匯智資訊 cloudmax

匯智 資訊股份有限公司
10058 台北市中正區八德路一段 23 號 6 樓
6F, 23 Bade Road, Taipei, Taiwan 100
t. +886-2-2718-7200
f. +886- 2-2718-1922

【SSL Apache 憑證申請與安裝】

以下 Apache 的安裝步驟僅供參考，詳細狀況依伺服器版本或所在網路環境、架構而有些微差別，請依實際狀況或系統提供商資訊為準。有任何問題可與我們聯繫，將有專員引導您排除障礙。

版權聲明

商標聲明

有限擔保責任聲明

Cloudmax 匯智盡力製作本說明文件其正確性，但不擔保本文件無任何瑕疵，亦不為使用本說明文件而引起之衍生利益損失或意外損毀之損失擔保責任。

若對本文見有任何指證或建議，請利用下列資訊與我們聯繫：

服務電話 (02)2718-7200
服務傳真 (02)2718-1922
電子信箱 service@cloudmax.com.tw

匯智資訊 cloudmax

匯智 資訊股份有限公司

10058 台北市中正區八德路一段 23 號 6 樓
6F, 23 Bade Road, Taipei, Taiwan 100

t. +886-2-2718-7200
f. +886- 2-2718-1922

【操作文件 – SSL Apache 憑證申請與安裝】

目錄

匯智資訊 cloudmax

匯智 資訊股份有限公司

10058 台北市中正區八德路一段 23 號 6 樓
6F, 23 Bade Road, Taipei, Taiwan 100

t. +886-2-2718-7200
f. +886- 2-2718-1922

一、選擇產生 CSR 檔案方式

CSR 檔案為提供給憑證中心驗證的檔案，透過此 CSR 檔案憑證中心將會簽發 CER 檔案；而產生 CSR 檔案的同時會一併會產出 KEY 檔案，而這三個檔案為互相匹配憑證才可正常運行。

1. 使用 OpenSSL 或透過線上生成工具產生 (申請 GeoTrust 使用)

若您為申請 GeoTrust 的憑證，我們建議您可以直接使用我們的 OpenSSL 線上產生工具，來快速產生 CSR 檔，並且將所產生出來的 CSR 檔案提交給匯智，一併產出的 KRY 檔案請您務必儲存，以利後續憑證安裝過程順利。

GeoTrust 線上生成 CSR 工具：http://geotrust.cloudmax.com.tw/OpenSSL/CreateCSR.asp

2. 透過 Apache 伺服器產生 (申請 GlobalSign 使用)

進入 OpenSSL 安裝的目錄，運行如下命令生成私鑰：

```
openssl genrsa -des3 2048 -out server.key
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
..........++++++
........++++++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
```

如果使用-des3 參數，將會需要輸入一個密碼對私鑰進行加密，如不需要對私鑰加密請不要使用-des3 選項。輸入兩次密碼後，將會生成 server.key 私鑰文件，運行如下命令生成憑證請求文件（CSR）

```
openssl req -new -key server.key –out server.csr
```

如是 Windows 系統，請使用下面命令生成憑證請求文件（CSR）

```
set OPENSSL_CONF=openssl.cnf
openssl req -new -key server.key -out server.csr
```

接下來提提示輸入私鑰密碼和申請數位憑證的詳細訊息

```
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

```
Country Name (2 letter code) []:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) []:Shanghai
Organization Name (eg, company) []:GlobalSign

Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your websites domain name) []:cn.globalsign.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

從 Email 地址開始，下面的訊息都不需要，請保留為空，直接 Enter 即可。需要輸入的訊息說明請見下表：

字段	說明	示例
Country Name	ISO 國家代碼（兩位字符）	TW
State or Province Name	所在省份	Shanghai
Locality Name	所在城市	Shanghai
Organization Name	公司名稱	GlobalSign
Organizational Unit Name	部門名稱	IT Dept.
Common Name	申請憑證的域名	TW.globalsign.com
Email Address	不需要輸入	
A challenge password	不需要輸入	

二、安裝前注意事項

數位憑證是由私密金鑰（private key）與公開金鑰（public key)兩個部分組成，在進行安裝及使用數位憑證前，須將私密金鑰與公開金鑰檔案放置於伺服器可讀取之儲存區中。

依伺服器網路環境不同而實際需求各異，以下列出安裝時常見忽略的狀況：

- 伺服器是否正常連上 Internet？
- HTTPS 協定之通訊埠是否開啟[1]？
- 部分狀況下，伺服器需要額外的固定 IP[2]支援；此時需調整網址之 A 紀錄[3]。
- 與伺服器串連的網路設備通訊埠的狀態是否設定完成[4]？

若無法確認網路環境，或您非相關設備或服務的權限擁有者，應與設備、系統所屬管理員或該服務、設備提供商諮詢及確認。

安裝過程中，因操作錯誤或其他不可預期因素，可能導致系統資料異常、毀損，請在系統更動前，將重要系統及資料進行備份。

[1] HTTPS 協定預設使用 Port 443，但使用者可依實際狀況進行調整。
[2] 多個網站共用同一台伺服器的情況下(如虛擬主機)，需要利用額外的固定 IP 以解決通訊埠不足的問題。
[3] 須注意您是否擁有修改 DNS(Domain Name Service) Server 權限，且 DNS 紀錄修改需要生效時間。
[4] 例如防火牆、負載平衡裝置、代理伺服器等，可能須調整規則、開啟通訊埠，甚至部分設備也需要安裝、支援數位憑證。

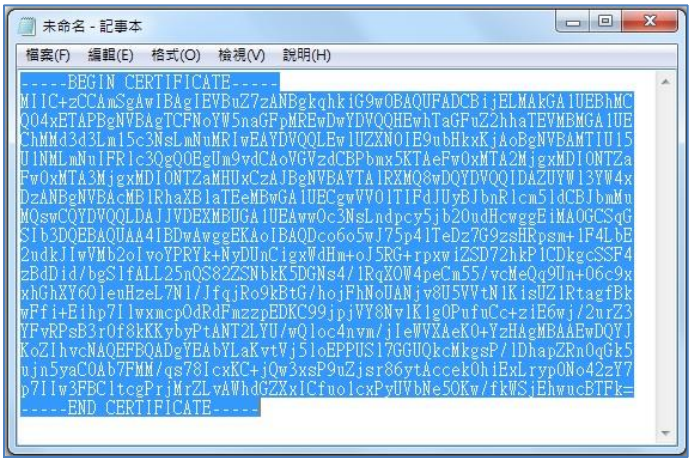
三、數位憑證安裝前準備確認事項

憑證核發成功後，指定的 Email 信箱將可收到國外認證中心發的英文通知信與匯智的中文通知信，而信中將會提供憑證中心所簽屬的 CER 檔案與憑證中繼憑證檔案，這些資訊將以純文字的方式來顯示，請您進行以下的動作確認所頒發的憑證資訊是否正確。

1 請協助查看憑證資訊檔案文本資料中

2 請複製憑證資訊(包含)『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』)

3 開啟純文字檔案，貼上您所複製的資訊



4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer)，所見的圖示將會變成 

5 請點擊憑證檔案，確認憑證網域、簽發者單位、有效期間是否為正常資訊

四、準備中繼憑證檔案

電腦運算能力於近十年內大幅提升，為確保憑證用戶網路資料傳輸安全，各大憑證中心於 2010 年起開始做根憑證 1024 升級為 2048 位元的作業，而舊的瀏覽器因缺少 2048 位元的根憑證資料，所以需要利用中繼憑證來進行交互驗證，確保於舊版本瀏覽器使用 HTTPS 連線時，不會出現錯誤或警告訊息，請您依照以下的步驟來完成中繼憑證匯入動作：

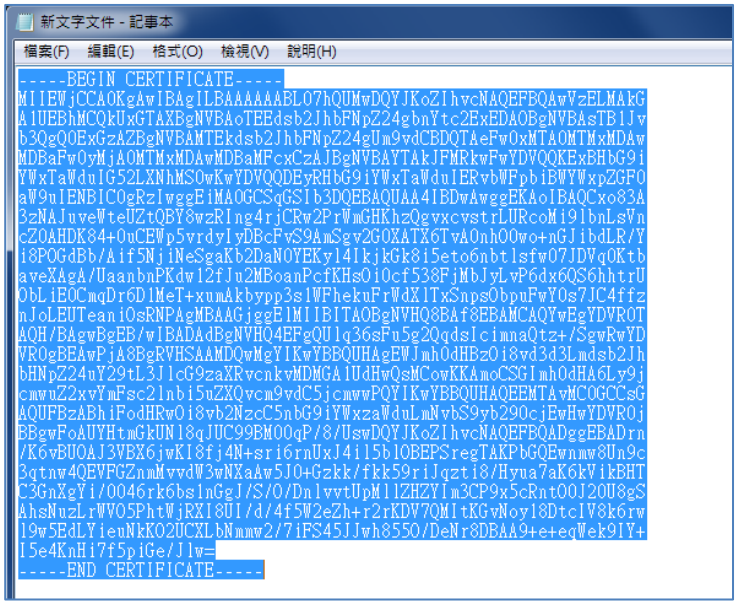
1 請協助查看憑證資訊檔案文本資料中「中繼憑證」

中繼憑證：

-----BEGIN CERTIFICATE-----
MIIEWjCCA0KgAwIBAgILBAAAAAABL07hQUMwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0xMTA0MTMxMDAw
MDBaFw0yMjA0MTMxMDAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMS0wKwYDVQQDEyRHbG9iYWxTaWduIERvbWFpbiBWYWxpZGF0
aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCxo83A
3zNAJuveWteUZtQBY8wzRIng4rjCRw2PrWmGHKhzQgvxcvstrLURcoMi9lbnLsVn
cZ0AHDK84+0uCEWp5vrdyIyDBcFvS9AmSgv2G0XATX6TvA0nhO0wo+nGJibdLR/Y
i8POGdBb/Aif5NjiNeSgaKb2DaN0YEKyl4IkjkGk8i5eto6nbtlsfw07JDVq0Ktb
aveXAgA/UaanbnPKdw12fJu2MBoanPcfKHsOi0cf538FjMbJyLvP6dx6QS6hhtrU
ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdX1TxSnpsObpuFwY0s7JC4ffz
nJoLEUTeaniOsRNPAgMBAAGjggE1MIIBITAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimnaQtz+/SgwRwYD
VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2Jh
bHNpZ24uY29tL3JlcG9zaXRvcnkwMDMGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly9j
cmwuZ2xvYmFsc2lnbi5uZXQvcm9vdC5jcmwwPQYIKwYBBQUHAQEEMTAvMC0GCCsG
AQUFBzABhiFodHRwOi8vb2NzcC5nbG9iYWxzaWduLmNvbS9yb290cjEwHwYDVR0j
BBgwFoAUYHtmGkUNl8qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEBADrn
/K6vBUOAJ3VBX6jwKI8fj4N+sri6rnUxJ4il5blOBEPSregTAKPbGQEwnmw8Un9c
3qtnw4QEVFGZnmMvvdW3wNXaAw5JO+Gzkk/fkk59riJqzti8/Hyua7aK6kWikBHT
C3GnXgYi/0046rk6bs1nGgJ/S/O/DnlvvtUpMllZHZYIm3CP9x5cRntO0J20U8gS
AhsNuzLrWVO5PhtWjRXI8UI/d/4f5W2eZh+r2rKDV7QMItKGvNoy18DtcIV8k6rw
l9w5EdLYieuNkKO2UCXLbNmmw2/7iFS45JJwh855O/DeNr8DBAA9+e+eqWek9IY+
I5e4KnHi7f5piGe/Jlw=
-----END CERTIFICATE-----

2 請複製憑證資訊(包含)『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』)

3 開啟純文字檔案，貼上您所複製的資訊



新文字文件 - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

-----BEGIN CERTIFICATE-----
MIIEWjCCA0KgAwIBAgILBAAAAAABL07hQUMwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0xMTA0MTMxMDAw
MDBaFw0yMjA0MTMxMDAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMS0wKwYDVQQDEyRHbG9iYWxTaWduIERvbWFpbiBWYWxpZGF0
aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCxo83A
3zNAJuveWteUZtQBY8wzRIng4rjCRw2PrWmGHKhzQgvxcvstrLURcoMi9lbnLsVn
cZ0AHDK84+0uCEWp5vrdyIyDBcFvS9AmSgv2G0XATX6TvA0nhO0wo+nGJibdLR/Y
i8POGdBb/Aif5NjiNeSgaKb2DaN0YEKyl4IkjkGk8i5eto6nbtlsfw07JDVq0Ktb
aveXAgA/UaanbnPKdw12fJu2MBoanPcfKHsOi0cf538FjMbJyLvP6dx6QS6hhtrU
ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdX1TxSnpsObpuFwY0s7JC4ffz
nJoLEUTeaniOsRNPAgMBAAGjggE1MIIBITAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimnaQtz+/SgwRwYD
VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2Jh
bHNpZ24uY29tL3JlcG9zaXRvcnkwMDMGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly9j
cmwuZ2xvYmFsc2lnbi5uZXQvcm9vdC5jcmwwPQYIKwYBBQUHAQEEMTAvMC0GCCsG
AQUFBzABhiFodHRwOi8vb2NzcC5nbG9iYWxzaWduLmNvbS9yb290cjEwHwYDVR0j
BBgwFoAUYHtmGkUNl8qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEBADrn
/K6vBUOAJ3VBX6jwKI8fj4N+sri6rnUxJ4il5blOBEPSregTAKPbGQEwnmw8Un9c
3qtnw4QEVFGZnmMvvdW3wNXaAw5JO+Gzkk/fkk59riJqzti8/Hyua7aK6kWikBHT
C3GnXgYi/0046rk6bs1nGgJ/S/O/DnlvvtUpMllZHZYIm3CP9x5cRntO0J20U8gS
AhsNuzLrWVO5PhtWjRXI8UI/d/4f5W2eZh+r2rKDV7QMItKGvNoy18DtcIV8k6rw
l9w5EdLYieuNkKO2UCXLbNmmw2/7iFS45JJwh855O/DeNr8DBAA9+e+eqWek9IY+
I5e4KnHi7f5piGe/Jlw=
-----END CERTIFICATE-----

4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer)，所見的圖示將會變成 

五、安裝憑證

用文本編輯器打開 httpd.conf 並更新以下內容

```
<VirtualHost xxx.xxx.xxx.xxx:443>
DocumentRoot "/var/www/html"
ServerName cn.globalsign.com
SSLEngine on
SSLCertificateFile /etc/ssl/crt/server.cer              //公鑰文件
SSLCertificateKeyFile /etc/ssl/crt/server.key    .    //私鑰文件
SSLCertificateChainFile /etc/ssl/crt/dvroot.cer      //中級憑證
</VirtualHost>
```

按照以上的步驟配置完成後，重新啟動 Apache

六、檢查憑證安裝是否正確

您可以透過此驗證工具來確認憑證是否已經正確掛載：

GeoTrust：http://geotrust.cloudmax.com.tw/OpenSSL/checkservercert.asp
GlobalSign：https://globalsign.ssllabs.com/