

附表一 PKI-Based 應用系統對公鑰憑證處理之安全檢查表  
(註：適用於使用新版 GPKI 憑證的系統)

安全檢查項目	是否合格
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	是 否
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 )	是 否
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 )	是 否
系統應該檢查 CA 本身的憑證確實為合法的 CA 憑證 ( BasicConstraints 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	是 否
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 )	是 否
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 )	是 否
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 )	是 否
系統應該檢查 CARL 是否為最新公佈的 CARL ( 當天公佈的 CARL )	是 否
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 )	是 否
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 )	是 否
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 )	是 否
系統應該檢查用戶的憑證是否已被廢止 ( 例如定期下載	是 否

安全檢查項目	是否合格		
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 )			
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 )	是 適用	否	不
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 )	是 適用	否	不
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	是	否	
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 )	是	否	
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 SSL 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 )	是 適用	否	不
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)	是	否	