認識「公鑰憑證處理安全事項檢查表」

中華電信股份有限公司
電信研究所
資通安全研究室
王文正 博士

公鑰憑證處理安全檢查表簡介

- 條列出應用系統在處理X.509公鑰憑證（一般檢簡稱「憑證」）時應注意的基本安全事項。應用系統上線前應逐項檢查是否符合各安全事項的規定，確定安全無虞後才可上線。
- 本安全事項檢查表僅列出與憑證相關的「基本」安全事項，不同的應用系統有不同的特性與複雜度，應用系統管理者應該根據系統的特性與複雜度，考慮是否有其他憑證相關的安全事項需納入檢查。
- 本安全事項檢查表僅列出與憑證相關的安全事項，憑證相關安全事項僅是整體系統安全的其中一個環節，其他與憑證無關的安全事項例如作業系統安全漏洞修補（Patch）、電腦病毒防治、防火牆設定、入侵偵測、系統安全功能的啟用、非必要服務的關閉等，應用系統管理者應該制定一套完整的安全政策（Security Policy），並實施必要的措施以符合安全政策對所有安全事項的要求。

公鑰憑證處理安全檢查項目

- 系統應該由安全管道取得Root CA的自簽憑證，並妥善地安全保存於系統中。
- 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。
- 系統應該檢查CA本身的憑證確實為Root CA所簽發的憑證。
- 系統應該檢查CA本身的憑證確實為合法的CA憑證。
- 系統應該檢查CA本身的憑證是否仍在有效期限之內。
- 系統應該檢查CA本身的憑證是否已被廢止。
- 系統應該檢查CARL是否確實是Root CA所簽發。
- 系統應該檢查CARL是否為最新公佈的CARL。

公鑰憑證處理安全檢查項目(續)

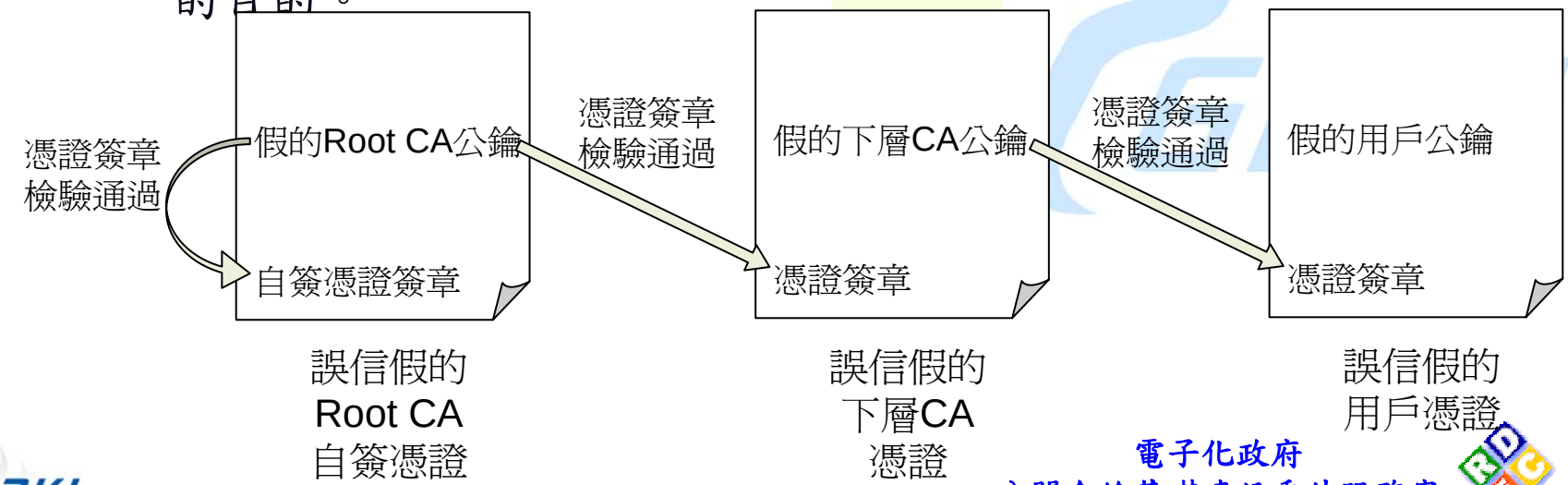
- 系統應該檢查用戶的憑證確實為合法CA所簽發的憑證。
- 系統應該檢查用戶憑證金鑰用途欄位所記載的金鑰用途符合使用目的。
- 系統應該檢查用戶的憑證是否仍在有效期限之內。
- 系統應該檢查用戶的憑證是否已被廢止。
- 系統應該檢查CRL是否確實是合法CA所簽發。
- 系統應該檢查CRL是否為最新公佈的CRL。
- 系統應該要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分。
- 系統應該要具備防止或偵測用戶加簽之訊息遭到非法重送的機制。
- 系統傳送用戶隱私資料時應該要以強度128 bits以上的安全通道加以保護。
- 系統應該定期校時，以保持系統時間之正確性。

系統應該由安全管道取得Root CA的自簽憑證，並妥善地安全保存於系統中

- 原因：
  - Root CA本身的憑證是自簽憑證（Self-Signed Certificate）。
  - 自簽憑證的特性是其憑證簽發者名稱（Issuer Name）與憑證主體名稱（Subject Name）是完全相同的，而自簽憑證的簽章可以被該自簽憑證所記載的公開金鑰檢驗通過。
  - 此自簽憑證中所記載的公開金鑰可以用來檢驗下層CA憑證的真偽，而下層CA憑證所記載的公開金鑰可以用來檢驗用戶憑證的真偽。所以說此自簽憑證是整個PKI的信賴起點（Trust Anchor）。
  - 然而自簽憑證卻沒有另外一張憑證的公開金鑰可以檢驗其真偽。（也就是說沒有另一個CA來為Root CA的自簽憑證背書。）
  - 意圖不法者如果擁有足夠的技術與工具，就可以自己產製一對金鑰對，並簽出一張自簽憑證，且故意讓該自簽憑證之憑證簽發者及憑證主體名稱都與真正的Root CA名稱相同，由於此憑證是自簽的，所以該自簽憑證簽章一定可以被其所記載的公開金鑰檢驗通過，所以容易被誤以為是真正的Root CA自簽憑證。
  - 所以Root CA的自簽憑證是可能被偽造的。

系統應該由安全管道取得Root CA的自簽憑證，並妥善地安全保存於系統中

- 誤信假的Root CA自簽憑證之後果：
  - 意圖不法者偽造Root CA自簽憑證後，可以使用假的Root CA私密金鑰簽發假的下層CA憑證，然後使用假的下層CA私密金鑰簽發加的用戶憑證。
  - 由於應用系統誤用假的Root CA自簽憑證為信賴起點，並以假的Root CA公開金鑰來檢驗下層CA憑證，結果就會誤信假的下層CA憑證，然後再以假的下層CA公開金鑰來檢驗用戶憑證，結果就會誤信假的用戶憑證，最後意圖不法者就達到偽冒用戶身分的目的。



系統應該由安全管道取得Root CA的自簽憑證，並妥善地安全保存於系統中

- 觀念澄清：
  - 拿自簽憑證所記載的公開金鑰來檢驗該自簽憑證的簽章，並沒有任何保護效果。（自己為自己背書，等於沒有背書。）
- 對策：
  - 確定Root CA自簽憑證的來源是可靠的。
  - 系統應設計一個安全的方式來保存所取得的Root CA自簽憑證，防止所保存的Root CA憑證被意圖不法者任意置換。
- GPKI為安全散播GRCA自簽憑證所實施的措施
  - 所有GPKI之IC卡內都含有一份GRCA自簽憑證，驅動程式光碟也都含有GRCA自簽憑證的安裝程式
  - GRCA網頁上提供了一種經由網路安全下載GRCA自簽憑證的方式
  - 行政院研究考核委員會於91年10月30日在中國時報、聯合報、自由時報及台灣日報公布GRCA之公開金鑰值

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

- 憑證政策之保證等級：
  - 憑證政策（Certificate Policy，CP）會因不同等級的應用需求制定不同的規範，不同等級的規範有的較寬鬆有的較嚴格，所以依據不同等級規範所簽發的憑證，便具有不同的保證程度，所以這些不同的等級便稱為保證等級（Assurance Level）。
- GPKI憑證政策之保證等級：
  - GPKI憑證政策規範了5個保證等級：
    - 測試級
    - 第一級
    - 第二級
    - 第三級
    - 第四級
  - 其中測試級之保證等級最低，第四級之保證等級最高。
  - GPKI中只有GRCA係遵照保證等級第四級的規範運作。
  - GPKI所有下層正式CA（GCA、MOEACA、MOICA、XCA）皆遵照保證等級第三級的規範運作。
  - GPKI之測試憑證管理中心GTestCA則依測試級之保證等級規範運作。

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

- 憑證政策之保證等級如何表示於憑證中？
  - X.509 v3憑證中可以有一個稱為CertificatePolicies的憑證擴充欄位（Certificate Extension），其中會記載Policy OID用來表示該憑證所依循的憑證政策。
  - 由於不同保證保級的憑證政策會有不同的Policy OID，所以Policy OID也代表了該憑證之保證等級。
- GPKI各保證等級之憑證政策之的Policy OID：
  - 測試級的Policy OID：2.16.886.101.0.3.0
  - 第一級的Policy OID：2.16.886.101.0.3.1
  - 第二級的Policy OID：2.16.886.101.0.3.2
  - 第三級的Policy OID：2.16.886.101.0.3.3
  - 第四級的Policy OID：2.16.886.101.0.3.4

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

- 應用系統應如何檢查憑證之Policy OID？
  - 上層CA發給下層CA的Cross-Certificate中所記載的Policy OID，表示上層CA授權下層CA可簽發什麼保證等級的憑證。
  - CA發給用戶的End-Entity Certificate中所記載的Policy OID表示該CA對該End-Entity Certificate的保證等級。
  - Root CA的自簽憑證無須包含Policy OID，應用系統也不必檢查Root CA自簽憑證的Policy OID。
  - 應用系統應該決定其所需要的保證等級，並確認所有下層CA憑證的CertificatePolicies擴充欄位中含有代表該保證等級的Policy OID，並且要確認用戶憑證的CertificatePolicies擴充欄位中也含有代表該保證等級的Policy OID。
  - 即使用戶憑證的CertificatePolicies擴充欄位中也含有代表該保證等級的Policy OID，但是如果其CA憑證的CertificatePolicies擴充欄位中並未含有代表該保證等級的Policy OID，則應用系統也應該拒絕該用戶憑證。

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

- GPKI應用系統對Policy OID的應注意事項：
  - 目前所有GPKI之正式憑證皆是保證等級第三級的憑證，所以應用系統正式上線時應該設定保證等級第三級的Policy OID為其所信賴的Policy OID。
  - 應用系統使用GTestCA簽發的測試憑證進行上線前測試時，應該設定測試級之保證等級的Policy OID為其所信賴的Policy OID，然而正式上線時務必要記得更改設定，將所信賴的Policy OID 改回第三級的Policy OID ，否則會造成用戶可以使用測試用IC卡及憑證進入正式系統的問題。
  - 應用系統應該檢查GPKI下層CA憑證（GRCA簽發給GCA、MOEACA、MOICA、XCA、GTestCA等CA之憑證）的CertificatePolicies擴充欄位中是否含有代表所信賴保證等級的Policy OID。
  - 應用系統應該檢查GPKI用戶憑證的CertificatePolicies擴充欄位中是否含有代表所信賴保證等級的Policy OID。

系統應該檢查CA本身的憑證確實為Root CA所簽發的憑證

- 原因：
  - Root CA是PKI的信賴起點，除非下層CA是經過Root CA授權的，否則應用系統不應該信賴該下層CA。
  - 所以應用系統應該檢查下層CA本身之憑證是否確實為Root CA所簽發。
- 方法：
  - 檢查憑證的Issuer Name (DN)是否與Root CA自簽憑證的Subject Name(DN)相符。
  - 以Root CA自簽憑證所記載的Public Key檢驗CA本身憑證的簽章。

系統應該檢查CA本身的憑證確實為合法的CA憑證

- 原因：
  - 唯有合法的CA才能簽發憑證，一般用戶是不能簽發憑證的。
  - CA Certificate與一般用戶的End-Entity Certificate之格式是有區別的，當Root CA簽發憑證給下層CA時，必定會採用CA Certificate的格式，表示該CA為經過Root CA授權的合法CA。
  - 所以應用系統應該檢查下層CA本身之憑證是否為CA Certificate。
- 方法：
  - 檢查該下層CA本身的憑證是否含有BasicConstraints擴充欄位（Extension），並且該欄位中的cA子欄位值為TRUE。
  - 檢查該下層CA本身的憑證是否含有KeyUsage擴充欄位，並且該欄位中設定的金鑰用途包含keyCerSign及cRLSign的用途。

    註：在GPKI中CA憑證的keyCerSign及cRLSign的用途會存在於同一張憑證中，但在有些PKI中， keyCerSign及cRLSign可能分開授權於兩張不同的憑證中。

系統應該檢查CA本身的憑證是否仍在有效期限之內

- 原因：
  - Root CA自簽憑證必須尚未過期，則該自簽憑證所記載之Public Key才能被用來檢驗下層CA憑證。
  - 下層CA本身之憑證必須尚未過期，則該CA本身憑證所記載之Public Key才能被用來檢驗用戶憑證。
- 方法：
  - 憑證之有效期限欄位含有兩個子欄位：一為notBefore子欄位，記載憑證有效期限的起始時間；一為notAfter子欄位，記載憑證有效期限的截止時間
  - 應用系統應檢查目前系統時間是否介於Root CA自簽憑證之有效期限之notBefore時間與notAfter時間之間。
  - 應用系統應檢查目前系統時間是否介於下層CA憑證之有效期限之notBefore時間與notAfter時間之間。

  註1：以上假設系統時間是正確的時間。
  註2：以上假設系統是要檢驗現時的資料，若是系統要檢驗的是舊有的資料（例如已經歸檔的資料），則應該要變成檢查當初資料產生時CA憑證是否仍有效

系統應該檢查CA本身的憑證是否已被廢止

- 原因：
  - 雖然下層CA憑證被Root CA廢止的機率非常低，但是一旦下層CA憑證被Root CA廢止，極有可能表示該CA發生重大事件（例如該CA的私密金鑰外洩），所以應用系統仍必須小心檢查CA本身的憑證是否被廢止了。
- 方法：
  - Root CA所公佈的CA憑證廢止資訊的憑證廢止清冊（Certificate Revocation List，簡稱CRL）特稱為憑證機構廢止清冊（Certification Authority Revocation List，簡稱CARL），其格式與一般CRL的格式並無差異，只不過CARL中只含有CA Certificate之廢止資訊，而不含一般End-Entity Certificate之廢止資訊。
  - 應用系統應依照CARL的公佈週期，定期下載新的CARL，並檢查下層CA本身之憑證的憑證序號是否已經被列在憑證機構廢止清冊中了，並了解其廢止原因（Revocation Reason）。
- 注意：
  - 當發現CA憑證被廢止時，應該停止信賴該CA憑證，並盡快向該CA或Root CA洽詢，以取得新的CA憑證。
  - Root CA自簽憑證如果被廢止，則其廢止資訊並不會出現在Root CA所公佈的CARL中，因為如果Root CA的金鑰變成不可信賴時（例如私密金鑰外洩），則Root CA的CARL也會隨著變成不可信賴。所以如果Root CA自簽憑證發生必須廢止的狀況時，必定會透過其他管道，例如電視、廣播、報紙、網際網路等盡速讓大眾知道。

系統應該檢查CARL是否確實是Root CA所簽發

- 原因：
  - 應用系統必須確認CRL的來源正確，才能信賴該CRL中所記載之廢止或停用資訊，否則可能會受到假造CRL之欺騙，而誤信錯誤的廢止或停用資訊。
- 方法：
  - 檢查CRL的Issuer Name (DN)是否與Root CA自簽憑證的Subject Name(DN)相符。
  - 以Root CA自簽憑證所記載的Public Key檢驗CARL的簽章。

系統應該檢查CARL是否為最新公佈的CARL

- 原因：
  - Root CA會定期公告新的CARL，所以CARL也是有效期的，所以應用系統在使用CARL時，應該檢查CARL的效期，以確定該CARL是最新公佈的CARL。
- 方法：
  - CARL內有一個成為thisUpdate的欄位，記載Root CA更新該CARL資訊的時間；另有一個稱為nextUpdate的欄位，記載下次Root CA預計更新CARL資訊的時間。
  - 應用系統應該檢查目前系統時間是否已經超過CARL的nextUpdate時間了。
  - 如過已經目前時間已經超過nextUpdate時間，則表示Root CA應該已經公告新的CARL了，所以應用系統應該去下載新的CARL。

註1：以上假設系統時間是正確的時間。
註2：以上假設系統是要檢驗現時的資料，若是系統要檢驗的是舊有的資料（例如已經歸檔的資料），則應該要變成檢查當初資料產生時CARL是否是當期的CARL

系統應該檢查用戶的憑證確實為合法CA所簽發的憑證

- 原因：
  - 除非用戶憑證是經過合法CA所簽發的，否則應用系統不應該信賴該用戶憑證。
- 方法：
  - 前面的步驟已經確定下層CA本身的憑證為合法憑證，接下來可用該下層CA本身憑證中所記載的資訊來檢驗用戶憑證。
  - 檢查用戶憑證的Issuer Name (DN)是否與下層CA本身憑證的Subject Name(DN)相符。
  - 以下層CA本身憑證所記載的Public Key檢驗用戶憑證的簽章。

系統應該檢查用戶憑證金鑰用途欄位所記載的金鑰用途符合使用目的

- 原因：
  - X.509標準對公鑰憑證定義了許多種的金鑰用途（Key Usage），憑證的使用必須符合該憑證所記載之金鑰用途，否則便是不合法的使用。
- 方法：
  - 憑證的金鑰用途係記載於KeyUsage擴充欄位中。
  - GPKI對於用戶的憑證依照X.509規範區分為簽章用及加解密用兩種的類別。
  - 應用系統必須檢查用戶憑證的KeyUsage擴充欄位，如果KeyUsage擴充欄位中設定了digitalSignature或是nonRepudation的用途位元，則該用戶憑證所記載的公鑰才可被用來檢驗用戶的簽章；如果KeyUsage擴充欄位中設定了keyEncipherment的用途位元，則該用戶憑證所記載的公鑰才可被用來封包進行資料加密的數位信封（即用來加密Session Key）。

系統應該檢查用戶的憑證是否仍在有效期限之內

- 原因：
  - 用戶憑證必須尚未過期，則該用戶憑證所記載之Public Key才能被用於該憑證所允許的金鑰用途上。
- 方法：
  - 憑證之有效期限欄位含有兩個子欄位：一為notBefore子欄位，記載憑證有效期限的起始時間；一為notAfter子欄位，記載憑證有效期限的截止時間
  - 應用系統應檢查目前系統時間是否介於用戶憑證之有效期限之notBefore時間與notAfter時間之間。

    註1：以上假設系統時間是正確的時間。
    註2：以上假設系統是要檢驗現時的資料，若是系統要檢驗的是舊有的資料（例如已經歸檔的資料），則應該要變成檢查當初資料產生時CA憑證是否仍有效

系統應該檢查用戶的憑證是否已被廢止

- 原因：
  - 即使用戶憑證仍在有效期限之內，用戶憑證仍然可能被廢止或暫停使用，所以應用系統仍必須用戶憑證是否被廢止或暫停使用了。
- 方法：
  - 應用系統應依照CA公布CRL的週期，定期下載新的CRL，並檢查用戶憑證的憑證序號是否已經因為廢止或暫時停用而被列在憑證廢止清冊中了。
  - 若CA另外也提供線上憑證狀態查詢（OCSP）服務，則應用系統可使用OCSP來查詢用戶憑證是否被廢止或暫停使用了。

系統應該檢查CRL是否確實是合法CA所簽發

- 原因：
  - 應用系統必須確認CRL的來源正確，才能信賴該CRL中所記載之廢止或停用資訊，否則可能會受到假造CRL之欺騙，而誤信錯誤的廢止或停用資訊。
- 方法：
  - 檢查CRL的Issuer Name (DN)是否與CA本身憑證的Subject Name(DN)相符。
  - 以CA本身憑證所記載的Public Key檢驗CRL的簽章。

系統應該檢查CRL是否為最新公佈的CRL

- 原因：
  - CA會定期公告新的CRL，所以CRL也是有效期的，所以應用系統在使用CRL時，應該檢查CRL的效期，以確定該CRL是最新公佈的CRL。
- 方法：
  - CRL內有一個成為thisUpdate的欄位，記載CA更新該CRL資訊的時間；另有一個稱為nextUpdate的欄位，記載下次CA預計更新CRL資訊的時間。
  - 應用系統應該檢查目前系統時間是否已經超過CRL的nextUpdate時間了。
  - 如過已經目前時間已經超過nextUpdate時間，則表示CA應該已經公告新的CRL了，所以應用系統應該去下載新的CRL。

    註1：以上假設系統時間是正確的時間。
    註2：以上假設系統是要檢驗現時的資料，若是系統要檢驗的是舊有的資料（例如已經歸檔的資料），則應該要變成檢查當初資料產生時CRL是否是當期的CRL

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

- 原因：
  - 在電子化／網路化的環境中，應用系統必須取得用戶的電子簽章，驗證簽章無誤後，才能向信用戶就是憑證身份資料所指之人。
- 觀念澄清：
  - 如果沒有驗證用戶的電子簽章，光是要求用戶輸入IC卡PIN碼及讀取IC卡內的憑證，並不能確保用戶就是憑證身份資料所指之人。
- 方法：
  - 應用系統應該設計Logon的功能，要求用戶使用IC卡對登入訊息進行電子簽章，藉驗證電子簽章以確認用戶身份。
  - 或是應用系統應該在設計訊息格式時，將訊息格式設計成含有電子簽章的格式，以便藉驗證電子簽章來確認身份。
  - 如果應用系統的訊息protocol能夠設計成雙方互相交換簽章訊息，達到「雙向認證」的效果，則對通訊雙方皆有較佳的保障。

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的機制

- 原因：
  - 電子簽章的訊息如果沒有包含防止或偵測訊息重送（Replay）的機制，則意圖不法者可能可以經由竊聽而將該訊息記錄下來，日後再重送給應用系統，應用系統會誤以為該訊息是真正的用戶所傳送來的。
- 觀念澄清：
  - 並不是將訊息加上電子簽章後，對簽章者的身份認證就安全無虞了，還必須注意訊息被意圖不法者非法重送的問題。
- 方法：
  - 利用Challenge-Response的機制（亦稱為Nonce機制），可以偵測出Replay的狀況。

    註：所謂Challenge-Response機制是說通訊的一方先送一串亂數（此稱為Challenge，或稱為Nonce）給另一方，另一方收到後要將該亂數含入要回傳給Challenge端的簽章訊息中（這個過程稱為Response），如此可以證明簽章訊息是此次新產生的（Freshness），而非重送的訊息。

  - 在訊息中加上時間戳記，也有助於偵測Replay。因為訊息中有時間戳記，則系統可以檢查訊息簽章時間的合理性，如果發現時間戳記太舊，則可假設此為意圖不法者非法重送的舊訊息。

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

- 原因：
  - 簽章機制並不能增加訊息的保密程度，如果訊息只加上簽章，則訊息仍然還是維持原有明文，所以如果要防止隱私資料外洩，還需要另外使用加密技術，而且加密強度要達到128 bits以上，其安全度才足夠。
- 方法：
  - 使用SSL安全通道，例如透過HTTPS通訊協定進行網站連線，但必須注意SSL安全通道之加密強度要達到128 bits 以上。
  - 或是使用數位信封對所傳送的訊息加密成為密文。

  註：SSL安全通道是一種透通性加密保護機制，其優點是能夠自動加密保護所傳送的資料，非常方便，但是資料送達另一端之後就會被自動解密成為明文。如果需要使資料送達另一端後仍維持密文的形式，則必須使用數位信封的技術。

系統應該定期校時，以保持系統時間之正確性

- 說明：
  - 由前面的安全檢查項目知道，系統時間的正確性對於決定憑證是否有效有重大的影響。
  - 如果系統使用時間戳記來輔助訊息重送的偵測，則系統時間的正確性也非常重要。
- 方法：
  - 系統自動校時最常見的方法是使用網路時間協定（Network Time Protocol，簡稱NTP），但必須注意所連接的NTP Server是否是可信賴的Server。國內有經濟部標檢局委託中華電信研究所成立的時間與頻率國家標準實驗室提供NTP網路校時服務。
  - 亦可透過接收標準時頻廣播或透過Modem撥接來接收校時資訊。時間與頻率國家標準實驗室亦提供標準時頻廣播及Modem撥接校時的服務。
  - 另外，全球衛星定位系統（GPS）所提供的校時資訊亦是可利用的校時資源。

總結

- PKI是資訊安全的重要推手之一，是重要的基礎建設，但是並不是說建置了 PKI之後就會非常神奇地把原本不安全的應用系統變得安全了。應用系統必須善加利用PKI所提供的各種機制及技術，才能發揮PKI的功用，提高系統的安全性。
- 所謂資訊安全是要全面性安全才算是真正安全，PKI所提供的安全機制僅是系統整體安全的環節之一，除了針對本安全檢查表所列的項目進行檢查之外，應用系統管理者也應該對其他環節的安全性進行全面檢視，已確保系統的整體安全性。