

【Mac】使用自簽憑證

產生憑證

在要放置自簽憑證資料夾

```
openssl req -x509 -out localhost.crt -keyout localhost.key -days 365 -newkey rsa:2048 -nodes -sha256 -subj '/CN=localhost' -extensions EXT -config <( printf "[dn] \nCN=localhost\n[req]\ndistinguished_name = \ndn\n[EXT]\nsubjectAltName=DNS:localhost\nkeyUsage=digitalSignature\nextendedKeyUsage=serverAuth")
```

```
openssl req -x509 -out localhost.crt -keyout localhost.key -days 365 -newkey rsa:2048 -nodes -sha256 -subj '/CN=localhost' -extensions EXT -config <( printf "[dn] \nCN=localhost\n[req]\ndistinguished_name = \ndn\n[EXT]\nsubjectAltName=DNS:localhost\nkeyUsage=digitalSignature\nextendedKeyUsage=serverAuth")
```

產生憑證檔跟key

localhost.crt
localhost.key

你可以使用 macOS 的 **Keychain Access (鑰匙圈存取)** 工具將 localhost.crt 憑證加入系統的信任憑證清單中。以下是詳細步驟：

【方法一】用 Terminal 安裝憑證到「系統」鑰匙圈

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain localhost.crt
```

參數說明：

- d：代表這是一個用來信任的憑證（不是用來簽署的憑證）。
- r trustRoot：將憑證標記為信任根（Trust Root）。
- k /Library/Keychains/System.keychain：安裝到系統層級的鑰匙圈（需要 sudo 權限）。
- localhost.crt：你生成的憑證檔案。

【方法二】手動用 GUI 加入（若你想看圖形介面）

- 開啟「**鑰匙圈存取**」（Keychain Access）
- 選擇左上角「**系統**」鑰匙圈
- 拖曳 localhost.crt 到右邊的憑證清單中
- 右鍵點選剛剛新增的 localhost 憑證 → 點選「**取得資訊**」
- 展開「**信任**」區塊
- 將「**使用此憑證時**」設為「**永遠信任**」
- 關閉視窗時，系統會要求你輸入管理員密碼以儲存變更

□ 驗證是否已信任憑證

你可以使用以下方式確認憑證是否信任：

```
security verify-cert -c localhost.crt
```

或是直接在瀏覽器打開 https://localhost，若沒有「不受信任」或「警告」的訊息，就代表成功。

🕒 修訂版本 #1

★ 由 treeman 建立於 13 🕒 2025 17:56:25

🔧 由 treeman 更新於 13 🕒 2025 18:02:12