第二十八章

電子認證風險評估與管理

Risk Management of Electronic Authentication System

何全德
Chuan-Te Ho
行政院研究發展考核委員會
資訊管理處 處長
Director, Department of Information Management,
Research , Development and Evaluation Commission, Executive Yuan

壹、前言

信任與信賴是所有商業交易的基礎。儘管目前電子商業活動蓬勃發展，但是網路安全的疑慮如電腦病毒、駭客入侵、個人隱私資料外洩及網路犯罪等問題，一直是社會各界關心的議題，也是主要國家推動電子化政府及電子商業，亟待解決的問題。要讓網路使用者能夠很放心、安心的在網路上申辦政府服務、購物、付款、轉帳、交易或通訊，必須以全方位的觀點，從技術、管理及法律層面，建構一個安全及可信賴的網路交易環境，才能增進使用者的信心，進而促進網路經濟活動的健全發展。

電子認證機制是網路安全的核心機制。立法院於民國九十年十月三十一日三讀通過「電子簽章法」，經　總統於九十年十一月十四日公布，行政院復於九十一年四月一日正式發布實施。我國「電子簽章法」是採取小而美的立法方式，條文中僅重點規範電子文件及電子簽章的法律地位，並以契約自由及市場導向原則，採低度管理方式規範憑證機構之營運。依我國「電子簽章法」之立法目的、

精神及內容觀之，該法最主要的功能是排除應用電子文件及電子簽章的法律障礙，使網路交易及通信的相對人，得以電子簽章及電子文件爲意思表示之方法。但是，對於如何建構電子交易的信賴機制，尚待政府進一步訂定詳細的規範。

是以，今後公私組織欲建立電子交易之信賴機制，除遵循電子簽章法之相關規定外，在實務運作上，仍有待政府主管機關、憑證機構、使用者等共同努力，逐步建立一個可爲大眾信任及信賴的公鑰基礎建設(Public Key Infrastructure, PKI)，才能增進民眾使用電子簽章的信心，進而促進電子交易的蓬勃發展。

「電子簽章法」不僅規範私經濟領域的電子交易活動，也同時規範公權力的電子化政府活動。由於政府的公文書及民眾申辦服務，涉及公權力的行使，影響民眾的權利義務至鉅。是以，「電子簽章法」規定有關電子簽章及電子文件之適用，行政機關得以法令或公告，排除其適用或就其應用技術與程序另爲規定。但就應用技術與程序所爲之規定，應公平、合理，並不得爲無正當理由之差別待遇。從「電子簽章法」之相關規定觀之，該法對於政府機關建置及經營的憑證機構之安全性，顯然課予較高的技術與程序安全要求，其目的是要保障及維護民眾的權益。

行政院研究發展考核委員會（以下簡稱行政院研考會）於八十七年二月委託中華電信公司建置「政府憑證管理中心」（Government Certification Authority，以下簡稱 GCA）提供各機關自然人、機關、公司行號等電子憑證服務，目前已廣泛應用於電子公文、電子採購、電子支付及網路報稅等各項線上申辦服務系統。本文即依據「電子簽章法」相關規定及 GCA 之實務運作經驗，從資訊系統風險管理的角度，分析電子簽章可能面臨的威脅及安全弱點，進而提出建構電子化政府 PKI 信賴機制之整體安全策略及對策，以供社會各界參考。

貳、電子認證系統風險評估

一、風險分析模式

風險是指測量負面影響的機率與嚴重程度。從資訊系統安全的角度言，就是

任何人為及自然因素對於組織安全所造成的危害，或是對於有價值的資訊資產所構成的威脅，泛稱為風險。風險分析方法在保險行業已行之有年，依據保險業的經驗，風險分析有四個要件，第一是分析資訊資產的價值，第二是分析可能的安全威脅，第三是分析可能的安全漏洞，第四是依據資訊資產的價值分析與可能的安全威脅及漏洞，採取適當及足夠的安全對策。

(一) 資訊資產價值分析

要有效保護電子認證系統，首先必須了解電子認證相關資訊資產的重要性及價值。如果電子認證系統沒有任何的價值，其風險程度幾乎是微乎其微。但是，只要任何人基於任何理由，對於電子認證系統產生興趣或好奇，就產生某種程度的風險。電子認證系統的價值可從三個面向分析，第一是分析電子認證系統（例如行政院研考會建立的政府憑證管理中心）的貨幣價值，第二是分析電子認證系統的隱藏價值（例如破解政府憑證管理中心的簽章金鑰，進而偽造國民電子憑證，冒名使用進行網路申辦所獲得的利益）。隱藏價值對於電子認證系統最大的危害是影響及破壞系統的真確性（integrity）、私密（confidentiality）及可用性（availability），進而影響使用者對於電子認證系統的信任及信賴。第三是從對手的角度分析電子認證系統的價值（例如，有些資訊資產對於組織內部員工而言，可能不是很有價值，可是從商業競爭對手的角度來看，價值卻很高，所以必須列為保護的對象）。

依據經濟合作暨發展組織（Organization for Economic Cooperation and Development，以下簡稱 OECD）訂定的九大資訊安全管理指導原則之一--**相稱原則**（Proportionality Principle），資訊安全之等級、成本、保護措施、實務應用及處理程序應該是適當的，且與資訊系統的價值及對該項系統的依賴程度是相稱的；當安全的需求隨著特定系統而改變時，應與資訊系統的嚴重性、受傷害的可能性及內容是相稱的。

依據以上安全原則，電子認證系統應該採取何種等級的安全措施，應該與電子認證系統的資訊資產價值相稱。從電子認證系統的實務作業分析，宜列入電子認證風險分析評估的資訊資產如下：

（1）資訊資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、業務永續運作計畫、預備作業計畫等。

（2）軟體資產：應用軟體、系統軟體、發展工具及公用程式等。

（3）實體資產：電腦及通訊設備、媒體資料及其他技術設備。

（4）技術服務資產：電腦及通信服務、其他技術性服務（如電源及空調）。

(二)威脅分析

從資訊系統的實務作業中，影響電子認證系統安全的因素有：

（1）天然災害－例如，颱風、地震、水災。

（2）其他意外災害－例如火災、鼠咬。

（3）故障－例如電腦主機故障、週邊設備故障、電力設備故障、通信線路、設備故障等。

（4）人為－例如能力不足（例如軟體未盡完善）、過失、蓄意破壞電腦與破壞通信網路、毀損各種媒體、盜取電腦硬體、未經同意使用電腦、放置電腦病毒、盜用電腦資料、程式等無形資產、非法輸入、竄改、刪除、查詢資料與程式、非法取得財物、非法侵入電腦、洩密等。

從影響資訊系統的安全因素分析，電子認證系統面臨的威脅可能來自憑證機構內部或外部，國內或國外；過去、現在及未來的員工，都可能對電子認證系統造成傷害；此外，外國競爭對手，電腦駭客、資訊服務廠商、外國情報機構、敵對或友好國家、組織犯罪集團或是恐佈份子，都可能是電子認證系統的潛在威脅者。其中人為疏失及意外，尤其是內部員工監守自盜或是無心的疏失，可能是影響電子認證系統的最大威脅。

(三) 安全漏洞分析

電子認證系統雖然可能面對各種自然及人為的威脅，但是只要系統有很好的技術及管理防護措施，沒有安全漏洞，也就不致於產生風險。惟世界上沒有一個電子認證系統是完美無瑕的，系統管理者能做的就是竭盡所能了解自已的安全漏洞，然後採取降低風險的對策。一般而言，可以將電子認證系統的安全漏洞分成下列四項：

（1）作業上的安全漏洞

作業上的安全漏洞指的是在憑證機構的實務作業程序下所產生的安全漏洞，這種作業上的安全漏是最具威脅性的，主要都是肇因於人為疏失

或致命傷。不當的安全政策及工作程序、意外及員工漫不經心、社交工程（social engineering）造成的疏失、資訊安全規定未能落實執行，員工閒聊漫談、供應商的供貨及服務記錄、內部資訊溝通不良等，都有可能造成電子認證系統的相關機密外洩，影響系統的安全。

（2）人員的安全安全漏洞

所有的資訊系統都必須依賴人去操作及維護，從國內外資訊安全的案例分析，資訊系統中最薄弱的一環是人。一個電子認證系統包括憑證中心的系統管理人員、系統操作人員、系統發展人員、憑證註冊窗口作業人員及憑證持有人等不同的角色，每一個成員角色都是電子認證系統安全的一環，任何一個環節產生疏漏，即有可能危害電子認證系統的安全。例如，雖然憑證機構建立極爲安全可靠的電子認證系統，但是憑證持有人可能因未善盡保管責任，將儲存私密金鑰的 IC 卡及密碼遺失，致遭人冒用影響自己的權益。

（3）有形的安全漏洞

天災（如水災淹沒憑證機構的機房）、警衛疏失（憑證機構門禁不嚴遭侵入）、影印機（影印電子認證系統的機密資料留下原卷或是影印的錯誤資料銷毀）、憑證中心作業人員電腦不使用時未登出或未設定保護的密碼等，都可能危及電子認證系統的安全。

（4）科技的安全漏洞

一個完整的電子認證系統是由最核心的密碼演算法（如使用 RSA、DES）以及密碼模組（security module）、密碼產品（product）、應用及系統（application/system）所構成。從系統工程的角度分析，已知的軟硬體安全漏洞（例如作業系統的安全漏洞、弱化的亂生產生器、金鑰長度不足、密碼設定不當、硬體保密器不夠完善、網路通信協定的安全漏洞）、系統設定錯誤，資料儲存及通信方式不當或未妥適保護等科技上的因素技術，都可能造成電子認證系統的安全漏洞。

(四)安全對策

風險分析的最後一個步驟是依據資訊資產的價值，衡量可能面臨的威脅及安全漏洞，再採取適當及足夠的安全對策及保護措施，將電子認證系統的安全風險降至最低。電子認證系統的安全對策可從技術工程、執行管理、教育訓練及倫理建立等四個層面訂定，相關細節將於下節說明。

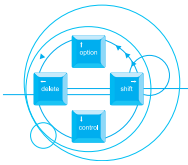
一、電子認證系統之風險

Carl Ellison及Bruce Schneier在"Ten Risks:What You're Not Being Told About Public Key Infrastructure"一文中，提出了十項PKI的可能風險，包括：你相信的CA是否值得你相信？它是否被授權可以執　行憑證簽發服務？你如何有效的保護你的簽章私鑰？驗證憑證及簽章真僞的電腦設備是否安全？會不會有人假造憑證機構的公鑰？你是否相信公鑰憑證上記載的憑證持有人身分？憑證機構的安全機制是否將憑證使用者納入安全的一環？憑證機構是否能夠正確無誤的辨識及核對憑證持有人的身分？憑證機構及註冊機構是否能夠作整體的安全管理？憑證實務作業的安全管理到底有多安全？

上述PKI可能的風險，有些是PKI本身安全上要防範的，有些則是PKI之外的整體通訊安全、系統安全、人員安全及資料安全必須要加以防範的。

以憑證機構的憑證核發作業過程爲例（憑證機構的安全風險不以此爲限），在實務作業上即有可能發生下列的風險：

1. 憑證機構金鑰之安全風險：憑證機構本身之金鑰管理含金鑰產生(Key Generation)、金鑰儲存、備援及復Key Storage，Key Backup and Key Restore)、金鑰啓用(Key Activation)、金鑰更新(Key Update)、金鑰停用(Key Deactivation)、金鑰銷 毀(Key Destruction)及金鑰存放(Key Archival)等，可能會因人爲、技術、作業或程序上的因素造成下列各項安全的風險。
2. 憑證當事人身分鑑別不正確的風險：憑證機構的註冊機構(Registration Authority，簡稱 RA)可能因人爲、作業或其他因素，未能依據憑證實務作業基準之規定，正確辨識公鑰憑證持有人的正確身分、未能辨識僞造的身分資料、未能正確檢驗公鑰憑證持有人的公鑰及私鑰是否成對、未能查驗另有其他未及



登載但足以影響憑證可靠性之事實等，則憑證機構簽發的公鑰憑證將會產生安全的問題，不被相對人所信賴，甚至因誤信而使持有人或善意第三者權益受損。

3.憑證內容不正確的風險:全型憑證機構簽發的憑證內容及對於憑證的使用政策及限制，是憑證機構建立信賴機制最重要基礎。以 X509 規範的憑證爲例，憑證本文及附註上記載的流水號、效期、憑證持有人之姓名、加密演算法、憑證簽發機構名稱、憑證機構簽章、憑證之使用限制、憑證持有人之公鑰等，如果因人爲、作業或其他因素，造成憑證內容不正確、簽章公私鑰不正確、存效憑證的軟硬體設備有安全疑慮，將會產生信賴的問題。

4.憑證製作、分送及接受過程的風險：在憑證的製作過程中，可能會有憑証應用範圍的限制與持有人的身分資格條件不相符的風險；在憑證分送及爲接受者認可的過程中，亦有可能因通信、未能提供足夠的憑證限制資訊或其他因素，造成憑證的信賴問題。

5.憑證管理上的風險：憑證機構對於憑證持有人或是信賴團體，如果未能提供適當的憑證資訊，可能會產生一些安全上的風險。例如，未能正確告知憑證註銷的方式及管道、憑証機構註銷清冊公布的時間及地點等，都可能造成憑證接受者誤信的問題。再如，憑證機構如果確知憑證所記載之部分事項不真實；確知憑證當事者之簽章私鑰遭冒用、僞造或破解；確知憑證機構本身之簽章私鑰或資訊系統遭冒用、僞造或破解，致影響憑證之可信賴性；確知憑證持有人之憑證已遭冒用、僞造或竄改，因人爲疏失或管理不善而未能及時逕行註銷憑證，將會影各界對於憑證的信賴。

參、電子認證系統安全管理策略

一.電子化政府之安全理念

電子化政府的各項網路安全措施，是本諸下列的基本理念，推動各項資訊安全作爲：

1.利用資訊與保護資訊同等重要

電子化政府既要充分利用資訊化及網路化所帶來的效益及便利，也要投入適當的資源維護及保護政府資訊安全。是以，對於諸如電子公文、電子支付、電子採購等各項網路應用系統，都必須事前進行安全風險評估，進而採取適當及足夠的安全防護措施。

2.事前的預防重於事後的補救

爲了強化電子化政府的整體安全結構，降低安全防護成本，各項系統的發展及設計，都應該在系統發展的生命週期初始階段，即依據資訊及系統的重要性及價值，訂定系統的安全等級，做好事前的安全防護措施。

3.資訊安全必須從全方位的觀念永續推動

電子化政府之資訊安全措施，除了要適度地採行各種技術安全措施外，也要從安全政策、管理、法律、教育、組織、人力、國際合作等各方面，以全方位的觀點推動。同時，也要以「網路國防」的思維，建立「資訊安全，人人有責」的觀念，把電子化政府的資訊安全工作，配賦在每一位機關的員工，而不僅限於是資訊單位的責任。

4.資訊安全是相對的觀念，而非絕對的觀念

政府機關不宜以追求絕對的安全爲思維，必須以各機關都有可能發生資訊安全事件作爲前提，預先規劃各種預警、防護、緊急應變及復原措施。

5.資訊安全應該是一種看得見的服務品質

爲了提供民眾安全及可信賴的網路應用環境，政府應投入適當的資源來保護電子化政府的安全。同時，電子化政府相關的安全管理措施，應遵循及符合國際組織訂定的安全標準及國家標準，並率先通過國內外認證機構的安全認證，讓政府資訊安全的品質爲社會各界所接受及認可，以增進民眾對於使用電子化政府各項網路申辦服務的信心。

二.公鑰基礎建設(Public Key Infrastructure)安全管理策略

電子化政府公鑰基礎建設的安全管理策略，必須以全方位的觀念推動。行政院研考會經參酌 OECD 及美國國家標準及科技中心（National Institute of Standards

and Technology， 簡稱 NIST）等機構訂頒的資訊安全指導原則，係採取四個 E 的整體安全策略，期能建立電子化政府的信賴機制。

(一)資訊安全技術（engineering）

爲了維護政府憑證機構的安全，首先必須從資訊技術工程的觀點，針對電子認證系統上的各種可能弱點及安全漏洞，依據國際組織的相關標準，適當地利用防火牆、數位簽章、加密、IC 卡、系統安全漏洞掃瞄及入侵偵測等各種安全工具或技術，建構憑證機構適當及足夠的安全防護體系。

以 ISO/IEC 9598-4 規定，電子認證系統必須針對以下的安全問題做好安全防護：

（1）使用者的私密金鑰被破解。

（2）憑證機構的私密金鑰被破解。

（3）憑證機構製作不正確的電子憑證。

（4）憑證機構與使用者串謀不軌。

（5）僞造的電子憑證。

（6）僞造的安全符記（token）。

（7）密碼攻擊。

再如，對於憑證機構的金鑰管理，應依下列的原則處理：

（1）金鑰應只能以 ISO 11568 規定的形式存在。

（2）沒有人能接觸到未加密的金鑰。

（3）系統須保護已使用的金鑰安全。

（4）系統應能偵測出金鑰是否已遭攻擊。

（5）系統應能偵防/偵測不當使用金鑰的企圖。

（6）產生金鑰的方式應是不可預期的。

（7）系統應能偵測出不當使用金鑰的企圖。

（8）金鑰須定期更新。

（9）在字典攻擊法生效前須更新金鑰。

（10）得知或懷疑金鑰已被瓦解前,須立即停用。

（11）不同金鑰之安全性不得相互影響。

（12）已遭破解的金鑰不得使用於更新作業。

（13）在下載使用金鑰前，密碼模組設備須能保障其安全性。

政府憑證管理中心係依據以上國際組織訂定的相關安全規範，進行系統的建構。以 GCA 使用的非對稱金鑰加解密演算法爲例：非對稱金鑰數位簽章演算法係採 RSA with SHA1，金鑰長度 2048 Bits（含）以上（GCA,GRCA）、1024 bits（含）以上（GCA,GCA），簽章格式符合 PKCS #1（V1.5/V2.1）。對稱金鑰加解密演算法：至少符合 Triple-DES，金鑰長度 128 bits（含）以上，未來可能增加 AES 等其他國際標準。再如，GCA 規定註冊機構私密金鑰係存在硬體密碼模組中，硬體密碼模組必須具備金鑰備援管理機制，並符合以下安全功能：A、實體安全機制之檢測，當實體保護被破壞時，密碼模組必須擁有自動清除秘密參數的功能。B、身分鑑別機制(Identity-Based Authentication)。C、私密金鑰輸入應使用安全(加密處理)之管道，或使用金鑰分持(Key Splitting)技術。GRCA 之 CA 主機在任何時候皆不允許直接或間接和外在網路(External Network)有任何連線，包括利用防火牆(Firewall)或路由器(Router)等網路裝置區隔內外網路的「間接」連線也是不允許。此外，GRCA 及 GCA 係參照美國聯邦政府資訊處理規範 FIPS 140-1 Level 3 硬體密碼模組來儲存私密金鑰。今後，如果經濟部制定相關規範，GRCA 及 GCA 亦將遵循國家標準辦理。

雖然 GCA 對於相關的密碼演算法及密碼模組的安全性已參照國外的標準及規範有所規定，但是目前經濟部等政府主管機關尚未建立密碼模組檢測及認驗證機制，因此，建立類似美國聯邦政府的檢測及認驗證機制，將是當務之急。依據美國聯邦政府公布的密碼指引，政府部門使用的密碼安全的檢測分成四個層次。最基層是演算法(algorithm)的安全，其次是密碼模組（security module）的安全，其次是產品（product）的安全，再其次是應用及系統（application/system）的安全。美國與加拿大政府共同推動的密碼驗證計畫(Crytographic Module Validation Program, CMVP)的經驗，堪供政府主管部門參考。美國訂定的 FIPS-1 及 FIPS-2 規定密碼模組所必須滿足的安全需求，並且提供四個安全等級。

密碼模組安全需求涵蓋了基本的設計及文件編纂、模組介面、授權的角色及服務、實體安全、軟體安全、作業系統安全、金鑰管理、密碼演算法、電磁干擾及電磁相容（EMI/WMC）、自我測試、設計保證及對其他攻擊方法的抵抗等。

以技術工程的角度觀察，密碼模組的安全檢測只是電子化政府公開金鑰基礎建設信賴機制的一部分而已，尚必須從產品、應用及系統層次，檢測其安全。在

系統及產品的安全檢測方面，經濟部正規劃推動將 ISO 15408(Common Criteria)制訂成爲國家標準。今後，政府建立的憑證機構將參考上述標準推動。

(二)有效執行管理（enforcement）

從資訊技術工程建構電子化政府 PKI，只是一個技術上的信賴基礎，必須進一步建構執行管理的機制，持續加強管理，才能建立民眾的信任及信心。爲推動各機關強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益，政府各管機關必須加強推動下列各項措施：

（1）資訊安全管理規範建立

行政院研考會經參酌歐美等主要國家政府部門的資訊安全管理實務作業，並特別參考英國政府推動的資訊安全管理規範(BS7799,Code of Practice for Information Security Management)，已經訂從定「行政院及所屬各機關資訊安全管理要點」（行政院於八十八年九月十五日函頒）及「行政院及所屬各機關資訊安全管理規範」（行政院研考會於八十八年十一月十六日函頒）。其中，英國政府訂定的 BS7799 標準，業已成爲國際標準組織的標準-ISO-17799，經濟部標檢局正推動將其訂爲國家標準。

由於「電子簽章法」第四條、第六條及第七條規定對於電子文件的適用，行政機關可以法令或公告方式，排除電子文件及電子簽章之適用或就其應用技術與程序另爲規定。上述規定固然是要以緩進的方式逐步推廣電子簽章的使用，另一方面的立法旨意當在以電子憑證在政府部門的使用，因涉及民眾的權益、社會的安定、國家的安全至鉅，是以，該法授權政府機關可另外就政府簽發電子憑證的應用技術及程序，另爲更安全的規定。再者，研考會已經考量行政機關的特性，將電子化政府公鑰基礎建設的架構訂定爲一層級式的信賴關係，並且規劃於九十年四月底建構完成「政府憑證總管理中心」（Government Root Certificate Authority，GRCA），今後各目地事業主管機關自行建置之憑證機構，研考會將要求（包括研考會建置的 GCA）必須率先通過經濟部標檢局的資訊安全管理系統驗證，以昭公信，進而增進民眾及社會各界對於政府憑證機構的信賴。同時，政府憑證機構尚須依據行政院訂定資訊安全管理要點及資訊安全管理規範之相關規

定，做好各種資通安全管理工作，建立整體性的資訊安全管理機制，包括：資訊安全政策訂定、資訊安全權責分工、人員管理及資訊安全教育訓練、電腦系統安全管理、網路安全管理、系統存取控制管理、系統發展及維護安全管理、資訊資產安全管理、實體及環境安全管理、業務永續運作計畫管等。

（2）憑證機構稽核及監督機制之建立

資訊系統安全稽核的主要目的，乃在於確保資訊系統是否能安全有效的運作。資訊系統安全稽核是指一套有系統蒐集受查對象對資訊系統安全的主張或聲明之相關證據，並評估其與規定標準或準則相符的程度，並將稽核結果報告予相關人員的管理活動。

政府機關在推動電腦化的過程中，爲確保資訊品質及資料的完整性與真確性，多少都已經建置了相關之控管措施。然而，資訊安全管理工作是否能夠落實執行，必須建立獨立的電腦稽核機制，由客觀的電腦稽核人員，依據國際相關標準組織、行政院及相關主管機關訂定的資訊安全管理政策及規定，持續評估機關推動資訊安全的實施績效，以確保資訊安全管理機制之落實執行。

爲了推動政府部門建立電腦稽核制度，行政院研考會正協調中華民國電腦稽核協會等專業機構，將電腦稽核的相關準則及實作經驗引進到政府部門，協助各機關建立電腦稽核制度。行政院國家資通安全會報在政策上亦正規劃推動電腦稽核制度。

在實務作業上，今後政府憑證機構之安全稽核工作將依電腦稽核的相關規範，區分內部稽核及外部稽核兩種方式，由專業的稽核人員定期對政府憑證機構之安全管理、網路安全、實體安全、系統軟體安全、應用系統安全及資訊安全進行稽核。至於對憑證機構的稽核項目，可以由專業機構進行下列事項的稽核，包括：憑證機構的獨立性、承擔風險之財務能力、管理人員的經驗及專業能力、永續經營能力、軟體及硬體的可靠性、稽核制度及能力、緊急應變及回復能力、人員甄選及管理、認證機構對自已私密金鑰的保護能力、內部安全控制能力、終止營業之安排、憑證實務作業基準、憑證機構的責任限制、保險政策、與其他憑證機構之互通性、電子憑證撤銷的程序及公布的週期。

（3）安全事件緊急處理機制之建立

世上沒有「完美無瑕的安全」，因此政府必須未雨綢繆，建立電子認證系統等資訊安全事件的緊急處理機制，以發揮事前預防、偵測，事中監督及事後有效處理的功能。以研考會建置的 GCA 爲例，已經規劃系統安全防護機制，並建立主動式入侵偵測系統（Intrusion Detection System, IDS），防止系統遭受安全上的危害，確保系統之正常運作；同時規劃如遭受分散式阻斷服務攻擊（Distributed Denial of Services, DDoS）及其他攻擊時之應變計畫及作業程序。同時，研考會已會同中華電信公司及交通大學建置電子化政府網際服務網緊急處理及通報機制（GSN-CERT）。今後，參考國外的經驗，研考會將進一步推動下列各項措施：

1. 結合產、政、學、研等有關資訊科技、犯罪、社會學、心理學等各方面的專家，建立電子化政府公鑰基礎建設安全事件緊急處理機制，以發揮類似「網路119」的應變及處理功能。
2. 要求各憑證機關從業務永續經營的觀點，評估各種人爲及天然災害對其業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
3. 要求各憑證機構建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施。

(4)憑證實務作業基準(Certificate Practice Statement)之安全規範

憑證機構提供的電子認證服務，不但涉及密碼技術的應用管理，也涉及憑證機構的人員及設施安全管理，同時也涉及使用者與憑證機構的法律責任及義務。因此，爲了能夠使這一套機制操作化，同時提供使用者透明化的資訊，使消費者瞭解憑證機構的實務作業程序，以利其選擇及評估某一憑證機構是否安全可信賴，各國在建立電子認證機制時，都會立法規定憑證機構必須對外公布一份「憑證實務作業基準」（certificate practice statement）作爲執行的準據，例如：要求憑證機構說明憑證機構應用的技術、安全控制措施、憑證的使用範圍、憑證的效期、憑證註銷及中止程序，憑證註銷清冊公布時間或方或等資訊，以示向社會大眾負

責；同時，亦以這份基準作爲規範憑證機構與使用者之間的法律責任及權利義務關係。我國「電子簽章法」第十一條第一項規定：「憑證機構應製作憑證實務作業基準，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關核定後，並將其公布在憑證機構設立之公開網站供公眾查詢，始得對外提供簽發憑證服務。其憑證實務作業基準變更時，亦同。」第十一條第二項規定：「憑證實務作業基準應載明事項如下：足以影響憑證機構所簽發憑證之可靠性或其業務執行之重要資訊；憑證機構逕行廢止憑證之事由；驗證憑證內容相關資料之留存；保護當事人個人資料之方法及程序；其他經主管機關訂定之重要事項。」依據以上規定，憑證機構對外公告的憑證政策及憑證實務作業基準，不但是憑證機構賴以運作的安全基準，也是規範憑證機構、憑證持有人及善意第三者法律關係的重要文件。

以現行 GCA 公布的憑證實務作業基準爲例，重要的內容包括憑證運作機制、憑證管理系統、憑證適用範圍、採用標準及格式、憑證申請及異動、金鑰管理、安全控管、權責控管及出版發行等事項。今後，GRCA 及 GCA 將依據「電子簽章法」之規定及 RFC2527 之規範，重新檢討修訂憑證實務作業基準，送請經濟部核定後對外公布實施。

憑證實務作業基準可以說是憑證機構必須遵守及遵辦的「憲法」，憑證實務作業基準送經主管機關（經濟部）核定並對外公布之後，憑證機構或電子憑證的使用者如未依據作業基準的相關規定行事，發生權益受損情事，憑證機構及當事人必須受到作業基準的約束及規範。例如，憑證機構如果未依憑證實務作業基準之規定，採用安全及可信賴之技術、方法及設施，雇用可信賴之人員執行其業務，致其簽發之電子憑證遭僞造、竄改，使當事人權益受損；或憑證機構對於憑證申請人，未忠實查驗其身分，確定申請人與「公開金鑰」之關係，或未依規定將憑證註銷清冊對外定期公布，致當事人權益受損時，憑證機構應負相關的責任。

除了憑證機構要依據實務作業基準維運及管理電子憑證外，電子憑證的使用者亦要依實務作業基準的相關規定使用及保管自已的私密金鑰；例如，假設當事人私密金鑰有安全之虞，必須依規定在一定的時限內向憑證機構通報註銷憑證；再如，爲了降低可能的風險，憑證實務作業基準會載明電子憑證的使用政策及應

用範圍，諸如：限定電子憑證只能使用在證明使用身分的相關應用，不能使用在與金錢有關的應用；或是限定電子憑證雖可以使用在與金錢有關的應用，但是限定只能在一定金額以下，或是限定每日最高的使用次數。假如憑證使用者未依實務作業基準的相關規定行事，如權益受損，憑證機構將不負相關責任。我國「電子簽章法」第十四條規定：「憑證機構對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行爲無過失者，不在此限。憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。」其立法目的即是植基於風險及責任適當配置在憑證機構、憑證持有人及善意第三者身上，以免風險過於集中，影響憑證機構之經營及憑證持有人之使用意願。

（5）憑證保險制度

以密碼學爲基礎的數位簽章及電子認證機制，雖然透過技術及管理措施可以確保相當程度的安全性，惟仍有可能因爲自然、人爲、管理等疏失，致當事者權益受損。爲分攤風險，增進使用者的信心，財政部正在研究建立憑證保險制度，以保障使用者的權益，增進民眾的信心。今後，政府憑證機構如因人爲及其他因素，導致使用者及第三者權益受損時，如果政府憑證機構不能證明非屬其過失，將涉及國家賠償問題，民間經營的憑證機構則將產生損害賠償的問題。

(三) 教育及宣導（education）

從各種統計資料及實務經驗顯示，人爲疏失、缺乏安全警覺，不瞭解問題的嚴重性，是公私組織面臨的最大的安全漏洞。任何系統最薄弱的一環是人，在各種資訊安全對策中，投資報酬率最高的安全對策，是持續不斷的進行安全警覺訓練及教育宣導。唯有透過不斷的資訊安全教育及訓練，建立資訊安全的組織文化，才能使電子化政府的資訊安全管理工作能夠落實。由於電子簽章是極爲新穎及高度複雜的技術，爲增進民眾的信心，確保民眾的權益，政府必須結合各界的資源及力量，加強對各政府部門及民眾進行必要的訓練及宣導，使各界正確認知及了解電子憑證的安全措施。尤其是要加強對一般社會大眾的宣導，使其了解電子簽章的基本概念、如何正確的操作及運用電子憑證、如何保護個人的私密金鑰、如

何辦理憑證的註銷、如何選擇一個可信賴的憑證機構等，進而保護使用者的權益。此外，政府也必須對於執法人員進行訓練，使其犯罪偵防、裁判訴訟過程中，了解電子簽章之基本概念及技術應用，進而保障民眾的法益。

(四) 道德規範及專業倫理(ethic)

憑證機構提供的電子認證服務，基本上是一種「安全」及「信賴」的服務；憑證機構最重要的資產就是它的技術專業人力及能力、安全管理能力及對消費者提供的保護，足以讓使用者產生信任及信賴，願意相信它所簽發電子憑證的安全性及公信力。在憑證機構安全環境中，最脆弱的環節是人的因素。由於憑證機構在今後網路安全交易中將扮演公正客觀第三者的角色，對不特定的民眾提供網路安全交易所需的安全認證服務，爲建立安全及可信賴的網路交易環境，健全電子認證市場秩序，保護消費者的權益，政府除了從技術工程、管理、教育訓練等面向，建立妥適的憑證機構管理機制，促進憑證實作的安全性，以增進民眾的信心外，尚必須加強道德規範及專業倫理的建立，以減少人爲故意或疏失造成的風險，進而增進使用者對於憑證機構的信賴。例如，憑證機構必須建立及依循憑證機構作業準則、程序及控制的專業道德規範；以忠誠的態度爲大眾服務，不可從事非法或不正當的活動；對於執行業務所獲取的個人隱私及營業秘密，應予保密；不斷學習以維持及提升本身應有的專業能力；勤於參與對於各界的教育訓練，以促進各界對於電子憑證應用及資訊安全管理的了解。

肆、結語

「電子簽章法」完成立法，最重要的意義是排除電子文件及電子簽章的法律不確定性，並建立憑證機構的管理機制。但是，徒法不足以自行，仍然必須從技術、管理、教育及專業道德等層面，推動各項安全措施，破除電子認證的「技術障礙」及「心理障礙」，增進民眾對於電子化政府公鑰基礎建設的信心，並以逐步漸進的方式，選擇風險較低的網路申辦服務及電子交易試行，建立風險管理的

制度，俟社會熟稔電子憑證的應用之後，再全面推廣。

爲健全我國的電子簽章機制，政府宜加速推動下列工作：

（一）儘速參酌國際相關標準，制定加密演算法、IC 卡等各項電子簽章的相關國家標準。

（二）儘速參酌歐美主要國家的經驗，建立密碼模組等安全產品、系統等安全檢測及驗証制度。

（三）參酌 ISO17799 安全管理標準，建立憑證機構的電腦稽核制度，並且定期對各政府憑證機構進行外部稽核，以昭公信。

（四）加強訓練電子簽章相關人才，提升各政府憑證機構的安全管理能力。

（五）建立政府憑證機構的安全風險管理制度，定期對各政府憑證機構進行安全威脅及弱點分析。

（六）審慎遴選政府憑證機構的從業人員，並且加強憑證機構從業人員的考核。

【原刊載於檔案管理局出版之檔案季刊（九十一年六月）第一卷第二期】

參考資料：

[1] 交通部電信總局。通信安全密碼模組檢測實驗室及認驗證體系建置規劃研究報告，民國89年11月。

[2] 中華民國電腦稽核學會。資訊安全管理系統之稽核與驗證，民國90年10月。

[3] 經濟部標準檢驗局。堅實我國資訊安全管理系統稽核作業泉列討論會—公開金鑰基礎建設與資訊安全管理，民國91年3月。

[4] Ellison, Carl and Bruce Schneier. Ten Risks of PKI:What you're not being told about Public Key Infrastructure, www.goci.com/PKIrisks.htm.

[5] Fred B. Schneider, E.. "Computer Science and Telecommunications Board," Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Trust in Cyberspaces. Washing, D.C.: National Academy Press, 1999.

[6] Hously, Russ, Tim Polk, Planning for PKI: Best Practices Guide for Developing Public Key Infrastructure. John Wiley & Sons, Inc. 2001.

[7] Nash, Andrew, William Duance, Celia Joseph, and Derek Brink. PKI: Implementing and Managing E-security. New York: Osborn/McGraw-Hill, 2001.

[8] NIST. Certificate Issuing and Management Components Protection Profile. Jan. 2001.

[9] NIST. Introduction to Public Key Technology and the Federal PKI. Feb. 2001.