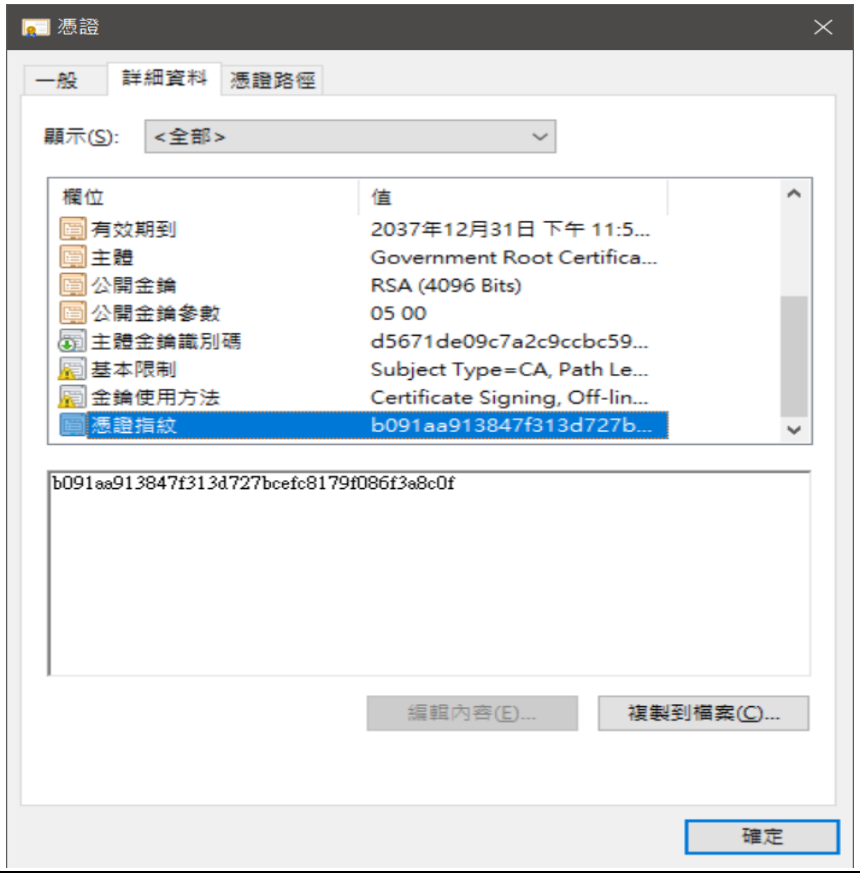
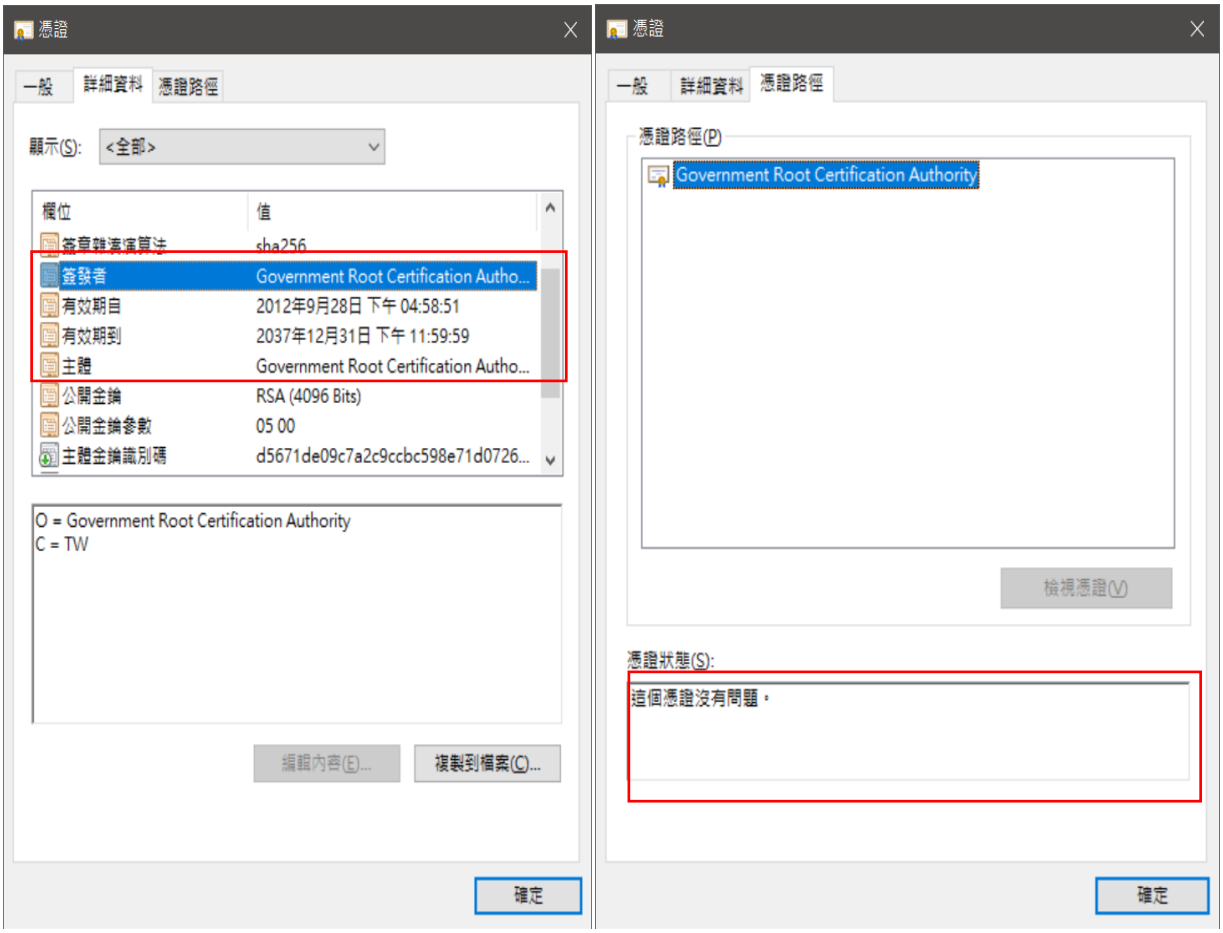
PKI-Based 應用系統對公鑰憑證處理之安全檢查表

檢查項目 1：系統應該由安全管道取得 Root CA 的自簽憑證（Self-Signed Certificate），並妥善地安全保存於系統中
建議做法：由 GRCA 網站 https://grca.nat.gov.tw/01-06.html 的儲存庫中下載 GRCA2 自簽憑證，並檢查其憑證指紋應為 b091aa913847f313d727bcefc8179f086f3a8c0f，才可放入應用系統中 
驗證結果：☐ 是 ☐ 否

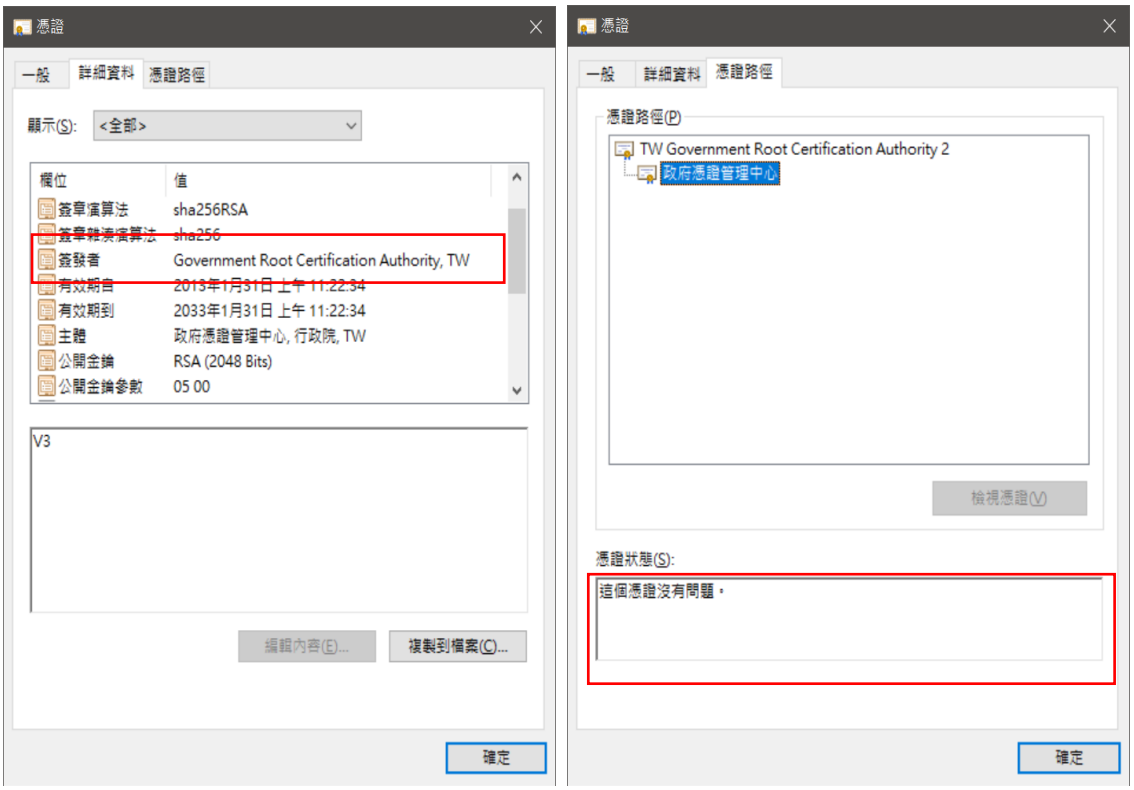
檢查項目 2：系統應該設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求，並對於不符保證等級的憑證應該加以拒絕（例如正式上線系統應該對測試等級的憑證加以拒絕）
建議做法：由 GTestCA 網站 https://gtestca.nat.gov.tw/ 申請測試憑證，並嘗試以該憑證登入系統，正式系統應拒絕測試憑證登入。
驗證結果：☐ 是 ☐ 否

檢查項目 3：系統應該檢查 CA 本身的憑證確實為 Root CA 所簽發的憑證（至少需檢查憑證的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CA 本身憑證的簽章）

建議做法：檢視 GRCA2 自簽憑證，並確認其 DN 與簽章值正確

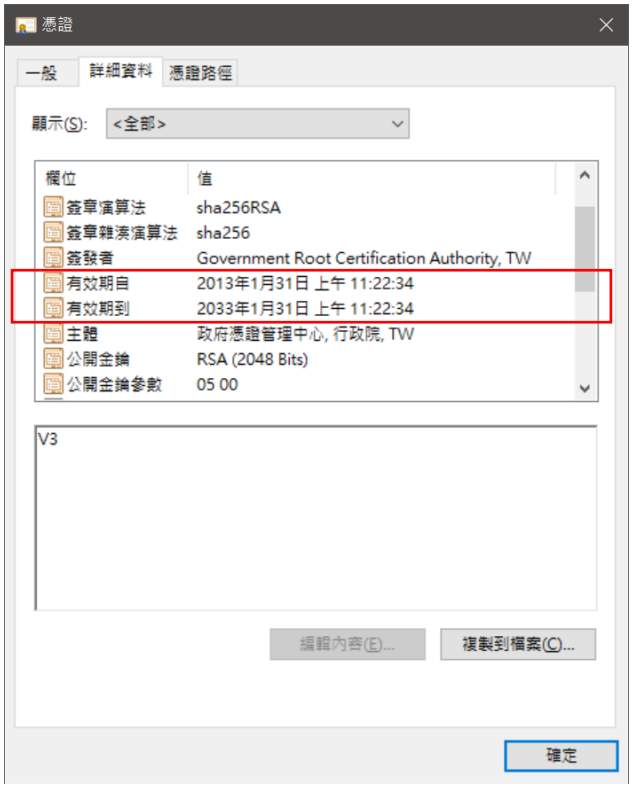


驗證結果：☐ 是 ☐ 否

檢查項目 4：系統應該檢查 CA 本身的憑證確實為 Root CA 所簽發的憑證（至少需檢查憑證的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CA 本身憑證的簽章）
建議做法：以第二代政府憑證管理中心為例，檢視 GCA2 憑證，並確認其 DN 與簽章值正確 
驗證結果：☐ 是 ☐ 否

檢查項目 5：系統應該檢查 CA 本身的憑證是否仍在有效期限之內（例如檢查系統時間是否仍落在憑證所記載的 Validity 時間範圍內）
注意：憑證是以世界標準時間（UTC，或稱為格林威治時間）來記載 Validity 時間範圍，因此系統不應拿本地時間（Local Time）直接與憑證 Validity 時間範圍相比較。

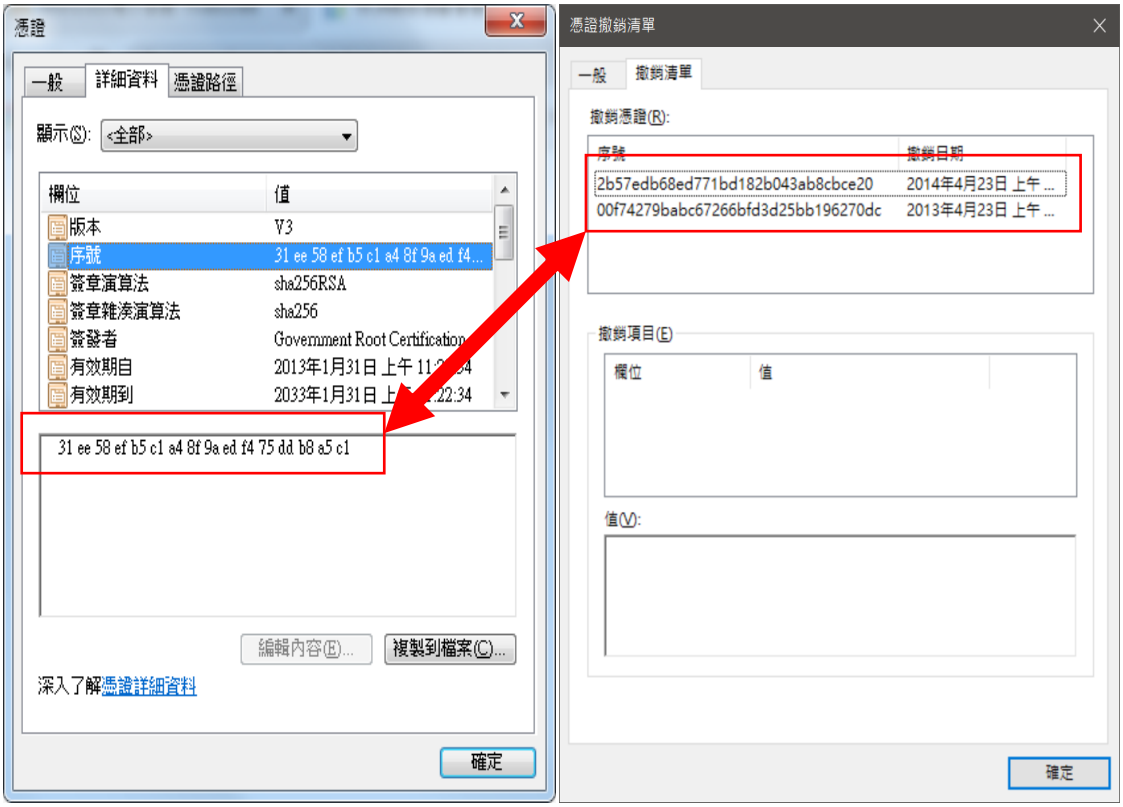
建議做法：以第二代政府憑證管理中心為例，檢視 GCA2 憑證，並確認其憑證效期(windows 檢視憑證會自動轉換成本地時間)



驗證結果：☐ 是 ☐ 否

檢查項目 6：系統應該檢查 CA 本身的憑證是否已被廢止（例如定期下載 Root CA 簽發的 CARL 來檢查憑證廢止狀態）

建議做法：以第二代政府憑證管理中心(GCA2)為例，應定期下載 http://grca.nat.gov.tw/repository/CRL2/CA.crl 於系統中，並確認 GCA2 之憑證序號未列於撤銷憑證清單中。

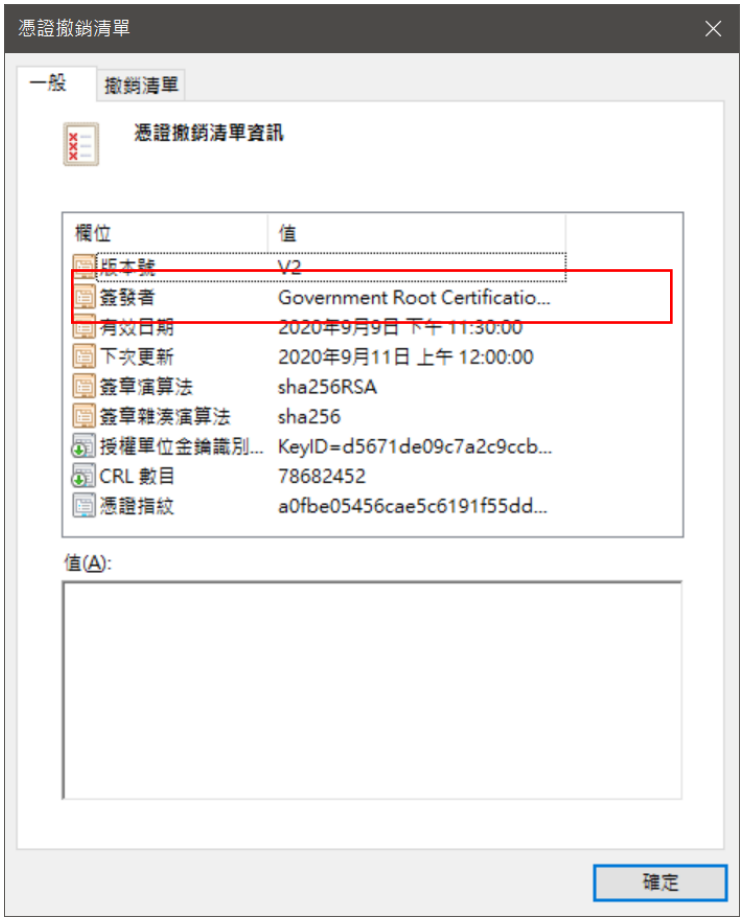


GCA2 憑證檔檔案　　GRCA CRL 廢止清冊

驗證結果：☐ 是 ☐ 否

檢查項目 7：系統應該檢查 CARL 是否確實是 Root CA 所簽發（至少需檢查 CARL 的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CARL 的簽章）

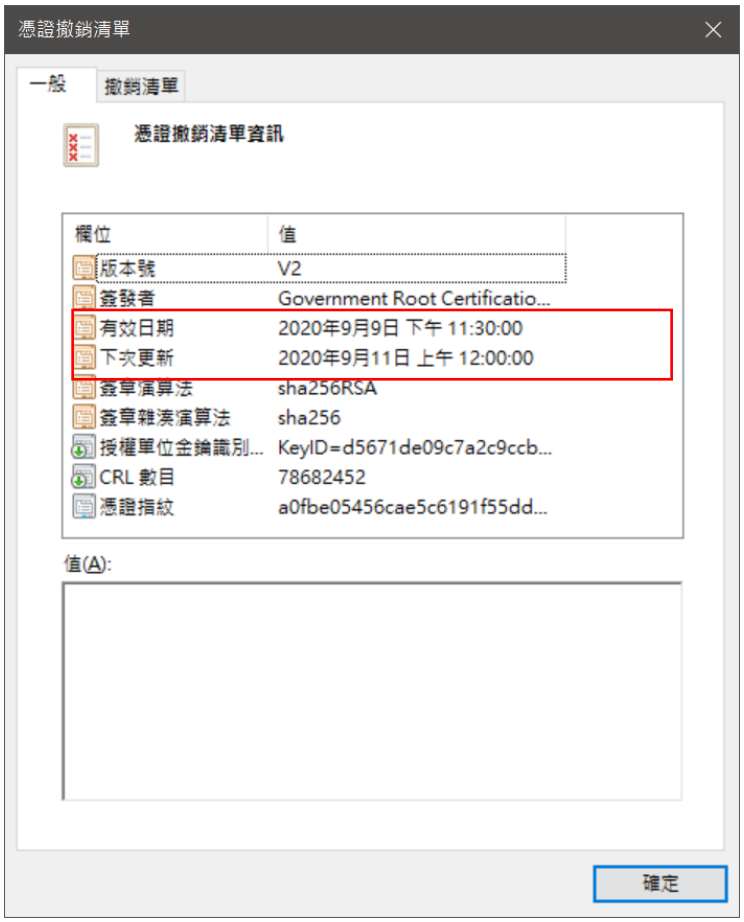
建議做法：檢視下載的 CARL 憑證廢止清單



驗證結果：☐ 是 ☐ 否

檢查項目 8：系統應該檢查 CARL 是否為最新公佈的 CARL（當天公佈的 CARL）注意：CARL 的更新時間也是是以世界標準時間（UTC，或稱為格林威治時間）來記載，因此系統不應拿本地時間（Local Time）直接與 CARL 的更新時間相比較。

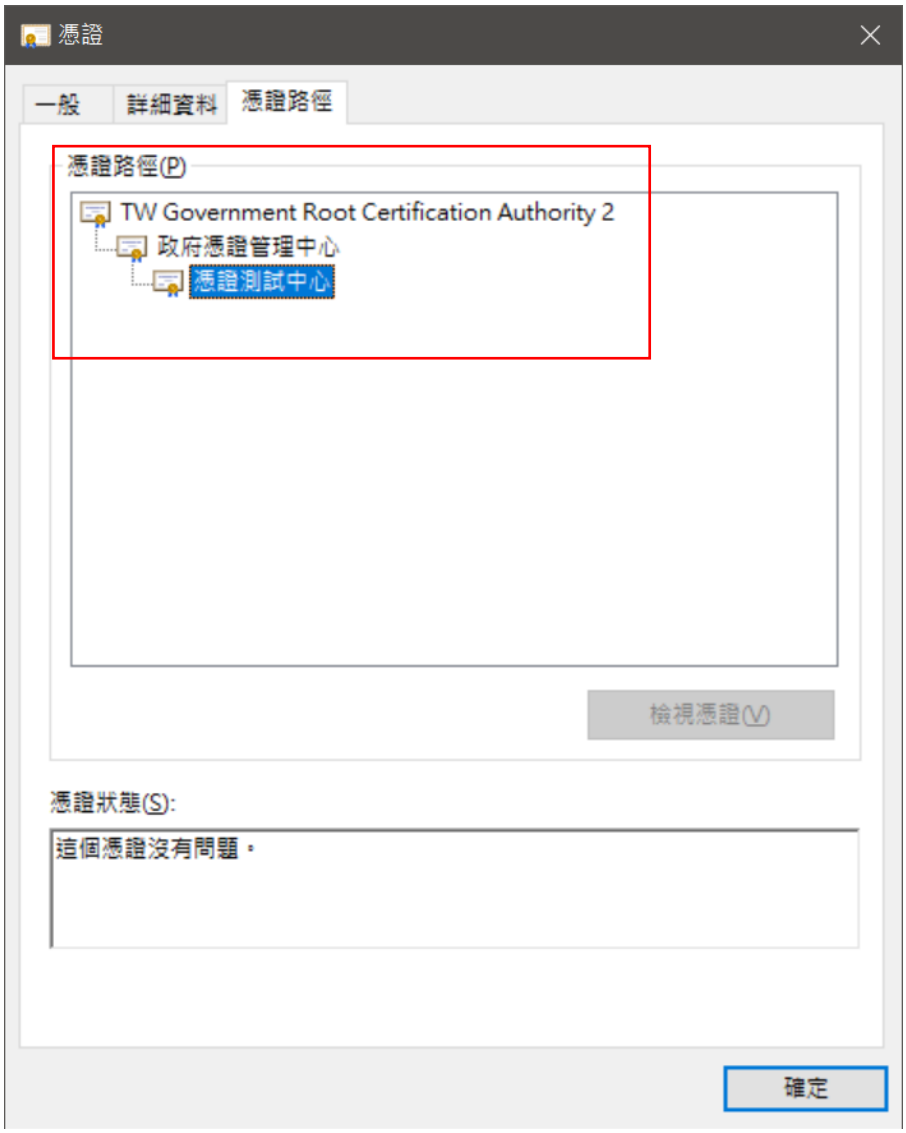
建議做法：檢視下載的 CARL 憑證廢止清單中的有效日期與下次更新，現在時間應落於兩者之間，windows 會自動轉成當地時間



驗證結果：☐ 是 ☐ 否

檢查項目 9：系統應該檢查用戶的憑證確實為合法 CA 所簽發的憑證（至少需檢查用戶憑證的 Issuer Name (DN)是否與 CA 憑證的 Subject Name(DN)相符，並以 CA 憑證所記載的
Public Key 檢驗用戶憑證的簽章）

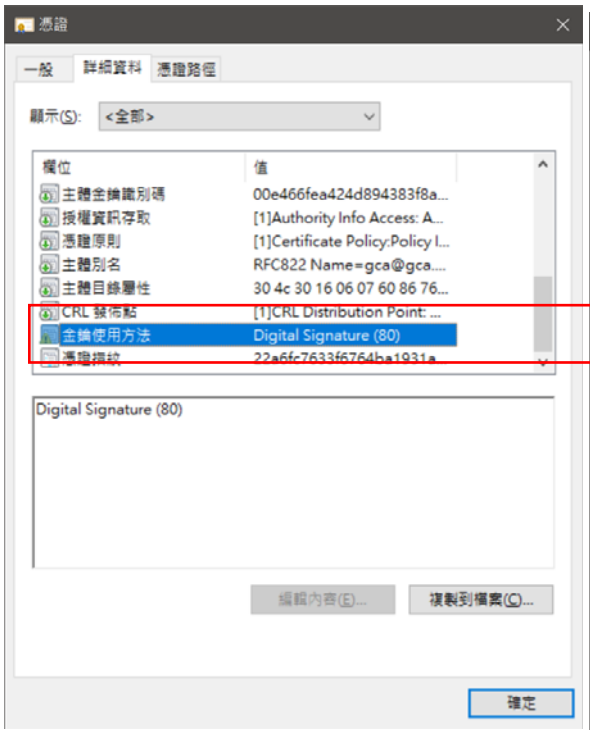
建議做法：請應用系統提供通過驗證之憑證，並檢視該憑證資料是否能通過憑證的路徑檢查如下圖



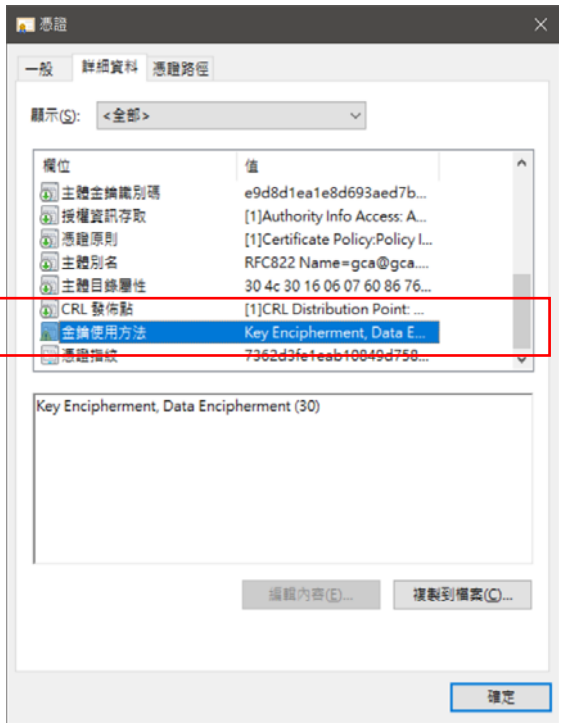
驗證結果：☐ 是 ☐ 否

檢查項目 10：系統應該檢查用戶憑證金鑰用途（KeyUsage）欄位所記載的金鑰用途符合使用目的（簽章/驗簽或加密/解密）

建議做法：請應用系統提供通過驗證之憑證，並檢視該憑證詳細內容是使用符合使用目的之金鑰用途



簽章用憑證

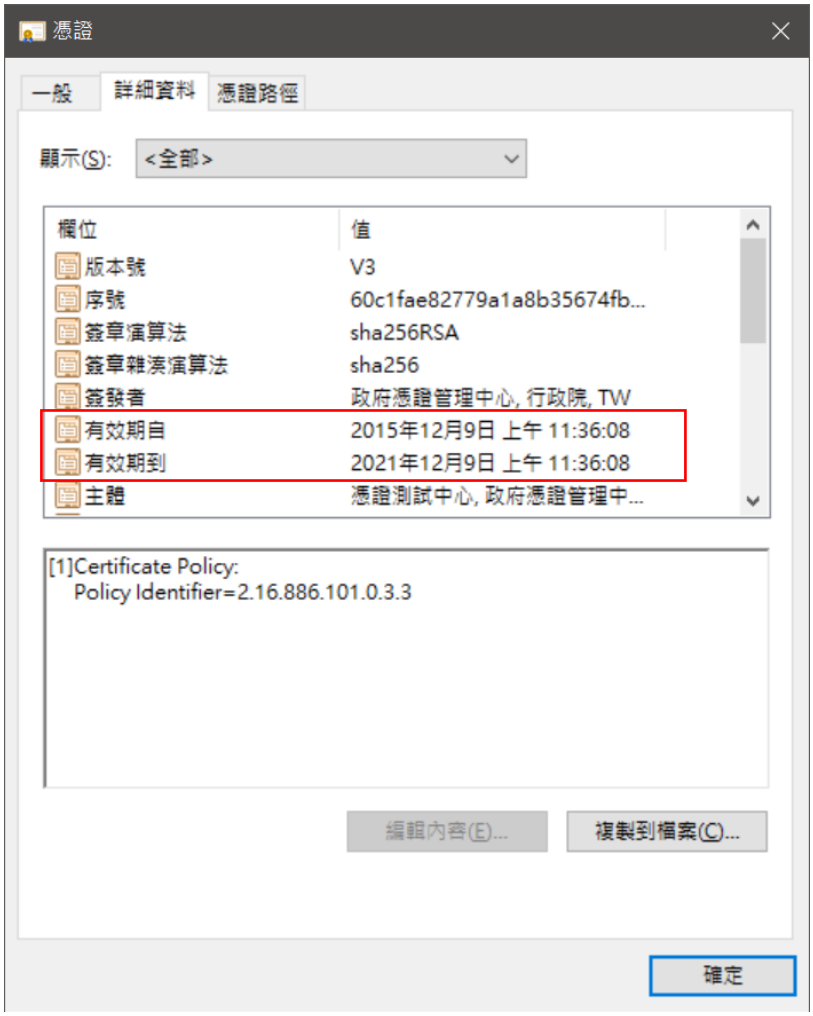


加解密用憑證

驗證結果：☐ 是 ☐ 否

檢查項目 11：系統應該檢查用戶的憑證是否仍在有效期限之內（例如檢查系統時間是否仍落在憑證所記載的 Validity 時間範圍內）
注意：憑證是以世界標準時間（UTC，或稱為格林威治時間）來記載 Validity 時間範圍，因此系統不應拿本地時間（Local Time）直接與憑證 Validity 時間範圍相比較。

建議做法：
新系統上線前的做法:
請應用系統調整系統時間至某張可通過驗證之憑證生效時間之前與後，再嘗試登入系統，系統應拒絕該憑證之登入。以下圖憑證為例，應調整時間至 2015/12/9 之前做一次測試，再調整時間至 2021/12/10 之後再做一次測試。
現行系統的做法:
建議使用一張確認已過期的憑證做測試，系統應拒絕該憑證之登入。

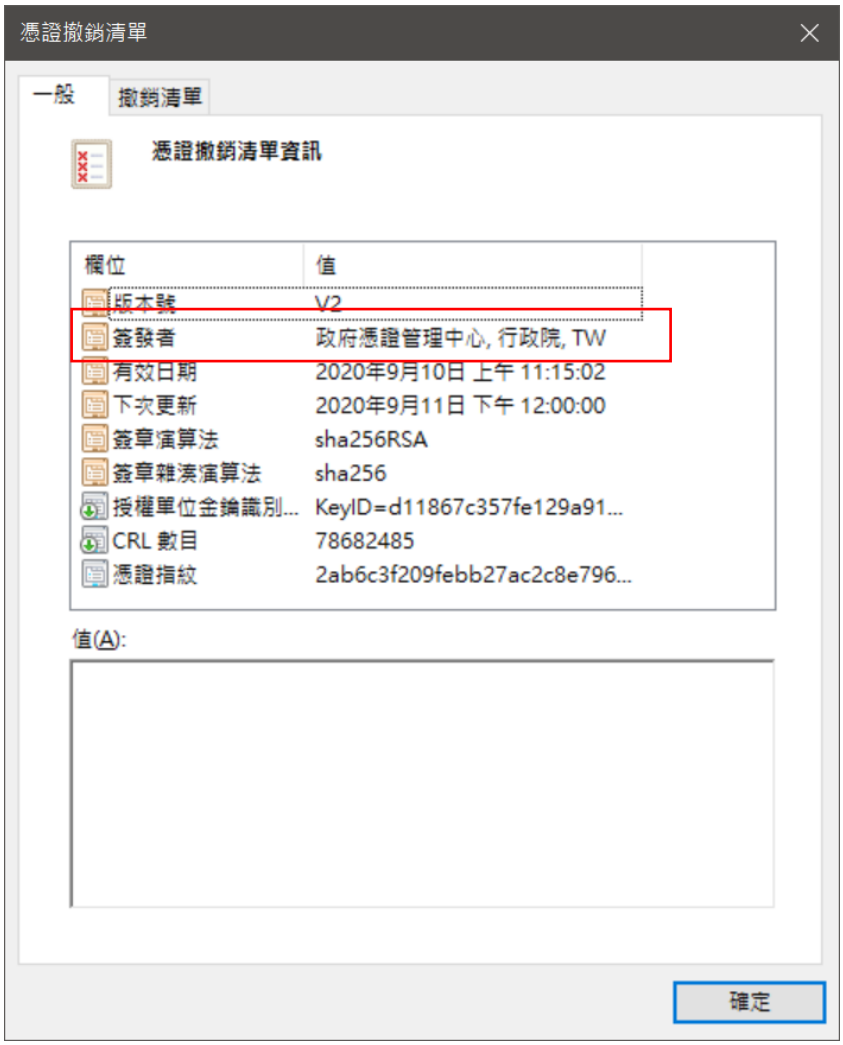


驗證結果：☐ 是 ☐ 否

檢查項目 12：系統應該檢查用戶的憑證是否已被廢止（例如定期下載 CA 簽發的 CRL 來檢查憑證廢止狀態或透過 OCSP 來檢查憑證廢止狀態）
建議做法： **方法一：系統採取 CRL 進行憑證廢止檢查** 1. 至憑證官方網站停用一張原本通過系統驗證之憑證。 2. 隔 1 日再以該張憑證進行登入/簽章，系統應拒絕該憑證登入/簽章。 3. 至憑證官方網站復用該張憑證。 4. 隔 1 日再以該張憑證進行登入/簽章，系統應接受該憑證登入/簽章。 **方法二：系統採取 OCSP 進行憑證廢止檢查** 1. 至憑證官方網站停用一張原本通過系統驗證之憑證。 2. 以該張憑證進行登入/簽章，系統應拒絕該憑證登入/簽章。 3. 至憑證官方網站復用該張憑證。 4. 再以該張憑證進行登入/簽章，系統應接受該憑證登入/簽章。
驗證結果：□ 是 □ 否

檢查項目 13：系統應該檢查 CRL 是否確實是合法 CA 所簽發（至少需檢查 CRL 的 Issuer Name (DN)是否與 CA 本身憑證的 Subject Name(DN)相符，並以 CA 本身憑證所記載的 Public Key 檢驗 CRL 的簽章）（如果使用 OCSP 查詢，則本項不適用）

建議做法：檢視下載的 CRL 憑證廢止清單，其簽發者應與 CA 憑證 Subject Name 相符。

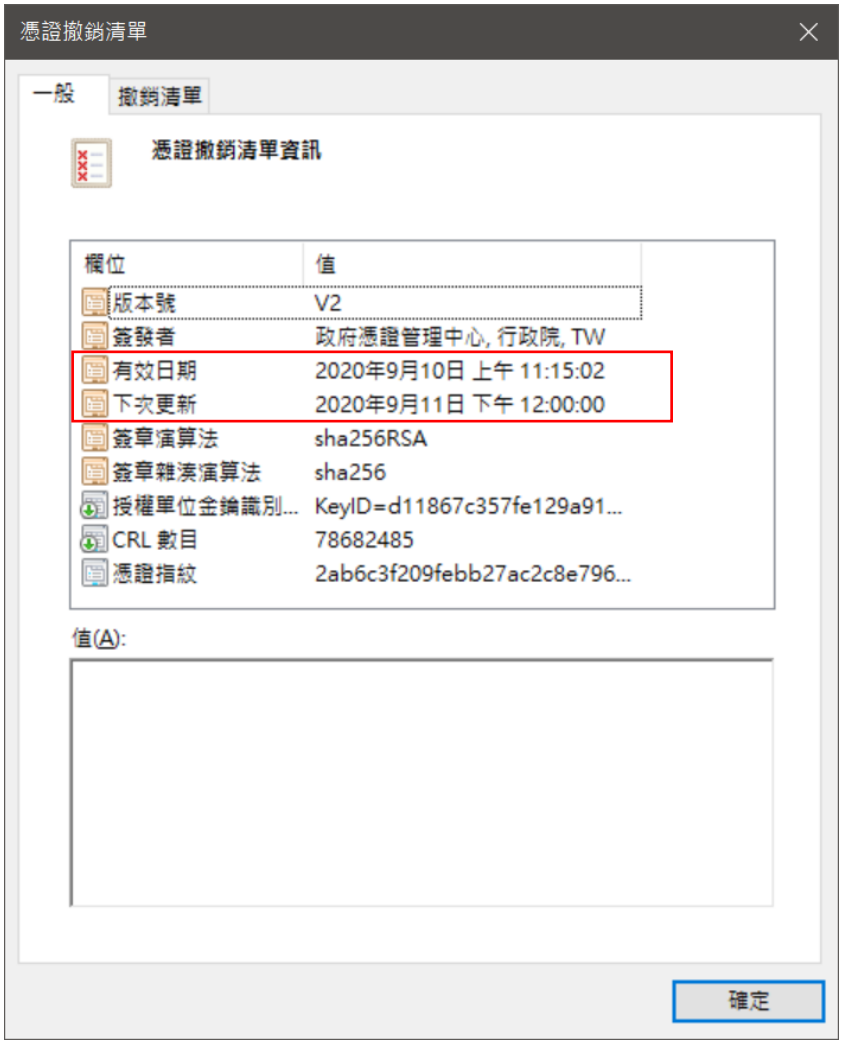


驗證結果：☐ 是 ☐ 否 ☐ 不適用

檢查項目 14：系統應該檢查 CRL 是否為最新公佈的 CRL（當天公佈的 CRL）（如果使用 OCSP 查詢，則本項不適用）

注意：CRL 的更新時間也是是以世界標準時間（UTC，或稱為格林威治時間）來記載，因此系統不應拿本地時間（Local Time）直接與 CRL 的更新時間相比較。

建議做法：檢視應用系統下載的 CRL 憑證廢止清單中的有效日期與下次更新，現在時間應落於兩者之間，windows 會自動轉成當地時間，。



驗證結果：☐ 是 ☐ 否 ☐ 不適用

檢查項目 15：系統應該要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分
建議做法：請應用系統提供可通過驗證的封包，並嘗試修改封包資訊的其中任何一個字元後，請應用系統再次驗證該封包，應用系統應回應該封包簽章不正確，並拒絕登入/簽章
驗證結果：□ 是 □ 否

檢查項目 16：系統應該要具備防止或偵測用戶加簽之訊息遭到非法重送（Replay）的機制（例如在加簽訊息中加入 Challenge-Response 或 Nonce 機制）
建議做法： 請應用系統提供可通過驗證的封包，並請應用系統再次嘗試驗證該封包，應用系統應回應該封包簽章為重送封包，並拒絕登入/簽章。
驗證結果：□ 是 □ 否

檢查項目 17：系統傳送用戶隱私資料時應該要以強度 128 bits 以上的安全通道加以保護（例如使用 TLS 安全通道或是對傳送的訊息以數位信封加密）(若系統並不涉及傳送用戶隱私資料時，則本項不適用）
建議做法： 使用第三方 TLS 檢驗，如 https://www.ssllabs.com/ssltest/ 並輸入應用系統網站，進行 TLS 安全強度檢驗
驗證結果：□ 是 □ 否 □ 不適用

檢查項目 18：系統應該定期校時，以保持系統時間之正確性(例如定期透過 NTP 自動校時)
建議做法： 檢查系統 NTP 自動校時設定，或是手動變更時間後，確認 NTP 能將時間校正回正確時間
驗證結果：□ 是 □ 否

檢查項目 19~21：附卡授權機制相關驗證
建議做法： 一般應用系統無須檢查此項目
驗證結果：□ 是 □ 否 ■不適用