以數位憑證強化資訊系統身分認證之研討

作者／李明坤上尉

提要

網路帶來便利快捷與內容豐富，卻也令使用者望之卻步，主要有兩個原因，一是使用者難以驗證對方的身分；二是無法保證資料在網路上傳輸的安全。未來陸軍在複雜電磁環境下遂行現代戰爭，為了提昇快速獲得戰場情資的能力，透過運作於網路上的資訊系統是一大利器。「憑證」利用雜湊函數簽章的驗證資料，內含簽署人的身分證明，其效力等同於印鑑證明，可達到身分識別性、機密性、完整性以及不可否認性等四項資訊安全主要特性，以數位憑證正可強化資訊系統身分認證的檢驗。

關鍵字：公開金鑰基礎建設、憑證、電子簽章法、網路安全、憑證管理中心

壹、前言

隨著網路蓬勃發展，致力於資訊安全領域的研究發展也隨之盛行。以公開金鑰演算法為基礎發展出公開金鑰基礎建設 (Public Key Infrastructure, PKI)，同時結合「憑證」的數位簽章技術，提供確認身分以及資料傳輸安全保密的方法。為了因應陸軍在複雜電磁環境下遂行現代戰爭，快速獲得戰場相關資訊情報的能力，透過網路交換各項情資已是世界趨勢，而傳送資訊同時，資訊安全是一關鍵性的考慮因素。國軍單位目前資訊系統大都採用通行密碼機制來達成身分確認目的，然而這種方式是最簡單身分識別方式，且易遭人入侵及無法得知使用者身分等缺點。本文以憑證為主體，探討憑證格式，特性以及所具備的應用，並提出利用國軍電子憑證所建立的資訊安全架構，可有效地提昇單位內部稽核網路安全。

一、研究動機

為了因應陸軍在複雜電磁環境下遂行現代戰爭，快速獲得戰場相關資訊情報的能力，透過網路交換各項情資已是世界趨勢，然而傳送資訊同時，也要考量資訊安全。國軍單位目前資訊系統大都採用通行密碼機制來達成身分確認目的，然而這種方式是最簡單身分識別方式，且易遭人入侵及無法得知使用者身分等缺點。目前資訊系統中，主要的安全問題來自於難以驗證使用者身分。網路有一句玩笑話「你不會知道跟你透過網路傳訊的對方，是一個人？或是一條

狗？」換言之，身分驗證一直是困擾資訊安全專家的問題。由於透過網路，不像人和人之間可以面對面地相互驗證身分，所以必須依賴使用者與電腦之間相互傳送一些訊息，用以驗證使用者身分。由CCITT 在1993年所提出的X.509協定是目前最有效的安全解決方式。國軍武器裝備日趨精良，資訊作業平台也隨花北高光纖電纜佈建完成，骨幹連至各作戰區與觸角末端延伸到作戰分區，網路化程度提昇迅速。網路的特性是快速、便捷、多元，但是安全性卻令人擔憂。軍以戰為主，嚴格訓練是國軍保障人民安全最堅強的基石，透過各項演訓可以訓練人員，更可以從中檢討過失改進。各項演訓系統的維護有賴資訊人員經心執勤，防止有心人士惡意破壞或竊取。登入系統的人員查核與權限控制是制定安全政策首要，本文研究動機以憑證作為身分驗證機制，可強化精進演訓系統人員稽核的工作。

二、研究目的

憑證是提供網路使用者身分認證的機制，具有機密性、完整性、有用性及不可否認性等特性。憑證管理伺服器擁有公正第三者身分，運用公開金鑰演算法計算上的安全，使得破密與解譯變成困難艱鉅，利用上述特性可確保網路安全，本文研究目的正基於此。

貳、本文

一、X.509 憑證格式介紹

公開金鑰基礎建設主要依照X.509 的相關標準所規劃，目的是為了達成開放網路上的使用者相互認證問題，其理論是以公開金鑰密碼系統為基礎。為連繫使用者和他的公開金鑰間的關係，需要由一公正單位，稱為憑證管理中心（Certificate Authority, CA），依其公正客觀地位，查驗憑證申請人身分資料正確性與其待驗證公開金鑰間之關連性，並據此為使用者發出一個證明文件，稱為公開金鑰憑證（public key certificate）。憑證具有以下安全特性[1]：

(一) 機密性：使用憑證加密 (預防洩密)。

(二) 驗證性：使用電子簽章驗章 (預防偽冒)。

(三) 完整性：使用電子簽章可驗證文件之完整性(預防竄改)。

(四) 不可否認性：電子簽章後不得否認。

公開金鑰憑證相當於為使用者提供一個聲明，證明該公開金鑰是屬於某一特定的使用者。X.509 標準另外採用目錄服務存取使用者的公開金鑰憑證，目

[1] 節錄憑證管理工具簡易使用手冊版本 1.01，國防部國防資訊中心，民國 92 年 9 月。

錄服務主要優點為使用者的公開金鑰憑證可以存放於目錄伺服器中，提供網路的使用者自由存取。

公開金鑰憑證(簡稱憑證)，係指經過憑證管理中心認證後可資證明的電子憑證。憑證格式內容包括：憑證序號、用戶名稱、用戶的公開金鑰、憑證有效期限及憑證管理中心之數位簽章等。憑證管理中心經多道步驟，驗證使用者申請的身分與其附上公開金鑰。檢查無誤後，發給憑證作為其網路身分識別的有效證明依據。憑證內容包含金鑰擁有人之基本資料及公開金鑰，並附以憑證管理中心之私密金鑰所作數位簽章保護、防止偽造及竄改。憑證管理中心所簽署憑證標準格式如表一所示。

表一 憑證標準與格式

	公開金鑰憑證欄位	內　　容
1	版本	憑證製作依據 X .509 版序（V 3）
2	序號	憑證管理中心所給定的唯一憑證序號
3	數位簽章演算法	憑證管理中心簽署該憑證所用的簽章演算法
4	簽發單位名稱	簽署該憑證之憑證管理中心名稱
5	憑證有效期限	憑證生效日期與截止日期
6	用戶名稱	依據 X .500 命名方式所命名的用戶名稱
7	公開金鑰資料	公開金鑰的值與演算法名稱
8	簽發者識別號	簽署該憑證之憑證管理中心獨有的識別號碼
9	用戶識別號	用戶獨有唯一識別碼
10	X.509 擴充欄位 (V 3)	憑證管理中心的政策與金鑰名稱補充
11	數位簽章演算法	憑證管理中心簽章所用的演算法
12	數位簽章	憑證管理中心對該憑證所作數位簽章

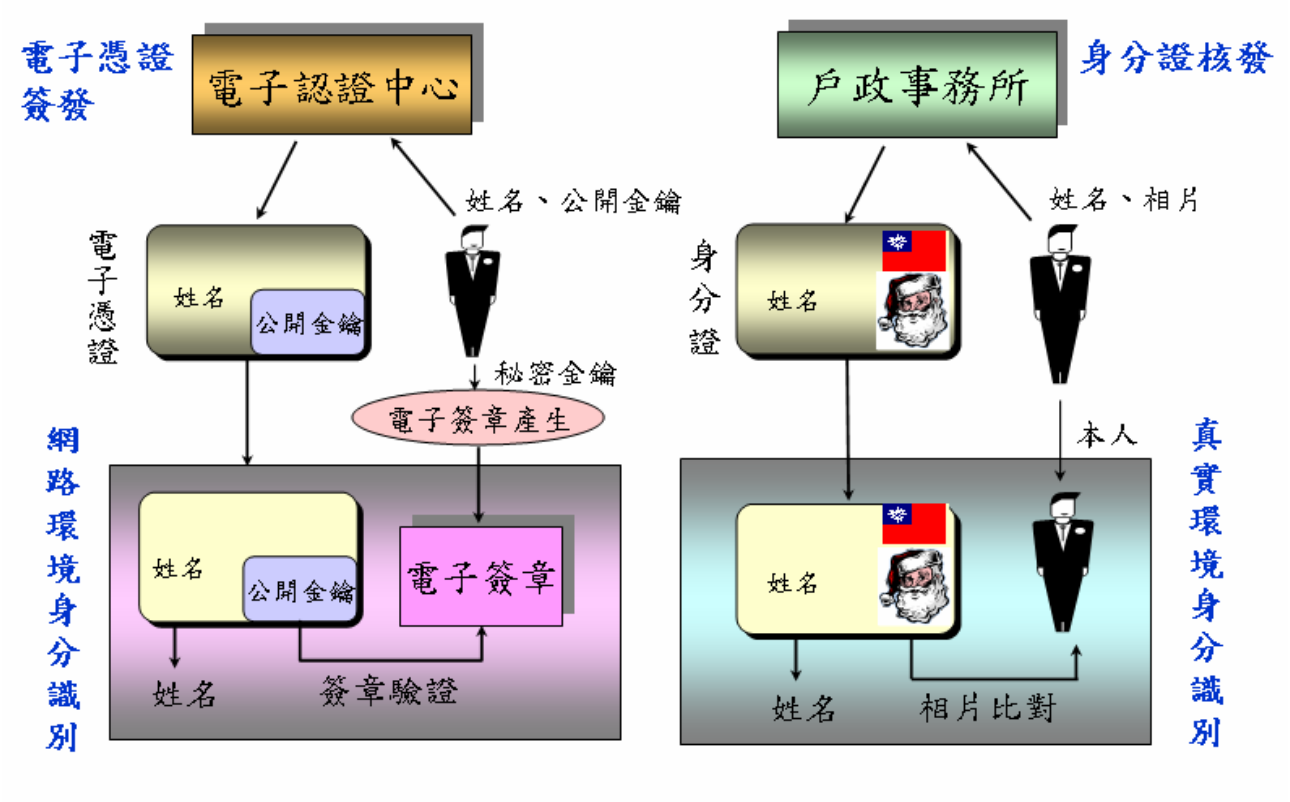
(資料來源：作者整理)

為使公開金鑰基礎建設能順利運作，須建立相關的資訊系統，用以管理使用金鑰與憑證。輔助公開金鑰系統運作的服務與系統包括憑證管理系統、目錄檢索服務、公證服務、不可否認服務、時戳服務、票證產生服務、數位掛號信遞送服務、金鑰保管回復中心和加解密的應用程式介面等。而公開金鑰基礎建設即為結合上述服務與系統共同運作。在所有系統中，以憑證管理中心系統是公開金鑰基礎建設中最重要的核心部分。

二、電子簽章法簡介

商業交易行為中，建置一個憑證中心來幫助交易時，尚須考量安全及可信賴的網路環境，確保資訊在網路傳輸過程中不易遭到偽造、竄改或竊取，且能鑑別交易雙方之身分，並防止事後否認已完成交易之事實，是電子交易重要的

課題。但是如果沒有法律作為基礎，那對交易雙方而言是沒有保障，尤其在網路上從事交易的信心也會減少。交易後如果交易雙方對交易有所疑問，其中的權責問題如沒有法律來規範，勢必會造成很大爭議。例如，對於一些必須製作書面或附有簽名或蓋章才符合法律規定的契約，在還沒有電子簽章法訂定以前，以網路或電子方式做成的交易，因為沒有以傳統書面或簽名的形式完成，這些交易就會變成不合規定而沒有法律效力的契約。我國電子簽章法的成立，就是為了順應科技發展，結合法律與瞬息萬變的社會演進，對上述問題提出的解答[2]。



圖一 相對關係圖(資料來源：國軍網頁式郵件Mail 2000用戶安裝與操作，異康股份有限公司)

經濟部於1997年委託資策會科技法律中心進行數位簽章法之研究，並建議政府應儘速制訂數位簽章法，以律定電子簽章及電子文件之法律地位，建立電子憑證機構之管理制度，界定憑證機構與使用者之權責，建立跨國認證之機制，以解決現有法令規範不足或不確定之處，參酌各國立法體例及聯合國與歐盟等國際組織訂定之電子簽章立法原則，擬具「電子簽章法」。電子簽章及電子文件與傳統使用手寫簽名、用印鑑蓋章、書面紙本等相同法律地位與效力，使電子簽章得以取代傳統簽名蓋章，是電子簽章法主要的目的，以減少各種適用法

[2] 節錄電子簽章法之攻略密技，經濟部資策會，民國 93 年 8 月。

律之爭議，相對關係如圖一。

我國電子簽章法於2001年11月14日由總統明令公佈，2002年4月正式施行。盼藉著電子簽章法之通過施行能積極促進我國電子商務發展及電子政府的推動工作。該法作為推動電子商務發展及電子化政府之法源依據為立法目的。其主要目的是為賦予符合一定程序做成之電子文件、電子簽章能取代實體書面、簽名蓋章之效力。此外因體認到擁有可供運用的電子認證技術之同時，亦必須制定相關法規以作為行為之依據，所以我國電子簽章法之另一規範重點即在於憑證機構之管理機制，期能透過相關規範架構之建置，於提升整體電子交易安全之同時，亦能有效保護民眾的權益。電子化政府之發展有賴電子認證體系之妥善運行作為基礎，而在電子商務方面，亦唯有在消費大眾之權益能夠獲得保障以及網路消費信賴環境建立後，電子交易才能獲得普遍運用。所以，為進一步的促進國家整體資訊發展，有必要訂定電子簽章法，以作為相關發展之法治基礎。

三、政府機關憑證之應用

政府於民國92年根據「內政部自然人憑證發證計畫」所推出的「自然人憑證」即是以公開金鑰基礎建設為基礎的一種憑證。因此自然人憑證具有網路身分認證以及確保資料傳輸安全的功能，幫助政府解決了上述的身分認證及資料傳輸安全的問題。所以自然人憑證可以說是推動政府電子化服務不可或缺的一環。自然人憑證是政府為了提供民眾在網路上作資料交換時，可以用來辨識雙方身分的工具，也可以說是政府頒發的網路身分證。雖然網路非常的方便，但過去政府無法在網路上為人民服務。主要有以下兩個原因：

(一) 難以確認網路上使用者的身分。

(二) 無法確保資料在網路上傳輸的安全性。

政府服務多要求申請人帶著身分證，親自到場辦理。隨著資訊科技的發展，政府採用了一種叫做「憑證」的工具。該「憑證」是由公開金鑰基礎建設的運作機制所發行的，包含了「數位簽章」跟「公開金鑰」，可以達到身分識別性、機密性、完整性以及不可否認性等四個資訊安全的需求特性。公開金鑰密碼系統區分「公開金鑰」與「私密金鑰」，「私密金鑰」可儲存在IC晶片當中。經由憑證使用人和憑證管理中心約定，日後使用這憑證，就可以辨認使用者的身分，並且可以用來加解密所要傳輸的資料。因此，不論以後要傳輸什麼樣的資料，經過加密之後，即便是被其他人竊取資料，也無法輕易的解開得知原始內容。而此憑證也就是所謂的「自然人憑證」。自然人憑證是由內政部憑證管理中心所簽發的，辦理了自然人憑證以後，可以使用許多政府提供的網路服務，

方便民眾在網路上辦理業務、查詢資料，只要經由網際網路即可享受政府的電子化服務。除了內政部有建置憑證管理中心外，其他政府機關與民間企業也有相關憑證中心建立，如表二。

表二 政府各機關憑證主要應用

憑證機構	憑證中心	主要應用
經濟部	MOEACA	E 政府相關服務應用
內政部	MOICA	E 政府相關服務應用
研考會	GCA、XCA	E 政府相關服務應用
衛生署	HCA	醫療電子化應用
銀行公會	TFRCA TFPCA TFUCA	網路銀行相關服務應用
台灣網路認證	NBCA EG+CA FEDI CA 關貿網路 PAA	電子商務、網路銀行、網路/期貨下單、電子支票、股務代理
中華電信	CHTCA、ECA	企業憑證應用、一般憑證應用
網際威信	VTN、商務CA	電子商務、金融交易、電子支票

(資料來源：經濟部商業司)

由上述可知，自然人憑證是政府為了推行電子化政府的各項服務，所發行的憑證，可以驗證身分以及保護資料的機密性，幫助民眾在更安全的機制之下使用政府的電子化服務。為配合內政部推廣自然人憑證，各機關提出相關應用項目有數千種，以下列舉(如表三)幾個推廣憑證成功的案例。

表三 推廣憑證成功的案例

應用項目	提供服務	具體成效
地政資訊網際網路服務	申辦地籍資料、地價資料、地籍圖、建物測量成果圖。	降低人力節省成本：核發時間節省（5 分鐘→0 分鐘）、申請謄本份用（20 元→0 元）、民眾往返之交通時間及交通費用。
公文電子交換系統	公文利用網路交換 G2G、G2B 、G2C（每天有超過100,000 筆公文進行交換）。	交換：傳統→公文電子 時間：2-3天→低於1小時 成本：35/份→4元/份 管理：困難→簡單檔案管理 形式：紙本→電子 再利用：無法再利用→可以

		安全控管：困難→PKI
勞保網路申辦查詢系統	查詢個人勞保、勞退相關資料及投保單位承辦人利用網路進行加退保及相關申請、異動辦理	1.個人投保及勞退資料查詢，減少雇主高資低報或是錯誤申報之情形，提供一個投保當事人驗證資料的公開、透明平台。 2.節省投保單位承辦人辦理勞保相關業務之交通往返時間及成本。 3.公開透明的資訊提高民眾的信賴感。
綜合所得稅網路申報作業	下載個人所得資料、報稅	1.節省成本：節省民眾郵寄成本。 2.節省報稅時間：網路報稅只需10分鐘，相較傳統往返國稅局及填寫申報書所花費時間，節省許多時間。 3.下載報稅軟體，由電腦計算繳稅金額，亦可避免人為計算之錯誤。 4.對稽徵機關而言，網路報稅可節省收件、建檔、審核及發生錯誤事後處理成本。（人工報稅處理成本 12.17 元/件，網路報稅約 3.41 元/件）。

(資料來源：服務、成效：內政部分自然人憑證發證及應用推廣計畫)

四、國軍憑證之應用

國軍憑證推廣行之有年，採用X.509 及業界主要認證技術標準，支援憑證申請、展期、中止等認證功能，提供一整合應用平台，能介接各種應用系統，所有系統操作皆有稽核紀錄。國軍電子憑證之種類有[3]：

(一) 單位電子憑證：代表單位交換資料時使用。

(二) 個人電子憑證：個人電子簽章、加密時適用。

(三) 資訊系統電子憑證：資訊系統伺服器端及使用者端驗證及加解密時使用。

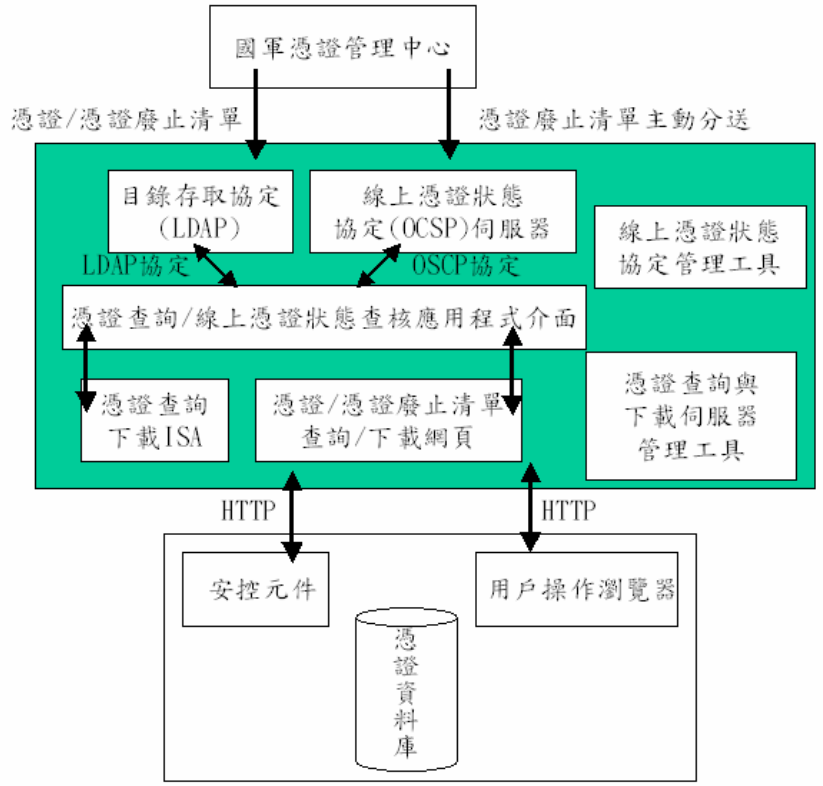
(四) 註冊中心（RA, Registration Authority）之電子憑證：RA成立時由國軍憑證機構核發。

(五) 國軍憑證機構（UCA, User Certificate Authority）之電子憑證：UCA成立時由國軍頂層憑證機構（RCA, Root Certificate Authority）核發。

可配合IC卡及其它多種憑證種類使用，更可搭配硬體密碼設備，強化系統應用安全性。而毋須為不同的應用系統使用不同套的安控中介軟體，可大量節省日後整合應用系統的成本。目前國軍憑證應用分階段逐步推廣，應用

[3] 國防部 93 年 1 月 8 日捷控字第 0930000049 號令修頒國軍電子憑證管理要點。

範圍有，電子公文交換、智慧卡開機登入系統、電子簽章加密軟體、辦公室自動化主系統與電子憑證整合[4]。國軍憑證安控管理平台之架構如圖二。

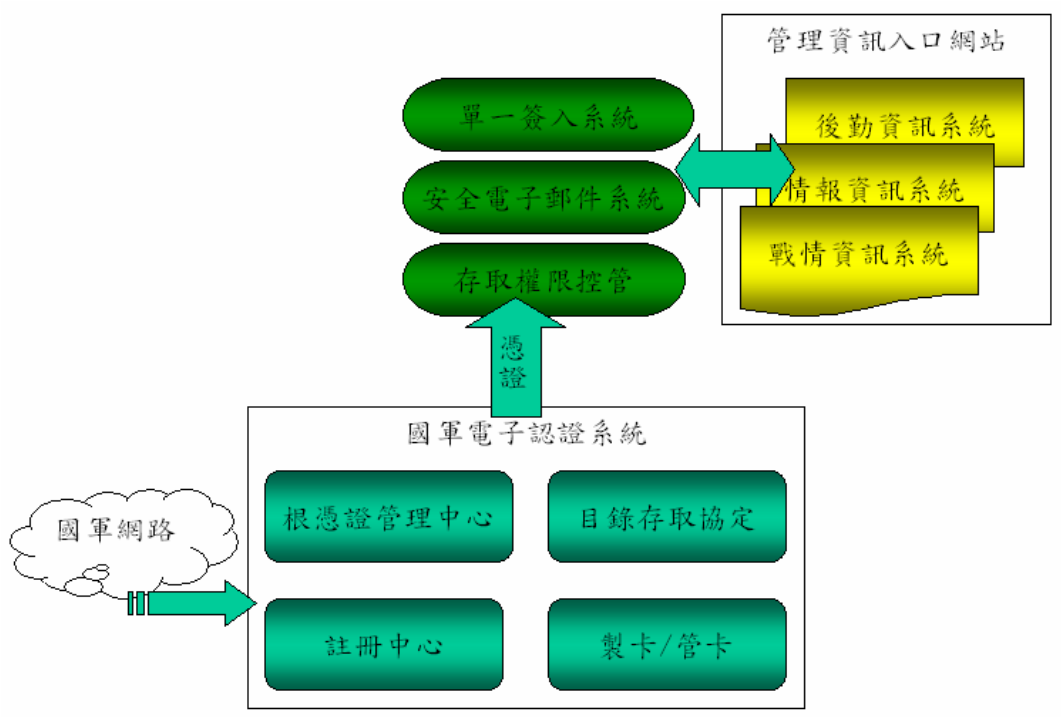


圖二 國軍憑證安控管理平台之架構(資料來源：作者整理)

五、整體資訊安全架構

本文所提供資訊安全規劃如圖三，藉由國軍憑證管理中心的 RA、LDAP、製卡與發卡等系統，利用憑證驗證身分，進入單一簽入系統，針對個別使用者分別給予存取權限控管與利用安全電子郵件傳輸加密內文與附件，整合各式管理資訊系統入口，執行各系統之身分認證及授權。滿足資訊安全及國軍憑證應用需求。結合國軍電子憑證以單一簽入方式，整合資訊管理及後勤資訊各系統，提供嚴謹可靠之電子憑證登入身分認證，以杜絕冒用身分登入之資安狀況發生，透過授權機制執行各系統之權限控管，使得系統資訊可以整合並達共享之目的。

[4] 國防部 91 年 10 月 17 日廣度字第 2789 號令頒「國防部電子憑證實施計劃」。



圖三　整體資訊安全架構(資料來源：作者繪製)

本系統規劃結合國軍註冊中心系統提供製卡、印卡及發卡作業，將國軍人員的單位級職、姓名、軍職代碼和照片等資料結合電子憑證一併處理，達到卡證合一的功能，作為人員身分與網路身分識別依據。

實際應用例如國軍戰演訓郵件系統，國軍網頁式郵件系統整合憑證作業，是將國軍電子憑證與現有「國軍網頁式郵件系統」進行整合，並作為「國軍戰演訓專用郵件系統」的備援，於網頁郵件系統上提供簽章、加密及簽章加密功能。此外，郵件系統本身會透過憑證查詢管理伺服器和電子簽章加解密程式元件，讀取並解譯 S/MIME 電子郵件之憑證資訊，以確認憑證之有效性（隱密、完整、來源辨識），網頁式郵件特性具有：

(一) 使用者端有瀏覽器，可完成所有信件的收發、備份、通訊錄管理等功能。

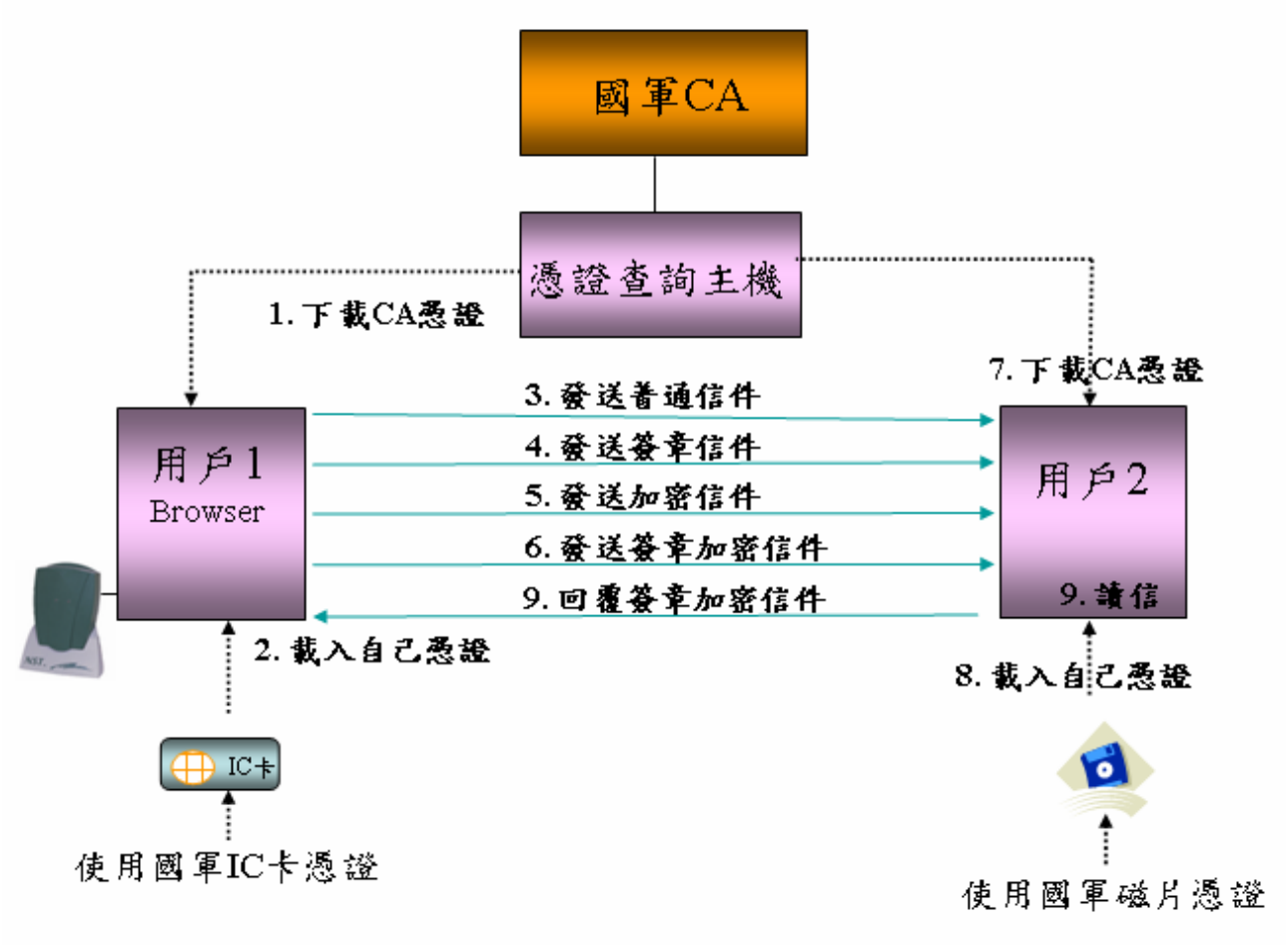
(二) 使用者端不記錄用戶帳號、郵件位址等資訊。

(三) 強調方便、功能完備、使用簡單，不受地理位置、作業平台影響[5]。

國軍電子憑證網頁郵件系統，整合國軍電子憑證與網頁式郵件系統，具備解析 S/MIME 電子郵件之功能，提供簽章、加密及簽章加密按鈕，於網頁郵件上能導引使用者進一步驗證該郵件數位簽章及解讀該加密郵件原文之能力。讓寄信者和收信者兩端可在安全的環境下進行資料交換或指令傳達，透過網頁的

[5] 國軍網頁式郵件Mail 2000 憑證用戶安裝與操作手冊版本 1.0 國防部參謀本部國防資訊中心，民國 93 年 3 月。

便利性簡化操作方式，導引使用者進一步驗證該郵件數位簽章及解讀該加密郵件原文，其應用架構如圖四。



圖四　應用架構 (資料來源：作者繪製)

提供網頁郵件客戶端瀏覽器，處理簽章與加密之對應程式元件，客戶端可透過手動安裝程式及網站自動偵測下載兩種方式取得元件。電子簽章與加解密程式元件程式碼須經過國防資訊中心核發之憑證簽章，在瀏覽器下載時得以驗證。使用者端可向 LDAP 伺服器查詢憑證。使用者端可選擇多種憑證媒體，包括智慧卡、磁片等。加密及解密方式包括 DES, 3DES, RC5, RSA-PKCS, AES 等演算法。使用雜湊函數功能，包含 SHA1, MD5 等方式。簽驗章與加解密均在使用者端瀏覽器上完成。網頁伺服器僅需專注於辨識 S/MIME 郵件，並對使用者端簽章及加解密之流程進行導引作業，所有實質之運算均於瀏覽器上完成。

另外為隔絕病毒、木馬與惡意程式入侵，在個人電腦使用上，建議採用精簡型電腦。基於資訊網路安全系統及遠端管理設定需求精簡型電腦可符合所列需求，當精簡型電腦沒有管理者權限時無法修改內建的作業系統、預先安裝的應用程式，或安裝新的軟體。使用者所做的修改無法儲存在系統中。此項功能

可隔絕病毒及木馬程式的入侵，即便是精簡型電腦暫存器中有病毒存在，然在電腦關機後便可移除，無用擔心病毒的入侵。

此外如果有特定的用途如限定 USB 埠、序列埠等裝置不得使用時，嵌入式作業系統便可預先移除該項驅動程式，即便用戶端欲連結該項裝置該項功能也無法驅動該項設備，有效隔絕內部人員資料外洩問題。人員需使用 IC 卡插入讀卡機藉此取得登入權限。透過精簡型電腦的防護機制，確實可以隔絕病毒及木馬程的入侵，並可限制或管理 I/O 埠的使用，確保機密資料不當下載或竊取。應用系統安控機制透過國軍憑證安控機制與單一簽入授權機制，整合於管理資訊入口網站，提供國軍人員整體安全作業環境。

參、結論與建議

網路與電腦科技的發展，突破了時空的限制，不僅影響生活，同時也衝擊國軍整軍備戰的需求，特別是透過網路中交換資訊的同時，各種網路安全問題亦不斷浮出抬面。如何在國軍資訊網路中安全傳送各項具有機密性的資訊資料，將是一個重要的課題。在目前網路電腦系統中，主要的安全問題來自於使用者身分驗證的問題，換言之，只要身分驗證問題能解決，網路安全問題也將可迎刃而解。CCITT 在 1993 年所提出的 X.509 協定為目前網路最有效的身分驗證解決方式。本文中，建議國軍資訊網路與組織內部的作業流程建置一套憑證申請與廢止機制的流程，並應用金鑰的產製與智慧卡進行結合，進而大幅提高了憑證中心整個架構的安全性。另外依據類似政府憑證管理中心組織架構與自然人憑證應用組織單位內憑證管理中心，並參考「政府憑證管理中心管理辦法」和「電子簽章法」之規定，訂定了憑證中心管理辦法與人員配置方式以真正有效來管理憑證中心。透過單一簽入認證伺服器之權限控管功能，達到不同權限的使用者登入入口網站後，整合國軍電子憑證，執行各類應用系統單一簽入認證機制，用戶僅需持有單一智慧卡憑證，即可依據系統管理者所設定的使用權限，進入各應用系統內使用。此種方法配合管理可確實有效地加強單位內部網路安全。

參考資料

一、林惠徵，公開憑證基礎建設之研究-屬性憑證運用在權限管理，中國文化大學資訊管理研究所碩士論文，民國 91 年。
二、吳順裕，粘添壽，資訊與網路安全技術。臺北市：旗標，民國 93 年。
三、朱建達，建立於公開金鑰基礎建設的單一簽入系統。交通大學資訊科學研

究所碩士論文，新竹市，民國 89 年。

四、張永志，中華民國海軍憑證中心之組織架構與建置，交通大學資訊管理所碩士論文，民國 90 年。

五、朱建達，建立於公開金鑰基礎建設的單一簽入系統。交通大學資訊科學研究所碩士論文，新竹市，民國 89 年。

六、廖雲傑，校園網路之身分認證與憑證基礎架構，大同大學資訊工程研究所碩士論文，民國 89 年。

七、羅傑帆，影響自然人憑證使用意願之因素探討，中央大學資訊管理研究所碩士論文，民國 94 年。

八、劉姿妙，我國政府電子憑證推廣方式之分析改善策略，成功大學工程管理專班碩士論文，民國 95 年。

九、憑證管理工具簡易使用手冊版本 1.01，國防部國防資訊中心，民國 92 年 9 月。

十、Stallings, W. (2003). Cryptography and Network Security: Principles and Practices (3rd ed.). Upper Saddle River, NJ: Prentice Hall.