TWCA 憑證置換工具 使用說明

適用對象：收到 TWCA「憑證置換」通知信的用戶。本工具不需要安裝 Java，也不需要技術背景。

1. 這個工具做什麼？

TWCA 已使用您原本的憑證申請檔（CSR）重新簽發新憑證，並以通知信附件（zip 檔）寄給您。 因為沿用**原本的金鑰**，zip 檔中只有「新憑證」與「中繼憑證」，沒有金鑰，不能直接安裝到伺服器。

本工具會將 **zip 檔中的新憑證** 與 **您原有的金鑰檔（或舊的 PFX / JKS 檔）** 合併，產生可直接安裝的新 PFX 或 JKS 檔。
Nginx / Apache 用戶則可直接將 zip 轉成單一 PEM 檔（不需要金鑰）。

工具完全在您的電腦上執行，不會上傳任何檔案或密碼。

2. 開始前請準備

項目	說明
通知信附件 zip 檔	就是 TWCA 寄給您的「憑證置換」通知信中的附件，檔名為貴單位的**統一編號**（例如 `12345678.zip`）。 請在信件中點選附件 →「下載」或「另存新檔」，存到電腦（例如「下載」資料夾）。**不需要解壓縮**。 zip 檔內含：新的伺服器憑證、中繼憑證。
舊的金鑰或憑證檔 （三種擇一）	**金鑰檔**：當初產生 CSR 時一起產生的檔案，副檔名通常是 `.key`（有時是 `.pem`）。 **PFX 檔**：目前伺服器使用中的憑證檔，副檔名 `.pfx` 或 `.p12`（IIS、Windows 常見）。 **JKS 檔**：Java / Tomcat 使用的金鑰庫，副檔名 `.jks` 或 `.keystore`。 手上有哪一種就用哪一種。不確定時請詢問系統管理員或網站維護廠商。
舊檔密碼	PFX / JKS 檔一定有密碼；.key 檔若當初沒有設密碼則不需要。

啟動工具

1. 將 `CertReplaceTool.zip` 解壓縮到任一資料夾（例如桌面）。
2. 開啟 `CertReplaceTool` 資料夾，雙擊 `CertReplaceTool.exe`。

> 若出現「Windows 已保護您的電腦」，請點「其他資訊」→「仍要執行」。

3. 操作步驟

工具畫面如下（範例資料），由上而下完成 5 個步驟，最後按「開始轉換」。



步驟 1：選擇通知信附件的 zip 檔

按「瀏覽...」，選擇剛才從通知信存下來的 zip 檔。選好後畫面會顯示以下資料，**請確認是貴單位的網站**：

欄位	說明
統一編號	zip 檔名
公司名稱 / 英文名稱	憑證所屬單位
網域（domain）	此憑證使用的網站網址
有效期間、簽發 CA	新憑證的效期與簽發單位

資料不正確時請勿繼續，並聯絡 TWCA 客服。工具也會自動在步驟 5 帶入建議的存檔檔名。

步驟 2：選擇舊的金鑰或舊憑證檔（三擇一）

1. 依手上的檔案種類，在對應的那一列按「瀏覽...」選擇檔案。
2. 在「舊檔密碼」輸入該檔案的密碼（.key 檔若無密碼可留空）。

若 JKS 檔內的金鑰另有不同密碼，轉換時會跳出視窗請您輸入。

輸出 PEM（Nginx / Apache）時本步驟**可不選**；有選的話，工具會幫您檢查金鑰與新憑證是否成對。

步驟 3：根憑證（可不選）

一般情況**留空即可**。只有系統管理員要求「完整憑證鏈（含根憑證）」時，才選擇根憑證檔（例如 `global_rca.cer`）。選錯可按「清除」。

步驟 4：選擇輸出格式並設定新檔密碼

輸出格式	適用
PFX（預設）	IIS、Windows Server、Exchange、F5、FortiGate 等大多數設備
JKS	Tomcat、WebLogic、WebSphere、JBoss 等 Java 系統
PEM	Nginx、Apache 2.4.8 以上。輸出伺服器憑證 + 中繼憑證合併的單一檔案（fullchain），不含金鑰

原本用 PFX 就選 PFX，原本用 JKS 就選 JKS。新檔密碼至少 6 個字元，需輸入兩次；也可按「同舊檔密碼」。**請記住此密碼**，安裝時會用到。PEM 不需要密碼。

PFX 的加密方式由工具自動決定，不需設定：舊檔是 PFX 時沿用舊檔的加密方式；舊檔是 .key 或 JKS 時，使用與 Windows 預設相同、相容舊版 Windows 的方式。

步驟 5：選擇存檔位置

已自動帶入建議檔名（與 zip 檔同一資料夾），通常不需修改。工具不會覆蓋原本的舊檔。

按「開始轉換」

工具會檢查舊金鑰與新憑證是否成對、憑證鏈是否完整，並在產生後重新讀取確認。成功後會顯示新檔案位置、憑證名稱、有效期間與憑證鏈，按「開啟所在資料夾」即可找到新檔案。

4. 轉換完成後

1. 將新檔案與新檔密碼交給系統管理員，安裝至伺服器取代舊憑證。
2. 安裝後用瀏覽器開啟網站，點網址列的鎖頭查看憑證，確認有效期間已是新憑證。
3. 舊的金鑰 / PFX / JKS 檔請妥善保存，確認新憑證正常運作前不要刪除。

系統管理員安裝參考

伺服器	作法
IIS	IIS 管理員 → 伺服器憑證 → 匯入新 PFX → 至網站「繫結」將 https 改用新憑證。
Tomcat	將 `server.xml` 中的 keystore 檔案指向新 JKS / PFX，更新密碼後重新啟動。JKS 別名（alias）請使用成功畫面上顯示的名稱。
Nginx	將 `ssl_certificate` 改為工具產生的 `..._fullchain.pem`；`ssl_certificate_key` 沿用原本的 .key，不用換。執行 `nginx -t` 確認後 `nginx -s reload`。
Apache	2.4.8 以上：`SSLCertificateFile` 改為「憑證CN_fullchain.pem」，`SSLCertificateKeyFile` 不用換；若原先有宣告 `SSLCertificateChainFile` 屬性，請務必註解，避免憑證鏈串接錯誤。

5. 常見問題

畫面訊息	處理方式
舊金鑰與 zip 檔內的新憑證不相符	選到其他網站的金鑰或舊檔，或 zip 不是本次通知信的附件。請確認網域相同，或改用伺服器上目前使用中的 PFX / JKS。
舊檔密碼錯誤	請確認大小寫、全形半形。若遺失密碼，請洽系統管理員。
此金鑰檔有密碼保護	請在「舊檔密碼」輸入 .key 檔的密碼。
檔案中找不到私鑰	選到的是憑證檔（.cer / .crt），不是金鑰檔。
Nginx 出現 key values mismatch	金鑰與憑證不成對。請確認 `ssl_certificate_key` 指向的是本網站原本的 .key；也可在工具步驟 2 選擇該 .key 再轉換一次，工具會幫您檢查。
舊檔中沒有私鑰	此 PFX / JKS 只有憑證，請改選伺服器上正在使用、含金鑰的那一份。
zip 檔內找不到任何憑證檔	請確認選擇的是通知信的原始附件 zip。
根憑證與此憑證鏈不符	步驟 3 選錯檔案，按「清除」留空即可。

找不到舊金鑰，也沒有 PFX / JKS？

本次換發沿用原金鑰，必須有原金鑰才能使用新憑證。若確定遺失，請聯絡 TWCA 客服，改以新的 CSR 重新申請。