# 產製兩對金鑰、憑證請求檔的方式

**前提條件**

- 已下載並安裝 OpenSSL Windows 版本。
- 已開啟 **CMD 命令提示字元**，並切換至 OpenSSL 所在目錄（例如 C:\OpenSSL3.4.0\bin）。
- 建議建立一個新的資料夾用來存放產出的金鑰與 CSR，例如：C:\OpenSSL3.4.0\bin\CSR，避免檔案混亂。

**步驟 1：產生兩組 RSA 2048 金鑰對(以 CHT、TWCA 命名)**

- cd C:\OpenSSL3.4.0\bin
- openssl genrsa -out CSR/CHT_key.pem 2048
- openssl genrsa -out CSR/TWCA_key.pem 2048

**步驟 2：產生 CSR（憑證請求檔）**

- openssl req -new -key CSR/CHT_key.pem -out CSR/CHT_csr.csr -subj "/C=TW/L=Taipei/O=行政院/OU=各級機關/CN=abc.gov.tw/emailAddress=abc@abc.gov.tw" -config openssl.cnf
- openssl req -new -key CSR/TWCA_key.pem -out CSR/TWCA_csr.csr -subj "/C=TW/L=Taipei/O=行政院/OU=各級機關/CN=abc.gov.tw/emailAddress=abc@abc.gov.tw" -config openssl.cnf

黃色部分記得修改成貴機關的聯絡人資訊

註: 有安裝 openssl 的機器上，不用加最後灰色的這一段，如採用的是免安裝版，則先找出 openssl.cnf，複製到 openssl 的所在目錄（例如 C:\OpenSSL-Win64\bin），再把灰色部分加上去才能正常產出。

執行後產出結果，兩個憑證請求檔(請求檔包含公鑰)，及兩個私鑰，再依據 CHT/TWCA 名稱的 CSR 到 GCP 網站投單申請。