
    display: inline-block;
    -webkit-appearance: -apple-pay-button;
  }
  .apple-pay-button-black {
    -apple-pay-button-style: black;
  }
}
@supports not (-webkit-appearance: -apple-pay-button) {
  .apple-pay-button {
    display: inline-block;
    background-size: 100% 60%;
    background-repeat: no-repeat;
    background-position: 50% 50%;
    border-radius: 5px;
    padding: 0px;
    box-sizing: border-box;
    min-width: 200px;
    min-height: 32px;
    max-height: 64px;
  }
  .apple-pay-button-black {
    background-image: -webkit-named-image(apple-pay-logo-white);
    background-color: black;
  }
}
```

(3) Apple Pay 付款檢查

1. 功能說明：檢查是否支援 ApplePay 付款

參考網址：

https://developer.apple.com/documentation/apple_pay_on_the_web/applepaysession#2166537

範例：

```
/* 檢查當前瀏覽器是否支援Apple Pay */
if (window.ApplePaySession) {
    var merchantIdentifier = 'Apple Pay Merchant ID'; //填入你申請的Apple Pay Merchant Identifier
    /* 檢查設備是否能夠支援Apple Pay付款，它不會驗證用戶在電子錢包中是否有綁定卡片 */
    if (ApplePaySession.canMakePayments()) {
        /* 檢查付款設備是否能夠支援Apple Pay付款，且用戶在電子錢包中必需綁定一張卡片 */
        /* 若Safari設定中的「檢查ApplePay設定」關閉時canMakePayments一律回傳True */
        var promise = ApplePaySession.canMakePaymentsWithActiveCard(merchantIdentifier);
        promise.then(function (canMakePayments) {
            if (canMakePayments) {
                $("#btnApplePay").click(beginPayment);
                //顯示ApplePay按鈕
                $("#PayMentDiv").show();
            }
            else {
                /* 無綁定卡片無法進行ApplyPay*/
                /* 執行錯誤提示或進行頁面跳轉*/
            }
        });
    }
    else {
        /* 此設備不支援ApplePay */
        /* 執行錯誤提示或進行頁面跳轉 */
    }
}
else {
    /* 無法支援Apple Pay的相關處理 */
    /* 執行錯誤提示或進行頁面跳轉 */
}
```


(4) 建立 Apple Pay Session 物件

1. 功能說明：設定付款物件，初始化 Apple Pay Session 物件

參考網址：

<https://developer.apple.com/reference/applepayjs/paymentrequest>

範例：

```
/* 建立 PaymentRequest */
/* 參考: https://developer.apple.com/reference/applepayjs/paymentrequest */
var request = {
  countryCode: 'TW', //國家代碼請填 TW
  currencyCode: 'TWD', //幣別僅接受 TWD
  supportedNetworks: ['visa', 'masterCard', 'jcb'], //卡別僅支援 visa masterCard jcb
  merchantCapabilities: ['supports3DS'], //付款方式僅支援 supports3DS
  lineItems: [{ label: '測試商品', amount: $("#Amount").val() }], //商品資訊
  total: { label: 'PayNow, Inc', amount: $("#Amount").val() } //商品統計
};
/* 建立 ApplePaySession */
/* 參考: https://developer.apple.com/reference/applepayjs/applepaysession/2320659-applepaysession */
var session = new ApplePaySession(2, request);
```

(5) 商店驗證 (前端)

1. 功能說明：將 ValidationURL 傳送到 Server 端，向 PayNow 發送請求驗證是否來自有效的商家。

範例：

```
/* 商店驗證事件 */
session.onvalidatemerchant = function (event) {
    /* 將ValidationURL拋到Server端，向PayNowAPI發送請求 */
    $.ajax({
        url: 'Server URL',
        method: "POST",
        data:
            {
                ValidationURL: event.validationURL
            },
        error: function (err) {
            /* 執行錯誤提示或進行頁面跳轉*/
            session.abort();
        }
    }).then(function (TransactionSession) {
        /* 取得Server回傳資訊 */
        session.completeMerchantValidation(JSON.parse(TransactionSession));
    });
};
```

(6) 付款授權 (前端)

1. 功能說明：向 PayNow 發送請求授權，依授權結果決定帶入 ApplePaySession 回應

範例：

```
/* 進行付款授權事件 */
session.onpaymentauthorized = function (event) {
/* 將payment物件拋至Server端，由Server端處理交易授權 */
$.ajax({
  url: 'Server URL',
  method: "POST",
  data:
  {
/* 依照 */
    Amount: $("#Amount").val(),
    payment: JSON.stringify(event.payment.token.paymentData)
  },
  error: function (err) {
/* 執行錯誤提示或進行頁面跳轉*/
    session.abort();
  }
}).then(function (result) {
/* 依授權結果決定帶入ApplePaySession的回應 */
/* 參考: https://developer.apple.com/reference/applepayjs/applepayjs/session/1778012-completepayment */
if (result.substr(0, 2) == "S_") {
  //執行交易完成的動作
  $("#divReMsg").html("<pre>交易完成</pre>");
  session.completePayment(ApplePaySession.STATUS_SUCCESS);
}
else {
  //執行交易失敗的動作
  /* 執行錯誤提示或進行頁面跳轉*/
  session.completePayment(ApplePaySession.STATUS_FAILURE);
}
}
```

3.3 PayNow 商家驗證

(1) 路徑：<https://mpay.paynow.com.tw/api/ApplePay/GetTransactionSession>

(2) 傳遞方式：Http POST method

POST 參數			
參數名稱	描述	型態	備註
DisplayName	顯示的商店名稱	String	Ex. PayNow
DomainName	註冊的 Domain 名稱	String	Ex. mpay.paynow.com.tw
MemCid	PayNow 商家帳號	String	PayNow 商家帳號
MerchantIdentifier	Apple Pay MerchantID	String	Ex. merchant.xxx.xxx
ValidationURL	event.validationURL 值	String	前端取得的值
Signature	商家驗證檢查碼	String	檢查碼

(3) 回傳參數：Json 字串

回傳參數(Json 字串)			
參數名稱	描述	型態	備註
MemCid	PayNow 商家帳號	String	PayNow 商家帳號
MerchantIdentifier	Apple Pay MerchantID	String	Ex. merchant.xxx.xxx
ErrMsg	異常訊息	String	
TradeStatus	呼叫狀態	String	S：成功 F：失敗
TransactionSession	Apple商家驗證資料	String	請以物件傳送給 ApplePaySession 呼叫 completeMerchantValidation
Signature	商家驗證檢查碼	String	失敗將原值回傳，成功回傳檢查碼

4. APPLE 開發者帳號申請說明

4.1 ApplePay 開發者帳號註冊需求

(1) 需有 APPLE ID 若無則需先註冊

註冊網址：<https://appleid.apple.com/account>

且需 Apple ID 雙重認證(Two-factor Authentication)

參考網址：<https://support.apple.com/zh-tw/HT204915>

Ps.若無雙重驗證將會無法進行開發者帳號註冊

[Sign Out](#)

Your Apple ID needs to be updated.

Before you can continue, you'll need to update the following information associated with your Apple ID ().

❗ Two-factor Authentication

Two-factor authentication must be turned on for your Apple ID. After you turn it on, signing in to your developer account will require both your password and access to your trusted devices or trusted phone number.

To learn more, see the [support page](#). If you have any questions, [contact us](#).

✅ Country / Region

On file.

✅ Email Address

Verified.

✅ Mobile Phone Number

Verified.

(2) APPLE 開發者帳號申請

1. 申請網址：<https://developer.apple.com/programs/enroll/>
2. 申請費用：每年 \$ 99 美元 (USD)

(3) 個人帳號

1. 僅限開發者自己
2. 不需填寫公司的鄧百氏編碼 (D-U-N-S Number)
3. 若有 App 則上架僅能顯示個人資訊(某些類別 App 無法通過個人帳號上架)

(4) 公司帳號

1. 允許多個開發者協作
2. 需填寫公司的鄧白氏編碼 (D-U-N-S Number)
3. 若無註冊鄧白氏碼，需花費較長時間申請

4.2 開發者帳號申請流程

(1) 點選申請網址並開始註冊

What You Need To Enroll

✓ Enrolling as an Individual

If you are an individual or sole proprietor/single person business, get started by signing in with your Apple ID with [two-factor authentication](#) turned on. You'll need to provide basic personal information, including your legal name and address.

✓ Enrolling as an Organization

If you're enrolling your organization, you'll need an Apple ID with [two-factor authentication](#) turned on, as well as the following to get started:

A D-U-N-S® Number

Your organization must have a D-U-N-S Number so that we can verify your organization's identity and legal entity status. These unique nine-digit numbers are assigned by Dun & Bradstreet and are widely used as standard business identifiers. You can check to see if your organization already has a D-U-N-S Number and request one if necessary. They are free in most jurisdictions. [Learn more >](#)

Legal Entity Status

Your organization must be a legal entity so that it can enter into contracts with Apple. We do not accept DBAs, fictitious businesses, trade names, or branches.

Legal Binding Authority

As the person enrolling your organization in the Apple Developer Program, you must have the legal authority to bind your organization to legal agreements. You must be the organization's owner/founder, executive team member, senior project lead, or have legal authority granted to you by a senior employee.

A Website

Your organization's website must be publicly available and the domain name must be associated with your organization.

[Start Your Enrollment](#)

(2) 輸入註冊資訊，再按下「Continue」按鈕

以下為欄位中英對照

確認您的個人信息

法定名字

法定姓氏

電話號碼

國家代碼 電話號碼 延期

地址

optional

城市/城鎮

郵編/郵政編碼

國家/地區

列出的國家/地區必須準確代表您當前的居住地。要更新您的國家/地區，請登錄您的Apple ID帳戶。

羅馬式聯繫信息

輸入您的羅馬式住所或公司地址。

名字

姓

地址

optional

城市/城鎮

郵編/郵政編碼

國家/地區

Confirm your personal information.

Legal First Name

Legal Last Name

Phone Number

Country Code

Phone Number

Extension

Address

optional

City / Town

Zip / Postal Code

Country / Region

The country/region listed must accurately represent where you currently reside. To update your country/region, sign in to your [Apple ID account](#).

Romanized Contact Information

Enter your Romanized home or business address.

First Name

Last Name

Address

optional

City / Town

Zip / Postal Code

Country / Region

注意！羅馬式聯繫信息(Romanized Contact Information)欄位皆需輸入「英文」

(3) 選擇註冊開發者帳號類型，再按下「Continue」按鈕

Select your entity type.

I develop apps as

Individual / Sole Proprietor ▼

Select

Individual / Sole Proprietor	個人/獨資
Company / Organization	公司/組織
Nonprofit	非營利組織
Accredited Educational Institution	認可的教育機構
Government Organization	政府組織

must be recognized as a legal entity in your country/region. Sole proprietors and single person companies located in countries where they are not recognized as legal entities will be enrolled and be listed for download under the enrollee's personal legal name, if selected for distribution by Apple.

Continue

(4) 個人註冊

1. 閱讀完條款並打勾，再按下「Continue」按鈕

Review and Accept

This is a legal agreement between your organization and Apple.

[Download PDF](#)

PLEASE READ THE FOLLOWING APPLE DEVELOPER PROGRAM LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE SOFTWARE OR APPLE SERVICES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOU AND APPLE.

Apple Developer Program License Agreement

Purpose

You would like to use the Apple Software (as defined below) to develop one or more Applications (as defined below) for Apple-branded products. Apple is willing to grant You a limited license to use the Apple Software and Services provided to You under this Program to develop and test Your Applications on the terms and conditions set forth in this Agreement.


Applications developed under this Agreement for iOS Products, Apple Watch, or Apple TV can be distributed in four ways: (1) through the App Store, if selected by Apple, (2) through the Custom App Distribution via Apple Business Manager, if selected by Apple, (3) on a limited basis for use on Registered Devices (as defined below), and (4) for beta testing through TestFlight. Applications developed for macOS can be distributed through the App Store, if selected by Apple, or separately distributed under this Agreement.

By checking this box and clicking the Continue button, I confirm that I have read and agree to be bound by the Apple Developer Program License Agreement. I also confirm that I am of the legal age of majority in the jurisdiction in which I reside (at least 18 years of age in many countries).

[Back](#) [Continue](#)

2. 完成後續付款作業後，等待帳號激活即可

Complete your purchase.



Once you complete your purchase, you'll receive a purchase acknowledgement and a membership confirmation email.

Membership Type

Enrollment ID

Cost

Duration

[Purchase](#)

(5) 公司註冊

1. 註冊提醒

公司註冊需擁有 DUSN 號碼 [註冊 DUSN 號碼](#)

也可直接點擊「[Check now>](#)」連至以下網址若已有 DUSN 號碼則按下「[Continue](#)」按鈕

參考網址：<https://developer.apple.com/enroll/duns-lookup> (需登入 Apple ID)

To enroll, you will need:

- **Legal Entity Status**
To enroll in a developer program, your organization must be a legal entity so that it can enter into legal agreements with Apple. We do not accept DBAs, fictitious businesses, trade names, or branches. The legal entity name must correspond with the tax ID you plan to use and will appear on your product page for apps you may distribute on the App Store and Mac App Store. Example: *Seller: ABC Company, Inc.*
- **The Authority to Sign Legal Agreements**
As the person enrolling your organization in a developer program, you must have the legal authority to bind your organization to legal agreements. You must be the organization's owner/founder, executive team member, senior project lead, or have legal authority granted to you by a senior employee.
- **A Website**
Your organization's website must be publicly available and the domain name must be associated with your organization.
- **A D-U-N-S® Number**
Your organization must have a D-U-N-S® Number so that we can verify your organization's identity and legal entity status. These unique nine-digit numbers are assigned by Dun & Bradstreet and are widely used as standard business identifiers. You can check to see if your organization already has a D-U-N-S® Number and request one if necessary. They are free in most jurisdictions. [Check now >](#)

[Continue](#)


2. 填寫公司名稱及 DUNS 編號及驗證碼，再按下「[Continue](#)」按鈕

Tell us about your organization.

Legal Entity Name

Include the entity type, such as Inc., LLC, GmbH, etc.

D-U-N-S® Number

Enter the characters in the image below. [Switch to audio](#)
 [Try another](#)

Letters are not case-sensitive.

[Back](#) [Continue](#)

3. 填寫完成資料後請按下「Continue」按鈕

Apple Developer Program Enrollment

Discover Design Develop Distribute Support Account

Sign Out

Just a bit more info.

Address

City / Town

Zip / Postal Code

Country / Region

Website

Phone Number

Country Code Phone Number Extension

Select a country code.

Tax ID / National ID optional

Confirm your signing authority.

- I am the owner/founder and have the authority to bind my organization to legal agreements.
- My organization has given me the authority to bind it to legal agreements.

Your Work Email

This is a number assigned by local government agencies to identify a business within the local market. Examples include the VAT Number in Europe, the Siret Number in France, the Company Number in Australia, and the State Registry Number in Brazil.

Confirm that you have the authority to sign legal agreements on behalf of your organization.

Back Continue

4. 填寫完成資料後請按下「Submit」按鈕

Apple Developer Program Enrollment

Developer Discover Design Develop Distribute Support Account

Apple Developer Program Enrollment [Sign Out](#)

Confirm your information.

Legal Entity Type

I develop apps as

The information on this account will be used for verification and legal agreements, so please make sure your information is correct. To edit your account information, [contact us](#).

Your Organization

Legal Entity Name

D-U-N-S® Number

Address

City / Town

Zip / Postal Code

Country / Region

Website

Phone Number

Reference to Verify Your Signature Authority

Your Work Email

5. 申請完成後您將收到 Apple 的通知信請耐心等待後續的申請步驟

The screenshot shows the Apple Developer Program Enrollment page. At the top, there is a navigation bar with links for Developer, Discover, Design, Develop, Distribute, Support, and Account. Below the navigation bar, the page title is "Apple Developer Program Enrollment" and there is a "Sign Out" link. The main content area displays the message "Your enrollment is being processed." Below this message, there is a box containing the "Enrollment ID:" and a note: "Once we verify your authority to sign legal agreements, we'll email you with instructions on how to complete your enrollment." Further down, there is a section titled "Legal Entity Type" with a form field for "I develop apps as" and a note: "The information on this account will be used for verification and legal agreements, so please make sure your information is correct. To edit your account information, [contact us](#)." Below that is a section titled "Your Organization" with a form field for "Legal Entity Name".

The screenshot shows an email notification from Apple Developer Relations. The email starts with the "Apple Developer" logo and the word "Developer". Below the logo, there is a horizontal line. The email content begins with "Dear" followed by a blank space. The main body of the email reads: "We've received your enrollment request. Once we verify that you have the a bind your organization to Apple Developer Program legal agreements, we'll with instructions on how to complete your enrollment." Below this text, there is a list of fields: "Enrollment ID:", "Email:", "Work Email:", "Legal Entity:", and "Address:". A large red rectangular box is drawn over the content area, covering the fields and the text "內容會顯示您的申請資料". Below the red box, there is a link: "If you have any questions, [contact us](#)." The email ends with "Best regards," and "Apple Developer Relations".

6. 申請 APPLE 鄧白氏號碼

請到 <https://developer.apple.com/support/D-U-N-S/>

點選 [D-U-N-S Number look up tool](#)

The screenshot shows the Apple Developer Support page for D-U-N-S Number. The page has a navigation bar with 'Developer', 'Discover', 'Design', 'Develop', 'Distribute', 'Support', and 'Account'. Below the navigation bar, there is a 'Support' section with 'Overview', 'Articles', and a 'Contact us' button. The main content area is titled 'D-U-N-S® Number' and contains several paragraphs of text explaining the D-U-N-S Number and how to request one. A red box highlights the link 'D-U-N-S Number look up tool' in the text.

D-U-N-S® Number

The D-U-N-S Number is a unique nine-digit number that identifies business entities on a location-specific basis. Assigned and maintained by Dun & Bradstreet (D&B), the D-U-N-S Number is widely used as a standard business identifier.

Your D-U-N-S Number will be used to check the identity and legal entity status of your organization as part of our enrollment verification process for joining the Apple Developer Program or the Apple Developer Enterprise Program. While many types of businesses can receive a D-U-N-S Number, your business must be recognized as a legal entity (e.g., a corporation, limited partnership, limited liability company) to enter into the legal terms and obligations of Apple Developer Program agreements. DBAs, fictitious businesses, trade names, and branches are not accepted.

Companies and educational institutions must provide a D-U-N-S Number registered to their legal entity, while a D-U-N-S Number is optional for government organizations. If you are enrolling as an individual, you do not need a D-U-N-S Number.

Requesting a D-U-N-S Number

D&B may have already assigned your organization a free D-U-N-S Number. Before enrolling, use the [D-U-N-S Number look up tool](#) to see if you have one. If your company is not listed, you'll have the option to submit your information to Dun & Bradstreet for a free D-U-N-S Number.

You will be asked for the following information when requesting a D-U-N-S Number using the [D-U-N-S Number look up tool](#):

- Legal entity name
- Headquarters address
- Mailing address
- Your work contact information

As part of their verification process, a D&B representative may contact you directly for more information (e.g., type of business, number of employees). Please have your business registration documents ready.

附錄 1. 商家驗證(後端)檢查碼

1.1 說明:

POST 時「ValidationURL」參數不需加入檢查碼，其餘參數將皆需加入檢查碼，

當檢查碼錯誤時將會直接回傳 **HttpStatusCode 400**。

回傳時「TransactionSession」參數不需加入檢查碼，其餘參數將皆需加入檢查碼，當檢查碼，失敗時將回傳原 POST 時的檢查碼，請務必確認檢查碼是否相同。

1.2 POST 時檢查碼組成:

(1)將參數依照英文字母，由 A 到 Z 的順序排序，若字母相同則以下一個字母判斷，以此類推，並將參數名稱與該參數值串聯。

```
DisplayNamePayNowDomainNamempay.paynow.com.twMemCid28229955MerchantIdentifier  
merchant.tw.com.paynow.pay
```

(2)將字串全部轉換成小寫後做 `UrlEncode`

```
displaynamepaynowdomainnamempay.paynow.com.twmemcid28229955merchantidentifiermerc  
hant.tw.com.paynow.pay
```

(3)將字串做 `SHA-256` 加密，加密 Key 為商家 PayNow 交易密碼

此範例以「1234567890」加密

```
613B0106B509B252C3D9468723FC7A75DD69101624353646E608F3E3C44E3A31
```

(4)將加密後的字串再次轉換成全部小寫，放入 `Signature` 傳遞給 PayNow

```
613b0106b509b252c3d9468723fc7a75dd69101624353646e608f3e3c44e3a31
```

1.3 回傳時檢查碼組成(僅成功呼叫，失敗呼叫將以原 POST 值回傳)

- (1)將參數依照英文字母，由 A 到 Z 的順序排序，若字母相同則以下一個字母判斷，以此類推，並將參數名稱與該參數值串聯。

```
ErrMsgMemCid28229955MerchantIdentifiermerchant.tw.com.paynow.payTradeStatusS
```

- (2)將字串全部轉換成全部小寫

```
errmsgmemcid28229955merchantidentifiermerchant.tw.com.paynow.paytradestatuss
```

- (3)將字串做 SHA-256 加密，加密 Key 為商家 PayNow 交易密碼

此範例以「1234567890」加密

```
184EA4BE92C23FF2B5FEA71929616098E22E651FA26D6AA1BD0FB57AA16C82F0
```

- (4)將加密後的字串再次轉換成全部小寫，放入 Signature 回傳給商家

```
184ea4be92c23ff2b5fea71929616098e22e651fa26d6aa1bd0fb57aa16c82f0
```

附錄 2. SHA-256 C#範例

2.1 範例

```
/// <summary>  
/// [雜湊] - HMAC_SHA256  
/// </summary>  
/// <param name="key">要處理的密碼</param>  
/// <param name="data">要加密的內容</param>  
/// <returns>字串SHA256 Hash值</returns>  
private string HMAC_SHA256(string data, string key)  
{  
    ASCIIEncoding encoding = new ASCIIEncoding();  
    Byte[] textBytes = encoding.GetBytes(data);  
    Byte[] keyBytes = encoding.GetBytes(key);  
    Byte[] hashBytes;  
    using (HMACSHA256 hash = new HMACSHA256(keyBytes))  
        hashBytes = hash.ComputeHash(textBytes);  
    return BitConverter.ToString(hashBytes).Replace("-", "");  
}
```

附錄 3. 信用卡授權

3.1 說明

請利用 HTTP POST Method 來發送訊息，其 URL 如下：

正式環境WSDL：https://www.paynow.com.tw/WS_CardAuthorise_JS.asmx

測試環境WSDL：https://test.paynow.com.tw/WS_CardAuthorise_JS.asmx

引用函式：CardAuthorise_P

※ 所有參數傳遞時，請以URL Encode 編碼，所有網頁字集為UTF-8

※ 正式、測試環境為個別獨立空間，帳號需個別申請，無法共通使用

3.2 參數說明

參數名稱	參數描述	型態	必須	備註
傳送 (Object)				
JStr/JStr2	信用卡交易內容	string	Y	<p>將下列參數組成 Json 格式字串：</p> <p>mem_cid：商家帳號(統編/身分證) mem_checkpw：交易密碼 OrderNo：商家自訂編號 OrderInfo：消費資訊 ECPlatform：EC 名稱 ReceiverID：消費者帳號 ReceiverEmail：消費者 Email ReceiverName：消費者姓名 ReceiverTel：消費者電話 TotalPrice：交易總金額 PassCode：交易驗證碼</p> <p>將以下的順序組合起來成一字串：(mem_cid & OrderNo & Total Price & mem_checkpw) 並使用 SHA-1 雜湊函數取得組合字串的雜湊值(不含&符號)(附錄 B)</p> <p>paymentToken：ApplePay PaymentToken Data appleMerchantID：ApplePay 驗證 ID UserIp：使用者 IP</p> <p>將上列參數組成 Json 字串後，以檢核碼系統發出的 Key 及 IV 做 AES256 加密(註 3)後，將加密後字串對分拆解成 JStr 及 JStr2 兩個參數，再做 UrlEncode 上傳 註 1</p>
mem_cid	商家帳號	string	Y	商家帳號(統編/身分證)
TimeStr	時間戳	string	Y	加密卡號時使用的 TimeStr
CheckNum	隨機檢核碼	string	Y	加密卡號時取得隨機檢查碼時回傳的 CheckNum

回應 (Object)			
	WS 回應	string	Object 型態資料組成 Json 字串，以檢核碼系統發出 Key 及 IV 做 AES256 加密(註 1)後回傳，請以檢核碼系統發出 Key 及 IV 做 AES256 解密(註 2)
Obj_Message	Json 解密後 Object 內容		
	WebNo	string	商家帳號
	BuySafeNo	string	PayNow 訂單編號
	OrderNo	string	商家自訂編號
	TotalPrice	string	交易總金額
	RespCode	string	授權回覆代碼
	TranStatus	string	授權交易結果
	ResponseMSG	string	授權回覆訊息
	ApproveCode	string	信用卡授權碼
	PassCode	string	交易驗證碼 將以下的順序組合起來成一字串：(WebNo & mem_checkpw & BuysafeNo & TotalPrice & RespCode) 並使用 SHA-1 雜湊函數取得組合字串的雜湊值 (附錄 B)
	last4CardNo	string	卡號末四碼
	CIFID_SN	string	預存授權帳號流水號 ※請妥善保存
	ErrorMessage	string	錯誤訊息(若有錯誤時產生，沒有錯誤則無)

附錄 4. 檢核碼系統串接

4.1 說明：

請利用 HTTP POST Method 來發送訊息，其 URL 如下：

正式環境WSDL： https://www.paynow.com.tw/WS_PayNowEncryptp.asmx

測試環境WSDL： https://test.paynow.com.tw/WS_PayNowEncryptp.asmx

※ 所有參數傳遞時，請以URL Encode 編碼，所有網頁字集為UTF-8

※ 正式、測試環境為個別獨立空間，帳號需個別申請，無法共通使用

4.2 取得隨機檢查碼/取得加密金鑰(參數說明)

呼叫函式：GetEncryptionStr

參數名稱	描述	型態	必須	備註
傳送 (Object)				
OP	判斷代號	string	Y	GP = 取得檢查碼 GK = 取得 Key 及 IV
JStr	檢核驗證資訊	string	Y	將下列參數組成 Json 格式字串，以 AES256 加密傳遞 (註 1) GP 取得隨機檢查碼： mem_cid: 商家帳號(統編/身分證) PassCode: 交易驗證碼 PassCode 產生方式請見(註 3) TimeStr: 時間戳 時間戳產生方式請見(註 4) GK 取得 Key 及 IV： 包含以上參數以及 CheckNum: 檢核碼 (8 碼)
回應 (Object)				
	WS 回應	string		Json 字串以 AES256 加密回傳，請以 AES256 解密 (註 2)
	Json 解密後 Object 內容			
	GP:			
	mem_cid	string		商家帳號
	PassCode	string		回覆驗證碼 (註 3)
	TimeStr	string		時間戳
	CheckNum	string		隨機檢核碼 (8 碼)
	GK:			
	PassCode	string		回覆驗證碼 (註 3)
	EncryptionKey	string		加密 Key

	EncryptionIV	string		加密 IV
--	--------------	--------	--	-------

檢核碼使用的 AES256 加密(註 1 及註 2)key 及 IV 固定為下：

Key: paynowencryptpaynowcomtw28229955

IV: encrypt282299550

註 1、AES256 加密；

說明：下列範例使用 C#.net 編寫，僅供參考使用

此系統傳遞之AES256加解密，以檢核碼系統取得的Key值(**EncryptionKey**)及IV值(**EncryptionIV**)做加解密

Content：需要加密的內容

Key：**EncryptionKey**

IV：**EncryptionIV**

Ex：C# code

```
public string AES256_Encrypt(string Content, string key, string IV)
{
    byte[] ByteString = Encoding.UTF8.GetBytes(Content);
    byte[] ByteKeyString = Encoding.UTF8.GetBytes(key);
    byte[] ByteIVString = Encoding.UTF8.GetBytes(IV);
    RijndaelManaged RDEL = new RijndaelManaged();
    RDEL.Key = ByteKeyString;
    RDEL.IV = ByteIVString;
    RDEL.Mode = CipherMode.CBC;
    RDEL.Padding = PaddingMode.Zeros;
    ICryptoTransform cTransform = RDEL.CreateEncryptor();

    byte[] ResultByte = null;
    ResultByte = cTransform.TransformFinalBlock(ByteString, 0, ByteString.Length);
    string ReturnStr = Convert.ToBase64String(ResultByte, 0, ResultByte.Length);
    return ReturnStr;
}
```


註 2、AES256 解密：

說明：下列範例使用 C#.net 編寫，僅供參考使用

此系統傳遞之AES256加解密，以檢核碼系統取得的Key值(**EncryptionKey**)及IV值(**EncryptionIV**)做加解密

Content：需要加密的內容

Keu：**EncryptionKey**

IV：**EncryptionIV**

Ex：C# code

```
public string AES256_Decrypt(string Content, string key, string IV)
{
    byte[] ByteString = Convert.FromBase64String(Content);
    byte[] ByteKeyString = Encoding.UTF8.GetBytes(key);
    byte[] ByteIVString = Encoding.UTF8.GetBytes(IV);
    RijndaelManaged RDEL = new RijndaelManaged();
    RDEL.Key = ByteKeyString;
    RDEL.IV = ByteIVString;
    RDEL.Mode = CipherMode.CBC;
    RDEL.Padding = PaddingMode.Zeros;
    ICryptoTransform cTransform = RDEL.CreateDecryptor();

    byte[] ResultByte = null;
    ResultByte = cTransform.TransformFinalBlock(ByteString, 0, ByteString.Length);
    string ReturnStr = Encoding.UTF8.GetString(ResultByte);
    return ReturnStr;
}
```

註 3、 PassCode 產生範例：

GP 取得隨機檢查碼

以 mem_cid 及 GP規則加權檢核碼 (註5) 串接後做 SHA256雜湊加密字串(註6)後轉大寫帶入

回覆時的PassCode規則：

以 mem_cid 及 GK規則加權檢核碼 (註5) 串接後，以隨機檢查碼(CheckNum)為加密鑰 做 SHA256雜湊加密字串(註7)後轉大寫帶入

GK 取得Key及IV

以 mem_cid 及 GK規則加權檢核碼 (註5) 串接後，以隨機檢查碼(CheckNum)為加密鑰 做 SHA256雜湊加密字串(註7)後轉大寫帶入

回覆時的PassCode規則：

以 mem_cid 及 GP規則加權檢核碼 (註5) 串接後做 SHA256雜湊加密字串(註6)後轉大寫帶入

註 4、 TimeStr 時間戳格式：

Ex：以日期 2019-11-24 00:50:18 產生 10 碼數字

第 1 至 4 碼：太陽日，第 1 碼取西元年最後一位 2019 = 9

2 至 4 碼為一整年的起算天數，11/24 為今年的 328 天，所以 2 至 4 碼 = 328

第 5 至 10 碼：5-6 為小時數字 = 00；7-8 為分鐘數字 = 50；9-10 為秒分數字 = 18

1 至 10 碼組成時間戳 TimeStr = 9328005018

註 5、加權檢核碼產生規則：

分別以加權權數(23 碼)與加權基數(23 碼)各個數字相乘之後取個位數字，再取得以 10 減去個數字相加後除以 10 得餘數後的數字獲得加權權數檢查碼 1 碼 (10-餘數)，若為 10 則取 0；之後將加權權數前 15 碼字串與加權權數檢查碼 1 碼串接取得 16 碼數字；GP 與 GK 模式取得規則如下：

GP：取得隨機檢查碼

EX：商家帳號(mem_cid) = 028229955 · TimeStr = 9328005018

加權基數(23 碼)：93193193193193193193

加權權數(23 碼)：商家帳號 9 碼，不足左補 0；取商家帳號前 5 碼(5 碼) = 02822 + TimeStr(10 碼) = 9328005018 + TimeStr 前 4 碼(4 碼) = 9328 + 商家帳號後 4 碼(4 碼) = 9955 · 加權權數(23 碼) = 02822932800501893289955

將權數與基數相乘取其個位數字相加

0	2	8	2	2	9	3	2	8	0	0	5	0	1	8	9	3	2	8	9	9	5	5	
X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3	
0	6	8	18	6	9	27	6	8	0	0	5	0	3	8	81	9	2	72	27	9	45	15	

取個數分別得到並相加：

$$0 + 6 + 8 + 8 + 6 + 9 + 7 + 6 + 8 + 0 + 0 + 5 + 0 + 3 + 8 + 1 + 9 + 2 + 2 + 7 + 9 + 5 + 5 = 114$$

$$114 / 10 \text{ 得餘數 } 4 \text{；加權檢查碼 取 } 10 - 4 = 6 \text{ 加權檢核碼} = 0282293280050186$$

※組成回覆 PassCode 時的加權檢核碼會以 GK 的規則替換

GK : 取得 Key 及 IV

EX : 商家帳號(mem_cid) = 028229955 · TimeStr = 9328005018

加權基數(23 碼) : 93193193193193193193

加權權數(23 碼) : 商家帳號 9 碼 · 不足左補 0 ; 取商家帳號後 5 碼(5 碼) = 29955 + TimeStr(10 碼) =

9328005018 + TimeStr 前 4 碼(4 碼) = 9328 + 商家帳號前 4 碼(4 碼) = 0282 · 加權權數(23 碼) =

29955932800501893280282

將權數與基數相乘取其個位數字相加

2	9	9	5	5	9	3	2	8	0	0	5	0	1	8	9	3	2	8	0	2	8	2	
X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3	1	9	3	
18	27	9	45	15	9	27	6	8	0	0	5	0	3	8	81	9	2	72	0	2	72	6	

取個數分別得到並相加 :

$$8 + 7 + 9 + 5 + 5 + 9 + 7 + 6 + 8 + 0 + 0 + 5 + 0 + 3 + 8 + 1 + 9 + 2 + 2 + 0 + 2 + 2 + 6 = 104$$

104 / 10 得餘數 4 : 加權檢查碼 取 10 - 4 = 6

加權檢核碼 = 2995593280050186

※組成回覆 PassCode 時的加權檢核碼會以 GP 的規則替換

註 6、SHA256 雜湊加密字串：

Ex : C# code

```
public string SHA256_Encrypt(string Content)
{
    System.Security.Cryptography.SHA256CryptoServiceProvider sha256 = new System.Security.Cryptography.SHA256CryptoServiceProvider();
    byte[] ByteString = System.Text.Encoding.ASCII.GetBytes(Content);
    ByteString = sha256.ComputeHash(ByteString);
    string ReturnStr = null;
    foreach (byte bt in ByteString)
        ReturnStr += bt.ToString("x2");
    return ReturnStr.ToUpper();
}
```

註 7、SHA256 雜湊加密字串：

Ex : C# code

```
public string SHA256_HMACSHA256(string Content, string Key)
{
    byte[] ByteString = System.Text.Encoding.ASCII.GetBytes(Content);
    byte[] ByteKeyString = Encoding.ASCII.GetBytes(Key);
    byte[] HasBytes;
    HMACSHA256 sha256 = new HMACSHA256(ByteKeyString);
    HasBytes = sha256.ComputeHash(ByteString);
    string ReturnStr = BitConverter.ToString(HasBytes).Replace("-", "").ToUpper();
    return ReturnStr;
}
```