產製一組金鑰與憑證請求檔的方式

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）。
- 建議在 OpenSSL 目錄下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：產生一組 RSA 2048 金鑰對 。（此範例以 TLS 命名）

請在 CMD 執行以下指令（假設 OpenSSL 所在目錄為 C:\OpenSSL3.4.0\bin）：

1. **切換目錄：**

   cd C:\OpenSSL3.4.0\bin

2. **產生私鑰 ：**

   openssl genrsa -out CSR/TLS_key.pem 2048

會在 CSR 資料夾下產生一個 2048 位元的 RSA 私鑰檔案。

步驟 2：產生 CSR（憑證請求檔）

1. 使用上一步驟產生的私鑰，執行以下指令來產生憑證請求檔:

   openssl req -new -key CSR/TLS_key.pem -out CSR/TLS_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

   黃色部分請修改成貴機關的名稱及網域名稱與聯絡人信箱

- 如果您機器上有安裝 OpenSSL，不必加上 -config openssl.cnf 。
- 如果您使用的是免安裝版 OpenSSL，需要先找出 openssl.cnf，將它複製到 OpenSSL 所在目錄（例如 C:\OpenSSL-Win64\bin），才能正常執行指令中 -config openssl.cnf 。

2. 執行完畢後，CSR 資料夾內將會產出兩個檔案：

- 私鑰檔案（請務必妥善保管，切勿外洩）
- 憑證請求檔（包含公鑰，此檔案可上傳至 GCP 網站投單申請）。