電子商務PKI發展在日常生活之應用

文／武俊麟

摘要

網際網路的應用帶動了電子商務的蓬勃發展，改變了人的生活與商業活動型態，企業為因應這新一波的競爭環境，紛紛建置企業網站、網路商店來爭取電子商務的潛在巨大商機。相對的要普及電子商務的交易行為，首要解決網路交易安全及交易雙方身分確認兩項問題，取得交易雙方信任（Trust）。而公開金鑰架構PKI（Public Key Infrastructure）的機制，配合密碼技術（Cryptography）的應用，可提供網路交易的四大保障，傳輸資料的保密性（Confidentiality）及完整性（Integrity）、交易雙方身份的確認性（Authentication）及不可否認性（Non-repudiation）。

PKI電子認證機制提供一個安全的電子交易環境，是電子商務普及應用的關鍵，而以密碼技術發展之數位簽章與資料加密，則是安全認證之核心，加以近年國際各國積極推動電子簽章相關法令制定（我國在九十年十一月十四日公佈施行），更明確奠立國家PKI架構運作模式。

PKI的系統技術及相關信賴環境（如電子簽章、網路智財權）的法制化，是健全電子商務環境重要關鍵，本文從電子商務PKI核心系統－憑證管理機制（Certification Authority，CA）運作與相關簽章法令制定，電子商務PKI系統發展應用及實例介紹等方面探討，希望有助剖析PKI在電子商務環境應用及未來發展之影響。

關鍵字：公開金鑰架構、電子商務、數位簽章、電子簽章

前言

前英代爾(Intel)總裁葛洛夫 (A.S.Glove)在1999年曾提出預言，五年以後所有的企業已是電子化的網際網路公司。網際網路的應用帶動了電子商務的蓬勃發展，改變了人的生活與商業活動型態，企業為因應這新一波的競爭環境，紛紛建置企業網站、網路商店來爭取電子商務的潛在巨大商機。相對的要普及電子商務的交易行為，首要解決網路交易安全及交易雙方身分確認兩項問題，取得交易雙方信任（Trust）。而公開金鑰架構PKI（Public Key Infrastructure）的機制，配合密碼技術（Cryptography）的應用，可提供網路交易的四大保障，傳輸資料的保密性（Confidentiality）及完整性（Integrity）、交易雙方身份的確認性（Authentication）及不可否認性（Non-repudiation）。

電子商務與PKI

一.電子商務與PKI之關聯性

美國有份針對百大資訊長（CIO）調查，結果只有9%的受訪者表示「安全問題」為公司營運焦點之首要技術議題；又根據Datamonitor的研究報告顯示，全球企業中有超過五成的公司僅提撥5%或更少的IT預算，用於網路的安全防護上，更有三成的公司還未部署足夠的安全系統。另在2001年全球電子商務阻礙與困境調查報告中，明白顯示安全相關問題在電子商務各類交易模式面臨十大課題排名及其比較：

名次	中小企業	名次	大型企業
1	網路駭客攻擊的安全性	1	使用者認證
2	安全與加密	2	安全與加密
3	公司文化	3	電子商務應用系統與舊有系統之間的互通性
4	電子商務應用系統與舊有系統之間的互通性	4	公司文化
5	缺乏專業知識與人才	5	電子商務網站之間的互通性
6	使用者認證	6	網路駭客攻擊的安全性
7	電子商務網站之間的互通性	7	付款機制能力
8	組織管理上的難題	8	缺乏標準
9	缺乏標準	9	組織管理上的難題
10	主管階層的認知	10	缺乏專業知識與人才

表一：B2B電子商務十大障礙—以企業大小觀點比較

名次	中小企業	名次	大型企業
1	安全與加密	1	安全與加密
2	顧客信賴度	2	顧客信賴度
3	成本評估	3	使用者認證
4	消費文化	4	成本評估
5	缺乏商業模式	5	國際貿易上之障礙
6	缺乏專業知識與人才	6	缺乏專業知識與人才
7	缺乏電子商務標準	7	網際網路的速度太慢而且不可靠
8	相互矛盾的課稅法令	8	消費文化
9	國際貿易上之障礙	9	缺乏商業模式
10	消費者找不到我的商店	10	消費者找不到我的商店

表二：零售業電子商務十大障礙—以企業大小觀點比較

名次	美國以外國家	名次	美國
1	安全與加密	1	電子商務應用系統與舊有系統之間的互通性
2	使用者認證	2	電子商務網站之間的互通性
3	網路駭客攻擊的安全性	3	組織管理上的難題
4	公司文化	4	公司文化
5	缺乏專業知識與人才	5	網路駭客攻擊的安全性
6	電子商務應用系統與舊有系統之間的互通性	6	缺乏標準
7	電子商務網站之間的互通性	7	安全與加密
8	缺乏標準	8	使用者認證
9	組織管理上的難題	9	缺乏專業知識與人才
10	付款機制能力	10	付款機制能力

表三：美國與美國以外國家發展B2B電子商務面臨十大阻礙

名次	純網路公司	名次	網路與實體並存	名次	純實體公司
1	電子商務應用系統與舊有系統之間的互通性	1	使用者認證	1	安全與加密
2	安全與加密	2	安全與加密	2	網路駭客攻擊的安全性
3	公司文化	3	網路駭客攻擊的安全性	3	公司文化
4	電子商務網站之間的互通性	4	公司文化	4	電子商務應用系統與舊有系統之間的互通性
5	缺乏標準	5	電子商務網站之間的互通性	5	組織管理上的難題
6	主管階層的認知	6	缺乏專業知識與人才	6	電子商務網站之間的互通性
7	缺乏專業知識與人才	7	電子商務應用系統與舊有系統之間的互通性	7	主管階層的認知
8	網路駭客攻擊的安全性	8	缺乏標準	8	使用者認證
9	缺乏商業模式	9	組織管理上的難題	9	缺乏專業知識與人才
10	商業夥伴對電子商務尚未就緒	10	付款機制能力	10	留不住專業人員

表四：B2B電子商務十大障礙—網路與非網路公司比較

名次	純網路公司	名次	網路與實體並存	名次	純實體公司
1	安全與加密	1	安全與加密	1	安全與加密
2	顧客信賴度	2	顧客信賴度	2	顧客信賴度
3	消費文化	3	成本評估	3	消費文化
4	付款機制能力	4	缺乏專業知識與人才	4	相互矛盾的課稅法令
5	使用者認證	5	消費者找不到我的商店	5	成本評估
6	缺乏商業模式	6	國際貿易上之障礙	6	使用者認證
7	相互矛盾的課稅法令	7	缺乏商業模式	7	缺乏專業知識與人才
8	缺乏專業知識與人才	8	使用者認證	8	合約、責任及其他法律相關因素
9	國際貿易上之障礙	9	消費文化	9	缺乏商業模式
10	成本評估	10	缺乏電子商務標準	10	消費者找不到我的商店

表五：零售業電子商務十大障礙—網路與非網路公司比較　　資料來源：台灣國際電子商務中心

電子商務(Electronic Commerce)憑藉著只有「信任」(Trust)，但要確保交易信任需具備保護隱私、身份認證、整合、不可否認性四項要件，但傳統使用帳號/密碼（ID/Password）和對稱式密鑰則都有缺陷。使用者/密碼的方法，只有身份認證的功能，對稱式密鑰可以確保文件隱私和雙方身份，但無法做到交易過程的整合，以及公正第三者確保交易雙方約定的不可否認性，只有PKI（Public Key Infrastructure）的數位認證可以同時滿足這四項要求。

二.電子商務定義及其運作模式

綜整國內外學者觀點概念分述如下：

（一）國外學者論點：

* Kalakota & Whinston：乃藉由電腦網路將購買與銷售、產品與服務等商業活動結合在一起，經由此方式可以滿足組織、商品與消費者的需要，進而改善產品、服務與增加傳送速度服務的品質，並達成降低成本的要求。

* Kalakota：乃透過使用電腦網路去搜尋與取得資訊，可以幫助個人與公司進行決策之制定。

* Ted Haynes：爲透過電腦與網路來處理企業溝通與交易的進行方式。

* Arie Segev，Dadong Wan & Carrie Beam：電子商務係藉由公共或私人的數位網路而被運用在提供產品之購買、銷售與服務以及資金之交易。

* Michael Bloch，Yves Pigneur & Arie Segev：爲經由數位電子設備，支援企業進行商業上之任何交易活動。

（二）國內學者論點：

* 周冠中認爲電子商業(Electronic business)是在企業的價值鏈上運用新的資訊科技以達到企業內部資源的運用能更加透明化及有效率，其連結企業、企業對個人(消費者)之商業行爲的價值鏈，並透過網際網路以有效整合企業核心流程、供給鍵管理、客戶服務、技術支援及配銷通路。

* 陳美雪提出電子商務應用大概可分爲三種不同的種類:組織間(企業對企業)、組織內部(在一個企業裡面)和客戶與企業之間。

（三）電子商務定義及運作模式類別：

綜上所述，電子商務(Electronic commerce)係指：「利用Internet所進行的商業活動，包括商品交易、廣告、服務、資訊提供、金融匯兌、市場情報、與育樂販售等。」而電子商務的任何一筆交易，應包含四個層面：交易的「商流」配送的「物流」轉帳支付的「金流」資料加值及傳遞的「資訊流」，另歸納電子商務行爲模式分爲三類：

*企業對企業(Business-to-Business；B2B)的商業行爲：主要是指企業間的整合運作，如電子訂單採購、投標下單、客戶服務、技術支援等。

*企業對一般消費者(business-to-Consumer；B2C)商業行爲：是指企業透過網際網路對消費者所提供的商業行爲或服務，包括線上購物、證券下單、線上資料庫等應用。

* 消費者對消費者(Consumer-to-Consumer；C2C)的商業行爲：主要是爲消費者者之間自發性的商品交易行爲，如一般個人式的拍賣網站或二手跳蚤市場等應用。

上述三類電子商務模式或多或少均會有重疊，但基本上的定位及運作方式有所差別；B2B重視的是關係的建立，例如：電子訂單採購是要與企業往來的廠商或商業夥伴合作，而B2C及C2C則是一視同仁，不需顧慮交易對象是誰，反倒是交易安全與身份驗證比較重要。

三.PKI定義及其運作方式

（一）PKI（Public Key Infrastructure，公開金鑰基礎建設）定義：

* PKI是一組作業系統和應用程式服務，使公開金鑰加密容易即且方便使用。[台灣微軟]

* PKI是利用非對稱金鑰（Asymmetric Keys）的概念，所發展出數位憑證、數位簽章等網路風險管理的一種技術。[國家資通安全會報]

* 發行用於公開金鑰密碼系統之公鑰(Public Key)及其憑證(Certificate)的系統稱之，基本處理有：確認(Certification)及驗證(Validation)兩項，亦是一個發行與提供公鑰憑證(Public Key Certificate)之存取的憑證管理基礎建設(Certificate Management Infrastructure)。[吳

宗成]

* 綜上定義PKI係指憑證(Certificate)結合密碼學應用所發展出來的一套資訊安全機制。而憑證是使用者在網路上的身分辨識證明，憑證與明文結合經由雜湊密碼演算(Hash Algorithm)，並加密簽章可驗證資料完整性，經加密機密訊息可確保資料安全性。

（二）PKI的運作方式與原理

PKI是以公鑰密碼學爲基礎衍生出來的架構，其基礎建置包含憑證機構（Certification Authority,CA)、註冊中心（Register Authority, RA)、目錄服務（Directory Service ,DS）伺服器。由RA統籌、審核用戶的憑證申請，將憑證申請送至CA處理後發出憑證，並將憑證公告至DS中。在使用憑證的過程中，除了對憑證的信任關係與憑證本身的正確性做檢查外，並透過憑證廢止清冊(Certificate Revocation List ,CRL）對憑證的狀態做確認檢查，了解憑證是否因某種原因而遭廢棄。憑證就像是個人的身分證，其內容包括憑證序號、用戶名稱、公開金鑰（Public Key)、憑證有效期限等。

CA必須同時爲傳送者與接收者所信任，而由具公信力的第三者來擔任；由CA經過認證，簽發公開金鑰憑證，以作爲檢驗私密金鑰的憑證。PKI包含一支公開金鑰（Public Key）與一支私密金鑰(Private Key)，前者公開給大眾知道，後者由持有者保管。這一組金鑰爲一組電子密碼，可作爲檢驗身分之用，且具有相對應的關係，其中一支金鑰將訊息進行加密，另一支金鑰則可進行解密而得到原來的訊息。

私密金鑰保管應兼顧安全、便利性以及成本考量，而私鑰儲存設備包含電腦之硬碟或軟碟、加解密運算卡、Smart Card（智慧卡）或Token（權杖）等相關儲存元件。由於Smart Card具有硬體保護機制，安全性較高，因此資金移轉或轉帳等金流交換以Smart Card較合適，惟目前一張Smart Card加上讀卡機成本超過新台幣1700元以上，對一般企業來說負擔不小，因此資訊流交換爲主的企業內部多選擇將私鑰存放在電腦軟碟或硬碟裡；較之Smart Card，其他方式雖然安全度較低，但要不要選擇Smart Card端視企業對安全的需求而定。

以公鑰與私鑰進行加解密對電子商務有何好處？例如甲商（傳送者）要傳送資料給乙商（接收者）時，甲商先到CA取得乙商的公開金鑰以進行資料加密，再將資料傳送給乙商，由乙商用自己的私鑰進行解密；如此一來，除了甲商與乙商，不會有第三者看到資料的內容。至於甲商送資料給乙商時，如何讓乙商在收到資料時，確認是甲商寄出的呢？甲商可先用自己的私鑰對所傳送的資料進行加簽，再傳送給乙商，乙商到CA取得甲商的公開金鑰，確認這一組公鑰/私鑰是否可以比對，若比對無誤，即可確定資料的傳送者的確是甲商。至於資料是否被竄改就要經過訊息摘要（Message Digest）的比對。

從以上乙商確認甲商是資料傳送者、資料加密、資料未被竄改，再加上只有甲商知道自己的私鑰，當乙商收到的資料含有甲商的私鑰，甲商就無法否認傳送的事實，再加上CA具有舉證的義務，當交易糾紛發生時，其必須提供相關證據資料，以協助仲裁單位處理糾紛；如此一來，也就達到了交易之保密、身分認證、交易資料完整、交易的不可否認性四大需求。

電子簽章法制重要性

隨著電子商務的興盛，電子簽章的法律效力被認爲與電子商務的發展息息相關，有鑒於電子簽章法草案已通過審核，面臨B2B、B2C電子商務市場蓬

勃發展，建立可靠的安全認證機制爲首要之務，由日前駭客入侵電子券商事件，再度突顯網路認證方式安全性不足問題，駭客只需竊取帳號及密碼等資料，便可透過網路下載認證，雖然滿足客戶便利需求，卻相對造成安全漏洞，降低資料安全性。

爲配合國家資訊通信基本建設之推展，我國首於民國86年由經濟部委託資策會科技法律中心進行數位簽章法之研究，並建議政府應儘速研訂數位簽章法，以律定電子簽章及電磁紀錄之法律地位。後經數年研議與修訂，電子簽章法終在90年11月14日公佈實行。至於喜歡上網購物的消費者，或是常需要透過網路傳輸重要機密資料的使用者，由於電子簽章法將使網路安全機制的規範更上軌道，同時確立電子簽章的法律效力，未來不論在電子商務或是電子文件的安全性及保密性上，都將更令人安心。另外，應用在公共工程招標方面，由於網路加密的過程中可以先過濾一些「特定對象」領標投標，再者透過網路領、投標的隱密性，黑道勢力將無法知曉要圍標的對象，這對於打擊黑金將有莫大的幫助。

電子商務PKI系統發展應用實例探討

PKI的概念可廣泛應用到各種領域，在公共領域方面，包括報稅、環保通報系統、健保、軍方行政相關應用、Smart Card（例如捷運悠遊卡、高速公路收費自動化）相關領域等；在私人企業方面，例如企業流程（Work Flow）管理、ERP、 SCM 等相關應用、B2B/B2C應用程式等，實際應用範圍如：員工差勤門禁系統、企業員工網路資料傳輸的加密及數位簽名、企業內部網路安控與使用權限機制、企業內部安全電子郵件及電子公文系統環境，以及電子供應商採購系統、電子經銷商訂貨系統、客戶分級與使用權限、安全電子交易加密與數位簽名、安全電子交易市集平台、跨國網路交易認證、交易認證國際漫遊功能等；企業或組織可透過PKI之應用，以支持網路企業經營模式發展，個人亦可藉由PKI機制，安全便利的完成交易或商業行爲。

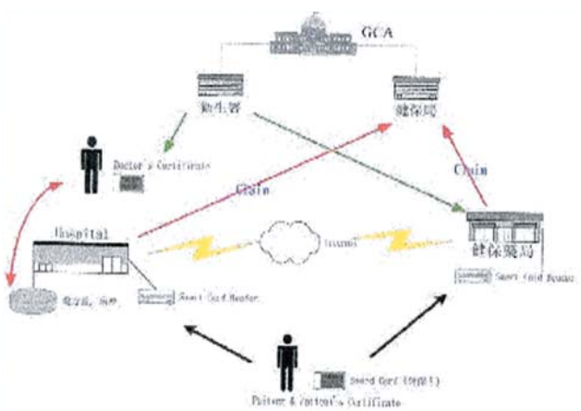
一.日常生活應用

電子商務的內容範圍非常廣泛，不只包括「商業交易」，還包括政府提供的各項電子化的服務、保險醫療的 申報、遠距離教學、電子銀行、跨企業共同研發、企業之間的協同運作(Collaboration)...等。在電子商務應用普及化之同時，PKI機制提供一個交易安全環境，不僅適用在電子商務商業交易模式，在未來亦可應用在日常生活中。

二.衛生醫療

隨著社會健保制度的普及，對病人的病情資料和健保投保資料的管理也日趨複雜，利用PKI的技術，可以讓相關人員更安全的得到所需的資料，而且不損及他人權益。

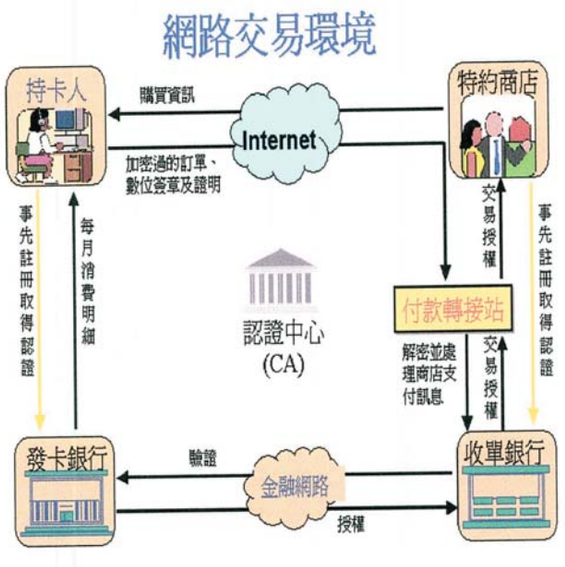
此時可利用PKI技術，將個人的醫療紀錄存放在健保局伺服器的資料庫，醫院透過讀卡機讀取病人的個人憑證或是健保IC卡，醫師可以使用自己的憑證透過網際網路經過健保局的授權去讀取病歷資料。而在醫師診斷完之後，再透過網路將醫療的處方傳送至該病患的檔案中，而病患前往藥局領藥時，藥劑師易可以經由同樣的方法來得到病患的處方簽。如此整個醫療體系串聯起來，並能更有效率的進行醫療工作。



圖一：醫療體制PKI建置示意圖

（一）網路購物

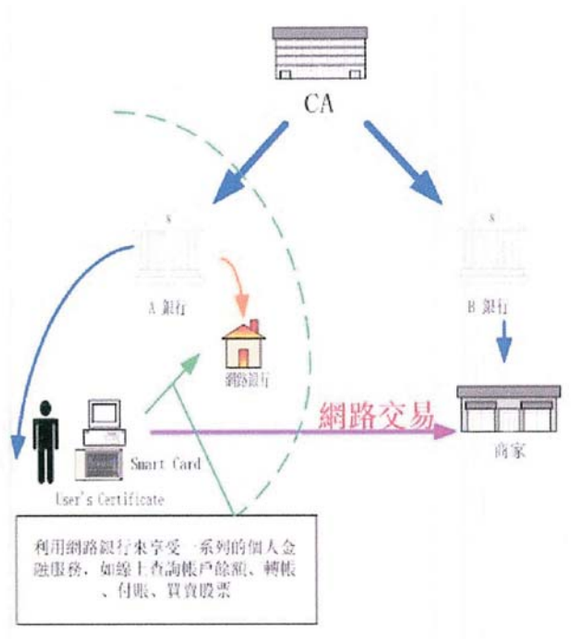
在電子商務時代，很多企業組織已經不再滿足於僅僅建立一個自己的網站，並希望透過Internet交換機密情報，甚至希望在網路上與自己的客戶、承包商和合作夥伴進行商業交易。爲達成此目的，參與網路交易各方首先必須建立相互信任關係（相當傳統面對面交易信任程度），所以將PKI技術與當前的Web瀏覽器、電子郵件程式或其他應用程式結合使用，就可以確保網路電子交易與商務活動的安全。



圖二：電子商務SET購物模式

（二）網路銀行

銀行和其他金融機構可以利用PKI的機制爲客戶提供更大的便利和安全性，客戶可以透過Internet執行一系列個人金融服務，如線上查詢、帳戶餘額、轉帳、付款、買賣股票和購買各種商品等，只需在瀏覽站前，把SmartCard插在和PC相連的讀卡機裡就行了，Web伺服器和客戶的Web的瀏覽器將會透過CA的驗證協議，自動確認彼此身份，目前國內已有卷商和銀行提供此服務機制，但僅限於使用該卷商或銀行，如何使消費者持有一憑證卡行遍天下將是未來發展趨勢，

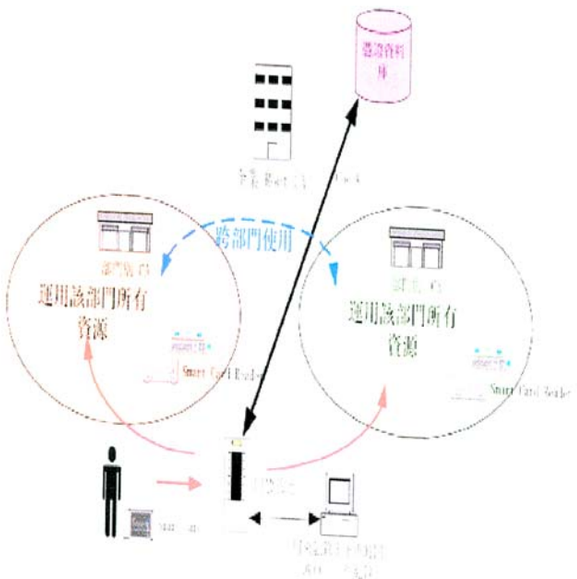


圖三：網路銀行與網路交易示意圖

（三）組織e化

PKI應用在企業內部可用來控管公司內部員工的一種機制，員工項公司的CA申請憑證後，可以利用自己憑證在網路上進行資料傳送的動作。比如：收發電子郵件或者具機密性檔案，運用PKI機制可使其能在網路上安全傳輸；而公司方面可以利用相關設備，了解員工的工作程序是否符合公司政策，比如：上下班時間或加班時間等。

新進員工上班第一天即可領到一張內崁憑證的IC工作證，員工可憑藉此證出入辦公室，亦可進入公司網路，而管理階層也可以依權限定時查看紀錄，確保員工工作效率。一旦員工離職，企業內部憑證發放中心可以即時將工作憑證作廢；對於遺失的處理除了立即作廢外，補發的新卡將使用新的數位憑證，但仍可使用原來公開及私有密鑰，不至影響工作進度。透過此種機制，企業除可提升行政效率外，亦可提升整體企業安全。



圖四：企業內部電子化示意圖

三.台灣證卷交易所網際網路申報作業

台灣證券交易所鑑公開金鑰基礎建設PKI架構之認證機制具有身分之確認性、資料之完整性、交易之不可否認性、資料之隱密性及證據留存仲裁之依　據等功能，是網際網路交易中，被視爲最安全的乙種方式，於此，要求臺灣網路認證公司提供安全認證服務，並開始進行申報資料網路認證及資料加密功能規劃；八十九年十月一日正式啓用網路申報認證作業。

台灣證券交易所率先採用國內發展的安控軟硬體，帶領證券市場於網際網路申報作業中，申報單位獲得了ｅ路安全的保障，從另一個角度來看，領導上市公司、證券商從申報作業的電子憑證引用，進而各上市櫃公司可藉由電子憑證的引導於開發電子商務商務軟體；另在虛擬社會交易環境中，限於各單位交易不同、設備不同、政策與策略不同，或許是各單位競爭關係，往往一個人申請數張憑證，使用於不同單位，不同系統，非常不方便，所以整合各金融 、證券等機構之CA作業，援用同一CA規範，構建CA互通性，使得單一電子憑證可適用各相關單位是未來電子商務發展之趨勢。

4.3.支付電子閘門（payment gateway）

「電子閘門」(Gateway)在「電子化／網路化政府」的計畫裏，主要是搭起民眾與政府機關、機關與機關間的網路溝通橋樑，使資訊交流的管道暢通，在資訊安全的前提下達到便民與便官的目標，它的服務形式是在一定的條件下，依據特定的供需原則，提供適當資訊服務的管理與控制之通道，「支付電子閘門」在技術與服務功能方面與一般電子閘門無異，只是「支付電子閘門」多了金錢交易行爲，除了在管理與控制上有其特殊性，也使得網路應用的功效更加完備，但目前現實環境下的限制條件還很多，必須逐步建立各種管理機制，健全其發展所需的週邊環境，達成各個不同階段性的目標後，才能提供一個理想的網路化服務及網路支付體系。

現行支付電子閘門在電子化政府中的應用最主要有三個方面，一是政府稅收，二是國庫預算撥款，三是政府採購與付款，而支付電子閘門的使用對象與政府電子支付的形式有關，政府電子支付的形式概略有幾種模式，包括民眾對政府、企業或法人對政府、政府機關對政府機關，因爲牽涉金錢往來，又涵括了金融機關，因此它的使用對象至少涵蓋了民眾、政府機關、企業或法人、金融機構。

結論

網際網路交易安全是每一個上網人的心願，PKI的安全架構與技術，從理論走向實務，由於PKI在電子商務系統應用所產生的效應是多方面的，對政府機關而言，它可以加速各級政府機關業務的電子化／網路化服務，進而催化政府機關間的業務及

系統整合，對民間而言，它帶動網路產品的需求與研發，使電子商務的時代早日來臨，進而促進產業升級，提高國家競爭力。（作者任職於海巡署通電資訊處科長）

參考文獻：

[1]"Security and E-Commerce International Developments" http://csrc.nii.org.tw/cnt/

[2]RSA Laboratories, PKCS #1:RSA Cryptography Standard, RSA Security, 2001.

[3]RSA Laboratories, PKCS #5:Password-Based Cryptography Standard, RSA Security, 1999.

[4]RSA Laboratories, PKCS #7:Cryptographic Message Syntax Standard, RSA Security, 1993.

[5]RSA Laboratories, PKCS #8:Private-Key Information Syntax Standard,RSA Security, 1993.

[6]RSAL aboratories, PKCS #11:Cryptographic Token Interface Standard, RSA Security, 2000.

[7]樊國楨，“電子商務高階防護－公開金鑰密碼資訊系統安全原理”，資訊與電腦出版社，民國八十六年。

[8]“政府憑證總管理中心及政府憑證管理中心委外服務需求說明書（草案）徵求意見書”，行政院研究發展考核委員會，民國九十年七月

[9]“政府憑證管理中心憑證實作準則”，http://www.pki.gov.tw/cps.htm

[10]http://www.secureonline.com.tw/

[11]http://www.nst.com.tw/PKI/

[12]http://www.pkiforum.org/

[13]http://www.gsncert.nat.gov.tw/

[14]http://csrc.ncsl.nist.gov/pki/

[15]http://www.taica.com.tw/

[16]http://www.trade.gov.tw/