中華電信 GlobalSign SSL/TLS 憑證（R46 根憑證）
PKCS #12 檔案（.pfx / .p12）製作教學（使用 OpenSSL 指令操作）

2026/04/14 初版

PKCS #12 格式（.pfx / .p12）通常用於 Windows Server (IIS) 或需要將私鑰與完整憑證鏈（含中繼憑證）封裝在單一檔案的場合。

開始前，您的電腦需事先安裝 OpenSSL → 請上網搜尋其他人的安裝教學

並確認已取得以下四個檔案，建議將它們放在同一個資料夾以方便操作：

檔案名稱（範例）	說明	來源
private.key	產製 CSR 時所生成的伺服器私鑰	**自行保管**
[憑證序號].cer	中華電信核發的伺服器憑證	中華電信
CHTOVCA.crt	中華電信新中繼憑證	中華電信
rootr46.crt	GlobalSign R46 根憑證	中華電信

一、使用 OpenSSL 製作 PFX 檔案

請開啟終端機（Linux/macOS）或命令提示字元（Windows），切換至檔案所在目錄後執行下列指令：

終端機指令

```
openssl pkcs12 -export -inkey private.key
               -in [憑證序號].cer
               -certfile CHTOVCA.crt -certfile rootr46.crt
               -out <輸出.pfx 路徑>
```

指令參數說明

- `-export`：執行匯出動作。
- `-inkey`：讀取私鑰檔案。
- `-in`：讀取伺服器憑證。
- `-certfile`：讀取中繼憑證 / 交互憑證 / 根憑證（若有多個，可重複使用此參數）。
- `-out`：指定輸出的 .pfx 檔名（自行命名）。

二、設定匯出密碼

指令執行後，系統會要求設定匯出密碼（Export Password）：

```
Enter Export Password： ← 請輸入欲設定的密碼（輸入時畫面不會顯示字元）。
Verifying - Enter Export Password： ← 再次輸入相同密碼以供確認。
```

完成後，目錄下即會生成 .pfx 檔案，此檔案可直接匯入至 Windows 憑證存放區或其他支援 PKCS #12 的設備。

⚠ **安全警告：** .pfx 檔案包含私鑰與密碼，在傳輸或儲存時應嚴格控管權限，避免外流。

附錄：PFX 檔案進階操作

以下為常見的抽取指令，適用於需要從既有 .pfx 檔案還原各元件的情況。

1. 抽取私鑰 (Private Key)

若需從 .pfx 檔案中分離出私鑰，請執行以下指令：

終端機指令

```
openssl pkcs12 -in <來源.pfx 路徑> -nocerts -nodes -out private.key
```

- `-nocerts`：代表不匯出憑證。
- `-nodes`：代表不對輸出的私鑰進行加密（No DES encryption）。

2. 抽取憑證 (Certificates)

若需從 .pfx 檔案中分離出憑證檔案，請執行以下指令：

終端機指令

```
openssl pkcs12 -in <來源.pfx 路徑> -nokeys -out <輸出憑證.crt 路徑>
```

- `-nokeys`：代表不匯出私鑰。
- <輸出憑證.crt 路徑>：自行命名，例如：`server.crt`、`cert.pem`。
- `-legacy`：選用參數，如果輸入密碼後出現 unsupported 錯誤，在指令中加上 -legacy 重新執行一次。

注意：	這個指令所輸出的憑證檔案，所含內容為憑證鏈中的所有憑證。若需取得中繼憑證，請用記事本開啟輸出的憑證抽取檔案，將所需的-----BEGIN CERTIFICATE-----（含）到-----END CERTIFICATE-----（含）雜湊碼區塊，複製貼上到新記事本另存新檔，製作中繼憑證檔案。

3. 將 PFX 檔案轉成文字檔案（私鑰+憑證）

若需單次轉換就能取得私鑰+憑證內容，請執行以下指令：

終端機指令

```
openssl pkcs12 -in <來源.pfx 路徑> -out <輸出.txt 路徑> -nodes
```

- <輸出.txt 路徑>：自行命名，例如：server.txt、server.pem。

這個指令輸出的文字檔案，所含內容為**私鑰+憑證鏈**中的所有憑證。

請將所需的雜湊碼區塊，複製貼上到新記事本另存新檔，製作私鑰或憑證檔案。

輸出的.txt 檔案

```
-----BEGIN CERTIFICATE-----
. . . . . .                    ← 伺服器憑證或中繼憑證，將區塊貼上新記事本另存.crt 憑案
. . . . . .                      即可獲得憑證。
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
. . . . . .                    ← 私鑰，將區塊貼上新記事本另存.key 私鑰檔案
. . . . . .                      即可獲得私鑰。
-----END PRIVATE KEY-----

# 複製雜湊碼區塊時，記得包含頭尾的 BEGIN 和 END 標籤橫列
```
