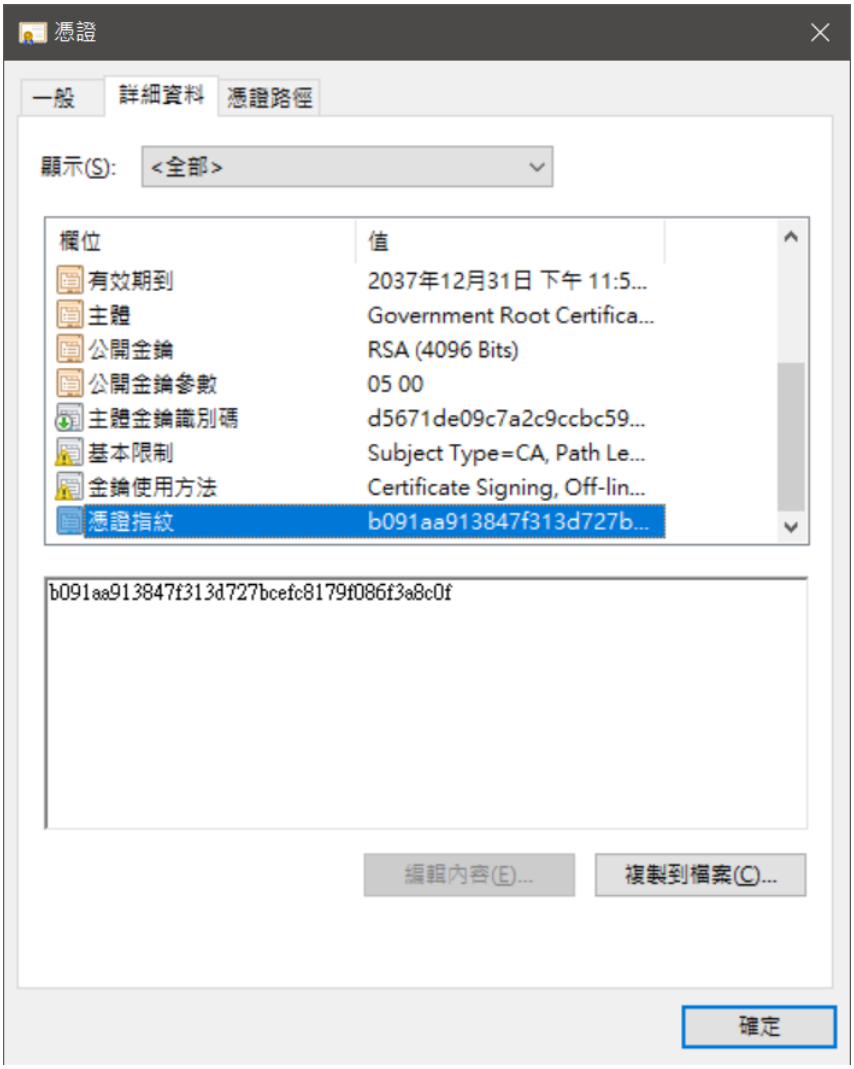
應用系統使用公鑰憑證處理之安全檢查表說明

檢查項目1：

系統應由安全管道取得 Root CA 的自簽憑證(Self-Signed Certificate)，並妥善安全保存於系統中

建議做法：

由 GRCA 網站 https://grca.nat.gov.tw/ 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。



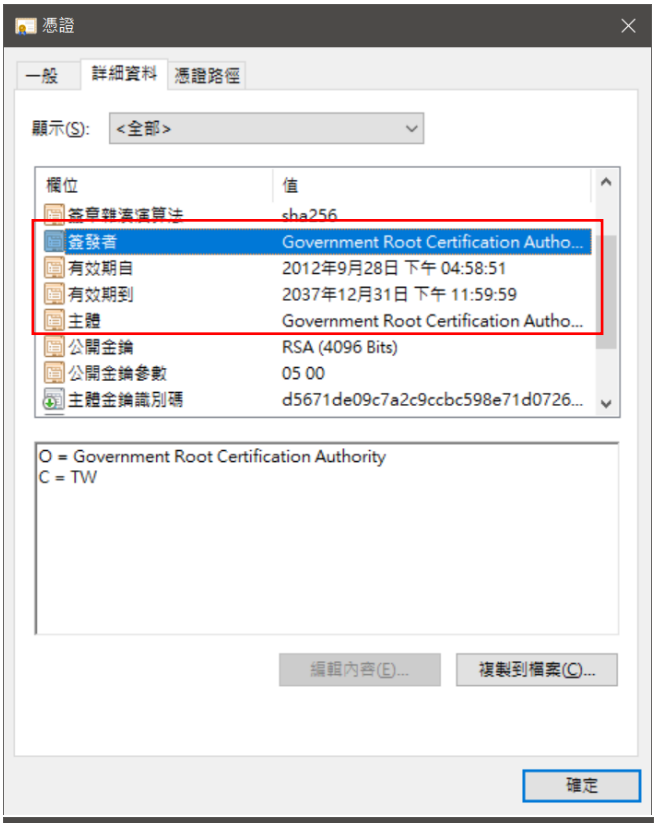
驗證結果：□ 是 □ 否

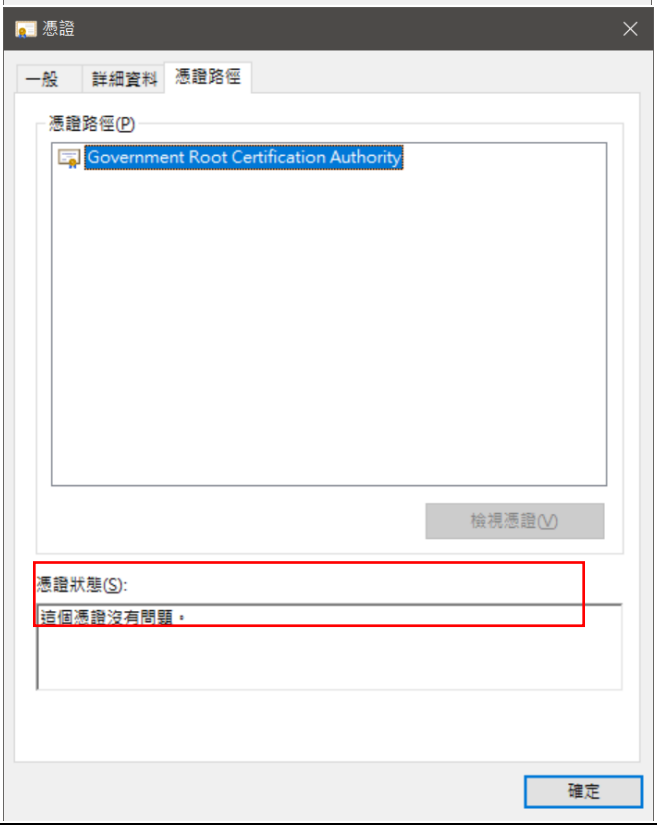
檢查項目2： 系統應設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求，對於不符保證等級之憑證應拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)
建議做法： 由 GTestCA 網站 https://gtestca.nat.gov.tw/ 申請測試憑證，並嘗試以該憑證登入系統，正式系統應拒絕測試憑證登入。
驗證結果：□ 是 □ 否

檢查項目3：

系統應檢查 CA 本身憑證確為 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。





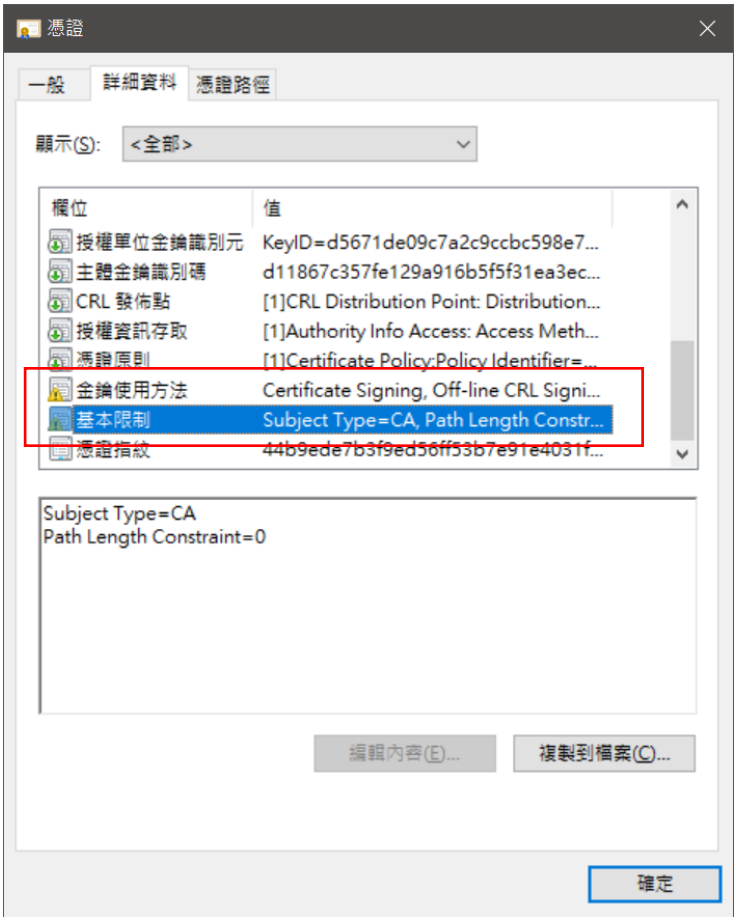
驗證結果：□ 是 □ 否

檢查項目4：

系統應檢查 CA 本身憑證確實為合法的 CA 憑證(Basic Constraints 欄位標示為 CA 憑證)，且憑證之金鑰用途(KeyUsage)欄位允許 keyCerSign 及 cRLSign 的用途

建議做法：

以第二代政府憑證管理中心為例，檢視 GCA2憑證，並確認其金鑰使用方法是 Certificate Signing, Off-line CRL Signing 及基本限制是 Subject Type=CA



驗證結果：□ 是 □ 否

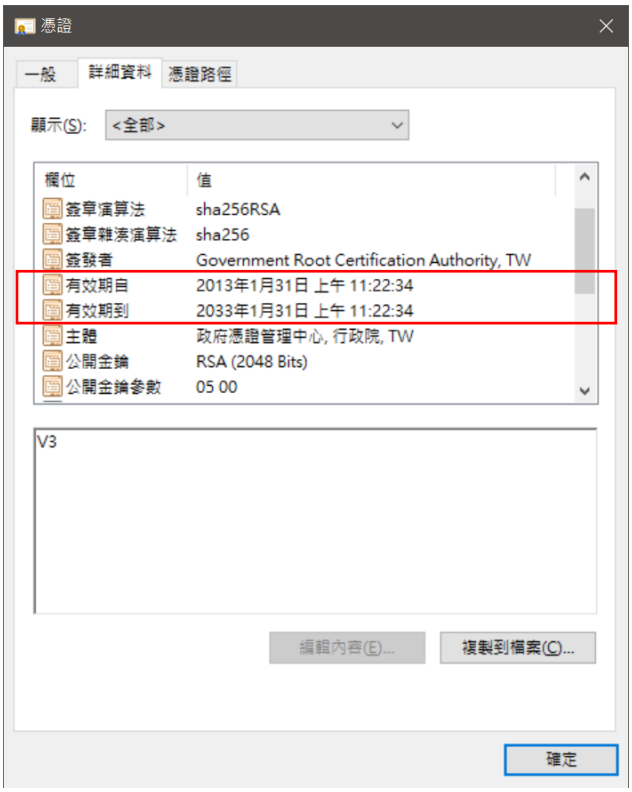
檢查項目5：

系統應檢查 CA 本身憑證是否在效期內(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)。



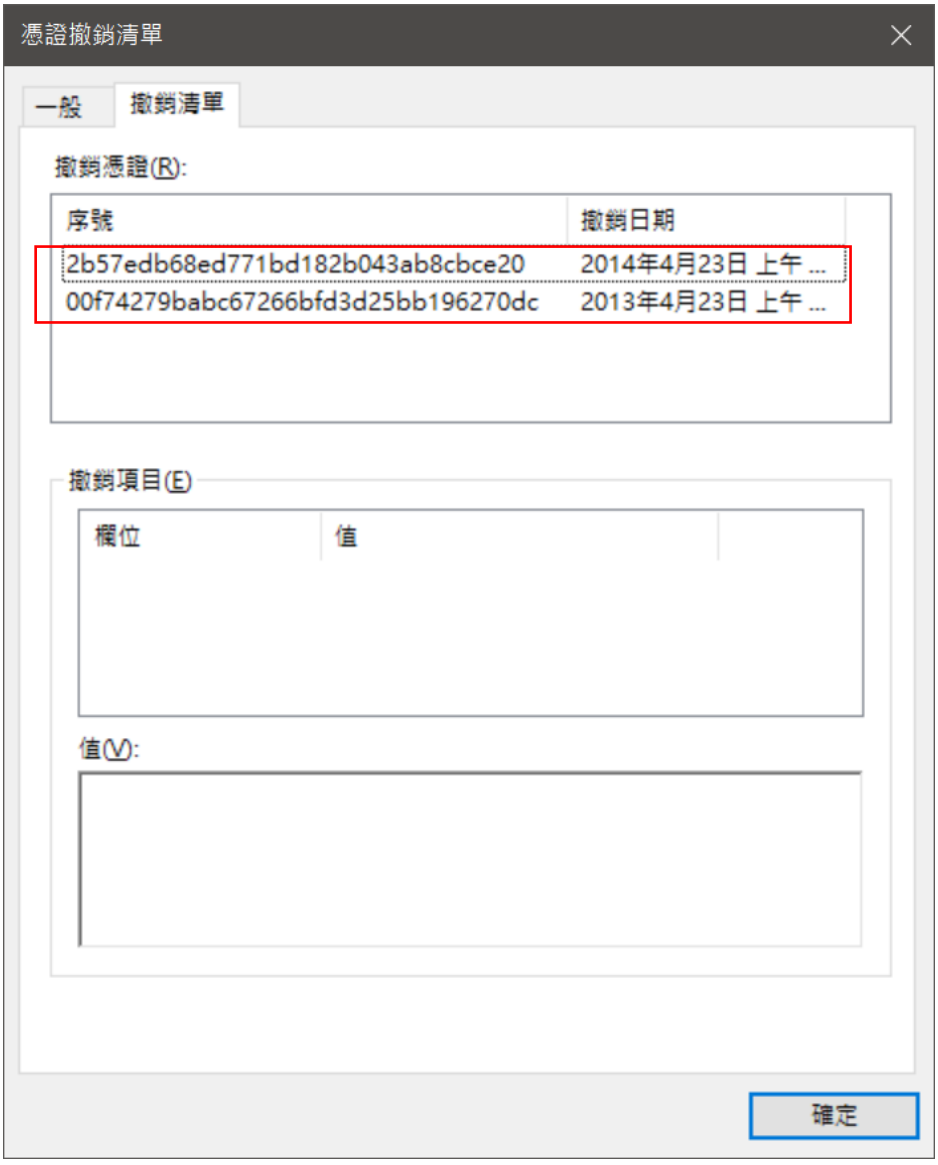
驗證結果：□ 是 □ 否

檢查項目6：

系統應檢查 CA 本身憑證是否已被廢止(例如定期下載 Root CA 簽發的憑證機構廢止清冊(CARL)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。



驗證結果：□ 是 □ 否

檢查項目7：

系統應檢查 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

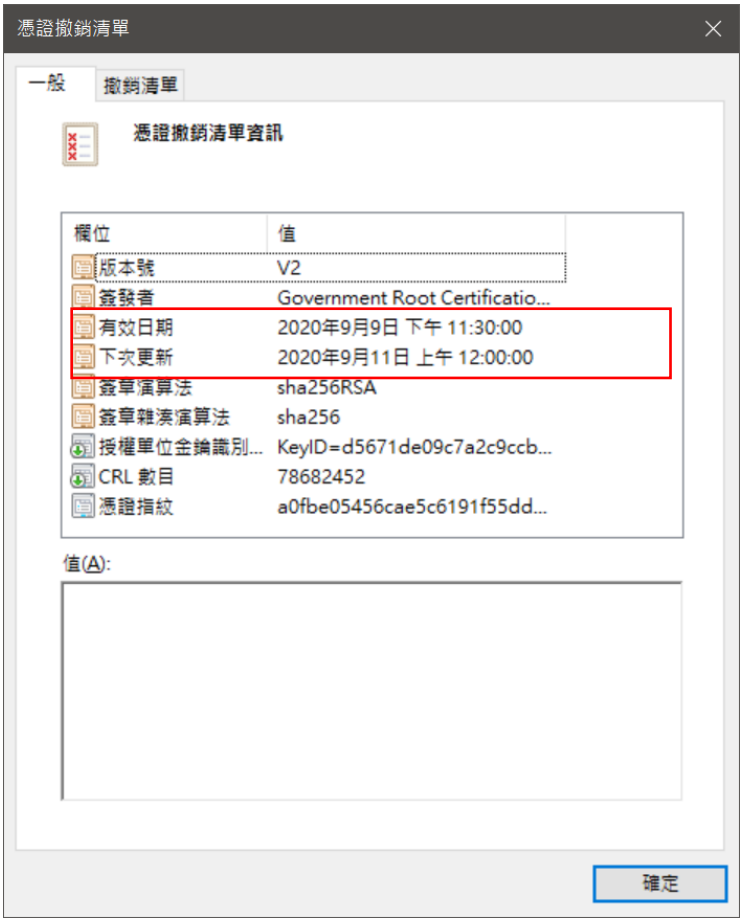
檢查項目8：

系統應檢查是否為最新的 CARL(當天公布的 CARL)

注意：CARL 的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與 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。



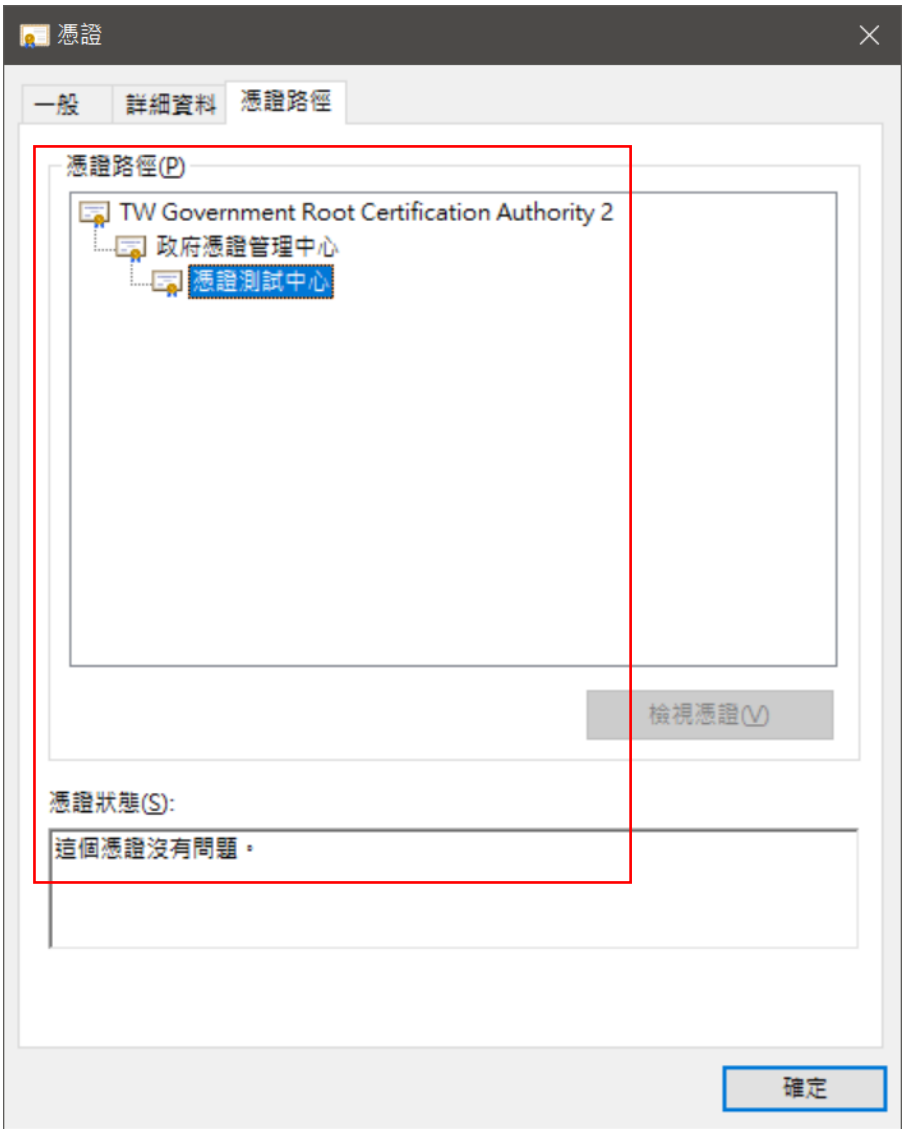
驗證結果：□ 是 □ 否

檢查項目9：

系統應檢查用戶的憑證為合法 CA 所簽發(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。



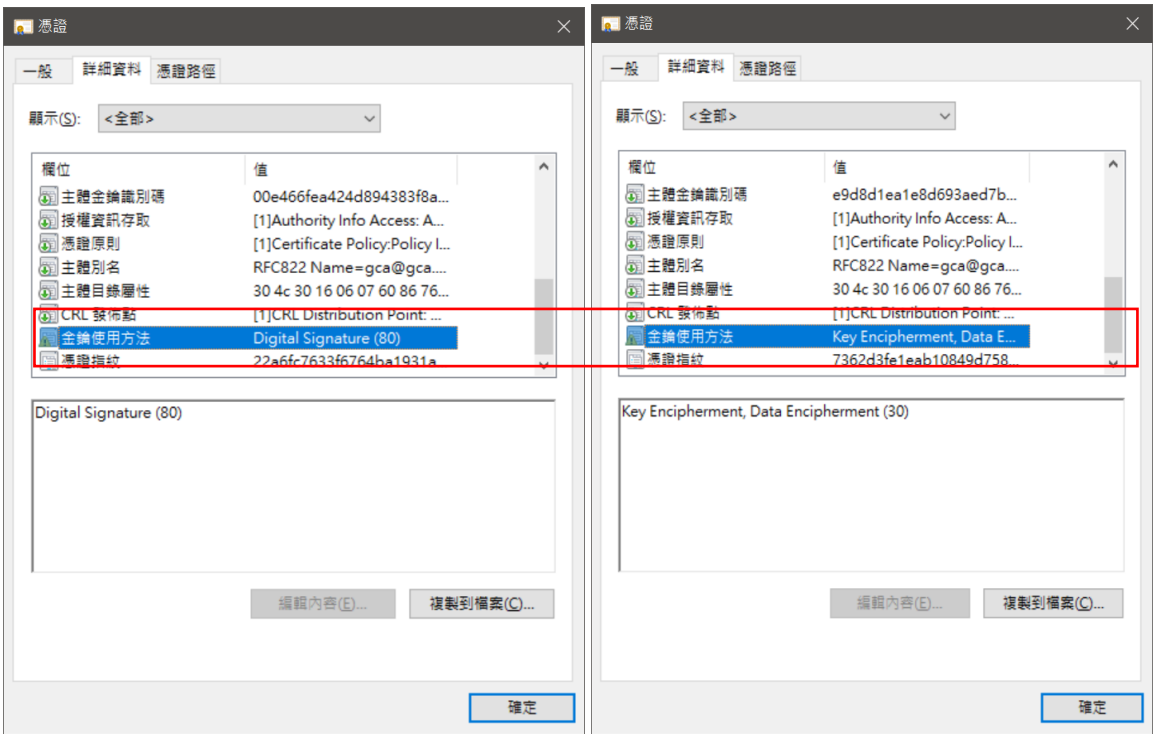
驗證結果：□ 是 □ 否

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

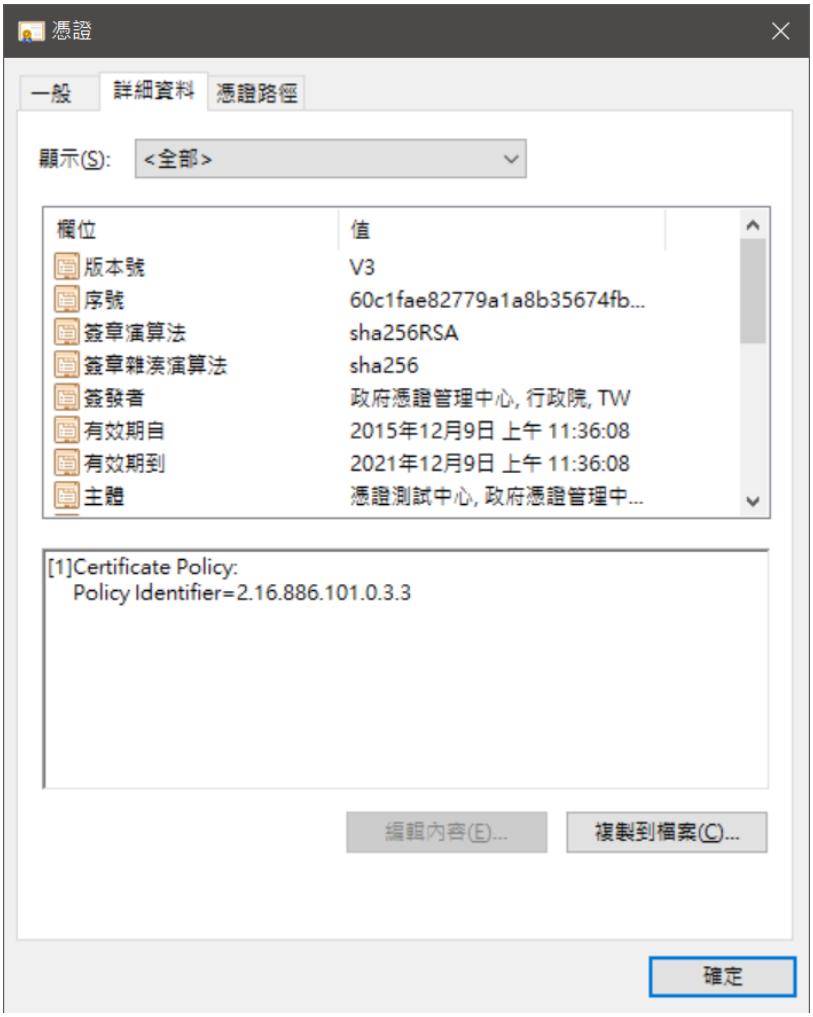
檢查項目11：

系統應檢查用戶的憑證是否在效期內(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來記載，因此系統不應拿本地時間直接與憑證 Validity 時間範圍相比較

建議做法：

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。



驗證結果：□ 是 □ 否

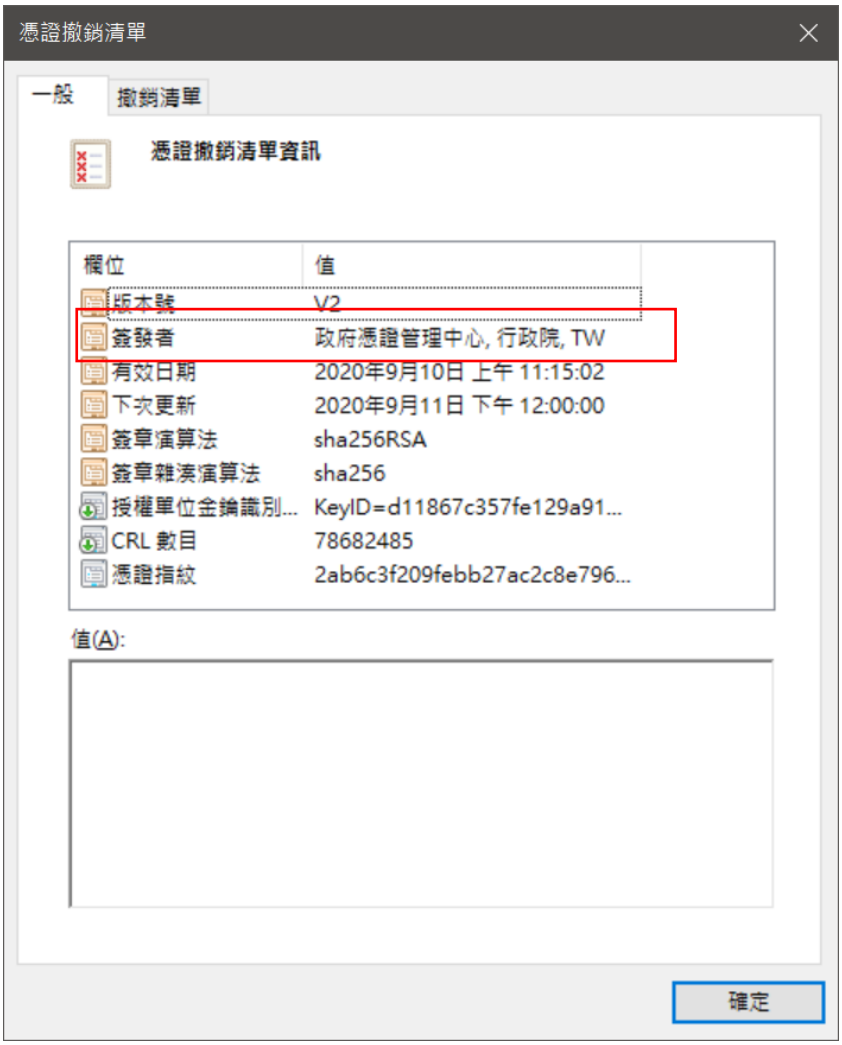
檢查項目12： 系統應檢查用戶的憑證是否已被廢止(例如定期下載 CA 簽發的憑證廢止清冊(CRL)檢查憑證廢止狀態，或透過 OCSP 來檢查憑證廢止狀態)
建議做法： 方法一：系統採取 CRL 進行憑證廢止檢查 至憑證官方網站停用一張原本通過系統驗證之憑證。 隔1日再以該張憑證進行登入/簽章，系統應拒絕該憑證登入/簽章。 至憑證官方網站復用該張憑證。 隔1日再以該張憑證進行登入/簽章，系統應接受該憑證登入/簽章。 方法二：系統採取 OCSP 進行憑證廢止檢查 1. 至憑證官方網站停用一張原本通過系統驗證之憑證。 2. 以該張憑證進行登入/簽章，系統應拒絕該憑證登入/簽章。 3. 至憑證官方網站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

系統應檢查 CRL 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

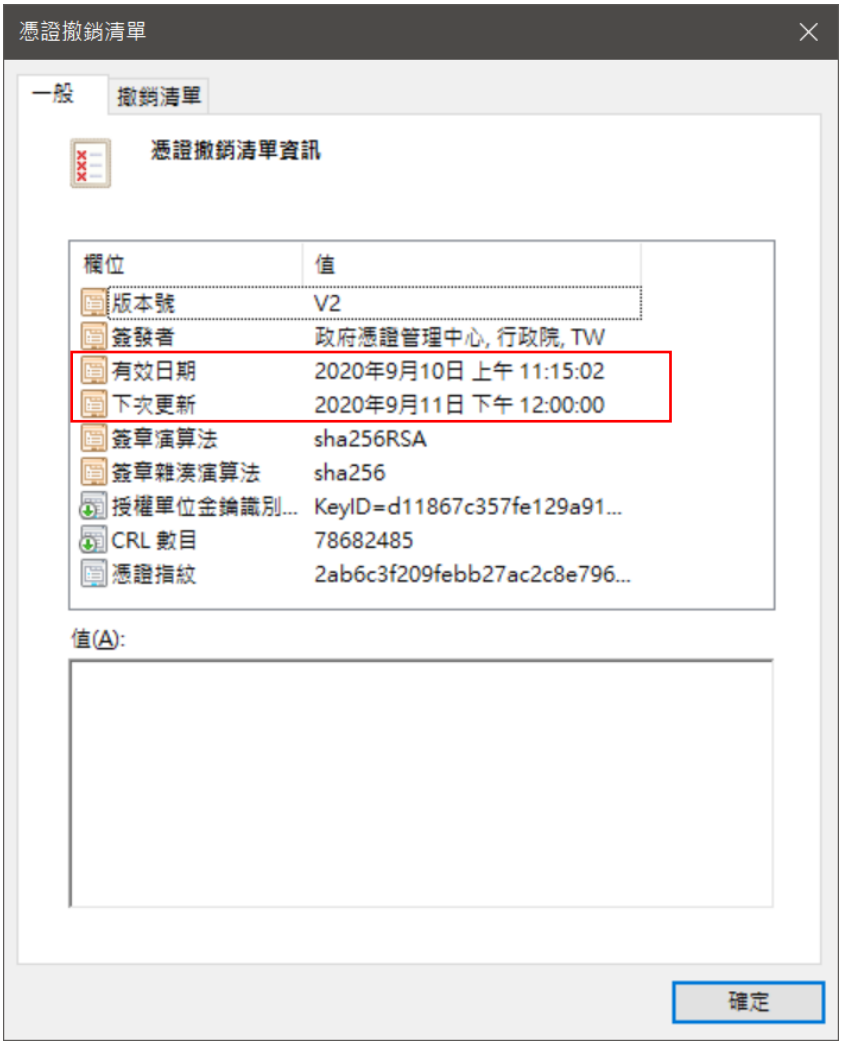
檢查項目14：

系統應檢查是否為最新公佈的 CRL(當天公布的 CRL)，如果使用 OCSP 查詢，則本項不適用

注意：CRL 的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與 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： 系統應具備防止用戶加簽之訊息遭到非法重送(Replay)之功能(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以強度128 bits 以上的安全通道進行保護(例如使用 SSL 安全通道或是對傳送的訊息以數位信封加密)，若系統未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： 政府憑證附卡授權機制相關驗證(服務已停止)
建議做法： 憑證應用系統無須檢查此項目。
驗證結果：■不適用