國防科技學術合作協調小組研究計畫成果報告

中華民國海軍認證中心雛形系統之建置

計畫編號：NSC90-2623-7-009-016(90.0101-90.12.31)

執行期間： 90 年 1 月 1 日至 90 年 12 月 31 日

計畫主持人：劉敦仁 副教授

共同主持人：羅濟群　教授

執行單位：交通大學資訊管理研究所

中華民國 90 年 12 月 31 日

國防科技學術合作協調小組研究計畫摘要表

計畫名稱	中文: 中華民國海軍認證中心雛形系統之建置				
	英文:A Certificate Authority Prototyping System for R.O.C Navy				
學術執行單位主持人	姓名	劉敦仁	軍方對應單位主持人	姓名	高廣圻
	單位級職	交通大學資訊管理研究所副教授		單位級職	海軍總部戰鬥系統署
計畫時程	本期計劃：自 90 年 1 月 1 日起 至 90 年 12 月 31 日止		計畫編號	NSC90-2623-7-009-016(90.0101-90.12.31)	
			金額	961,000	
計劃歸屬	（ ）材料與應用化學 （ V ）電子與資訊系統 （ ）系統管理 （ ）遙測 （ ）航空技術 （ ）機械製作與應力 （ ）兵器系統 （ ）其他				

研究內容摘要：

為了增加海軍在未來戰爭急速因應快速獲得相關資訊情報的能力，透過網路快速地交換各項情蒐資訊已是不可抵擋的趨勢，而在使用海軍內部網路傳送資訊的同時，資訊安全將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的方式來達成安全的目的，然而這種方式具有易遭人入侵及無法確實得知使用者身份等缺點，對於任務具有高度機密性性質的海軍單位，實是一大弱點。因此，如何及早建置符合 X.509 的安全管理系統，將是海軍目前刻不容緩的課題之一。一旦憑證系統開發完成後，將可提供網路上完整身份驗證機制，對海軍內部網路安全的防護工作將有莫大的幫助。

在目前網路電腦系統中，主要的安全問題來自於使用者身份驗證的問題，換言之，只要身份驗證問題能解決，網路安全問題也將可迎刃而解。但由於透過網路，不像人和人之間可以面對面地相互驗證身份，所以必須依賴使用者與電腦之間共享的一些訊息，來驗證一個使用者的身份，由 CCITT 在 1993 年所提出的 X.509 協定為目前網路最有效的安全解決方式，如研考會所推動的國家公開金鑰基礎建設，亦採用 X.509 憑證管理方法解決網路使用者身份識別。

學術或技術上之貢獻：（包括民間工業應用之可能性、發表論文、申請專利）

註：本表格如不敷使用，請另紙繕附。

九十年度國防科技學術合作研究計畫

中華民國海軍認證中心雛形系統之建置

(A Certificate Authority Prototyping System for R.O.C Navy)

期末報告

計畫主持人：交大資管所　劉敦仁副教授

計畫協同主持人：交大資管所　羅濟群教授

研　究　生：謝文川

林國良

張永志

執行日期：90/01/01 至 90/12/31

目錄

圖目錄

中文摘要

本計畫擬探討軍事組織建構內部網路技術面時所面臨網路安全的相關課題，包括資料傳輸所使用的機制與協定、資料加密與身份驗證方式、金鑰管理協定、公開金鑰基礎建設、認證中心協定以及與上層的資訊作業流程應用機制的配合等，相關的技術問題也將進行深入的討論。將卓參目前所使用的資訊安全技術，歸納出一套適合海軍內部作業所需的憑證管理中心架構。

探討實作憑證管理中心(CA)時的相關問題與解決方案，並建立一適合海軍內部網路安全管理之憑證管理中心雛形系統，從而加強海軍內部網路使用者身份認証以提供不可否認性、資料隱密性、資料真確性的安全功能。

關鍵詞：企業內網際網路(Intranet)，身份識別(Authentication)，認證中心(Certificate Authority , CA)，公開金鑰基礎建設(Public Key Infrastructure, PKI)，數位憑証(Digital Certificate)

一、緒論

1.1 研究動機

為了增加海軍在未來戰爭急速因應快速獲得相關資訊情報的能力，透過網路快速地交換各項情蒐資訊已是不可抵擋的趨勢，而在使用海軍內部網路傳送資訊的同時，資訊安全將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的方式來達成安全的目的，然而這種方式具有易遭人入侵及無法確實得知使用者身份等缺點，對於任務具有高度機密性性質的軍事單位，實是一大弱點。

在目前網路電腦系統中，主要的安全問題來自於使用者身份驗證的問題，換言之，只要身份驗證問題能解決，網路安全問題也將可迎刃而解。但由於透過網路，不像人和人之間可以面對面地相互驗證身份，所以必須依賴使用者與電腦之間共享的一些訊息，來驗證一個使用者的身份，由 CCITT 在 1993 年所提出的 X.509 協定為目前網路最有效的安全解決方式，如研考會所推動的電子化政府公開金鑰基礎建設，亦採用 X.509 憑證管理方法解決網路使用者身份識別。

因此，如何及早建置符合 X.509 的安全管理系統，將是海軍目前刻不容緩的課題之一。一旦憑證系統開發完成後，將可提供網路上完整身份驗證機制，對海軍內部網路安全的防護工作將有莫大的幫助。

1.2 計畫目標

計畫的目標是協助海軍總部，根據針對海軍的需求，建置 ITU-T X.509 相關安全標準，符合適用於海軍內部網路之認證中心雛形系統。這個以公開金鑰基礎建設為基礎的認證中心系統可提供不可否認性、資料隱密性、資料真確性等各項安全功能，加強海軍內部網路使用者身份驗證之功能，從而確保海軍內部網路安全。另外，並訂定認證中心的安全管理政策，數位憑證的核發管理流程與相關規範等安全管理政策的擬定，？。

1.3 章節簡介

本篇報告我們將於第二章介紹整個公開金鑰基礎建設的安全系統架構，以電子化政府公開金鑰基礎建設（Public Key Infrastructure ，PKI）的整體架構為例，說明目前的憑證管理中心應提供的各項憑證運作服務，包含憑證管理服務、目錄查詢服務、註冊管理服務。其中使用者如何進行透過憑證管理中心進行各項身份驗證、資料傳輸、以及憑證申請等流程。並且說明現行公開金鑰基礎建設系統架構下在各項憑證管理中心所提供的運作服務，如何提供使用者網路的安全保障。

第三章簡介海軍總部公開金鑰基礎建設整體架構

- 憑證管理〈Certificate Management〉
- 憑證簽發〈Certificate Generation〉
- 憑證註銷〈Certificate Revocation〉
- 憑證註銷清單〈CRL〉的產生與維護
- 金鑰管理〈key Management〉
- 金鑰產生〈Key Generation〉

在第四章中本報告擬依照政府憑證管理中心的建置營運模式，設計出適合一套適

用於海軍憑證管理中心的組織人員配置與各項管理辦法。

在第五章中，介紹海軍憑證申請、展期、廢止的範本(Scenario)。

在第六章中將對目前成果以及未來努力的方向做一綜合的敘述。

二、公開金鑰基礎建設安全系統架構

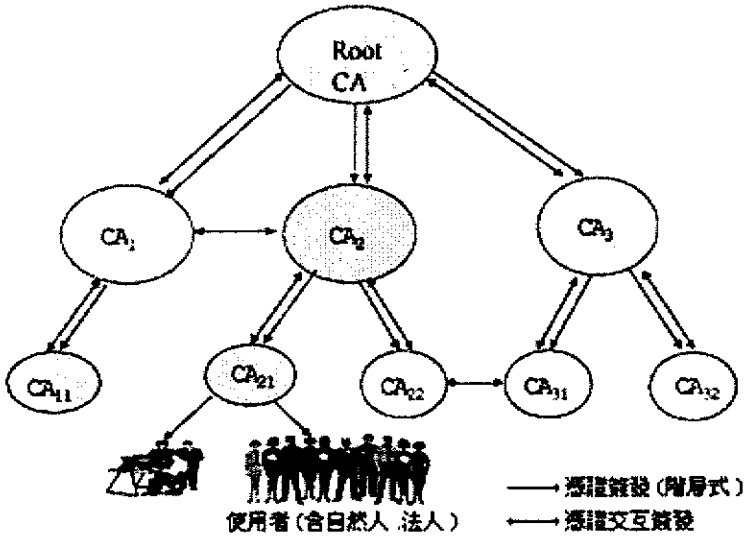
2.1 簡介

公開金鑰基礎建設全名 Public Key Infrastructure（簡稱 PKI），係運用公開金鑰及公開金鑰憑證以確保網路交易的安全性及確認交易對方身分之機制。公開金鑰基礎建設藉由憑證管理中心做為網路交易中的公正第三人，驗證交易雙方電子憑證之有效性及真實性，進而克服網路交易匿名性所造成之不信任感，交易雙方相互地信任其憑證管理中心，搭配金鑰對之產製及數位簽章等功能，即可經由其憑證管理中心核發之電子憑證確認彼此的身分，提供資料完整性、資料來源辨識、資料隱密性、不可否認性等四種重要的安全保障[16]。

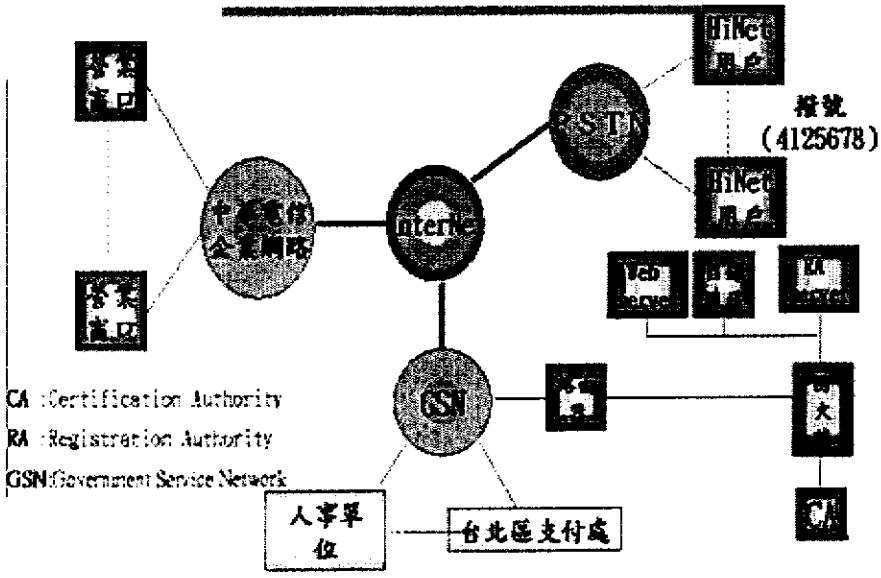
目前全球各主要先進國家如：美、英、法、澳洲及日本等國均已致力於公開金鑰基礎建設。公開金鑰基礎建設主要依照 X.509 的相關標準所規劃，X.509 全名為開放系統相互連接下的「目錄：身份識別」架構，原本為 X.500 的標準之一，主要目的是為了達成開放網路上的使用者相互鑑別問題，其中的識別方法是以公開金鑰密碼系統為基礎。為聯繫使用者和他的公開金鑰間的關係，需要由一公正單位，稱為憑證管理中心（Certificate Authority, CA），以公正客觀地位，查驗憑證申請人身分資料正確性及其與待驗證公開金鑰間之關連性，並據為使用者發出一個證明文件，稱為公開金鑰憑證（public key certificate）。公開金鑰憑證相當於為證書的收受人提供一個聲明，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，目錄服務主要優點為使用者的公開金鑰證書可以存放於目錄中，提供網路的使用者自由存取。

上述公開金鑰憑證(簡稱憑證)，係指經過憑證管理中心認證後之可資證明的公開金鑰。憑證內容包括：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。憑證管理中心經必要流程，驗證申請者之身分與其公開金鑰後，發給此憑證作為其公開金鑰之有效證明依據。憑證管理中心驗證客戶之身分與其公開金鑰後，發給憑證作為其公開金鑰的有效證明依據。憑證內容

包含金鑰擁有人之基本資料及公開金鑰，並以憑證管理中心之數位簽章保護、防止偽造及竄改。



電子化政府公開金鑰基礎建設架構示意圖（資料來源：http:www.pki.gov.tw）



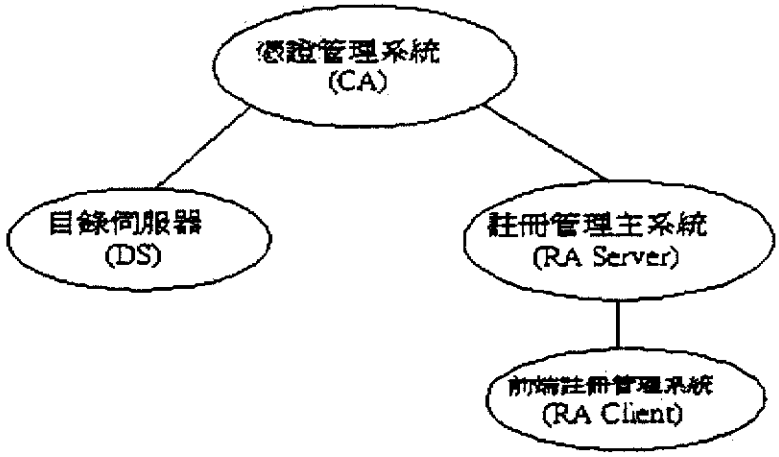
GCA 系統架構圖

為使公開金鑰基礎建設能順利運作，需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(Certificate Management System)、目錄檢索服務〈Directory Service〉、公證服務〈Notarize Service〉、不可否認服務 〈Non-repudiation Service〉、時戳服務 〈Digital Time-stamping Service〉、票證產生服務 〈Ticket Granting Service〉、數位掛號信遞送服務 〈Digital Certified Delivery Service〉、金鑰保管回復中心〈Trusted Key Recovery Center, TKRC〉和加解密的應用程式介面〈CAPI〉等。而公開金鑰基礎建設即為結合上述所有服務與系統，共同運作，在所有系統中，以憑證管理中心系統為公開金鑰基礎建設中最重要的部分。

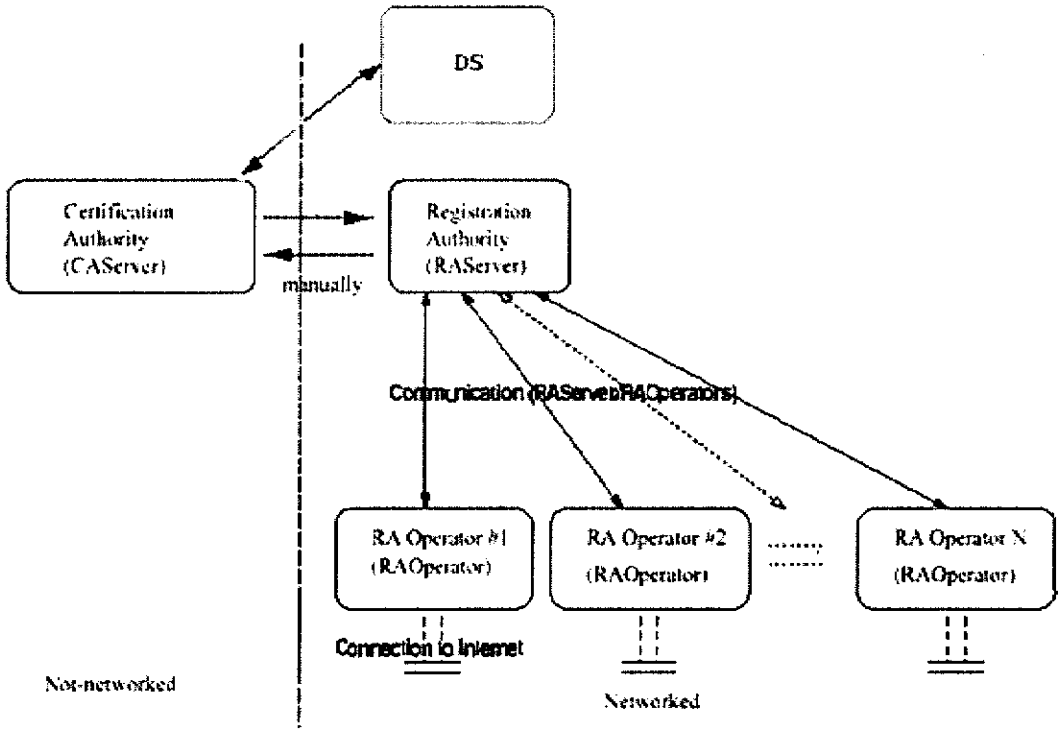
2.2 憑證管理服務

為了使公開金鑰密碼系統得以順利運作，必要設法緊密結合並証明某一把金鑰確實為某人所擁有，讓他人無法假冒、偽造。解決方法是由可信賴的第三者或機構，來當作公鑰簽証中，以簽發公開金鑰憑証的方式來証明公鑰的效力。憑證管理中心便是做為可信賴的第三者(Trusted Third Party, TTP)，負責簽發公鑰電子憑證(Public Key Certificate)，以証明公鑰的效力。

憑證管理中心所提供的服務，稱為憑證管理服務，這些服務係由各個憑證管理系統所組成，茲就公開金鑰基礎建設架構中最重要的部分--憑證管理中心下各個管理系統：憑證管理系統、目錄服務系統、註冊管理系統三個資訊系統作一介紹：



憑證管理資訊系統架構圖（資料來源：http://www.pki.gov.tw/cps/index.htm）



圖一 、憑證管理資訊系統網路架構圖（資料來源：？）

2.2.1 憑證管理(Certificate Management)

憑證管理系統 〈Certificate Management System, CMS〉 加以說明。憑證管理系統負責憑證簽發(Certificate Issuance)、憑證廢止(Certificate Revocation)、憑證註銷清單(CRL)的產生與維護、金鑰管理(key Management)、金鑰產生(Key Generation)、金鑰備份與回復(Key Backup and Recovery)、金鑰托管(Key Escrow)、金鑰更新(Key Update)、憑證管理等核心工作，並將所簽發之憑證及憑證廢止清冊公佈於目錄伺服器以備外界查詢或下載。

2.2.2 目錄服務系統

目錄伺服器之主要提供功能係除提供外界目錄查詢服務，如憑證及憑證廢止清冊之公佈，並提供憑證廢止訊息、新版、舊版憑證實作準則之查詢及憑證相關

軟體下載等服務。所採用的標準是 ITU-T X.509 所提的「目錄認證架構」(Directory Authentication Framework)，透過目錄建構的方式，可用來管理、散佈並認可各主體的「公開金匙」(public key)，讓各主體毋需貯存各往來夥伴的金匙，以簡化管理過程。目錄服務最早在 X.500 標準中提出，主要為配合憑證機構 (Certification Authority, CA) 運作的網路服務，提供一類似電話簿的功能，可存放關於單位機構、部門或個人等的資料，例如：地址、電話、生日、電子郵件地址、職稱、自我介紹、照片、憑證…等資料。LDAP 是 Lightweight Data Access Protocol 的縮寫。LDAP 是一個低成本用來存取 X.500 目錄之用，但 X.500 標準中的目錄存取協定 (Directory Access Protocol，簡稱 DAP) 效率不佳，不符合實際用途。因此，密西根大學 (University of Michigan) 另外發展較有效率的 LDAP，LDAP 協定架構在主從式環境上，客戶端透過 TCP/IP 網路連接到 LADP 目錄伺服器，進而存取需要的資訊與服務。以便在 client-server 的環境中存取與修改目錄資料。目前在網際網路上已有的目錄伺服器主要依照 LDAP 的規格實作完成，所以 LDAP 已成為 IP 網路上各類型目錄服務應用所選擇的主要解決方案。在公開金鑰基礎建設，目錄服務中心負責提供外界目錄檢索查詢服務，包括憑證與憑證廢止清冊之公佈。

2.2.3 註冊管理中心(Registration Authority, RA)

註冊管理系統負責受理憑證申請、廢止與相關資料審核，並將審核通過之資料傳送至憑證管理系統，進行憑證簽發、廢止等作業。本註冊管理系統在實體架構上分為前端註冊管理系統(RA Client)及註冊管理主系統(RA Server)兩部份。前端註冊管理單位負責現場或網路線上受理申請人之申請、書面資料審核及身分認定等作業，註冊管理主系統之主管單位負責與憑證管理系統連線並進行憑證簽發、廢止等作業。前端註冊管理單位須能驗證憑證申請者本人及其書面證明資料之正確性，或具備公正的用戶資料庫得以驗證憑證申請者本人身分之正確信[4]。

2.3 憑證中心管理服務流程

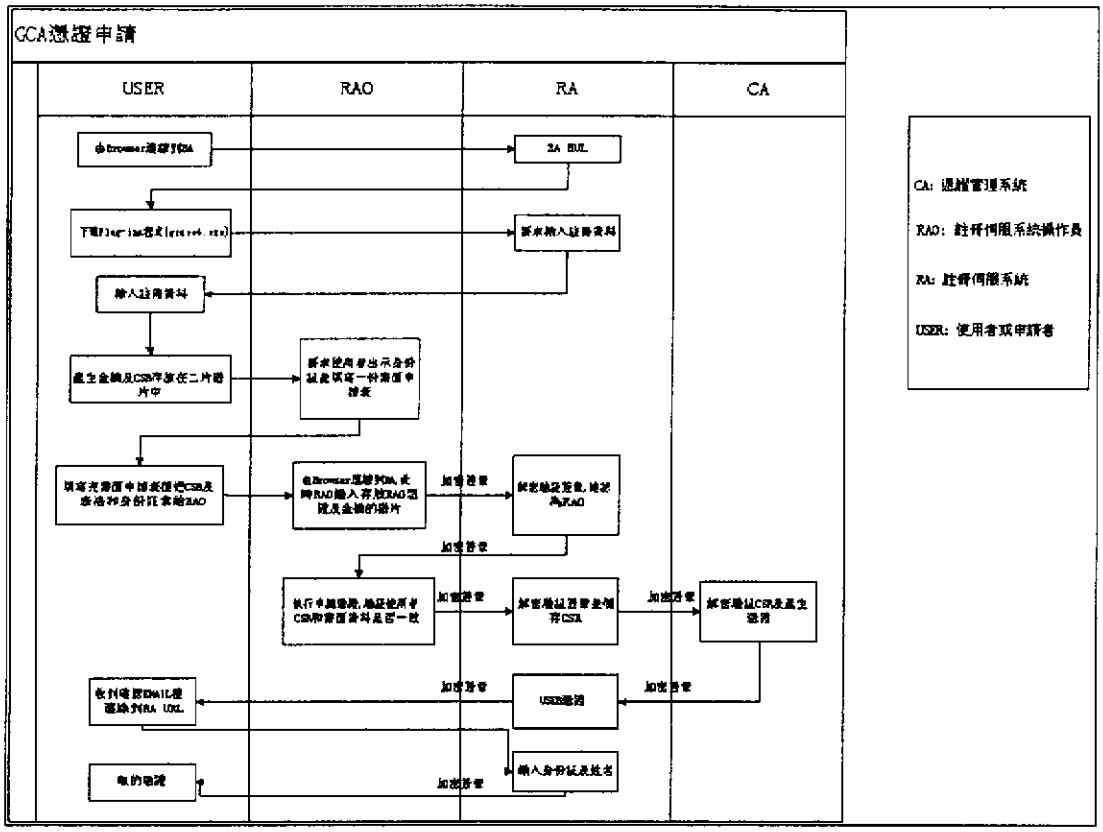
本節簡介政府憑證管理中心、環保署憑證管理中心、網際威信三家憑證管理

中心憑證申請、廢止、展期三個流程與流程說明。

2.3.1 政府憑證管理中心

2.3.1.1 憑證申請

GCA 憑証申請流程圖



流程說明

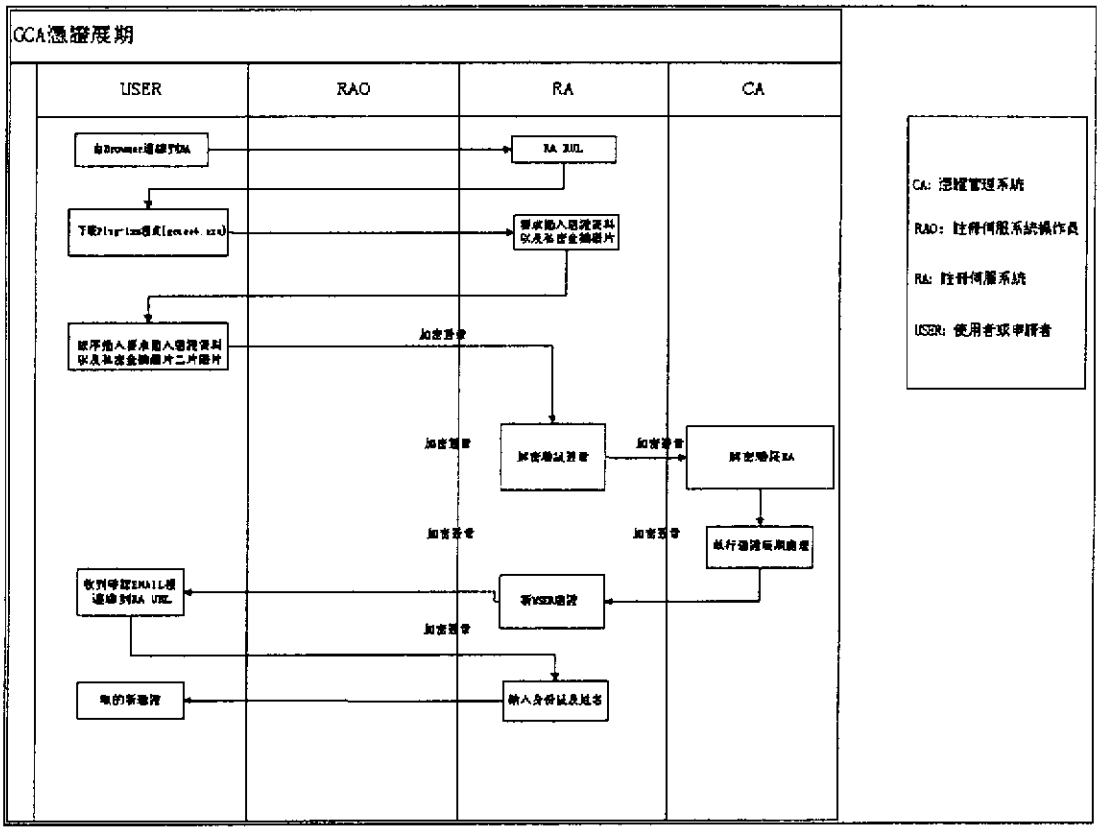
1. 使用者(User)先到RA URL (http://www.pki.gov.tw/apply/flow_chart_ee3.htm)。
2. 使用者(User)下載並安裝Plug-ins程式(產生金鑰及CSR程式，gcaee4.exe)到使用者之電腦上。
3. RA URL要求使用者填入個人資料。
4. 使用者(User)填入個人資料申請表。
5. 在使用者(User)端產生金鑰及憑證申請資料(CSR)共二張磁片。
6. RAO要求使用者出示身份証並填寫一份書面申請書。
7. 使用者(User)寫好書面資料並拿出CSR磁片向註冊伺服系統操作員(RAO)申

請註冊。

8. 由Browser連線到RA, 此時RAO插入存放RAO憑證及金鑰的磁片。
9. RA解密驗証簽章, 確認為RAO。
10. RAO確認為使用者(User)本人後，登錄到RA URL並輸入使用者身份字號以及名字，驗証使用者所填資料與書面資料註冊資料是否一致。最後將使用者憑證申請資料(CSR)磁片，簽章加密送到RA。
11. RA 解密驗證CSR 無誤後，將CSR送到CA。
12. 經過一個工作天，經CA 產生使用者憑證並傳送給RA
13. 由RA發出Email給使用者，並附上使用者憑證。
14. 使用者接收到憑證後，再將憑證儲存到磁片。

2.3.1.2 憑證展期

GCA 憑證展期流程圖



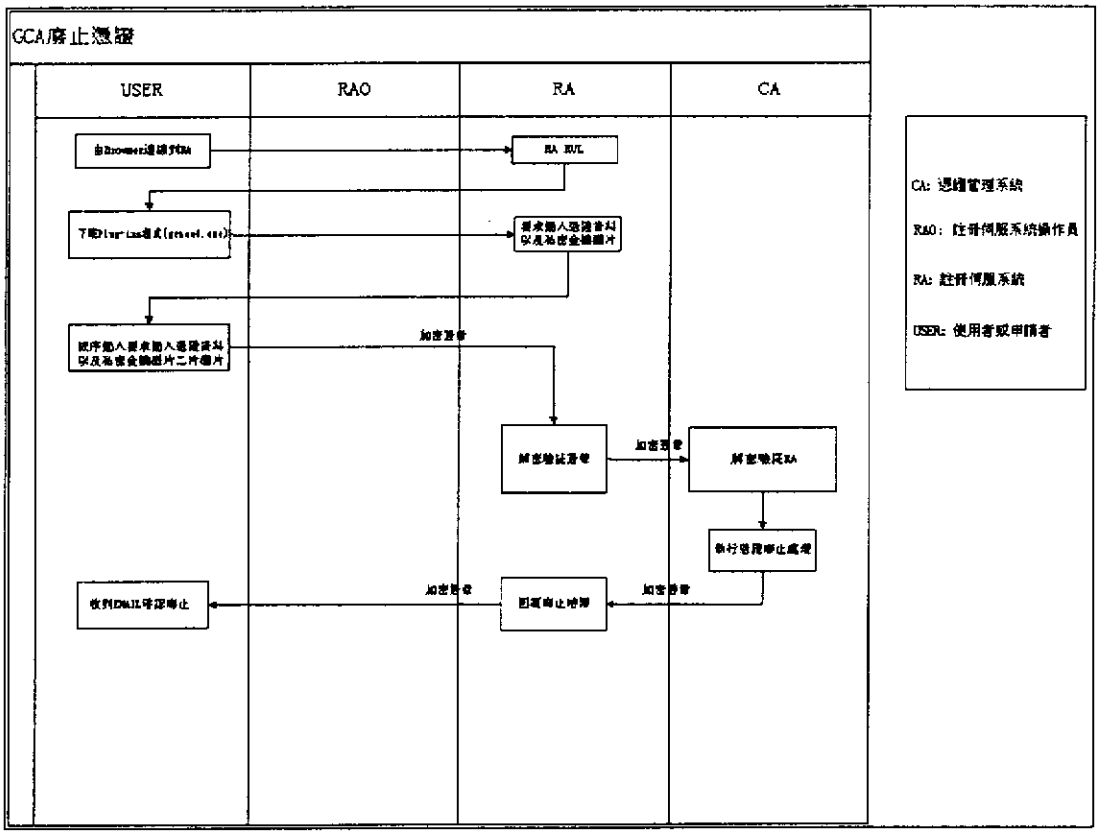
流程說明

1. 使用者(User)先到RA URL。

2. 使用者(User)下載並安裝Plug-ins程式(產生金鑰及CSR程式，gcaee4.exe)到使用者之電腦上。
3. RA要求插入憑證資料以及私密金鑰磁片。
4. 使用者依序先插入憑證資料磁片、私密金鑰磁片系統會在此刻作解密及憑證之基本檢查，若檢查無誤就把資料傳送到RA。
5. RA系統會在此刻作解密及憑證之基本檢查，若檢查無誤，再將憑証送到CA經過一個工作天，經CA 產生使用者新憑證並傳送給RA
6. RA用email通知user。
7. 使用者接收到新憑證後，再將憑證儲存到磁片中並自行匯入。

2.3.1.3 憑證廢止

GCA 憑證廢止流程圖



流程說明

1. 使用者(User)先到RA URL。
2. 下載並安裝Plug-ins程式(產生金鑰及CSR程式，gcaee4.exe)到使用者之電腦

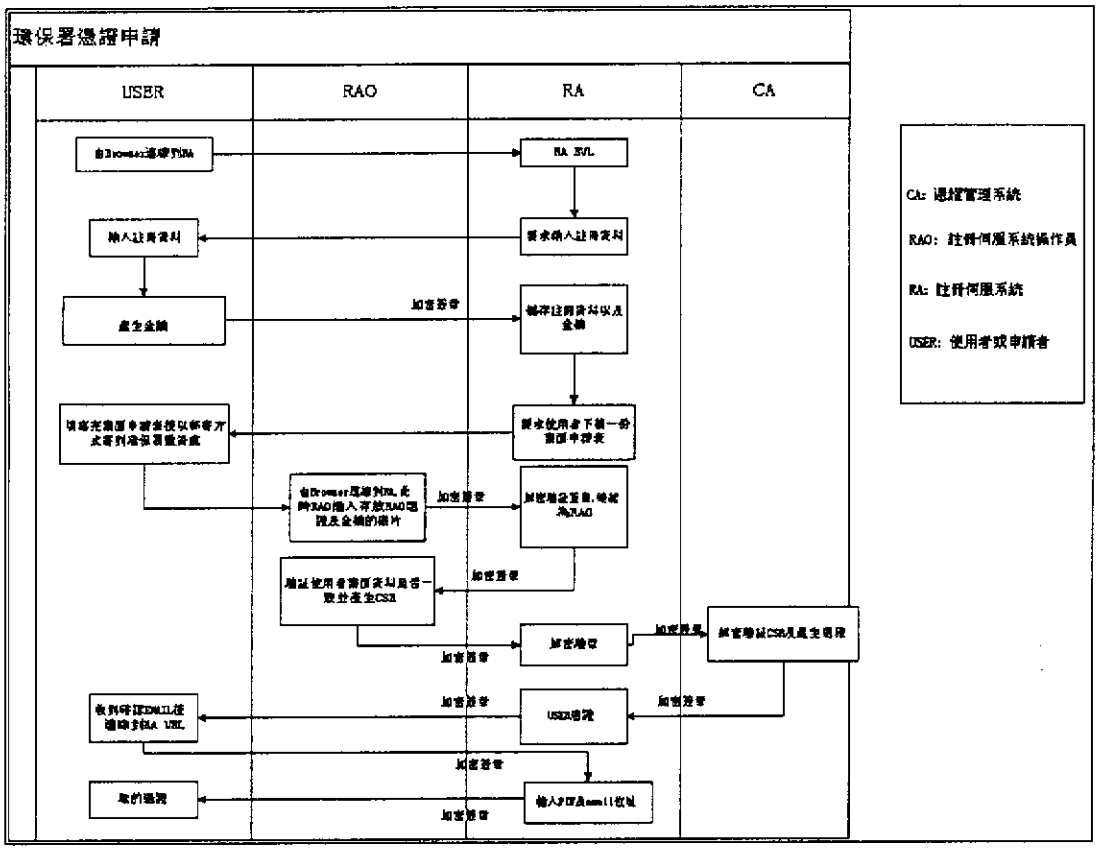
上。

3. RA要求插入憑證資料以及私密金鑰磁片。
4. 使用者依序先插入憑證資料磁片、私密金鑰磁片系統會在此刻作解密及憑證之基本檢查，若檢查無誤就把資料傳送到RA。
5. RA系統會在此刻作解密及憑證之基本檢查，若檢查無誤，再將憑証送到CA
6. CA將讓使用者憑證廢止並將憑證廢止清冊公佈於目錄伺服器。

2.3.2 環保署憑證管理中心

2.3.2.1 憑證申請

環保署憑證申請流程圖

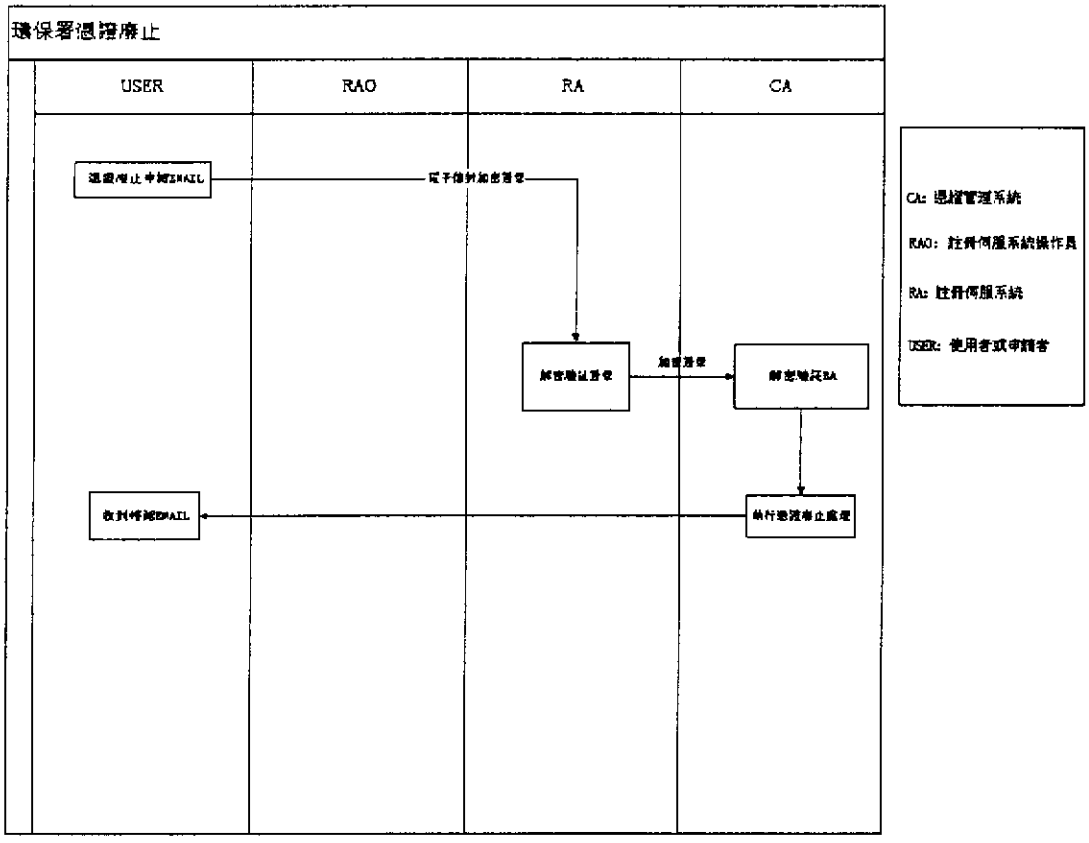


1. 使用者(User)登錄到RA URL。
2. 使用者(User)填入個人資料申請表，並產生金鑰。
3. 網站將剛剛所產生的金鑰以及使用者憑證申請資料(CSR)送到憑證中心。
4. 使用者(User) 下載並填寫用戶契約書

5. 用印並郵寄身分證件影印本及用戶契約書至環保署註冊伺服系統操作員(RAO)申請註冊。
6. RA 操作員登錄到RA URL並輸入使用者身份字號以及名字，驗証使用者所填資料與書面資料註冊資料是否一致。最後將使用者憑證申請資料(CSR)磁片，簽章加密送到RA。
7. RA 解密驗證CSR 無誤後，將CSR送到CA。
8. 經過幾個工作天，經CA 產生使用者憑證並傳送給RA
9. 由RA發出Email給使用者，附上取回憑證的PIN碼。
10. 使用者登錄到網站取回憑證後，再將憑證儲存到磁片中並自行匯入。

2.3.2.2 憑證廢止

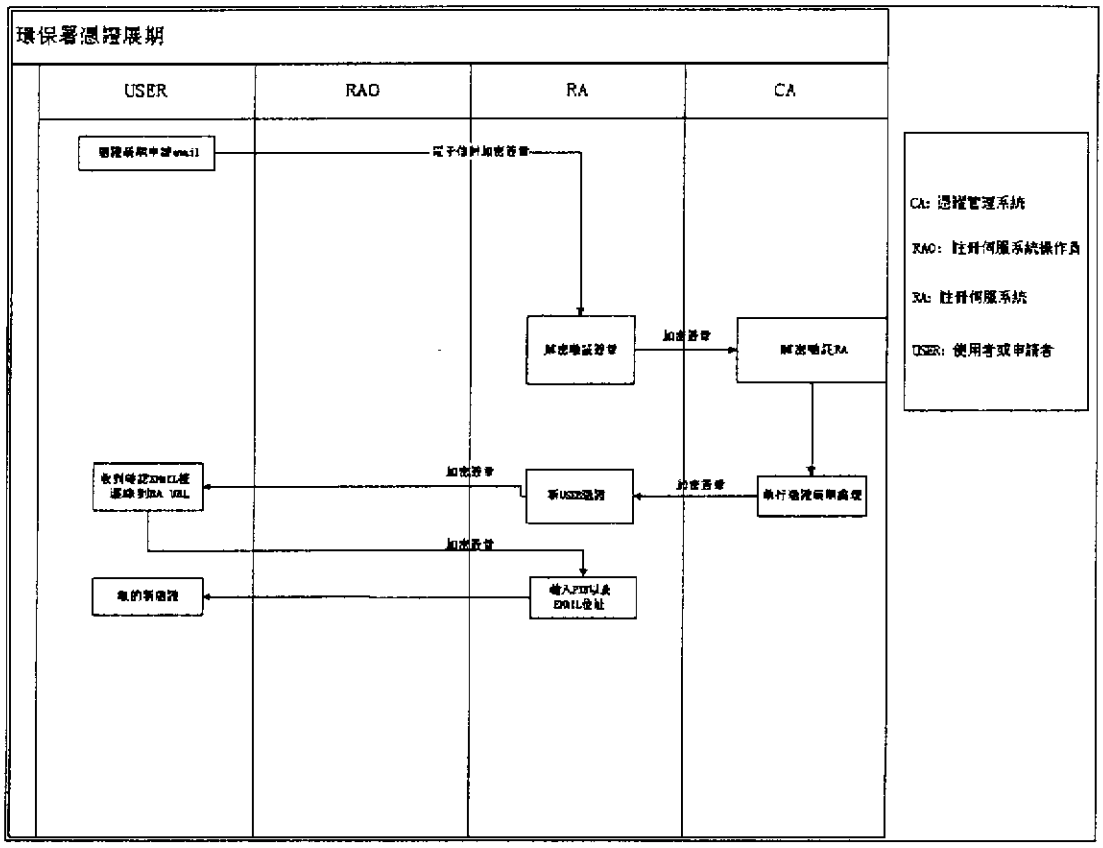
環保署憑證廢止流程圖



憑證有效期間為二年，期滿後用戶欲繼續使用者，以經環保署憑證簽章加密之電子郵件向環保署申請憑證重發。重發有效期間為二年。

2.3.2.3 憑證展期

環保署憑證展期流程圖

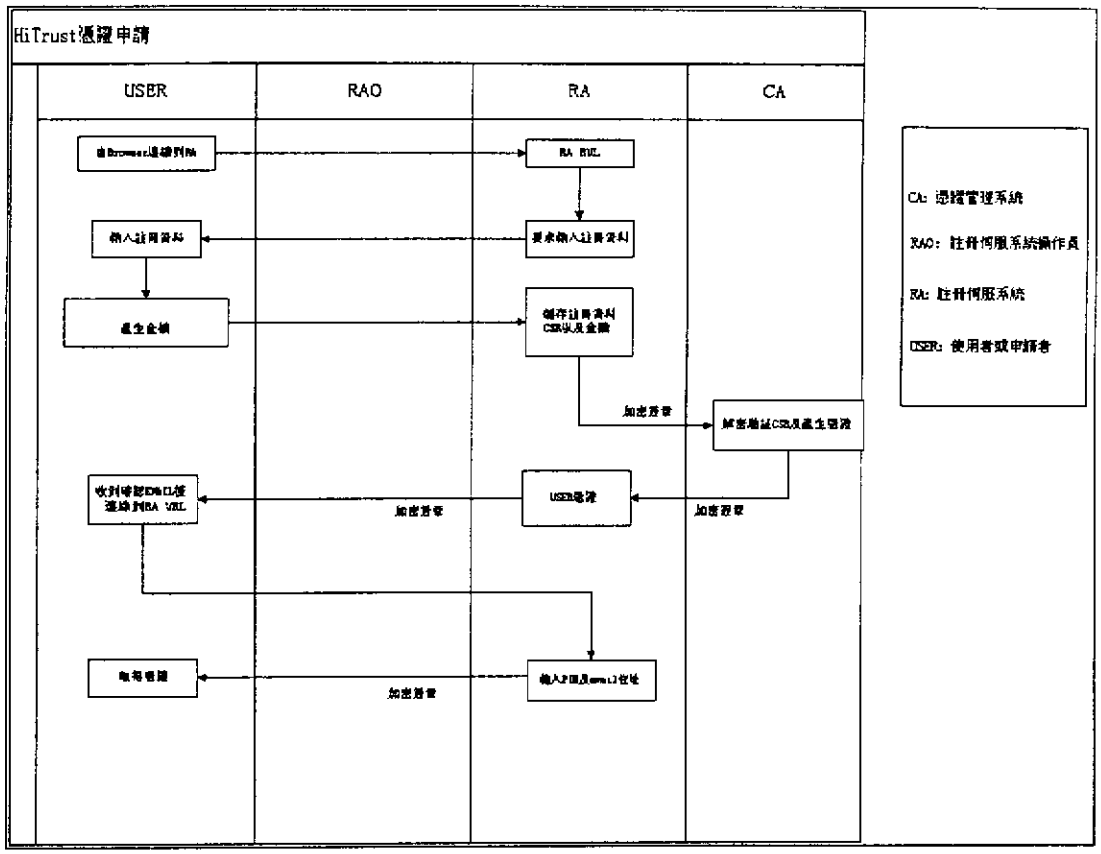


主動向環保署以電話、電子郵件、傳真、信函或本人攜帶書面證明資料親洽環保署辦理憑證凍結，經本署確認屬實得停止核發或終止該憑證

2.3.3 網際威信憑證管理中心

2.3.3.1 憑證申請

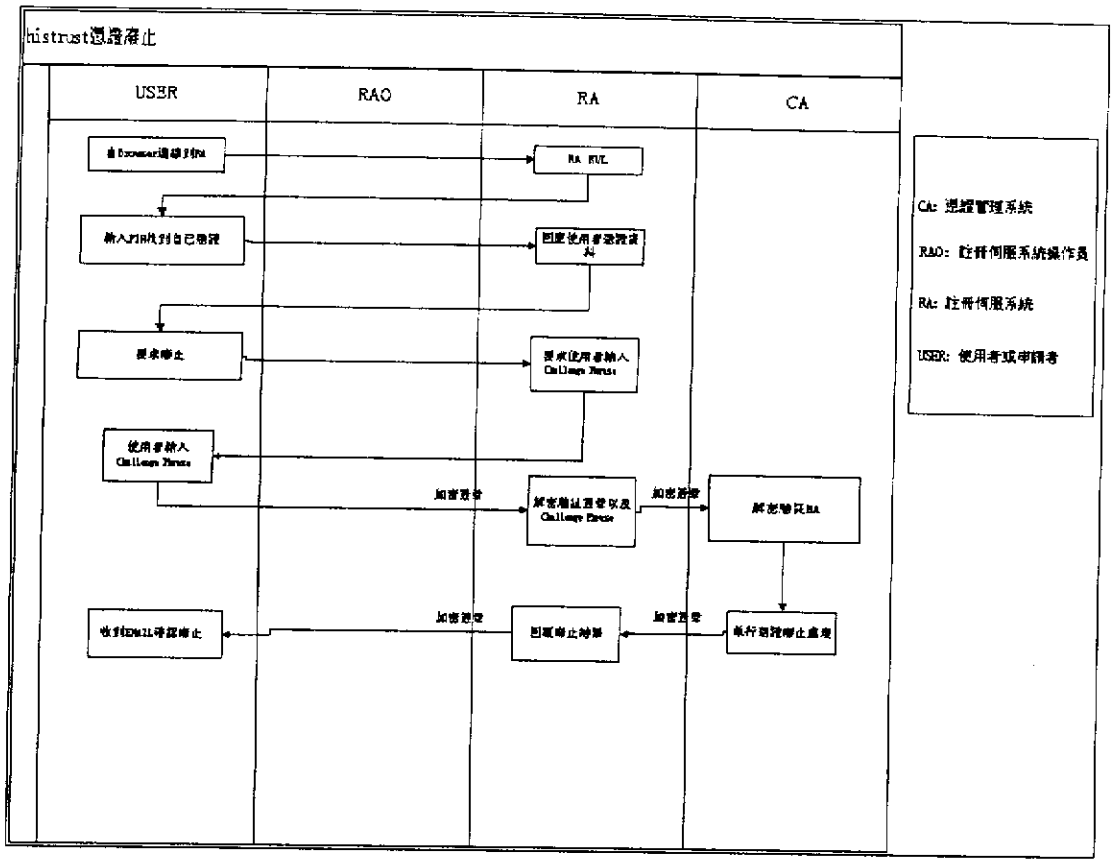
網際威信憑證申請流程圖



1. 使用者(User)登錄到RA URL。
2. RA URL要求使用者填入個人資料。
3. 使用者(User)填入個人資料申請表
4. 使用者(User)產生金鑰，網頁就會將剛剛所產生的金鑰以及使用者憑證申請資料(CSR)送到憑證中心。
5. RA 解密驗證CSR 無誤後，將CSR送到CA。
6. 經CA 產生使用者憑證並傳送給RA
7. 由RA發出Email給使用者，附上取回憑證的PIN碼。
8. 使用者登錄到網站取回憑證後，再將憑證儲存到磁片中並自行匯入。

2.3.3.2 憑證廢止

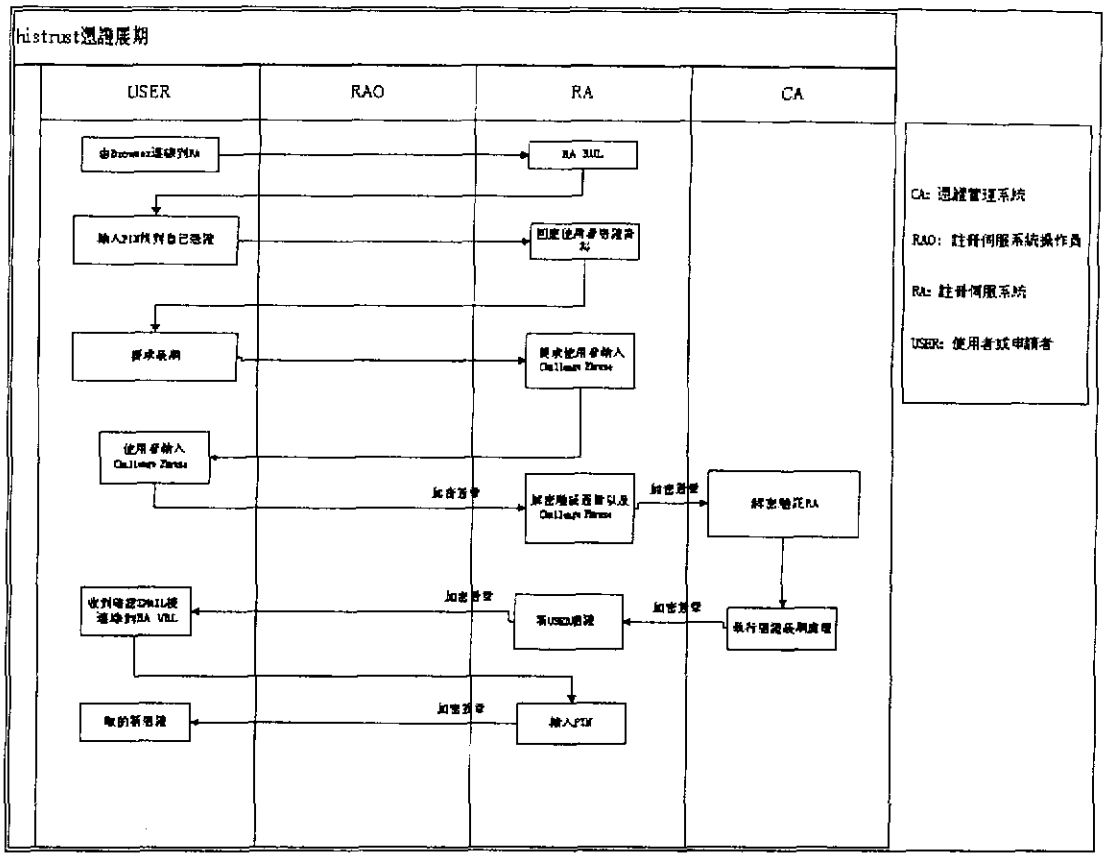
網際威信憑證廢止流程圖



1. 使用者(User)登錄到網站。
2. 輸入PIN or email找到自己的使用者憑證。
3. 網站要求使用者輸入 Challenge Phrase ，使用者必須輸入之前在申請時所填的Challenge Phrase。
4. 網站驗証使用者所填的Challenge phrase是對的後，便對立刻廢止使用的憑證。
5. 由 RA 發出 Email 給使用者，確認已廢止。

2.3.3.3 憑證展期

網際威信憑證展期流程圖



1. 使用者(User)登錄到網站，
2. 輸入PIN or email找到自己的使用者憑證。
3. 網站要求使用者輸入 Challenge Phrase ，使用者必須輸入之前在申請時所填的Challenge Phrase。
4. 網站驗証使用者所填的Challenge phrase是對的後，便對立刻廢止使用的憑證，並產生一個新的憑証。
5. 由RA發出Email給使用者，附上取回憑證的PIN碼。

使用者登錄到網站取回憑證後，再將憑證儲存到磁片中並自行匯入。

2.4 憑證管理中心採用的標準與格式

2.4.1 採用標準

政府的憑證管理中心（GCA）之憑證管理資訊系統採用標準如下表所示：

表一 憑證管理資訊系統採用標準

	憑證管理資訊系統元件	採用標準
(1)	命名方式 〈Naming〉	採 X.509 命名方式。其他標準包括電子郵件 E-mail (RFC 822)、網域名稱服務 Domain Name Service Name (RFC 1035)、O/R Address (X.400, 1988)、目錄名稱 Directory Name (X.501,1993)、電子文件交換 EDI part Name、URL (RFC 1630)、網際網路位址 IP address (RFC 791) 及註冊識別碼 Registered ID (X.660) 等。
(2)	加密演算法	採 Triple DES CBC 112 bits 演算法。
(3)	數位簽章演算法	採 RSA 演算法，其金鑰長度為 1024 bits，並配合雜湊函數 SHA-1 作訊息摘要。
(4)	金鑰的交換	利用 RSA 演算法長度為 1024 bits 之金鑰作金鑰交換。
(5)	憑證的公佈 〈Certificate Distribution〉	採用 X.500 (1993) 標準。
(6)	憑證的格式 〈Certificate Format〉	採用 X.509 (V3，1993) 標準。
(7)	廢止清冊 〈CRL〉	採用 X.509 (V2，1993) 標準。
(8)	憑證編碼的方式	a. ASN.1 (Abstract Syntax Notation One)：描述資料欄位的形態與數值 (定義在 CCITT X.208, 1988) b. BER (Basic Encoding Rule)：描述資料

	憑證管理資訊系統元件	採用標準
		標碼規則（定義在 CCITT X.209, 1988） c. DER（Distinguish Encoding Rule）：對 ASN.1 提供唯一編碼方式，DER 是 BER 的 Subset（定義在 ITU-T X.690, 1994）
（9）	個人密鑰	採用 PKCS#5 （Public Key Cryptographic Standard #5）公開金鑰密碼標準格式加密格式。
（10）	通信協定	● LDAP（RFC 1777）[25-27] ● TCP/IP ● HTTP

2.4.2 公開金鑰憑證內容

政府憑證管理中心所使用之公開金鑰憑證內容如下表所示：

表二 公開金鑰憑證內容

	公開金鑰憑證欄位	內容
（1）	版本	該憑證製作所依據的 X.509 版序（V3）
（2）	序號	由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	該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

	公開金鑰憑證欄位	內容
(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 (V3)	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	憑證管理中心對以上資料作數位簽章

政府憑證管理中心所使用之公鑰憑證擴充欄位〈Certificate Extensions〉項目如下表所示：

表三 公鑰憑證擴充欄位

	公鑰憑證擴充欄位〈Certificate Extensions〉
(1)	金鑰識別符 (Key Identifier)
(2)	金鑰的用途〈Key Usage〉
(3)	憑證簽發原則與政策 (Certificate Policies)
(4)	替代名稱 (Alternative Name)
(5)	基本限制 (Basic Constraints)
(6)	儲存預備使用之下一把 CA 公鑰的雜湊值

2.4.3 憑證廢止清冊格式

憑證廢止清冊是當某些金鑰已經有安全顧慮時，用來通知各相關單位，以避免使用該有疑慮的金鑰。政府憑證管理中心所使用之憑證廢止清冊內容如下表所示：

表四 憑證廢止清冊內容

	憑證廢止清冊內容
(1)	版本序號
(2)	簽章演算法
(3)	憑證管理中心名稱
(4)	本次發佈時間
(5)	下次發佈時間
(6)	廢止憑證串列：憑證序號、廢止時間、廢止憑證串列項目之擴充資料〈廢止原因〉
(7)	廢止憑證清冊擴充資料
(8)	簽章方法
(9)	數位簽章：憑證管理中心對以上資料，使用其私密金鑰做數位簽章運算所得的數位簽章

2.5 現有目前憑證管理中心架構的缺失

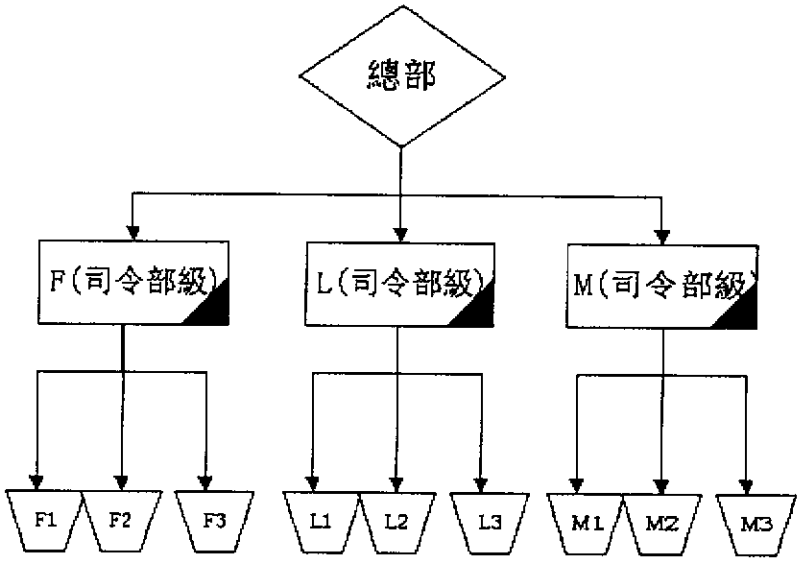
- 私密金鑰的產生由使用者自行產生，無法進行控管。
- 私密金鑰的儲存，以磁碟片作為儲存媒介，易於被使用密碼暴力破解法破解。
- 電子化政府公開金鑰基礎建設需使用者自行產生私密金鑰，需要相當程度的資訊操作能力，才能進行憑證管理。
- 尚未建立目錄伺服器，所核發憑證無法以中文查詢。

三、海軍總部公開金鑰基礎建設整體架構

本報告研究出符合海軍需求的公開金鑰基礎建設之架構。在去年第一階段的計畫中，對海軍目前資訊化網路建置的情形作一認識，並對公開金鑰基礎建設相關系統協定與機制進行廣泛且深入的探討，選擇適合海軍使用的公開金鑰基礎建設的協定與機制，提出一套適用於海軍且以公開金鑰基礎建設為基礎之憑證管理中心架構。

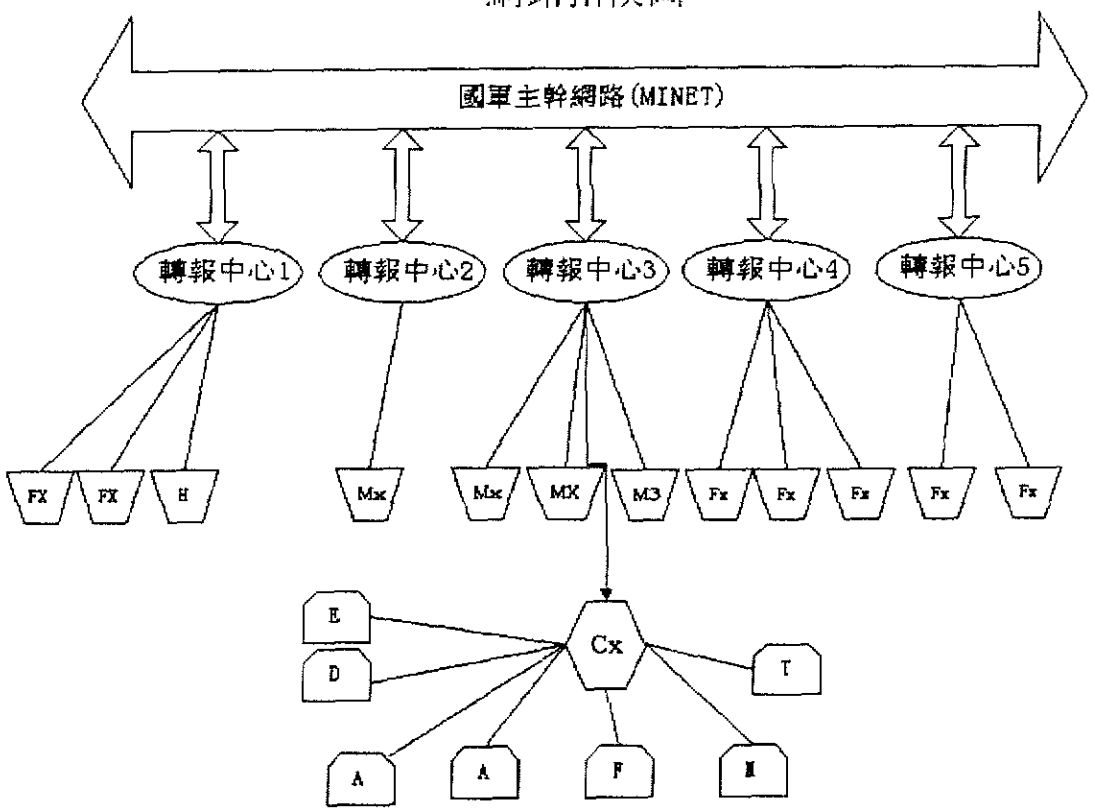
3.1 海軍內部組織架構與網路建置發展現況

海軍內部組織架構



海軍內部組織架構圖

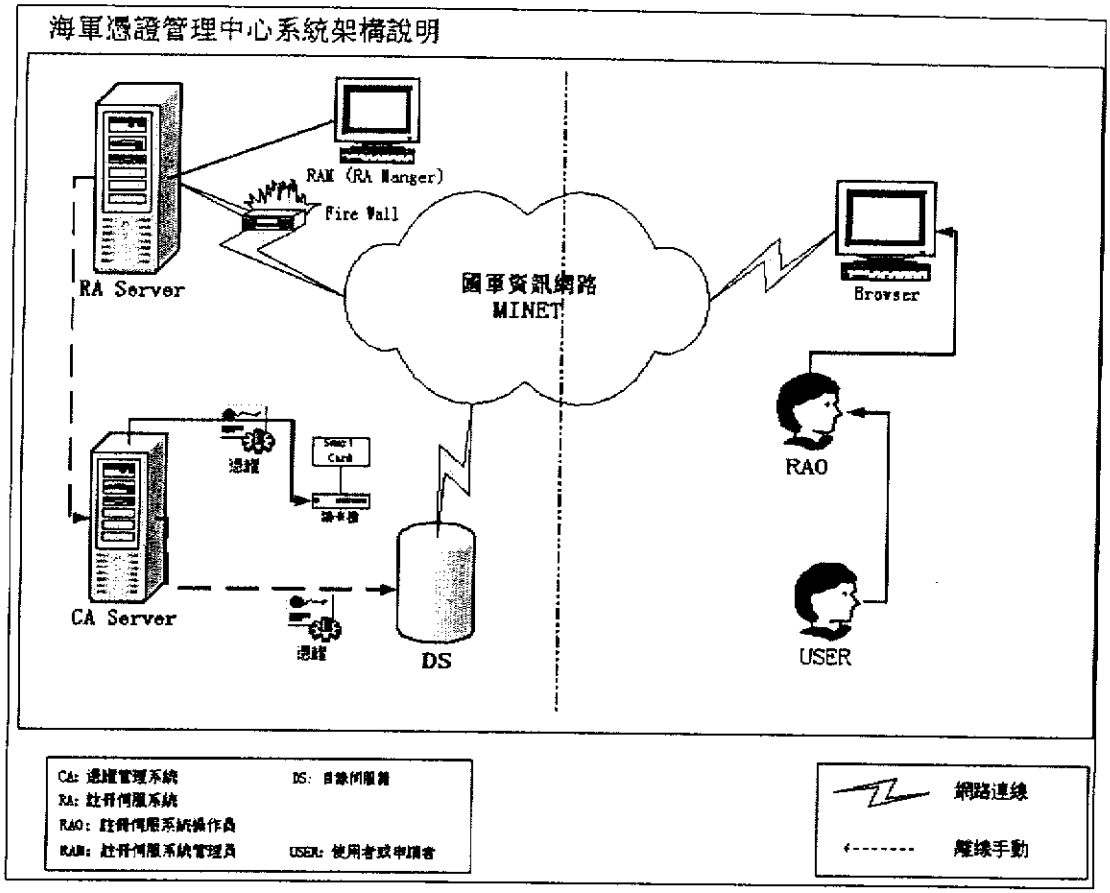
網路拓樸圖



海軍內部網路拓樸圖

本報告以去年第一階段所提出的適用於海軍之認證中心架構為出發點，開發憑證管理中心的資訊系統雛形，並訂定憑證管理中心的安全管理政策，數位憑證的核發管理流程與相關規範等安全管理政策的擬定。

3.2 海軍憑證管理服務



海軍憑證管理中心系統架構圖

3.2.1 憑證管理(Certificate Management)

憑證管理系統的主管單位，也就是指海軍總部，必須負責憑證簽發〈Certificate Issuance〉、憑證廢止〈Certificate Revocation〉、憑證管理等工作，並將所簽發之憑證及憑證廢止清冊〈Certificate Revocation List〉公佈於目錄伺服器以提供給外界查詢或下載。

3.2.2 註冊管理系統（RA, Registration Authority）

註冊管理系統的主管單位，規劃由指海軍總部，必須負責受理憑證申請、廢止與相關資料的審核，並將審核通過之資料傳送至憑證管理中心，進行憑證簽發、廢止等作業。本註冊管理系統在實體架構上可分為前端註冊管理系統(RA

Client）與後端註冊管理主系統（RA Server）兩部份。前端註冊管理單位，也就是指海軍有連上國軍資訊網路（MINET）的組織。負責受理申請人之申請、書面資料審核及身份認定等作業，它必須能驗證憑證申請者本人及其書面證明資料之正確性，或具備公正的用戶資料庫得以驗證憑證申請者本人身份之正確信；而後端註冊管理主系統的主管單位，則為海軍總部，負責與憑證管理系統連線並進行憑證簽發、廢止等作業。

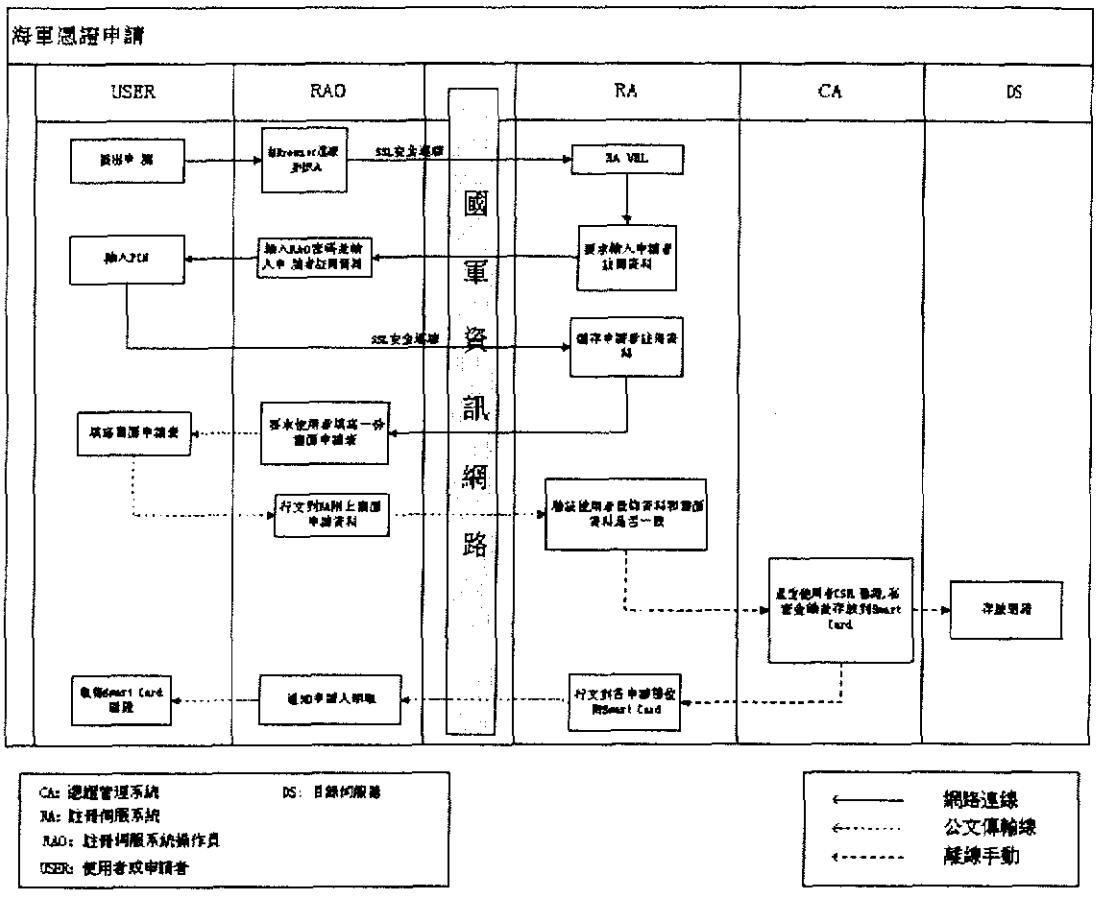
3.2.3 目錄伺服系統（Directory Service）

目錄伺服器的主管單位必須能提供外界目錄查詢的服務，如憑證及憑證廢止清冊之公佈，並提供憑證廢止訊息、新版、舊版憑證實作準則之查詢及憑證相關軟體下載等服務，此目錄服務系統的規劃是預設以海軍組織架構中的司令部級的資訊部門下，設置目錄伺服器，提供相關憑證查詢服務。

3.3 海軍憑證管理中心服務流程

3.3.1 憑證申請

申請者欲申請憑證使用時，攜帶可驗證申請者本人身份的書面證明資料（此書面證明資料可為身份證或其他附有相片之證件），親自前往所屬單位人事官辦理，各單位人事官需驗證用戶之數位簽章或書面證明資料無誤，審核通過後即可將申請者個人基本資料，包括姓名、身份證字號、出生年月日、性別、戶籍地址等。透過線上提出，向本報告所規劃的憑證管理中心進行初始註冊，另行發函（呈）送海軍總部資訊處憑證註冊管理中心辦理，而註冊管理中心收到申請憑證公文，即受理憑證申請作業。



海軍憑證申請流程圖（資料來源：本研究）

流程說明：

1. 使用者(User)到RAO提出申請。
2. RAO連線到RA URL(透過SSL安全連線)。
3. RA URL要求RAO輸入申請者個人資料。
4. RAO輸入RAO密碼並輸入申請者註冊資料。
5. 使用者(User)輸入PIN。
6. 透過SSL安全連儲存申請者註冊資料在RA。
7. RAO要求使用者填寫一份書面申請書。
8. 使用者(User)寫好書面資料交由 (RAO)以行文方式送到RA。
9. RA有RAM來負責驗証使用者登錄資料和書面資料是否一致
10. RA 驗證無誤後，將申請者個人資料以離線方式送到CA。
11. 經過一個工作天，經CA 產生使用者CSR、憑證、私密金鑰並存放到Smart

Card。

12. 由CA以離線方式放上使用者憑證到DS(目錄伺服器)。

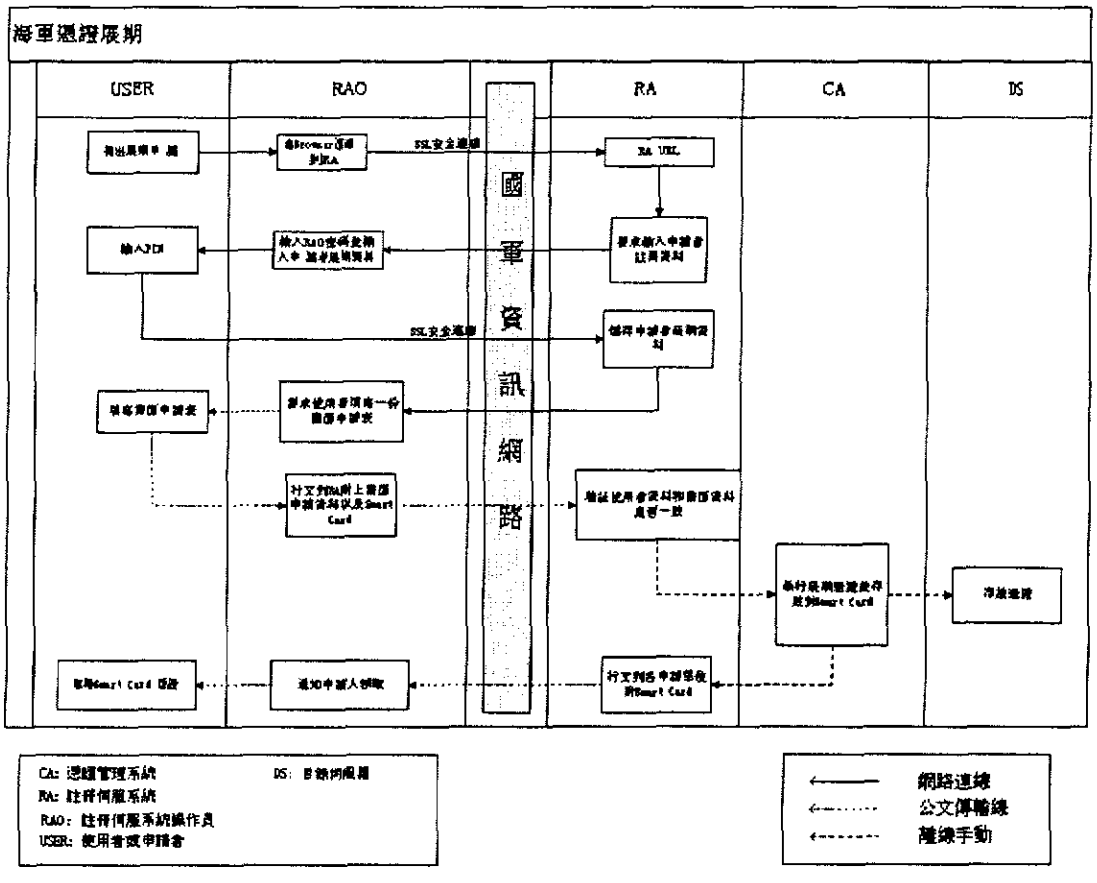
13. 由CA以離線方式將Smart Card 交由RA。

14. RA行文到各申請RAO單位並加上附件Smart Card。

15. RAO通知申請人領取。

16. 取得Smart Card 憑證。

3.3.2 憑證展期



海軍憑證展期流程圖（資料來源：本研究）

流程說明：

1. 使用者(User)到RAO提出展期申請。

2. RAO連線到RA URL(透過SSL安全連線)。

3. RA URL要求RAO輸入申請者個人資料。

4. RAO輸入RAO密碼並輸入申請者註冊資料。

5. 使用者(User)輸入PIN。

6. 透過SSL安全連儲存申請者註冊資料在RA。

7. RAO要求使用者填寫一份書面申請書。

8. 使用者(User)寫好書面資料交由 (RAO)以行文方式送到RA。

9. RA有RAM來負責驗証使用者登錄資料和書面資料是否一致

10. RA 驗證無誤後，將申請者個人資料以離線方式送到CA。

11. 經過一個工作天，經CA 產生使用者CSR、憑證、私密金鑰並存放到Smart Card。

12. 由CA以離線方式放上使用者憑證到DS(目錄伺服器)。

13. 由CA以離線方式將Smart Card 交由RA。

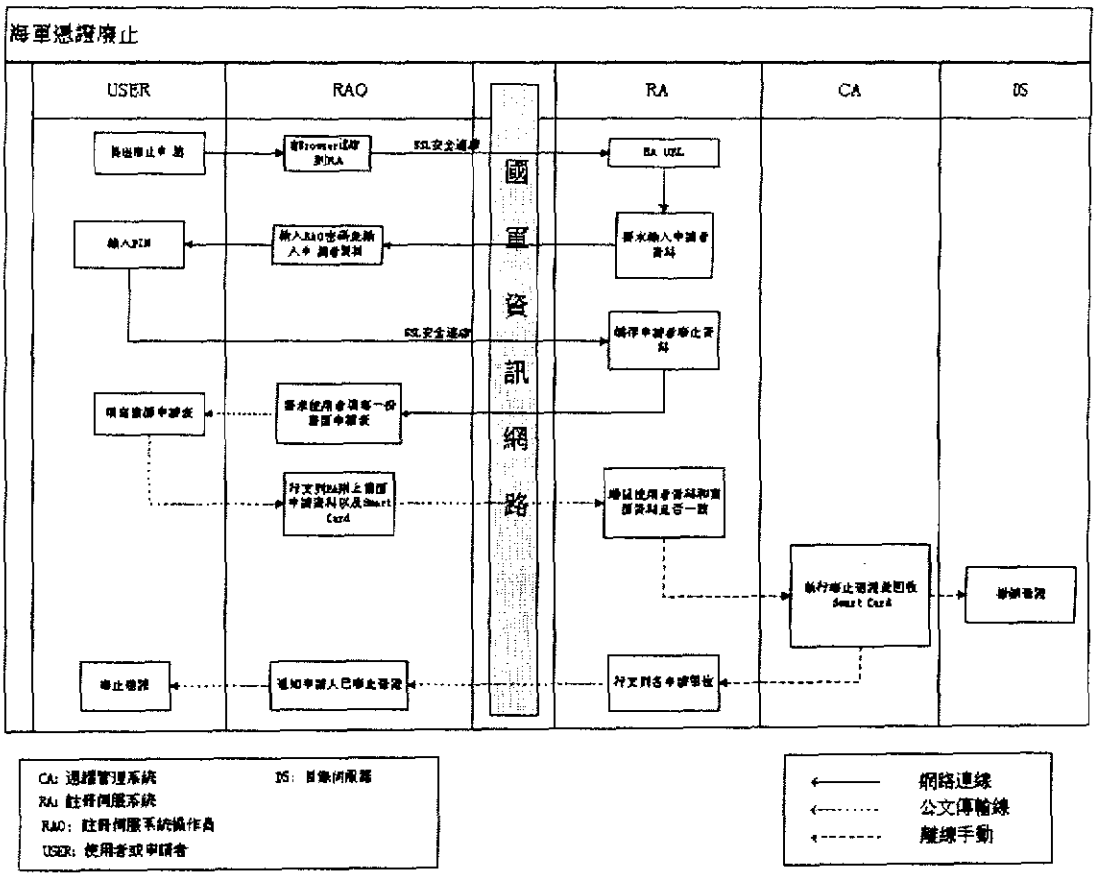
14. RA行文到各申請RAO單位並加上附件Smart Card。

15. RAO通知申請人領取。

16. 取得Smart Card 憑證。

3.3.3 憑證廢止

用戶欲停止其憑證的使用時，可向攜帶書面證明資料親自前往當地人事單位辦理，各單位人事官須驗證用戶之數位簽章或書面證明資料無誤，即可透過線上提出廢止申告，另行發函（呈）送海軍總部資訊處憑證註冊管理中心辦理，而註冊管理中心收到相關廢止申告公文，即受理憑證廢止申告。



海軍憑證廢止流程圖（資料來源：本研究）

流程說明：

1. 使用者(User)到RAO提出廢止申請。
2. RAO連線到RA URL(透過SSL安全連線)。
3. RA URL要求RAO輸入申請者個人資料。
4. RAO輸入RAO密碼並輸入申請者註冊資料。
5. 使用者(User)輸入PIN。
6. 透過SSL安全連儲存申請者註冊資料在RA。
7. RAO要求使用者填寫一份書面申請書。
8. 使用者(User)寫好書面資料交由 (RAO)以行文方式送到RA。
9. RA有RAM來負責驗証使用者登錄資料和書面資料是否一致
10. RA 驗證無誤後，將申請者個人資料以離線方式送到CA。
11. 經過一個工作天，經CA 執行憑證廢止並回收Smart Card。

12. 由CA以離線方式撤銷在DS(目錄伺服器)使用者憑證。

13. RA行文到各申請RAO單位。

14. RAO通知申請人憑證已經廢止。

15. 廢止憑證。

3.4 金鑰產製

公開金鑰基礎建設的用戶之金鑰產製有兩種方式，第一種由用戶自行產生，再將公開金鑰交給憑證管理中心進行憑證的簽發；第二種由具有公信力的第三者代為產生金鑰對後，將秘密金鑰對交給用戶保管使用，並將與產生該金鑰有關的所有相關資料銷毀，然後再把公開金鑰傳送憑證管理中心簽發憑證。海軍可依其政策採用其中一種方式。本計畫建議由海軍總部以擔任公正的第三者代為產生金鑰對。

金鑰的產生及管理：為了確保金鑰的機密性，防止破解，除必定義金鑰的使用週期外，也必須規範金鑰的產生方式，以確保只有金鑰的擁有者知曉該密鑰。因為政府的磁碟片儲存，而在 X.509 建議採用智慧卡(Smart Card)來儲存使用者的金鑰對、使用者的公鑰憑証與其 CA 的金鑰憑証，我們認為以磁片來儲存會有一些安全上的漏洞，所以本計畫建議以智慧卡來解決金鑰的儲存。

由於金鑰的長度往往超過一般人能記憶的範疇，所以通常均使用個人識別密碼〈PIN，Personal Identification Number〉，做為實體及其所使用的金鑰關聯間的驗明正身的方法。原文形式的 PIN，不能存在於任何裝置中，除非是該實體具有適當的安全裝置。若 PIN 遭到破解〈或者懷疑被竊取〉，應適當的立刻停止 PIN 的使用。

個人私密金鑰(Private Key)實體的安全係儲存在 IC 卡中，利用 PIN/PIN2/PUK 等密碼來保護：茲說明如下：

●PIN（Personal Identification Number）：使用者輸入一組PIN，讀卡機將此組PIN和儲存在IC卡內的PIN相比較。如果二者相符，則代表使用者已經有權利使用該IC卡。

●PIN1 = CHV1（Card holder verification 1）：當IC卡認證通過後，便需要輸入PIN1，方能存取儲存在IC卡內的個人私密金鑰。如果連續輸入三次錯誤，使用者必須輸入八位數的PUK（Personal Unblocking Key）才能解開鎖住的IC卡。

●PUK是儲存在IC卡中，並且海軍總部的管理人員才知道。若PIN1或PIN連續輸三次錯誤，IC卡會完全鎖住，需要送回給海軍總部的管理人員處理後，交還持卡人，方能使用。

四、海軍憑證管理中心組織及管理政策

4.1 海軍憑證管理中心之組織架構

4.1.1 組織架構規劃配置

本研究建議海軍總部的憑證管理中心，設立在海軍總部的資訊處下面，並依政府憑證管理中心組織架構，以及行『政院所屬各機關資訊機構設置要點』(參考附錄 B)設立對應的單位負責對應的管理活動。

在政府憑證管理中心設有五個分組如下[]：

(1) 綜合規劃分組：負責策略性及綜合性分析規畫、計畫追蹤等工作。

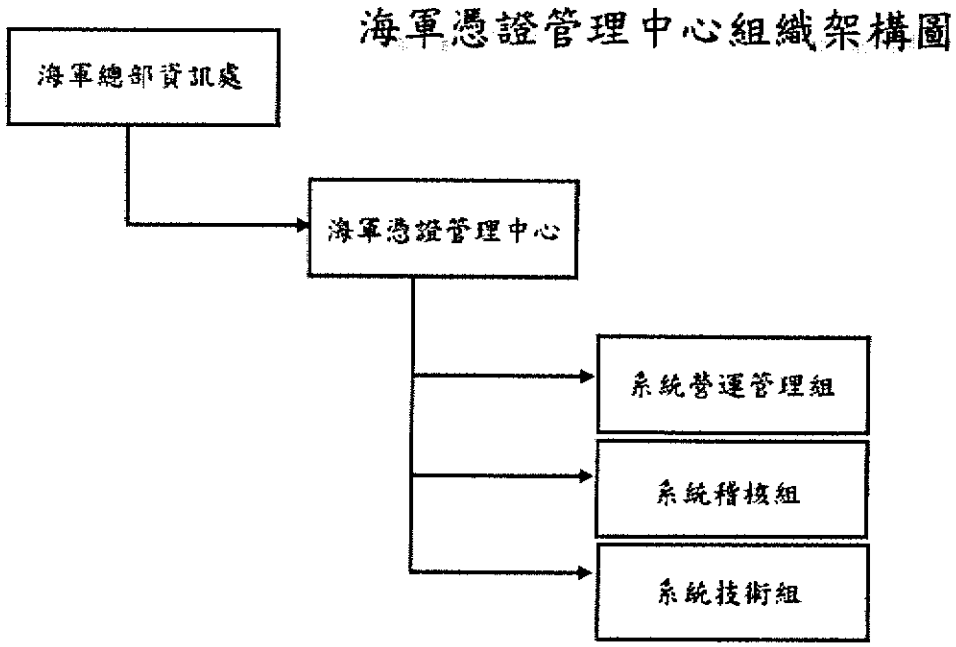
(2) 營運管理分組：負責營運相關規畫、執行與管理工作。

(3) 系統維運分組：負責系統建置與維運等工作。

(4) 技術發展分組：負責技術探討、引進與開發等工作。

(5) 稽核分組：負責控制、確認系統之安全程序，紀錄分析並偵測可能侵入系統之安全漏洞。

本研究將海軍憑證管理中心組織架構規劃如下：



海軍憑證管理中心組織架構圖(資料來源：本研究)

在憑證管理中心組織架構中共分成三個小組，其主要工作項目如下表：

單位	主要工作項目
系統營運管理組	負責營運相關規畫、分析、執行開發建置、維護與管理工作。
系統稽核組	負責控制、確認系統之安全程序，紀錄分析並偵測可能侵入系統之安全漏洞以及輔導使用者作教育訓練。
系統技術組	負責技術探討、開發建置、維護以等硬體維修等工作。

4.1.2 人員配置

在人員配置上，因為國軍組織在人員編制上實行精實案，人員及幹部一人多用現象極為普遍。所以憑證中心的實際運作需事先評估國軍內部人力規模（尤其是人力配置），再要求如何以最有效、「可行」之人力調度來運作一個憑證管理中心。

以下是以運作一個憑證管理中之人員最小配置來作估算，海軍方面可以視情況來加以增減人員：

※海軍憑證中心人員配置表

職稱	單位	主要負責工作	人數
系統管理工程官	系統營運管理組	1. 規劃整個憑證系統運作與管理， 2.CA 主機的操作、智慧卡操作 3.RA 主機操作	約二至三名
硬體維護工程官	系統技術組	1. 系統硬體設計規劃建置 2. 硬體設備當機之原因偵測及修護 3. 網路規劃以管理	一名
軟體開發工程官	系統技術組	1. 軟體瑕疵時程式之修改 2. 軟體功能擴充時系統分析與程式之撰寫。	約二至三名
上線輔導工程官	系統稽核組	電腦上線時管理應用系統操作之教育、輔導	約一至二名
系統稽核工程官	系統稽核組	確認系統之安全程序，紀錄分析並偵測可能侵入系統之安全漏洞	一名
附註: 各基層單位以人事官為 RA 操作人員，負責登錄申請憑證者資料到 RA 網站。			

4.2 管理政策

4.2.1 資訊安全政策制定及評估

制訂資訊安全政策，應定期進行獨立及客觀的評估，以反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，確保資訊安全之實務作業，確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。

（一）資訊安全政策評估作業，可責由具有專業技術及知識之內部稽核單位、獨立客觀的資深主管人員，或是委請公正超然的民間專業組織或團體，進行資訊安全政策執行成果之評估。

（二）應定期對所屬單位及人員進行資訊系統及技術應用之安全評估，以確保其遵守資訊安全政策及規定。

1、應列入資訊安全評估的對象如下：

（1）資訊設施及系統提供者。

（2）資訊及資料擁有者。

（3）使用者。

（4）管理者。

（5）系統維護者。

（6）其他有關人員。

2、資訊系統擁有者應配合定期的資訊安全評估，檢討相關人員是否遵守機關資訊安全政策、規範及有關安全規定。

3、應定期檢討及評估各項軟、硬設備的安全性，以確保其符合機關訂定的安全標準；評估對象應包括作業系統之評估，以確保系統軟體及硬體的安全措施，正確及有效地執行。

4、如專業人力及經驗不足，得委請民間專業組織團體或學者專家之協助。

5、系統安全評估應由具有專業知識及豐富經驗的系統工程人員，在權責主管人員的監督下，以人工的方式執行，或是以自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。

（三）資訊安全政策及規定之宣達

1、資訊安全政策及人員在資訊安全應扮演之角色及責任等有關規定，應在工作說明書或有關作業手冊中載明。

2、工作說明書或作業手冊規定之資訊安全政策、說明及規定，應包括執行及維護資訊安全政策的一般性責任規定、保護特定資訊資產的特別責任規定，以及執行特別安全程序及作為的特別責任規定。

3、員工如違反資訊安全相關規定，應依紀律程序處理。

4.2.2 資訊安全政策制定注意事項

（一）應指定副首長或高層主管人員，負責推動、協調及督導下列資訊安全管理事項：

1、資訊安全政策之核定、核轉及督導。

2、資訊安全責任之分配及協調。

3、資訊資產保護事項之監督。

4、資訊安全事件之檢討及監督。

5、其他資訊安全事項之核定。

（二）得視需要成立跨部門資訊安全推行小組，推動下列事項：

1、跨部門資訊安全事項權責分工之協調。

2、應採用之資訊安全技術、方法及程序之協調研議。

3、整體資訊安全措施之協調研議。

4、資訊安全計畫之協調研議。

5、其他重要資訊安全事項之協調研議。

2. 資訊安全組織權責

（一）資訊安全責任分配

1、應訂定保護個人資訊資產及執行特定資訊安全作業，有關人員應負之責任。

2、應訂定有關人員在資訊安全作業應扮演之角色，責任分配之一般性指導原

則，以作為各單位之權責分工依據。

3、每一系統應指定系統擁有者，並課予必要的安全責任。

4、應明定每一管理者應負的資訊安全責任。

5、應訂定每一系統的資訊資產項目，並訂定必要的安全程序及措施。

6、應指定每一項資訊資產及資訊安全程序的管理人員，並以書面、電子或其他方式告知其責任。

7、應訂定資訊安全之授權規定、授權等級及授權程序等，並以書面、電子或其他方式記錄之。

（二）資訊安全分工原則

1、資訊安全管理之分工原則如下：

（1）資訊安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊單位負責辦理。

（2）資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

（3)資訊機密維護及稽核使用管理事項,由政風單位會同相關單位負責辦理。

2、設有稽核單位者，稽核使用管理事項由稽核單位會同政風單位辦理。

3、未設置資訊及政風單位者，由機關首長指定適當的單位及人員負責辦理資訊安全管理事項。

4、業務性質特殊者，得視實際需要由首長調整上述資訊安全分工原則。

（三）資訊設施之使用授權

1、引進及啟用新資訊科技（如軟體、硬體、通信及管理措施等），應於事前進行安全評估，瞭解新資訊科技之安全保護措施及水準，並依行政程序經權責主管人員核准，始得引用，以免影響既有的資訊安全措施。

2、新資訊科技設施之使用，應依下列行政程序辦理：

（1）業務上的核准程序

・每一項系統及設備的裝置及使用，應經權責主管人員的核准始得使用。

・系統及設備如有遠地連線作業需求，亦應獲得負責維護當地資訊安全之權責主管人員之同意。

（2）技術上的核准程序：所有連上網路的設施，或是由資訊服務提供者維護的設施，須經技術上的安全評估程序及權責主管人員之核准，始得上線使用。

（四）跨機關之合作及協調

1、資訊安全管理人員應與外部的資訊安全專家或顧問加強協調聯繫，相互合作，分享經驗，以評估機關可能面臨的資訊安全威脅，據以研擬及推動資訊安全實務措施。

2、應與業務密切相關的機關、執法機關、資訊服務提供者及通信機構等，建立及維持適當的互動管道，以便在發生資訊安全事件時，能迅速獲得外部的資源協助，即時解決相關問題。

3、記載資訊安全事項之有關文件或資訊，在提供外界使用及進行經驗交流時，應予適當的限制，以防止載有資訊安全細節的敏感性資訊，遭未經授權的人員取用。

（五）資訊安全顧問及諮詢

1、資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。

2、對委請資訊安全顧問，或負責資訊安全之人員，各單位及人員應予必要的協助及支援。

4.2.3 人員安全管理及教育訓練

一、人員進用之評估

（一）人員進用之安全評估

1、進用之人員，如其工作職責須使用處理敏感性、機密性資訊的科技設施，或須處理機密性及敏感性資訊者，應經適當的安全評估程序。

2、人員進用之安全評估參考項目如下：

（1）個人性格。

（2）申請者之經歷。

（3）學術及專業能力及資格。

（4）人員身分之確認。

（5）財物及信用狀況。

（二）機密維護之責任約定

1、員工使用資訊科技設施，應依相關法令課予機密維護責任，並應儘可能簽署書面約定，以明責任。

2、當人員任用及約聘僱條件或契約有所變更時，尤其是人員離職或是約聘僱用契約終止時，應重新檢討機密維護責任約定之妥適性。

二、使用者資訊安全教育訓練

（一）資訊安全教育訓練

1、應定期對員工進行資訊安全教育及訓練，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

2、應以人員角色及職能為基礎，針對不同層級的人員，進行適當的資訊安全教育及訓練；資訊安全教育及訓練的內容應包括：資訊安全政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊科技設施之訓練等。

3、在同意及授權使用者存取系統前，應教導使用者登入系統的程序，以及如何正確操作及使用軟體。

4、對員工進行資訊安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

4.3 電子簽章法重要條文簡介(資料來源:行政院經濟部商業司)

建立安全及可信賴之網路環境，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，乃電子化政府及電子商務能否全面普及之關鍵。為推動安全的電子交易系統，政府

及民間企業正致力於利用現代密碼技術，建置各領域之電子認證體系，提供身分認證及交易認證服務，以增進使用者之信心。

為配合國家資訊通信基本建設之推展，國內首於八十六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（Certificate Authority, CA）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。為建立安全及可信賴之電子交易環境，裨益電子商務之發展，爰參酌各國立法體例及聯合國及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」。

4.3.1 電子簽章法之立法原則

（一）技術中立原則：鑒於科技進展神速，任何可以確保資料在傳輸或儲存過程中之完整性、可以鑑別使用者身分之技術，皆可用來製作電子簽章，並不以「非對稱型」加密技術為基礎之「數位簽章」為限，以免阻礙其他技術之發展。本法草案爰採聯合國及歐盟等國際組織倡議的「電子簽章」（electronic signature）為立法基礎，而不以「數位簽章」（digital signature）為限，以因應今後諸如生物科技等電子鑑別技術之創新發展。

（二）循序漸進原則：鑒於以密碼學為基礎所發展的電子簽章及認證機制，係一創新措施，預期政府、企業及社會大眾可能須經一段較長的學習時間，方能建立正確的觀念，熟悉使用方法及建立妥善的管理制度；另為降低電子簽章之可能風險，保障民眾的權益，爰採循序漸進的原則，規定與人民生命、重大財產及其他重要權益攸關的項目，不適用電子簽章及電子文件，並授權主管機關可視主客觀環境變化，調整不適用電子簽章及電子文件的項目。另為尊重民眾的選擇，規定政府機關及民間機構不得強制要求民眾使用電子簽章及電子文件。

（三）安全及隱私保護原則：為了增進民眾對於使用電子簽章及電子文件之信心，規定憑證機構必須從技術、管理、流程及損害賠償等層面建構安全

及可信賴的認證環境；另為確保網路通信及交易行為之個人隱私，規定憑證機構得應申請人所請，以使用者之別名或代號作為憑證持有者，以便進行匿名交易；另規定憑證機構要求申請者提供之資訊，亦必須以簽發憑證所須者為限。另亦規定憑證機構須提供申請者充足的資訊，以保障消費者的權益。

（四）契約自主原則：對於民間的電子商務行為，宜在契約自主的原則下，由交易雙方自行決定以那一種技術、那一種程序、那一種條件之下作成的電子簽章或電子文件，是雙方可以共同信賴、共同遵守作為事後相關法律責任的基礎；是以，不宜以政府的公權力介入交易雙方的契約原則；交易雙方除了利用法定的技術製作電子簽章之外，亦可自行約定雙方可以共同信守的技術。另憑證機構與其使用者之間，亦可以契約方式規範雙方的權利及義務。

（五）權責平衡原則：為使憑證機構不致因預期須承擔極大的風險而阻礙我國電子認證產業之健全發展，復為避免使用者預期毋須為保管電子簽章不周而負責，進而疏忽其應盡的管理責任，爰在權責平衡原則下，釐定憑證機構及使用者各應盡之責任與義務。

（六）市場導向原則：除了政府機關基於公權力可以提供自然人及法人等身分認證服務之外，將由民間主導發展電子商務的認證服務，完全開放民間機構依法經營認證服務。

4.3.2 電子簽章法之用詞定義

（一）電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

（二）電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。

（三）數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。

（四）加密：指利用數學演算法或其他方法，將電子文件以亂碼方式處理。

（五）憑證機構：指簽發憑證之機關、法人。

（六）憑證：指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

（七）憑證實務作業基準：指由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。

（八）資訊系統：指產生、送出、收受、儲存或其他處理電子形式訊息資料之系統。

4.3.3 電子簽章得以取代傳統簽名蓋章

電子簽章及電子文件均以電子方式存在並能在網路進行傳送，與傳統使用手寫簽名、用印鑑蓋章、書面紙本等顯不相同。電子簽章、電子文件等新興科技能否與實體「書面紙本、簽名蓋章」等同視之，賦予法律地位與效力， 是電子簽章法關心焦點。簡單來說，「電子簽章」（Electronic Signature）係指以電子形式存在，依附在電子文件並與其邏輯相關，可用以辨識電子文件簽署者身分，及表示簽署者同意電子文件內容者。而「電子文件」（Electronic Document）係指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認知與識別之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

電子文件能在螢幕上顯示文字與符號，但從技術層面來看，電子文件的每一次顯示均屬數位電磁記錄 0與1重組產生，並無所謂有體物可供附著存在，與使用紙張的文書不同。倘若電子文件遭到第三者 惡意修改，只是位元的增減，無法如實體紙本可能顯出塗改等痕跡；因此電子文件更容易竄改且很難 察覺。這些與實體書面紙本的差異性質，使電子文件明顯無法符合現有法律「書面」要式行為規定要 求，無從具有相同法律效力；而電子簽章也面臨著相同困境。要突破現有法律障礙，必須賦予電子簽章、電子文件使用之法律效力，所以需要積極制定電子簽章法相關法律，奠定完善使用環境，以減少各種適用法律之爭議。

4.3.4 電子簽章之法律效力

建置電子簽章及文件使用規範制度，奠定完善運用環境，並賦予電子簽章及文件法律效力，此為電子簽章法主要任務之一。再者，使用電子簽章及文件，無法符合現有法律規範要求簽名與書面等法定要式行為之規定，需要突破此法律障

礙，此為電子簽章法主要任務之二。

確定電子簽章及文件使用之法律效力：

首先賦予電子簽章及文件法律承認地位（Legal Recognition），對待電子簽章及文件不能僅因其以電子記錄形式存在，無法符合簽章、書面要件條件，而逕否認其效力，參酌聯合國 UNCITRAL、美國伊利諾州、澳洲、新加坡、馬來西亞亦有法律承認地位規定；其目的在對電子簽章及文件法律不可存有歧視態度，也就是「非歧視」原則。現今電子商務眾多活動，普遍來說可能一般均僅屬於 E-Mail 文件往來或線上交易等單純行為，絕大部分均屬「非要式行為」，法律規定必須履行要式行為」的比例並不高。此條文之訂定能夠教育民眾在日常生活，將自己使用的電子簽章及文件與實體簽章、書面持同等看待的態度。當事人間一般的要約、承諾、溝通往來等等行為，只要不是法定要式行為，法律本來就不會介入規範當事人必須以電子文件亦或必須書面來作成。所以絕大部分線上交易行為、溝通往來，將更確定其具有的法律效力，其他人不得任意否定。此為首要原則，不僅具有宣示意義，更有使電子簽章及文件取得法律上普遍地位之效力。

突破現有「法定『書面簽章』要式行為」法律規定之障礙：

如果屬法律要求必須簽章或書面等要式行為，若採取電子簽章、電子文件等傳輸行為，因為無法符合法律要件，無法具有相同法律效力。為消除法律適用上障礙，世界各國均制定「行為以電子簽章及文件行之，如其內容可以電子方式完整呈現，並可於日後取出供查驗真偽者，視為可符合法律上『簽章、書面』要件之要求」等類似規定。聯合國 UNCITRAL 更明白闡述此「功能相等 Functional-Equivalent」」原則，其思考點並非使電子簽章及文件直接等同於傳統簽章、紙本，而是考量法律規定「簽章、書面」之理由與其要求，歸納出必要功能要件，具備相同功能要件之電子簽章及文件就符合所謂簽章、書面法律要求。此部分立法，在於突破電子簽章及文件在法律適用上之難題，而使其具有與簽章、書面相同之效力。

五、範本流程

中華民國海軍認證中心雛形系統之建置主要是以 Web base 為主，所以在系統中大多都是以瀏覽器做為執行程式的工具，這樣一來就可以免除要設計 Client 端程式的問題而且同時讓使用者有個熟悉的使用介面。而在這一章中主要是要說明三種主要功能的範本流程。

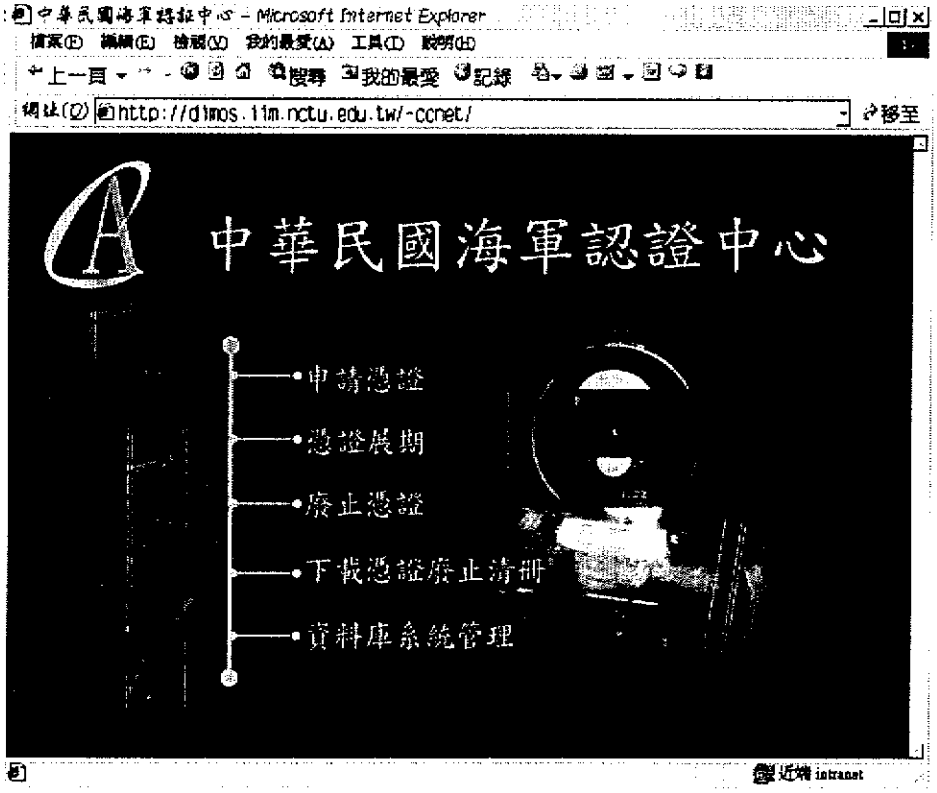
5.1 憑證申請

一、RA 操作員方面

RA 操作員主要的工作是為單位內的使用者服務，使用者對於憑證的各種要求（如申請、展期以及廢止）皆需要透過 RA 操作員來進行。

1. 開啟 IE，進入海軍認證中心網頁：

共有五種功能，分別為申請憑證、憑證展期、廢止憑證、下載憑證廢止清冊以及資料庫系統管理。這五種功能要使用前必須要進行使用者登錄，只有合法的 RA 操作者才可以使用這五種功能。

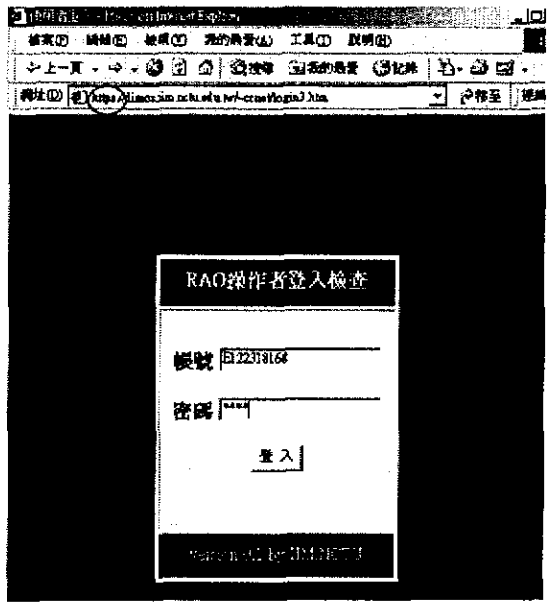


2. 申請憑證登錄網頁：

要進入這個網頁，會要求 RA 操作者輸入帳號以及密碼，為了確保使用者輸

入資料的安全性，在這裏會使用 SSL 連線，以確保輸入的資料不會被他人使用竊聽程式偷取。（請注意紅線的部份）

而 RA 操作者的帳號及密碼是由海軍總部配發，而每一個 RA 操作者可以在登錄之後，自行修改密碼及個人資料。



3. 申請憑證畫面：

在這個畫面讓 RA 操作者輸入申請憑證者個人基本資料。同樣的，為了資料的安全，這個畫面仍然是使用 SSL 連線。

將來核發的憑證其中的內容是以申請憑證者個人基本資料來產生的，以下將對各欄位以及憑證中的資料項加以說明：

(1) 中文姓名：這個欄位會產生憑證中的 CN（Common Name）欄位，也就是這個憑證所有人的名字。

(2) 身份證字號：這個欄位不會產生憑證中的任何欄位，只是留存於資料庫中備查

(3) 出生日期：和身份證字號一般不會產生任何的欄位。

(4) 服務單位：服務單位在憑證中會產生兩個欄位分別為 O（Organization）以及 OU（Organization Unit）。而 O 我們一律填入"海軍"，而 OU 則是 RA 操作員的所屬單位。

(5) 級職：這個欄位不會在憑證中產生任何欄位，但是會儲存在目錄伺服器中的個人資料。

(6) 戶籍地址：這個欄位會在憑證中產生三個欄位，包含了 C（Country 國家）、S（State 省）以及 L（Location 區域）以及一個非憑證的欄位 address。

在憑證中，C 這個欄位是用兩個英文代表的國家（中華民國是 TW，而美國是 US），所以不需要 RA 操作員填入。

而同樣的理由，S 這個欄位也一樣有預設值（臺灣省）。

L 這個欄位的內容則是縣市

Address 這個欄位的內容會存至目錄伺服

(7) 通訊地址：這個欄位則是用來留存於資料庫備查

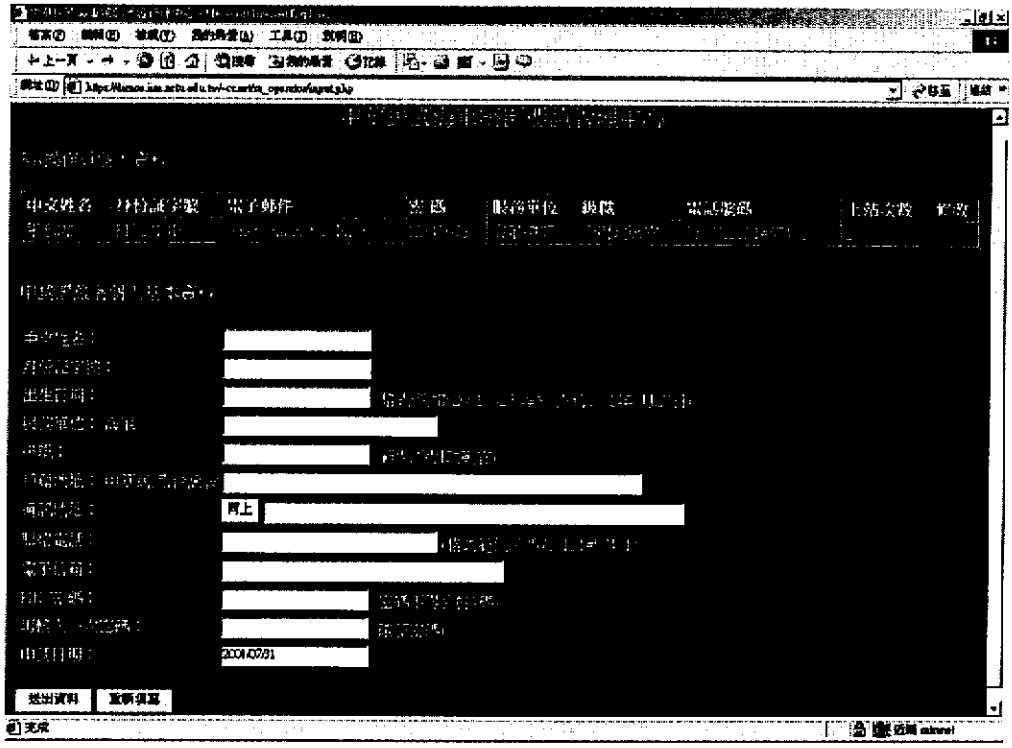
(8) 電子郵件：申請憑證者的電子郵件，同時這個欄位也會產生憑證中的欄位 E（Email）

(9) 密碼：這個密碼是用來做為智慧卡上的 PIN 碼，這個密碼要由申請憑證者來輸入，而不是 RA 操作員來輸入，這是因為使用智慧卡的是申請憑證者而不是 RA 操作員。

(10) 確認密碼：讓申請憑證者確認密碼，以避免密碼錯誤。

(11) 送出資料：將所填寫的資料送出。

(12) 重新填寫：將所有資料清除，重新填寫。

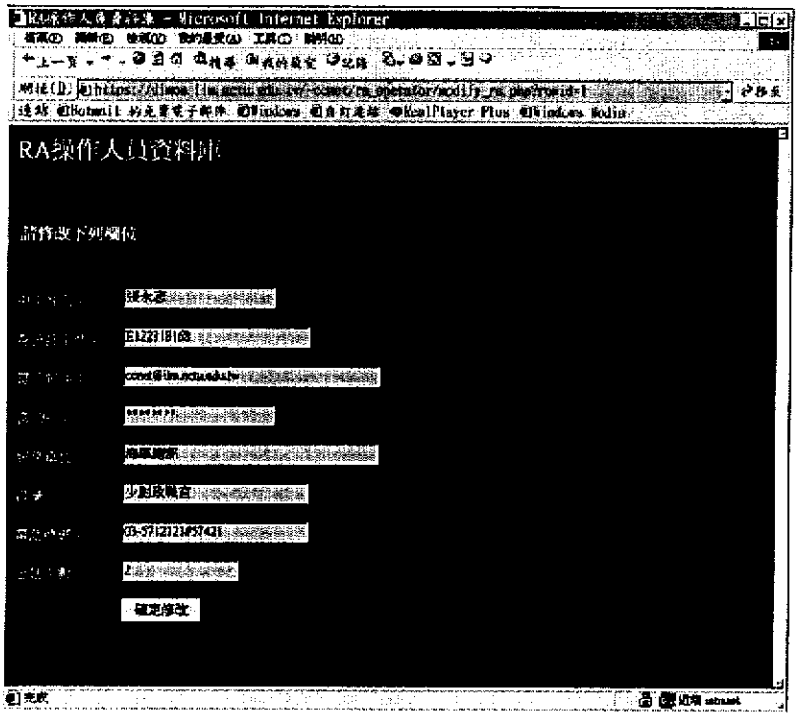


在送出資料之後會出現如下圖的畫面，來告知 RA 操作員申請憑證的動作已經

完成。

4. 修改 RA 操作員資料：(option)

在這個畫面中只要按下修改便可以進入下面的畫面，可以讓 RA 操作員修改個人資料及密碼

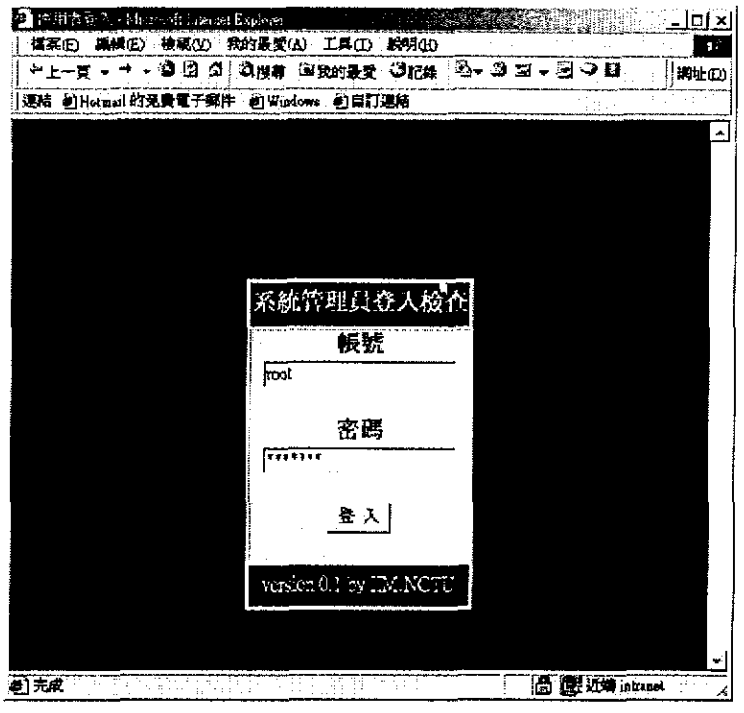


二、RA 管理者方面

RA 管理者主要的工作是處理各單位 RA 操作員所提出的各項申請資料，當 RA 管理者當接到相關的申請憑證公文後，就要進入資料庫核與申請人員名冊相核對驗證是否正確，其主要的步驟如下：

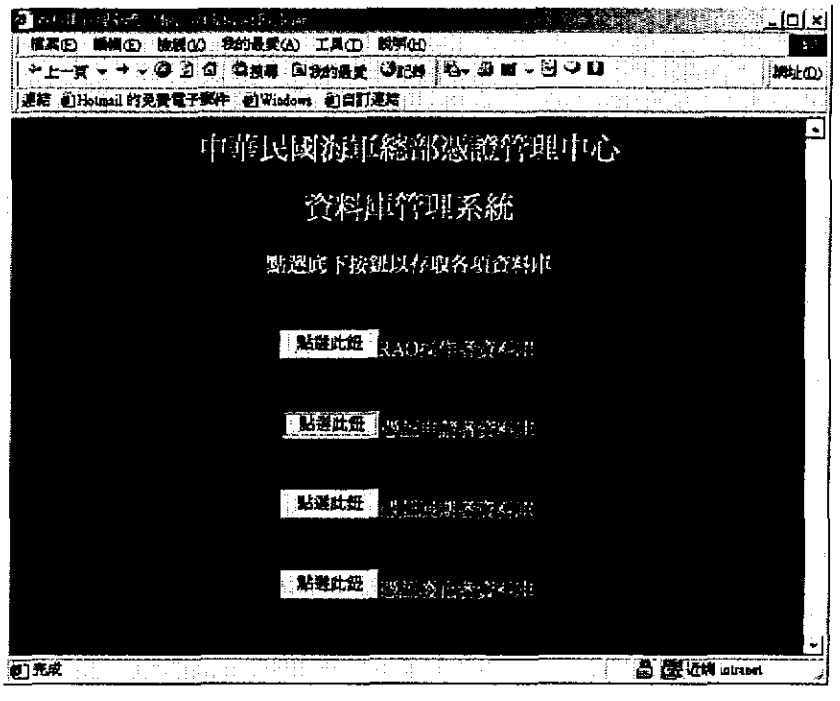
1. RA 管理者登入

RA 管理進入資料庫管理前必須要先登入才能行使管理者的權限。

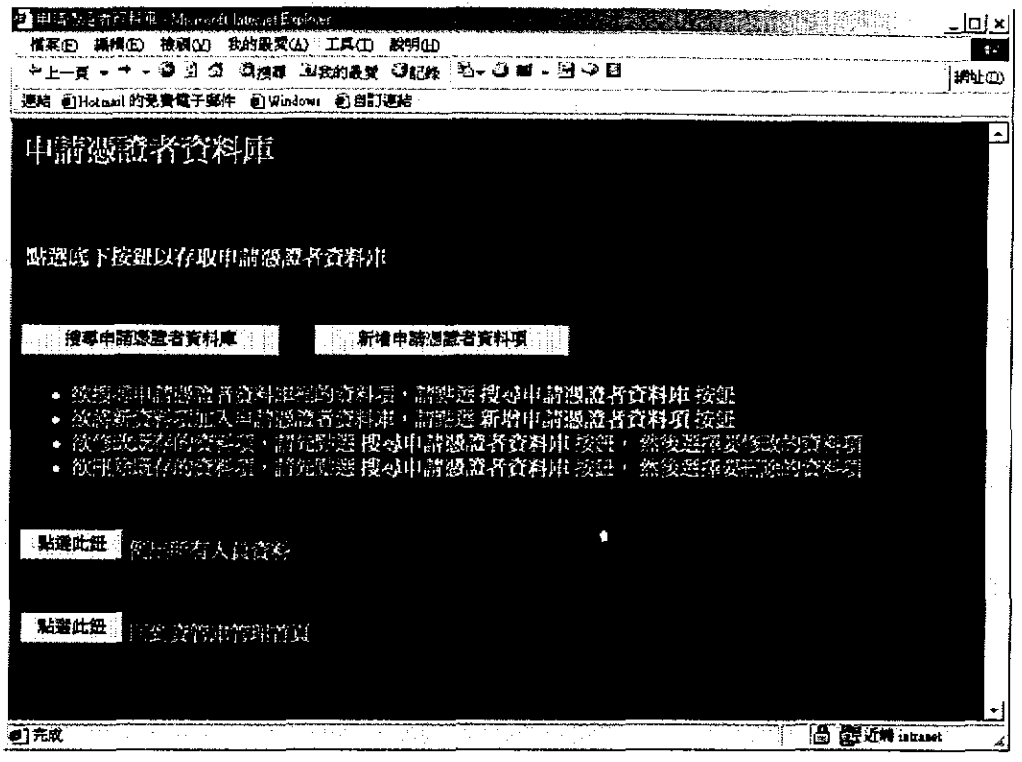


2. 選擇憑證申請者資料庫

進入資料庫管理系統的主畫面後，選擇憑證申請者資料庫

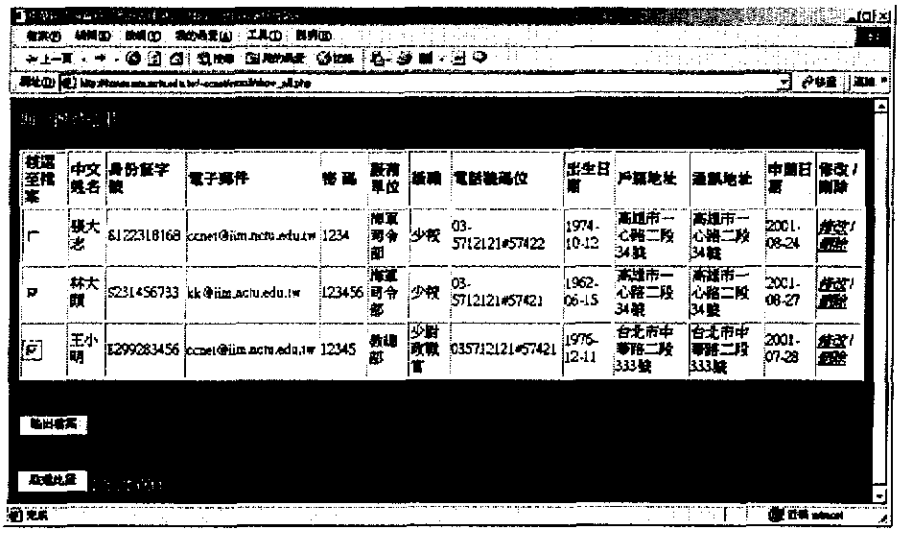


再選擇“列出所有人員資料”這個選項，列出所有申請憑證的人員資料。



3. 輸出申請憑證的人員名單

在上一個步驟中列出了所有申請憑證的人員名單，接下來 RA 管理者必須核對憑證申請公文中所列出的人員清冊，並將公文中所列出的人員名單勾選後，再點選輸出檔案。這時會產生一個 enroll.txt 的檔案



4. 複製輸出清單至 CA 伺服器

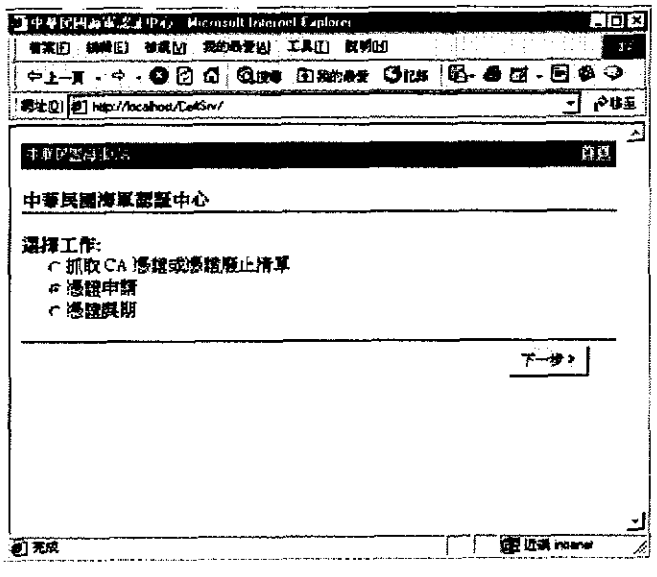
RA 的管理者，將申請憑證人員的資料輸出為一個檔案後(也就是 enroll.txt)，將這個檔案複製至 CA 伺服器，交由 CA 管理者來處理。

三、CA 方面

在 CA 這端是由 CA 的操作員來進行操作。要注意的是，因為這台 CA 的伺服器可以發出單位所信任的憑證，所以在管理上一定要非常的小心謹慎，嚴禁非相關人士接觸、操作，所以一定要是一台 Off Line 的電腦，以避免有惡意使用者透過網路入侵這台伺服器。

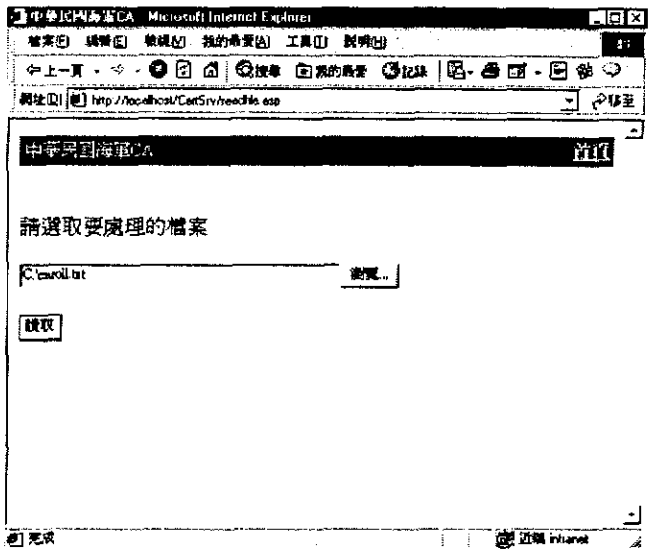
1. 開啟 IE，進入 CA 憑證申請網頁

因為我們所發展的系統都是 Web base 為主，所以即使 CA 伺服器是一台離線的電腦，我們仍可以使用 IE 來操作程式。



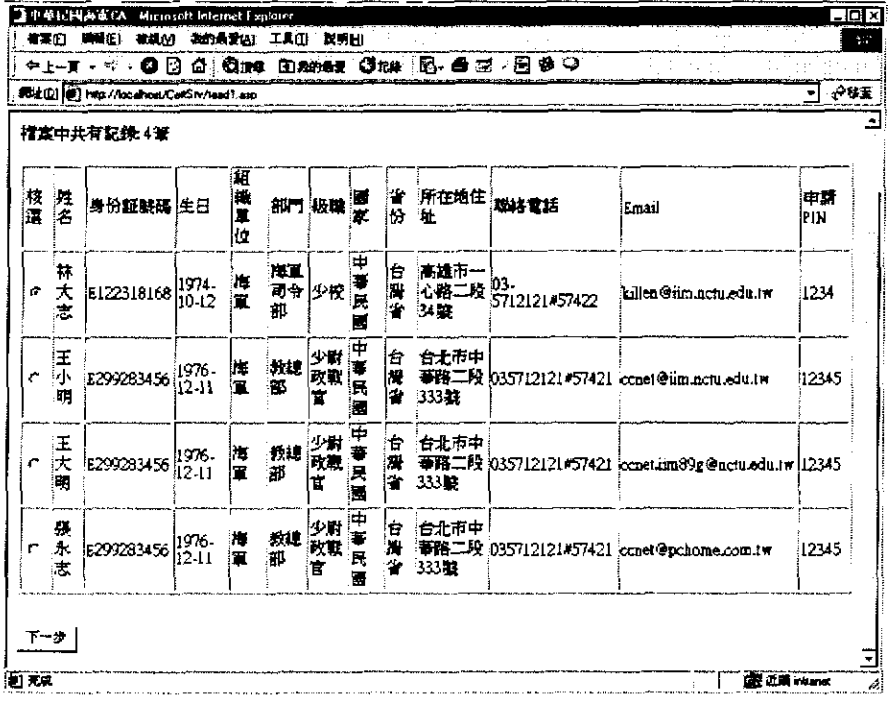
2. 選擇所要處理的使用者憑證申請資料檔

在這個步驟中，我們要選擇從 RA 伺服器上所取得的使用者憑證申請資料檔（在這邊是 c:\enroll.txt），在這個資料檔中包含了這一次要處理的使用者申請資料。



3. 選擇所要處理的申請者

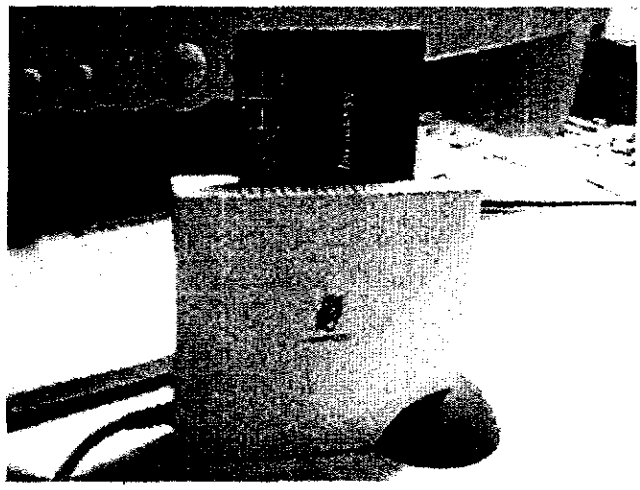
在這個畫面中所看到的就是這次所有的申請者，我們每次可以選擇一位使用者來處理其申請的資料。

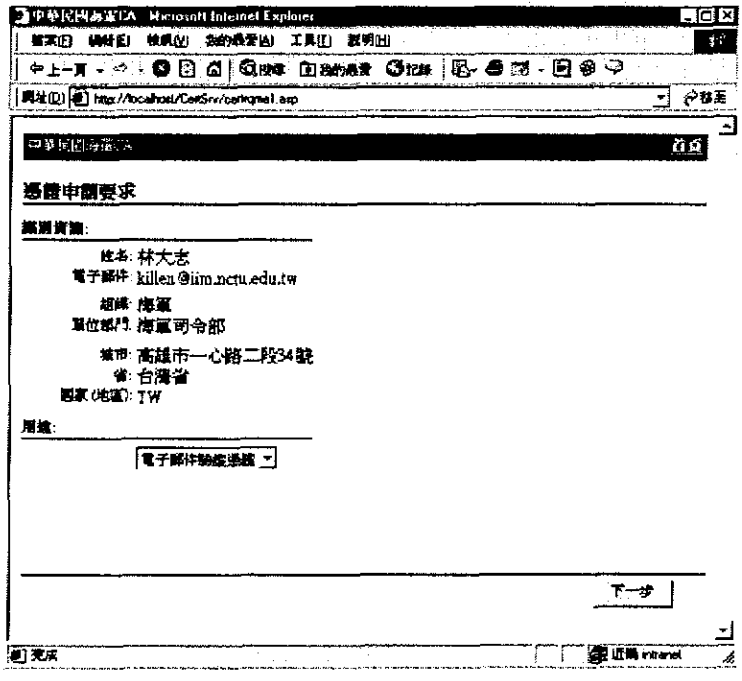


核選	姓名	身份証號碼	生日	組織單位	部門	級職	國家	省份	所在地住址	聯絡電話	Email	申請PIN
○	林大志	E122318168	1974-10-12	海軍	海軍司令部	少校	中華民國	台灣省	高雄市一心路二段34號	03-5712121#57422	allen@iim.nctu.edu.tw	1234
○	王小明	E299283456	1976-12-11	海軍	教總部	少尉政戰官	中華民國	台灣省	台北市中華路二段333號	035712121#57421	ccnet@iim.nctu.edu.tw	12345
○	王大明	E299283456	1976-12-11	海軍	教總部	少尉政戰官	中華民國	台灣省	台北市中華路二段333號	035712121#57421	ccnet.im89g@nctu.edu.tw	12345
○	張永志	E299283456	1976-12-11	海軍	教總部	少尉政戰官	中華民國	台灣省	台北市中華路二段333號	035712121#57421	ccnet@pchome.com.tw	12345

4. 確認使用者資料

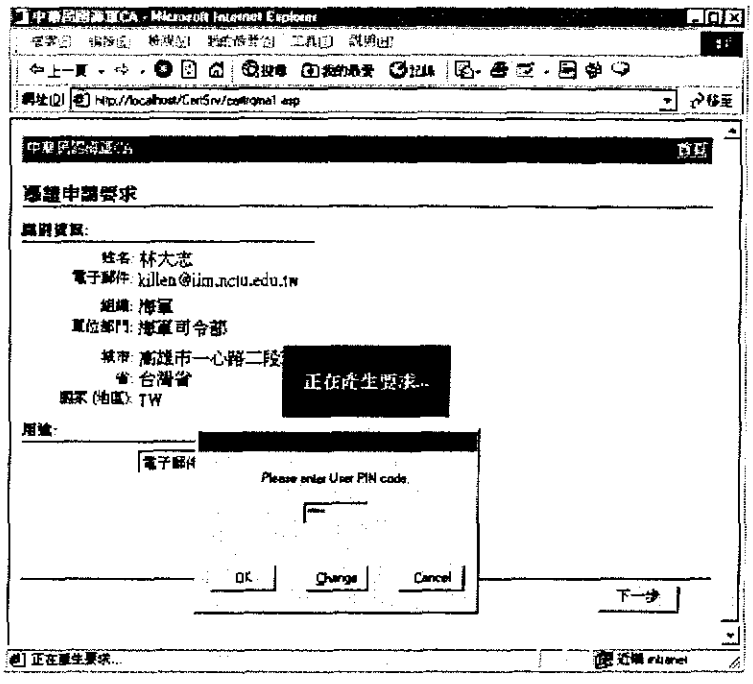
確認使用者的明細資料，在這同時就可以將準備發給該使用者的 Smart Card 插入讀卡機中，準備下一個步驟的進行。





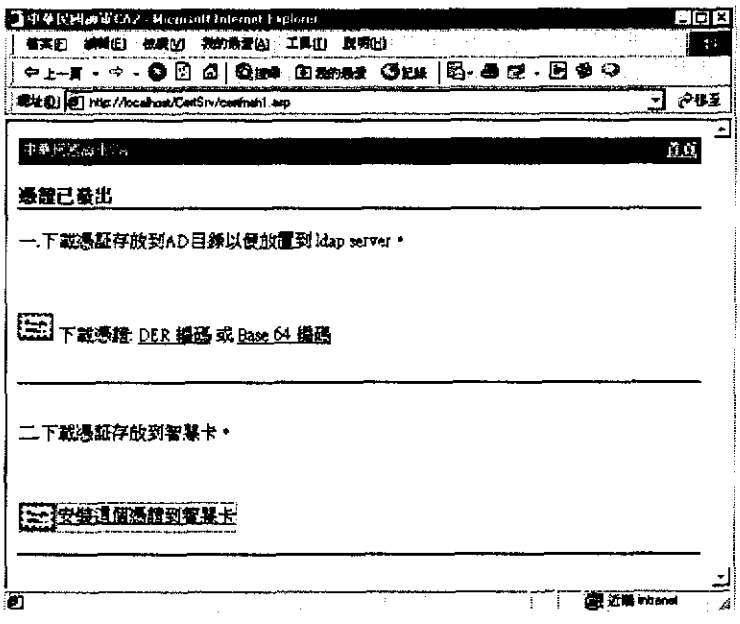
5. 產生金鑰對及憑證

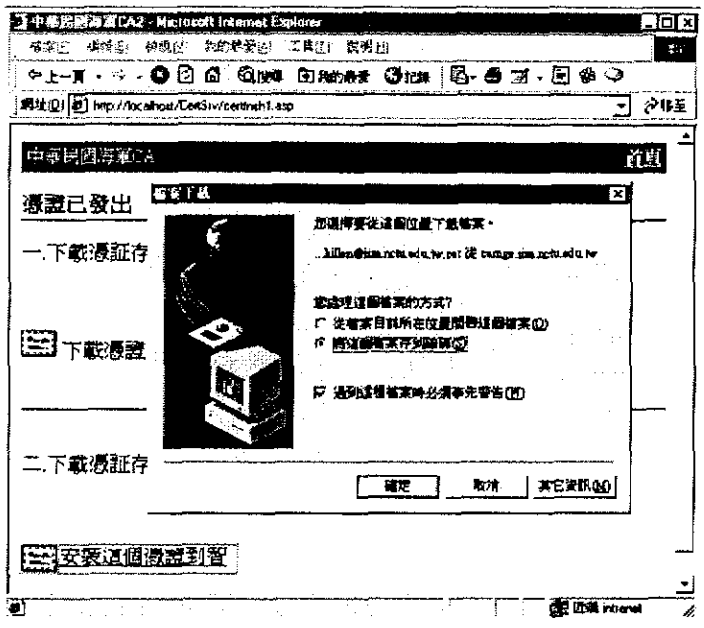
在這個階段中，我們會產生金鑰對，並且直接將金鑰對寫入 Smart Card 中，所以即使用 CA 的操作員也不會知道這組金鑰對的內容，大大的增強了這組金鑰對的安全性。但是在寫入 Smart Card 的同時，Smart Card 也會要求 CA 操作員輸入這張卡的 PIN code，在輸入正確的 PIN code 之後，這組金鑰對才能夠被寫入 Smart Card 之中。

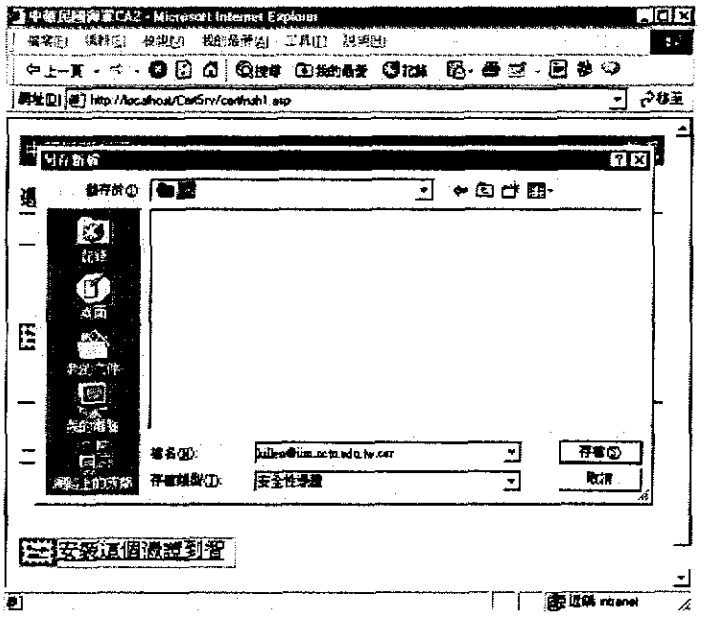


6. 下載憑證檔

在這個畫面中，有兩個選項，第一、下載憑證存放至ＡＤ目錄以便放置到 ldap server。第二、下載憑證存放到 Smart Card。首先我們要將憑證下載存放至一個固定的目錄中：這是為了方便在目錄伺服器的階段中將每個人的憑證上傳至目錄伺服器中，我們選擇 DER 格式的憑證檔下載至固定的目錄，而檔名就使用申請者的 Email 帳號來加以儲存。

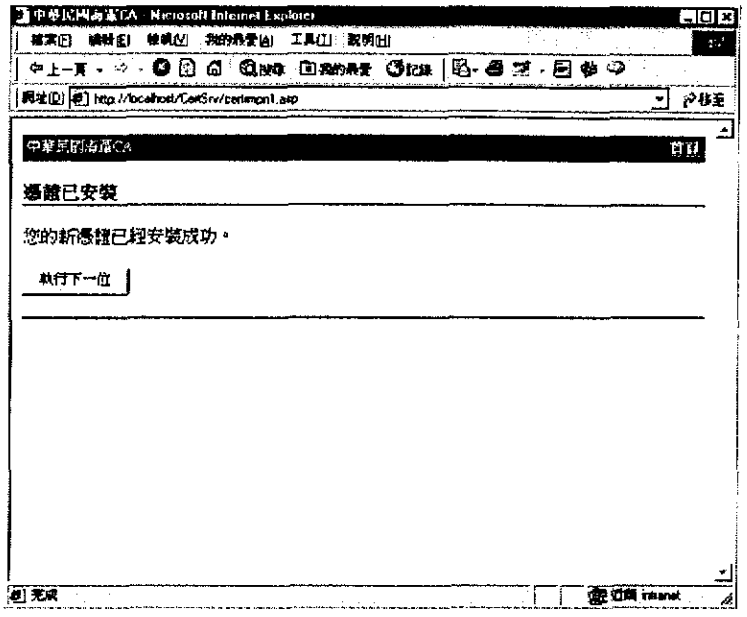






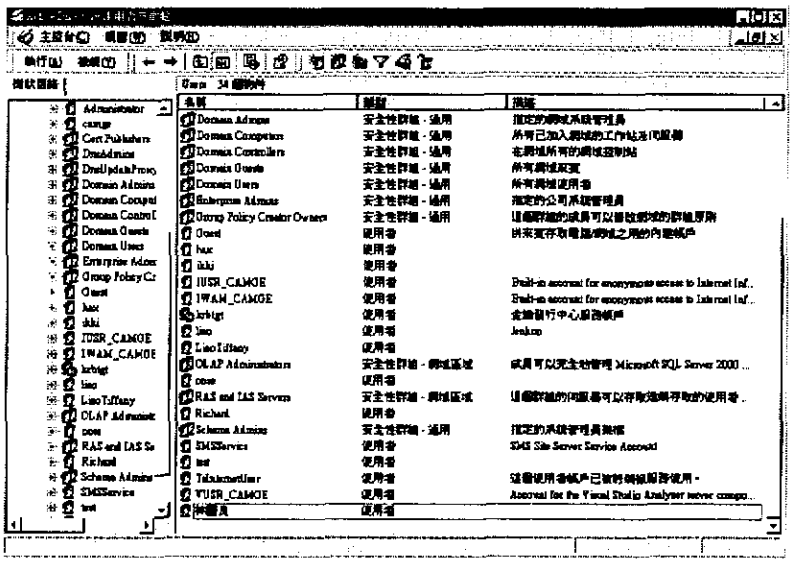
7. 完成安裝憑證至 Smart Card 中

完成上一個步驟後，我們就可以執行第二個超連結來安裝憑證至 Smart Card，完成了這一個步驟後，就算完了一位使用者的申請程序，可以接著下一位使用者；將所有使用者的 Smart Card 都建置完成後，CA 的工作就算是完成了。

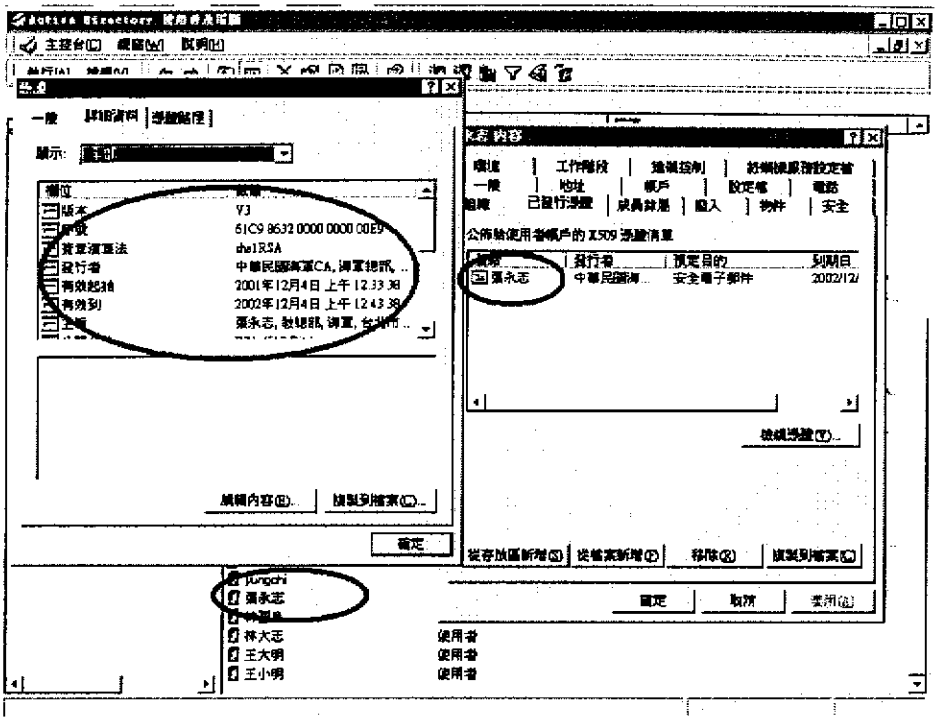


四、目錄伺服器方面

將憑證及輸出清單複製至目錄伺服器上，這個動作並不是完成將資料上傳至目錄服務中，只是為上傳使用者資料及憑證至目錄服務做準備，在這邊，我們使用微軟的 Active Directory Server 來做為我們的目錄服務的伺服器。在這個步驟中，我們要執行新增使用者資料程式，將所有的憑證儲存至目錄伺服器中，同時也會將申請憑證者的基本資料儲存目錄伺服器中。再重新檢視一次目錄伺服器的使用者就會發現新增了使用者以及其數位憑證。



執行前



執行後

5.2 憑證展期

一、RA 操作員方面

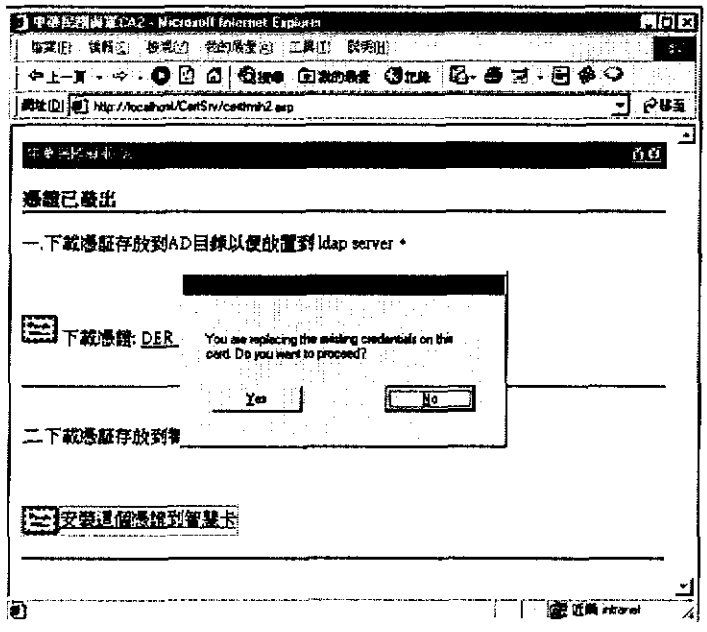
在憑證展期方面，RA 操作員所要進行的動作與憑證申請很類似，同樣需要透過網頁來輸入展期人員的資料。

二、RA 管理者方面

在憑證展期方面，RA 管理者所要進行的動作與憑證申請很類似，同樣會在收到公文後核對申請展期人員名冊後再進行輸出人員清單，再提供這份清單給 CA 管理者進行作業。

三、CA 方面

憑證展期的操作與申請憑證幾乎是一樣，直到安裝展期後的憑證至 Smart Card 時，我們必須使用原來存放憑證的 Smart Card 才能夠進行安裝展期後的憑證。在安裝展期後的憑證時，會問“要不要覆蓋原有的憑證？“回答要即可。



四、目錄伺服器方面

將展期後的憑證及輸出清單複製至目錄伺服器（與憑證申請相同），為上傳使用者資料及憑證至目錄服務做準備。在這個步驟中，我們要執行更新使用者資料程式，將儲存在目錄服務中的憑證更新成為展期後的憑證。再重新檢視一次目錄伺服器的使用者就會發現使用者以及其數位憑證的資料更新了。

5.3 憑證廢止

一、RA 操作員方面

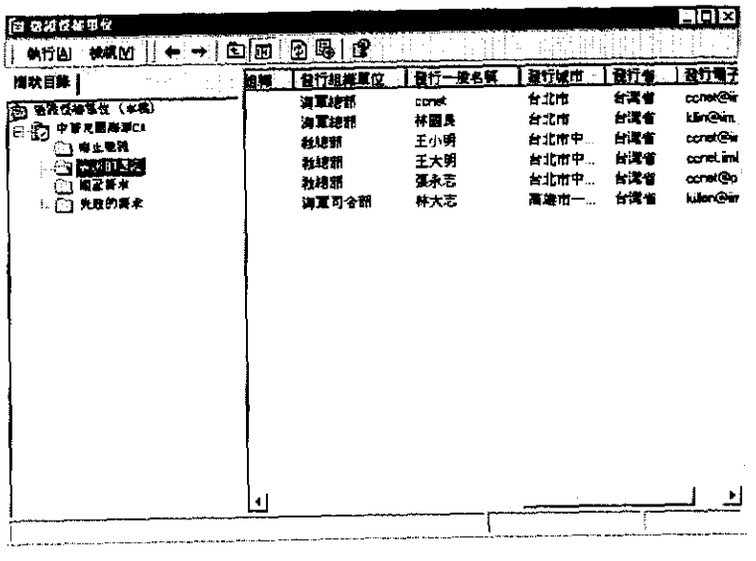
與前二項作業方式皆同

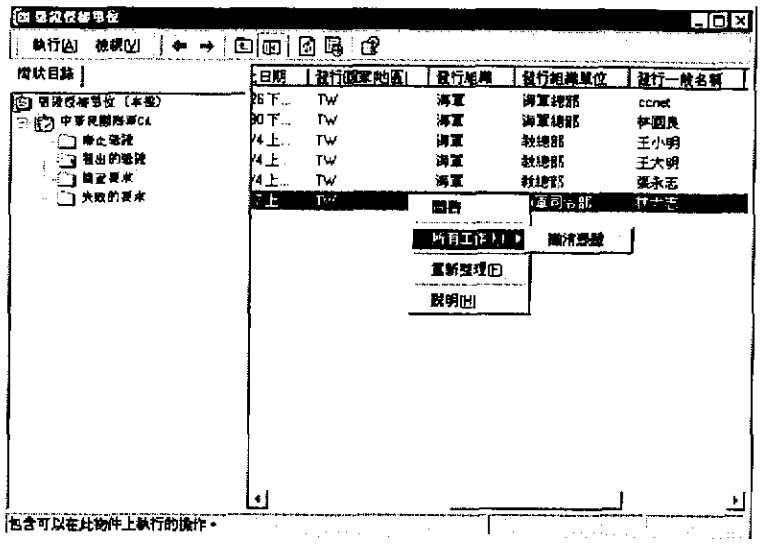
二、RA 管理者方面

與前二項作業方式皆同，但是之後 CA 伺服器的管理者會下載一份廢止清單，需要 RA 管理者將這份清單放至下載廢止清冊的超連結中，以供大眾下載使用。

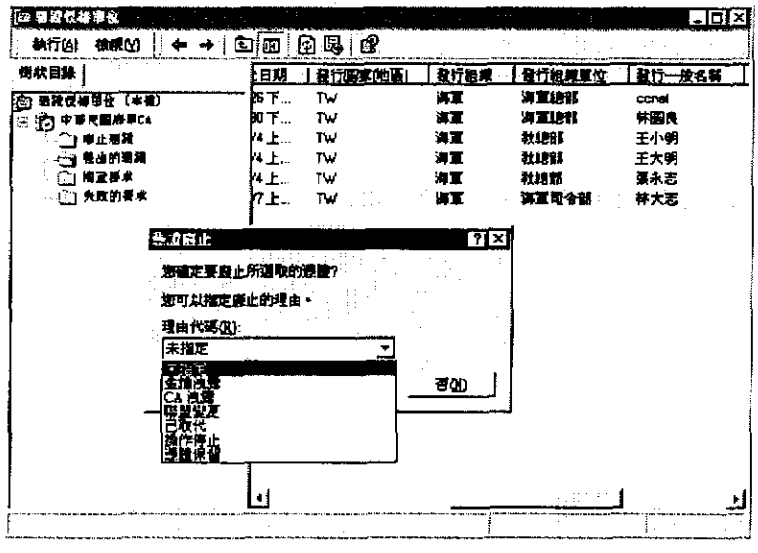
三、CA 方面

在這個步驟中，CA 管理者直接使用微軟 CA 的管理程式（憑證授權單位）來進行憑證的廢止。在這個程式的畫面中可以分為二部份，左邊是樹狀目錄，右邊是憑證資料。在左邊先選擇“發出的憑證”，在右邊就可以看見目前所有發出的憑證資料。選取所要廢止的憑證，按滑鼠右鍵選取所有工作中的撤消憑證，就可以廢止這位使用者的憑證。



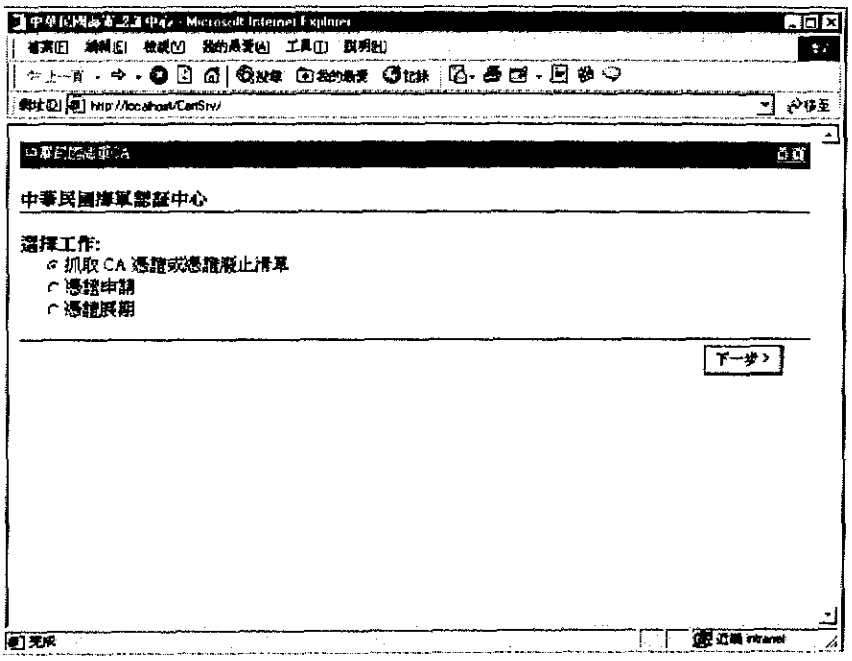


程式在執行廢止前先會先詢問廢止的原因，可任意指定，並不會影響執行結果，原因只是用來做為參考用，無其他用途。被廢止的憑證可以藉由點選左邊樹狀結構中的“廢止憑證”來查看其狀態。



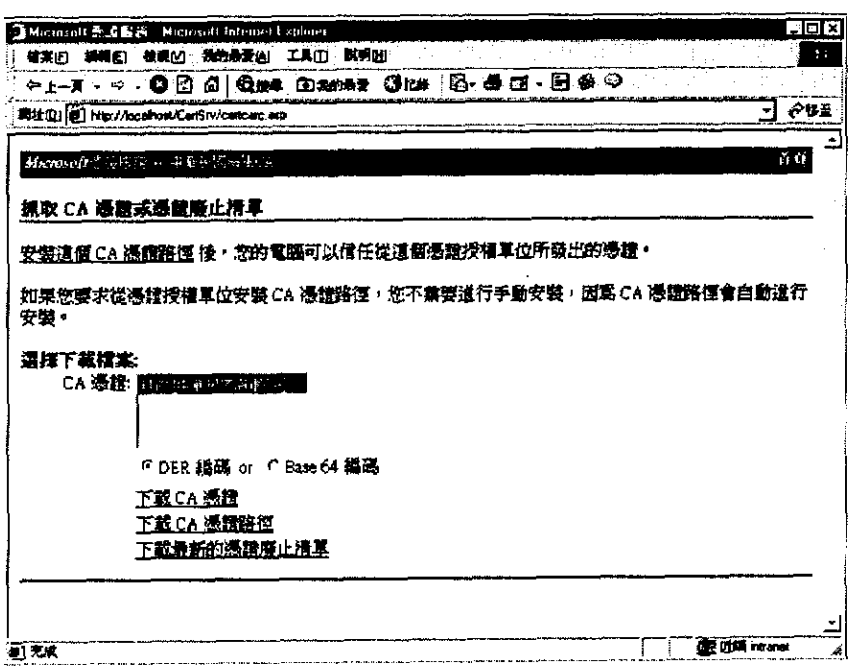
在完成憑證廢止後，CA 管理者可以再使用原來管理程式來輸出憑證廢止清冊，並將廢止清冊公布在 RA 的網頁，以供大家下載，其步驟如下：

1. 開啟 IE，進入抓取 CA 憑證或憑證廢止清單網頁



2. 下載憑證廢止清單

點選下載最新的憑證廢止清單，就可以從 CA 伺服器中下載憑證廢止清單，因為 CA 伺服器是一台離線的電腦，所以只有 CA 伺服器的管理者才能夠下載廢止清單，為了讓所有的使用者都可以取得廢止清單，所以要將這份廢止清單下載後放至 RA 伺服器，供所有的人下載。



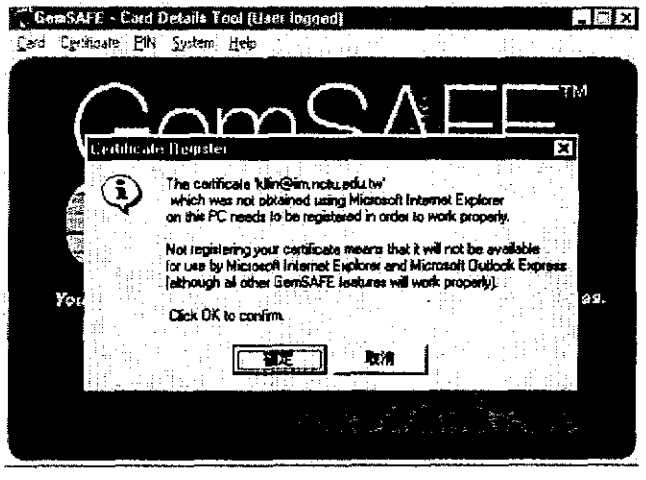

http://localhost/CertSrv/certcarc.asp
抓取 CA 憑證或憑
安裝這個 CA 憑證
如果您要求從憑證
安裝。
選擇下載檔案:
CA 憑證:
DER
下載 C
下載 C
下載最新的憑證廢止清單
localhost
確定
取消

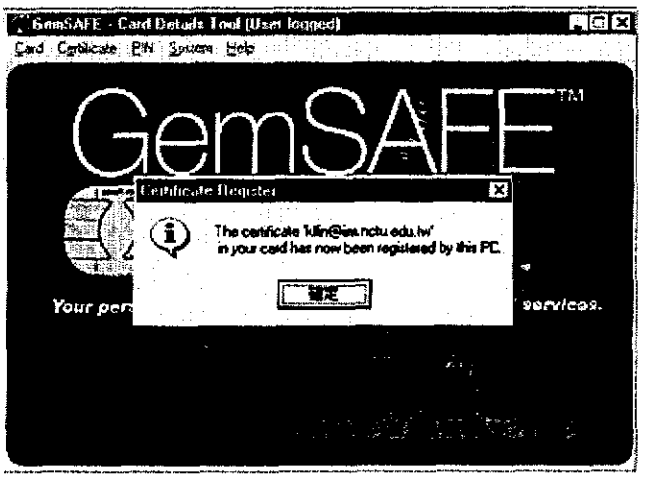
5.4 使用憑證

在配發給使用者 Smart Card 後，使用者就可以使用這張 Smart Card 中所包含的憑證以及私密金鑰來進行發送具有身份識別的電子郵件或是使用以 Smart Card 管制的電腦。因為使用 Smart Card 管制的電腦，需要整個電腦系統配合，所以在這邊將不說明如何使用，在這僅說明如何在發送電子郵件時使用 Smart Card 上的私密金鑰及憑證。

1. 將 Smart Card 內的憑證登錄至所使用的電腦上：

   這個過程可以使用 Smart Card 廠商所提供的程式，將 Smart Card 內的憑證在所使用的電腦上登記，經過這個動作後，Smart Card 內的憑證會記錄在電腦中。



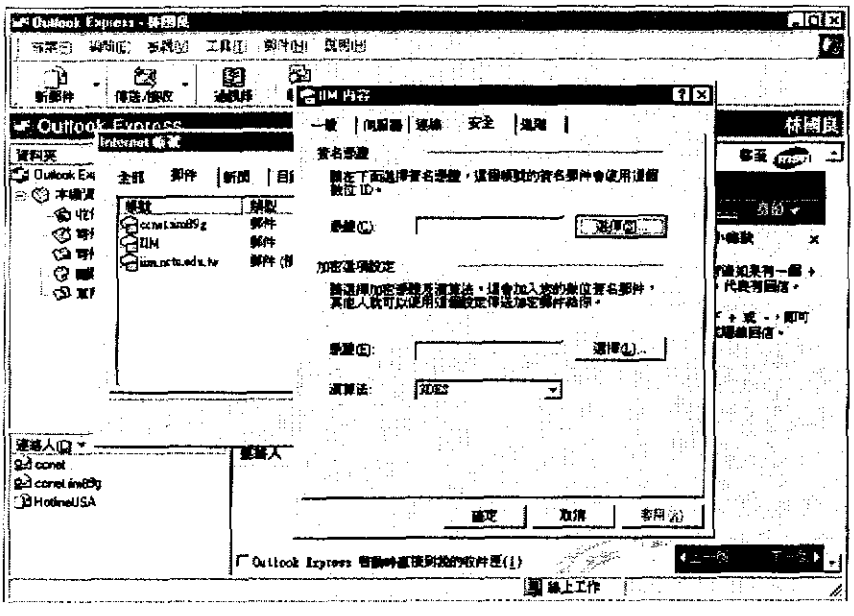


2. 設定 E-mail 帳號

   以下的說明皆是使用 Outlook Express。

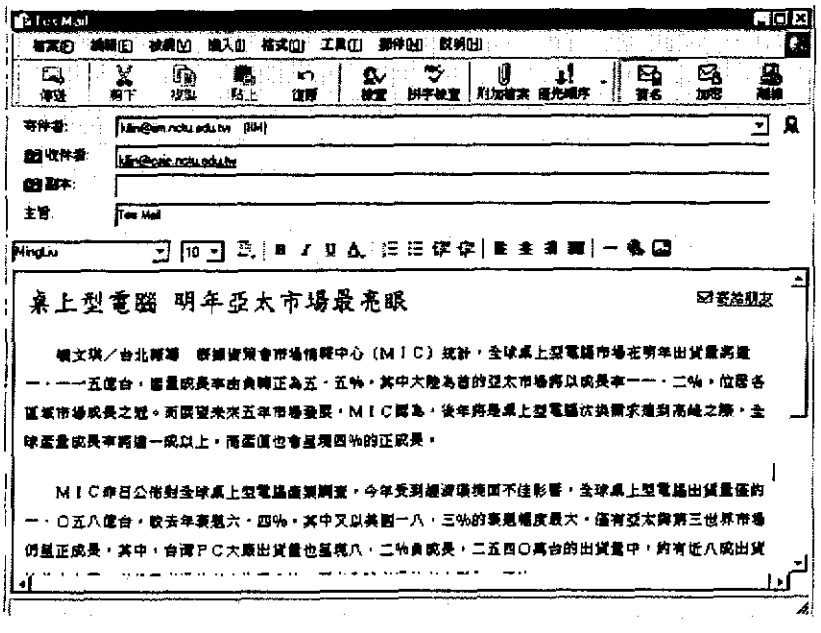
   (1) 我們必須先設定好一組 E-mail 帳號，而這個 E-mail 帳號必須與憑證中所登記的 E-mail 相同。

(2) 設定 E-mail 帳號內容中的安全選項，可以看到三個選項，分別是簽名憑證、加密憑證及演算法。按下二個憑證的選擇都可以看到我們先前所登記的憑證，所以同樣都選擇這個憑證；而演算法方面就可以任意選擇一種演算法即可。



3. 發送電子郵件

帳號設定完成後，就可以為自己的電子郵件做數位簽章，只需按下簽名的按鍵，送出的電子郵件就會自動完成所要求的任務，而電子郵件的收件者只要先取得發信人的數位憑證就可以完成驗證簽名的動作。

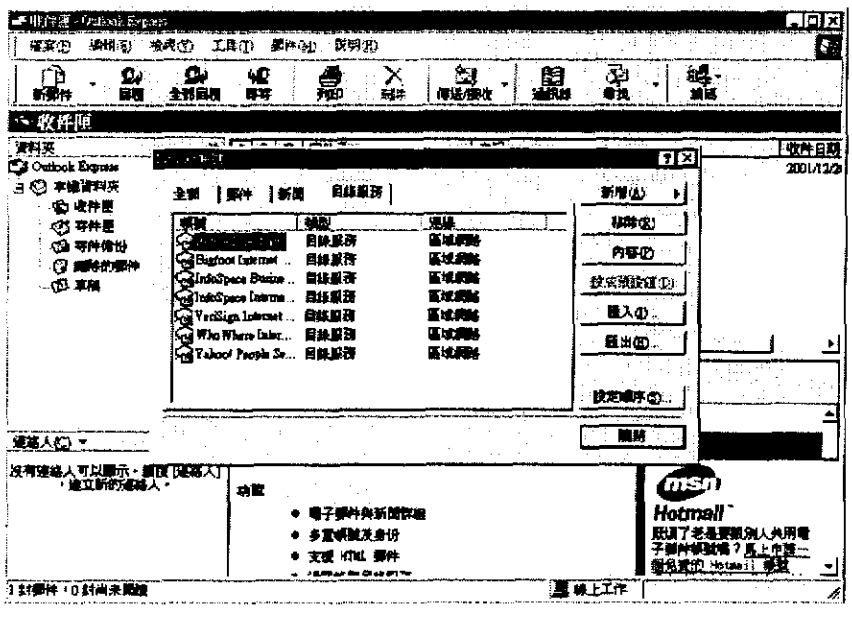


5.5 搜尋憑證

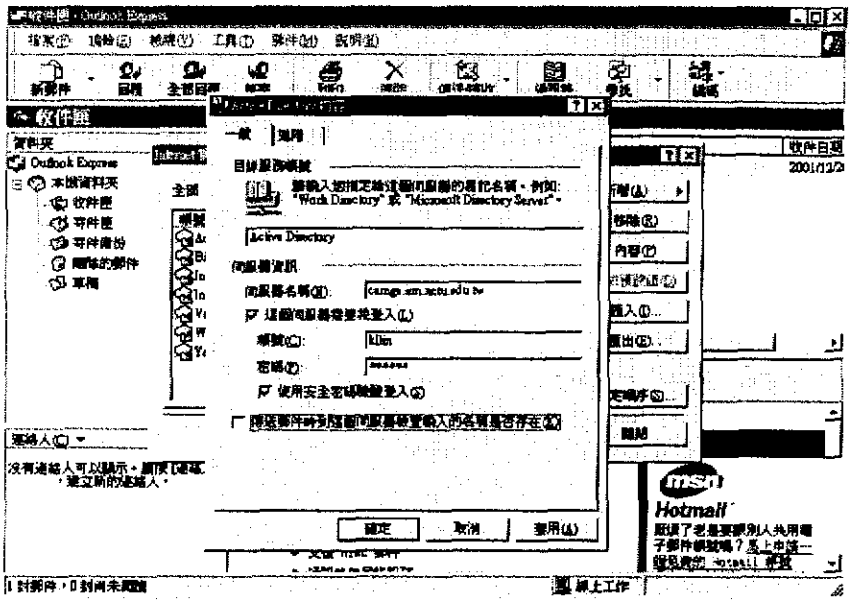
除了可以使用自己的憑證為自己的電子郵件簽名外，我們也可以使用其他使用者的憑證來為寄給這位使用者的電子郵件加密。因為在 CA 的架構中，發行新的憑證後，都會將這些憑證放置於目錄伺服器中，所以使用者想要取得他人的憑證，可以透過以下的方法來取得其他使用者的數位憑證。要使用目錄服務，首先要有能提供搜尋功能的軟體，而最常見的就是 Outlook Express，所以我們就以 Outlook Express 來說明。

1. 設定目錄服務帳號

   Outlook Express 設定帳號的功能可以設定多種服務的帳號，有一項是目錄服務。在目錄服務中有許多預設的帳號，我們可以選擇其中的一項：Active Directory 來修改。

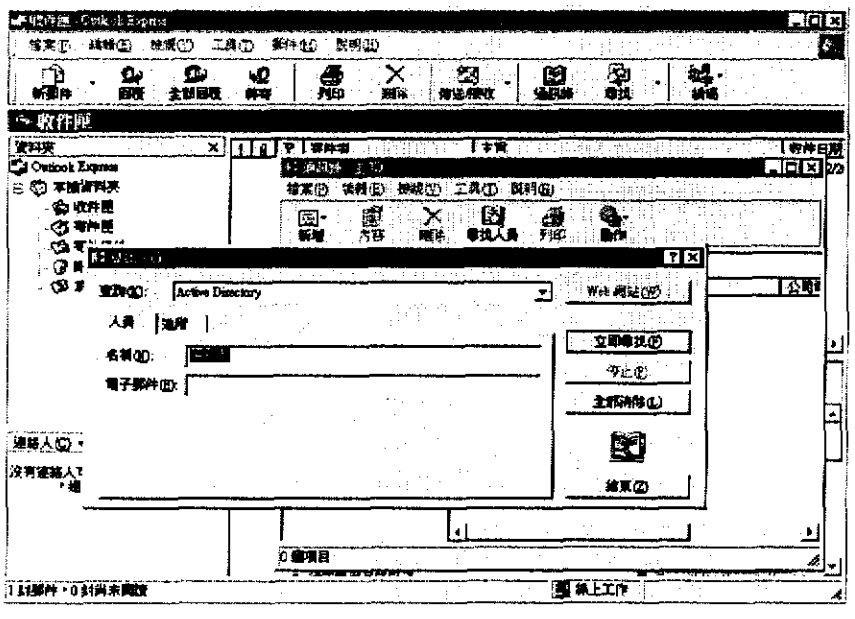


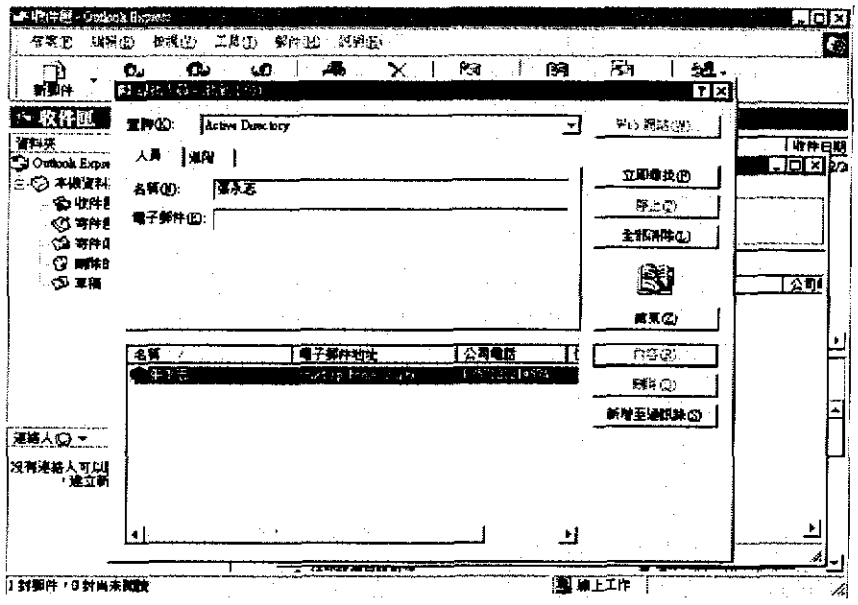
先設定目錄伺服器的位置及你自己的帳號密碼(依目錄伺服器的設定而可能有所不同)，將資料鍵入完成後，按確定即完成設定。



2. 搜尋收件者

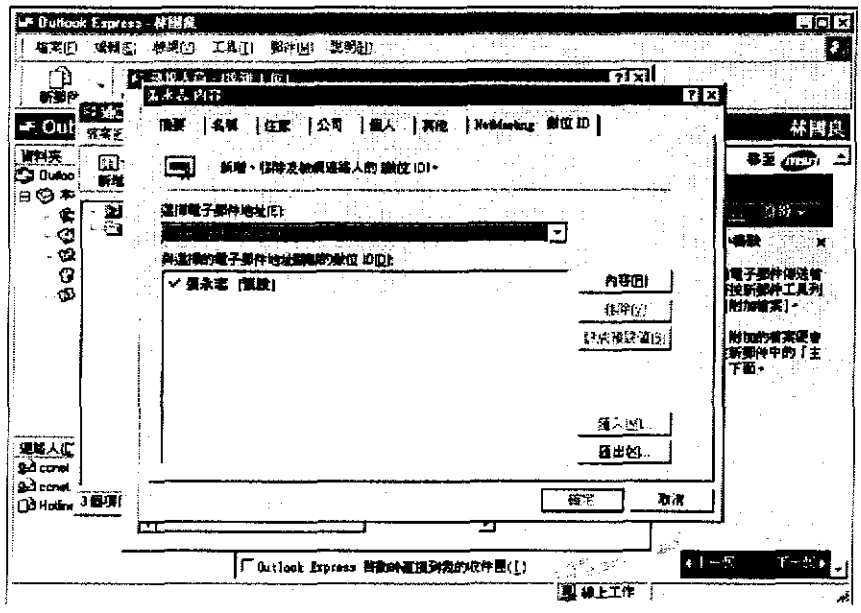
若要透過目錄伺服器來搜尋使用者，我們可以選擇通訊錄中的尋找人員的圖示，並將查詢內的選項內通訊錄改為 Active Directory，接下來再打入搜尋的條件，就可以找到這名使用者的資料了（如果他有登記在目錄伺服器上）。





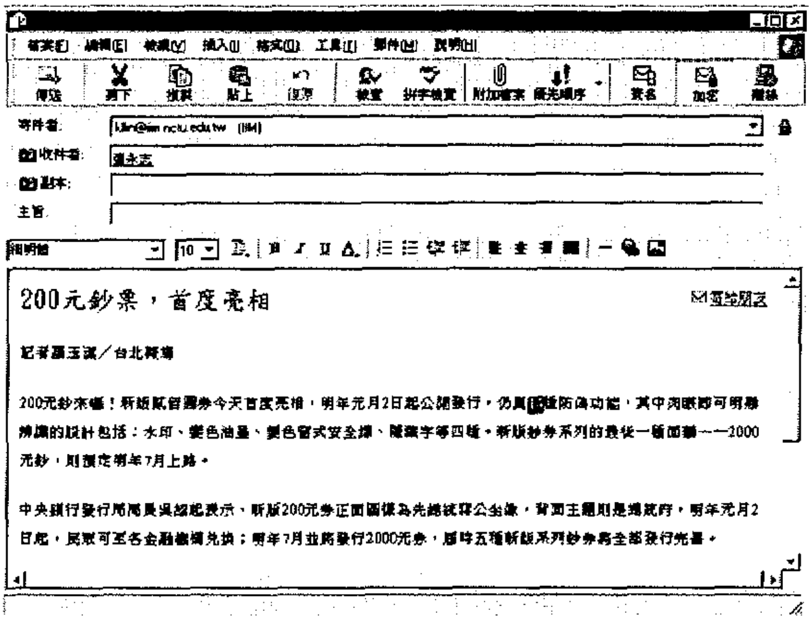
3. 取得數位憑證

點選搜尋到的資料，我們就可以看到這位使用者的資料及其數位憑證，只要找到收件者的數位憑證，我們就可以使用憑證內的公開金鑰來加密電子郵件。在“摘要”這個項目中有一個選項是新增至通訊錄，只要點選了這項，我們的通訊錄中就會增加這筆資料（包含數位憑證）。



4. 發送加密電子郵件

經過以上的動作後，我們已經有了這位使用者的 Email 帳號及數位憑證了，我們現在就可以寄發加密後的電子郵件給這個使用者，因為加密是使用這個憑證內的公開金鑰，所以只有擁有私密金鑰的人才能夠閱讀這封加密後的電子郵件。


200元鈔票，首度亮相
記者羅玉潔／台北報導
200元鈔來囉！新版新臺幣券今天首度亮相，明年元月2日起公開發行，仍具有多種防偽功能，其中肉眼即可明顯辨識的設計包括：水印、變色油墨、變色窗式安全線、隱藏字等四種。新版鈔券系列的最後一個面額——2000元鈔，則預定明年7月上路。
中央銀行發行局局長吳紹起表示，新版200元券正面圖像為先總統蔣公坐像，背面主題則是總統府，明年元月2日起，民眾可至各金融機構兌換；明年7月並將發行2000元券，屆時五種新版系列鈔券將全部發行完畢。

六、結論

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份驗證的問題，換言之，只要身份驗證問題能解決，網路安全問題也將可迎刃而解。由 CCITT 在 1993 年所提出的 X.509 協定為目前網路最有效的安全解決方式，本計畫主要以探討海軍組織內部對於認證中心的需求，來建置一個海軍認證中心的雛型系統。

本計畫針對國軍資訊網路與海軍組織的作業流程設計了一套新的憑證申請、展期、廢止機制的流程，並特別針對金鑰的產製與 IC 卡進行結合，將可大幅加強了海軍公開金鑰基礎建設整個架構的安全性，可作為往後海軍建置公開金鑰基礎建設的基礎。本計畫詳細地說明了憑證資訊系統的架構與各子系統的間的關係，並且也指出現行電子化政府憑證管理中心安全缺失，無法適用於國軍的特殊安全需求。到目前為止，我們的成果包括完成憑證管理資訊系統、註冊管理系統、和目錄服務系統。此外我們也研究探討「電子簽章法」等相關的法律問題。希望能在往後對國軍推行認證中心時，能提供一個參考的資料。

參考文獻

[1]. 樊國楨，電子商務高階安全防護－公開金鑰密碼資訊系統安全原理，1997 年 10 月初版，財團法人資訊工業策進會 資訊與電腦出版社。

[2]. 陳昱仁，電子資料傳輸安全機制之研究，1999 年，交通大學資訊管理所未出版博士論文

[3]. 中華電信研究所http://www.chttl.com.tw/forum/ca

[4]. 政府憑證管理中心網站 http://www.pki.gov.tw/

[5]. http://www.openssl.org/

[6]. ITU-T Recommendation X.500 (ISO/IEC 9594-1) (1993 E), Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services.

[7]. Netscape Directory Server Administrator' s Guide for Windows NT, Netscape Communications Corporation, 1996.

[8]. S. Kent, Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based Key Management, RFC 1422, IAB 1993

[9]. Miller, S., "Civilizing Cyberspace", ACM Press, 1996

[10]. Crocker, D. H., "Internet System Books", Addison-Wesley, 1993

[11]. Chapman, D.B. and Zwicky E., "Building Internet Firewalls", O' Reilly & Associates Inc., 1995

[12]. S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", April 1989, Computer Communications Review, vol. 19, no. 2, pp. 32-48.

[13]. Charlie Kaufman, Radia Perlman, Mike Speciner "Network Security" 1995

[14]. Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", 3/10/1998,

[15]. C. Rigney, A. Rubens, W. A. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)." RFC 2058, January 1997

[16]. www.firsttaiwan.com.tw/stock/caqa.htm

附錄 A：系統環境說明

整個認證中心雛形系統的環境如下所說明：

RA 伺服器

因為 RA 伺服器是一台位於網路上的電腦，所以在安全方面要比較多考量，為了避免駭客透過網路以作業系統以及伺服器軟體的漏洞來入侵伺服器而危害整個系統，故使用 Open Source 的作業系統及網頁伺服器軟。

作業系統	Linux RedHat 7.2
網頁伺服器	Apache 1.3.22

認證伺服器

因為認證伺服器是一台離線的電腦，所以不需要顧慮到網路安全的問題，再加上要與 Smart Card 作搭配整合，所以可以使用較為方便易用的 Windows 系統，而 Smart Card 則使用最為通用普及的 GemPlus 公司所出的 GemSAFE Enterprise Smart Card 套件。

作業系統	Windows 2000 Advance Server + SP2
Smart Card	GemSAFE Enterprise
網頁伺服器	IIS 5.0 + Service Pack

目錄伺服器

目錄伺服器主要的目的是要讓所有使用者能夠查詢到其他使用者的數位憑證及其他資料，為了方便起見，我們使用 Windows 2000 做為這方面的作業系統。

作業系統	Windows 2000 Advance Server + SP2
目錄伺服器	Microsoft Active Directory

附錄 B：政府憑證管理中心管理辦法

1. 安全控管

政府憑證管理中心之營運安全控管體系，分為系統安全、通信安全、人員管制及作業管制。

1.1 系統安全

本中心之系統安全措施包括設置獨立機房、門禁管制、防火、防磁、防震、防水、防盜、溫度控制、濕度控制、獨立電源迴路、電源備援能力、不斷電系統及監視系統等。

（1）電源

市電供電採雙迴路，並設有柴油發電機及不中斷電源系統，提供最佳穩定供電源，系統無斷電之虞。

（2）空調

提供中央空調冰水機及恆溫恆濕箱型空調系統，並引進新鮮空氣，確保機房具最佳運作環境。

（3）防電磁干擾

磁帶、磁碟及其他磁性媒體應予保護免於磁場之影響。設備受保護免於靜電影響，例如人造地毯會引致靜電。

（4）防止侵入

電腦系統具有防火牆設置，在工作區域內的電腦作嚴格的管制，非經授權許可絕不可動用。且電腦的登入登出均有詳細的記錄，以減少未經授權接取的風險。

（5）門禁

電信機房一向是警衛森嚴，本憑證管理中心的門禁要比一般電信機房更為嚴密，不僅有層層的警衛人員管制，更有嚴密的監控措施，例如個人密碼門鎖及進出錄影監視設備等，足資信賴。

（6）其他

本中心係設置於中華電信之電信機房，其各項防護措施諸如防火警

報、滅火設施、防盜警報、防天災等一應俱全。各項防護設備均定期維護保養，在任何時間均保持最佳之運轉狀態。機器維運與障礙申告維運日誌等，工作人員均依規定記錄，以利查核。

1.1.1 操作之安全

本憑證管理中心設備操作遵循以下原則：

（1）服務及維護

與軟硬體設備供應廠商簽訂維護合約，以維護設備正常運作。

（2）資料存檔與備援

依照"憑證管理中心營運安全作業流程"執行原始備援複製。其目的在確保資料安全，即確保正常運作所需資料不致漏失。適當的資料備援，將使因環境更佚、設備故障或操作失誤，所造成之資料漏失，得以及時恢復正常。該作業流程應明訂人員責任、時間排程表、儲存環境、儲存媒體、儲存位置、備份執行程序及回復處理程序等。資料備份原則如下：

- 每星期對整體相關資料庫作備援複製。
- 每天對相關資料庫作遞增式備份〈Incremental Backup〉。

原始備援複製之儲存位置與原始文件儲存位置分開。建立資料備援處理之書面文件， 作為資料備援之依據。

（3）待機設備

為儘可能消除因嚴重設備故障引起之長久當機時間，資料經過備份，並且準備適合之待機設備、適當處理程序及人員純熟訓練。

1.1.2 文件內容的安全

（1）授權

有關授權收/發電子文件、讀取/複製、檢查/認可、修正/廢止電子文件，均依照“憑證管理中心營運安全作業流程“以達一定程度之安全保證。每位經授權人員必須有唯一識別密碼，並由權責主管認可其授權程度且指派專人管理。

（2）警示用語

遵照個人資料保護法、國家機密保護辦法及軍方相關法令，將每一份相關文件加註警示用語，此警示用語附加於任何實體之儲存媒體等記錄文

件上。當在通訊媒體上傳輸時，此警示用語出現在資料檔的起始及結束處。

1.2 通信安全

1.2.1 安全協定檢查

依照「憑證管理中心營運安全作業流程」，檢查所傳送資料規則，確定資料已定義之輸入或輸出形式，並符合相關各個安全協定的檢驗。

1.2.2 資料傳送保護

對傳送的資料均以加密方式提供適當的保護，輸出資料為已定義之形式。

1.2.3 稽核

建立獨立且完整的進、出記錄等稽核追蹤體系。

1.3 人員管制

1.3.1 人力配置

本憑證管理中心之人力配置依服務範圍及客戶端數量之成長，增加所需之人力。

1.3.2 人員資格審定

本憑證管理中心對於系統管理者及相關工程人員皆在初任時予以資格審查，且每年予以複查，若無法通過審查之人員，則調離其職，改派其他符合資格人選擔任。

1.4 作業管制

1.4.1 系統維運作業

系統維運作業包括：

(1) 例行維護作業。

(2) 障礙之處理。

(3) 系統儲存媒介之管理。

(4) 備援作業管理。

(5) 電源、空調等設備及防火系統檢測。

(6) 機房報表、工作日誌記載。

1.4.2 危機處理作業

危機處理作業包括：

(1) 災難、應變及復原程序。

(2) 駭客侵入後之緊急處理，及追蹤防制作業。

(3) 病毒感染後之清除及復原作業。

1.4.3 安全稽核作業

本中心建立獨立且完整的進、出記錄營運安全作業過程等稽核追蹤體系，定期稽核並提交安全稽核報告。本憑證管理中心於電腦設備安裝偵測軟體，裝設錄影系統，並對作業系統與應用軟體之安全執行管制。定期查核門禁管理、使用日誌、使用授權等之適當性。

附錄 C：行政院所屬各機關資訊機構設置要點

壹、 目的：

本院為使所屬各級機關研訂、修正或審核其資訊機構之組織及員額有所準據，特訂定本要點。

貳、 資訊機構之型態：

一、 資訊機構之設置，區分為機關型態及單位型態兩種。

二、 以單位型態設置，區分為正式建制單位及臨時任務編組兩種，

前者應循法定程序修訂其組織法規設置；後者應經權責機關核准設置之。

參、 資訊機構之任務：

一、 關於資訊業務之策劃、督導、協調、審查及管理，或資訊系統之設計及資料處理等事項。

二、 關於資訊系統之管理及維護事項。

三、 關於資訊應用之教育訓練與諮詢服務事項。

四、 關於辦公室自動化之規劃、協調與推動事項。

五、 其他有關資訊業務事項。

肆、 資訊機構之設置原則：

一、 以機關型態設置者稱為「資訊中心」，應視主管機關之組織型態及任務，訂定其組織法規。以單位型態設置者，依其機關層級，比照機關內部相當層級之單位名稱訂定，如與各部會內部之司處相當層級者稱「資訊處」，與各科室相當層級者稱「資訊室」，與股（課）相當層級者稱資訊股（課），先以臨時任務編組方式設置者稱為「資訊小組」。

二、 各主管機關設有機關型態之資訊機構者，應設置主機系統，負責承辦其主管機關之資訊業務，並綜理、督導、協調、考核及支援其所屬各機關資訊業務。

三、 各主管機關未設有資訊機構者，得視業務需要，報經權責機關核准設置單

位型態之資訊機構。

四、 各機關在新設單位型態之資訊機構時，應就現有可運用之人力，先以臨時任務編組方式設置為原則，但如中長程資訊計畫已奉核定者，得循機關組織法規修訂程序，報請設置資訊單位。

五、 各機關資訊系統之規劃、分析、設計等事宜，如本機關尚無資訊專業人員，或專業人員不足，應以洽請其他機關支援或委託民間承包為原則。

六、 各資訊機構視業務需要得置分析設計人員、系統管理人員及系統操作人員。

伍、 資訊機構之等級區分：

以單位型態設置之資訊機構，其等級區分如左：

資訊單位	設置標準			備考
編制等級	機關層級	任務	設備	
甲級資訊單位	須為本院各部會處局署及其附屬機關（即中央三級以上機關）或省市政府各廳處局及其附屬機關（即地方三級以上機關）之內部一級單位。	負責統籌規劃本機關及直屬機關資訊業務及協調督導有關機關資訊業務。	中型以上電腦系統設備。	一、所稱各部會處局署及其附屬機關〈均含相當層級機關〉之內部一級單位，係如：如內政部之 各司處室及內署之各組室。 二、所稱省市政府各廳處局及其附屬機關〈均含相當層級機關〉之內部一級單位，係如：臺灣省 政府財政廳之各科室及財政廳所屬臺灣省稅務局之各組室。
乙級資訊單位	須為本院各部會處局署、省市	負責統籌規劃本機關及直屬	小型以上電腦系統	一、所稱本院各部會處局署、省市政府暨其所屬各級

	政府暨其所屬各級附屬機關之內部一級單位或內部二級單位。	機關資訊業務及協調督導有關機關資訊業務。	設備。	附屬機關，指中央及地方各級機關，不分機關層級。
丙級資訊單位	須為本院各部會處局署、省市政府暨其所屬各級附屬機關之內部二級單位或內部二級以下單位。	負責規劃處理本機關資訊業務。	小型以上電腦系統或個人電腦網路設備。	以臨時任務編組為原則。

陸、 資訊機構分部門辦事：

一、以單位型態設置之資訊機構得視業務資料量、功能區分、作業型態、工作對象及工作人員之多寡，依左列規定分部門辦事：

（一）甲級資訊單位：分「規劃及設計」、「資料管理」、「操作」等三部門辦事或分「規劃及設計」、「資料管理」、「操作」、「訓練」等四部門辦事。

（二）乙級資訊單位，分「規劃及設計」、「資料管理及操作」等二部門辦事，或分「規劃及設計」、「資料管理」、「操作」等三部門辦事。

（三）丙級資訊單位，分為「設計及維護」、「操作及資料管理」二部門辦事，作業型態單純者，不分部門辦事。

但為因應業務特性，得按系統應用區分（如計畫、技術、稽核、應用等），或按混合方式區分（如系統設計、推廣、資料管理等），經專案核准者，不受前項之限制。

二、資訊機構各部門之分工掌理事項表，如附表一。

柒、資訊機構人員之職稱及官職等：

一、各機關資訊人員之職稱，除主管職務外，依其業務需要，得就左列選用為原則：

（一）分析設計人員：「高級分析師」、「分析師」、「設計師」、「助理設計師」、「設計員」、「系統設計員」、「程式設計員」。

（二）系統管理人員：「高級管理師」、「管理師」、「助理管理師」、「管理員」、「電腦工程員」。

（三）系統操作人員：「操作師」、「助理操作師」、「操作員」。

二、各機關資訊人員之官職等應依考試院核定發布之「職務列等表」訂定。

捌、資訊機構員額配置：

一、以單位型態設置之資訊機構員額配置原則，除情形特殊，得由權責機關專案核定外，依左列規定辦理：

員額配置人數

編制等級區分	主管人員及技術人員	資料登錄人員	備考
甲級資訊單位	四〇人以下	各機關操作終端機之工作人員以機關現有人員	一、員額配置人數含編制內專兼任職人員及聘僱人

		調充為原則，如有大量資料鍵入，仍以儘量外包辦理原則，至已購置有資料打驗輔助機器設備之資訊單位，其人員之計算標準，每台每班以配置鍵入人員一．一人〈含維護管理人員〉為原則。	專兼任職人員及聘僱人員。 二、主管人員及技術人員，在所定上限範圍內視業務情形訂定。 三、「技術人員」係指規劃設計、資料管理及主機操作人員在內，得以聘僱方式進用。 四、「資料登錄人員」係指終端機或輔機操作人員，以約僱方式進用為原則，惟原已納入編制之操作人員，仍准維持。 五、資訊單位之行政人員以機關原有行政人員兼任為限。 六、資訊單位改制為資訊機關時，原有終端機或輔機操作人員維持約僱方式進用，原則不予納編。

二、現有資訊機構，其人員操過上列標準者，以出缺不補方式逐步裁減；其未達此標準者，視財力及業務狀況逐步充實。

玖、各機關擬成立資訊機構時，所需人員應以現有人員選訓轉用為原

則，其擬購置設備時，應同時提報員額編制、人力配置與轉用計畫。

拾、各機關新訂或修正其資訊機構編制、等級或員額時，應檢附「行政院所屬各機關資訊機構新訂、修正員額編制請核單」（如附表二）及有關資料，循組織修編程序辦理。

拾壹、各機關報經核准之資訊員額，應依照計畫進度進用，不得流用。

拾貳、各主管機關應定期檢討所屬資訊機構之業務與人力運用績效，如有人力節餘，應即修正機關編制或減列預算員額。

拾參、公營事業機構及學校設立資訊機構時，參照本要點之規定辦理。

拾肆、本要點未規定事項，依其他有關法令規定辦理。

附錄 D：資料庫設計（本計畫使用 open source My SQL 資料庫系統)

對於整個計畫在資料庫設計上， 我們將會設計出四個資料庫分別儲存使用者申請憑證、展期憑證、廢止憑證者以及 RAO 操作員資料庫管理系統。我們將以 MySQL 作為實作資料庫系統的平台。表一為在 MySQL 上我們實作時的資料庫以及資料庫管理者帳號的相關資料。

其中主要是實作出二個資料庫，ra_operator 以及 CERT_DB。在 ra_operator 資料庫中我們 create 一個 table 叫 operator，主要是作為 RAO 操作人員的資料庫管理用。在 CERT_DB 資料庫中實作 table ENROLL、RENEW、REVOKE。主要用來儲存申請者的輸入資料包括：申請憑證者（ENROLL 如表二）、展期憑證者（RENEW 如表三）、廢止憑證者（REVOKE 表四）。

在 ENROLL、RENEW、REVOKE 三個 table 的設計上，其實在資料庫裡的欄位，三者都是一樣的。主是原因是當申請憑證者申請時一定要先在 web 上填好資料到各個資料中並儲存到 ENROLL。而如果有使用者想展期憑證，此時 web 會要求輸入當初輸入到 ENROLL 中的身份証字號以及 PIN 碼。Web 會根據這二個欄位來對 ENROLL 作搜尋，如之前有申請者就可以將這筆紀錄再另存到 RENEW 這個 table。而同樣的，廢止憑證時，也是 web 會要求輸入當初輸入到 ENROLL 中的身份証字號以及 PIN 碼。Web 會根據這二個欄位來對 ENROLL 作搜尋，如之前有申請者就可以將這筆紀錄再另存到 REVOKE 這個 table。

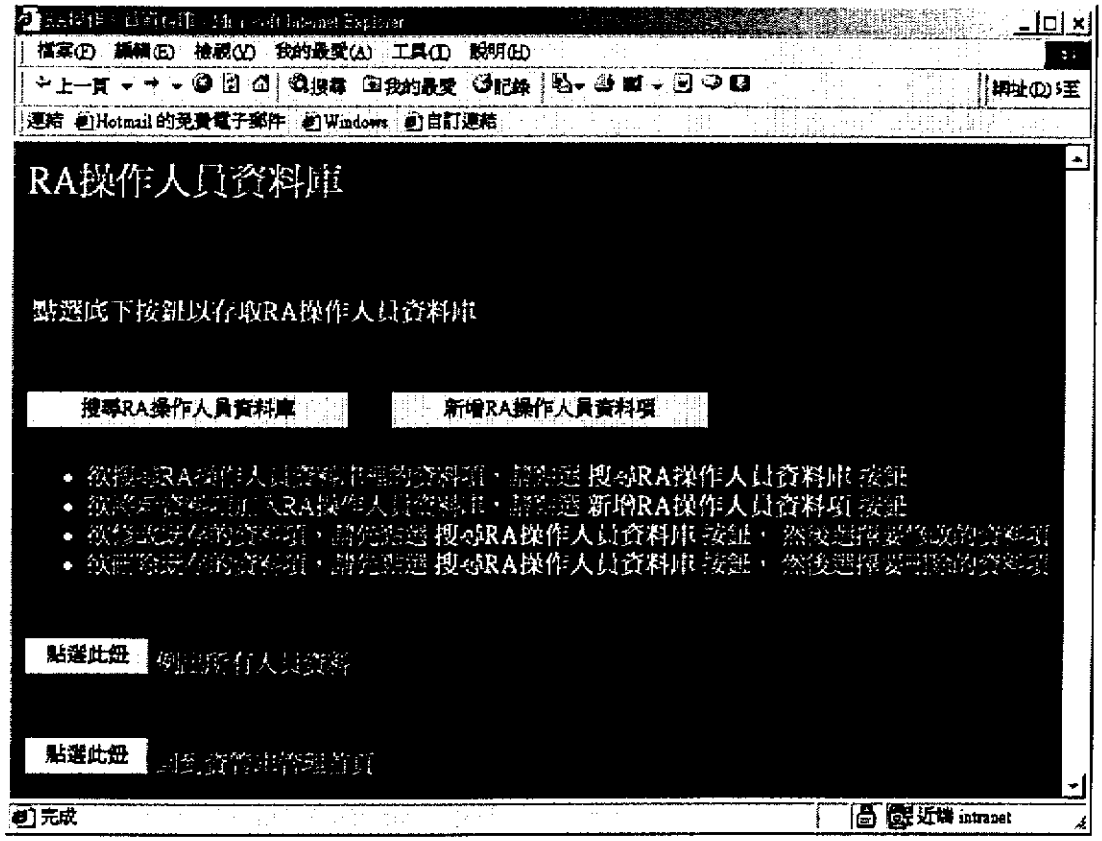
表一、MySQL 資料庫名稱設計及管理者帳號

	RAO 操作員	申請憑證者	展期憑證者	廢止憑證者
資料庫名稱	ra_operator	CERT_DB	CERT_DB	CERT_DB
資料庫 Table	operator	ENROLL	RENEW	REVOKE1
資料庫管理者登入帳號	ra	ra	ra	ra
資料庫管理者登入密碼	ra	ra	ra	ra
資料庫系統 ROOT	root	root	root	root
資料庫系統 ROOT 密碼	ca2000	ca2000	ca2000	ca2000

表二、RAO 操作員資料庫設計 (Table: operator)

欄位	型態	NULL 支援	主要鍵	初始值	備註
PID	varchar(255)	YES		NULL	身份証字號
NAME	varchar(255)	YES		NULL	中文姓名
EMAIL	varchar(255)	YES		NULL	電子信箱
PASSWD	varchar(255)	YES		NULL	PIN
DEP	varchar(255)	YES		NULL	服務單位
POS	varchar(255)	YES		NULL	級職
TELEPHONE	varchar(255)	YES		NULL	聯絡電話
LOGIN_TIME	int(11)	YES		NULL	上站次數
ROWID	int(11)	NO	YES	NULL	auto_increment

圖一、RA 操作員資料庫 WEB 管理畫面

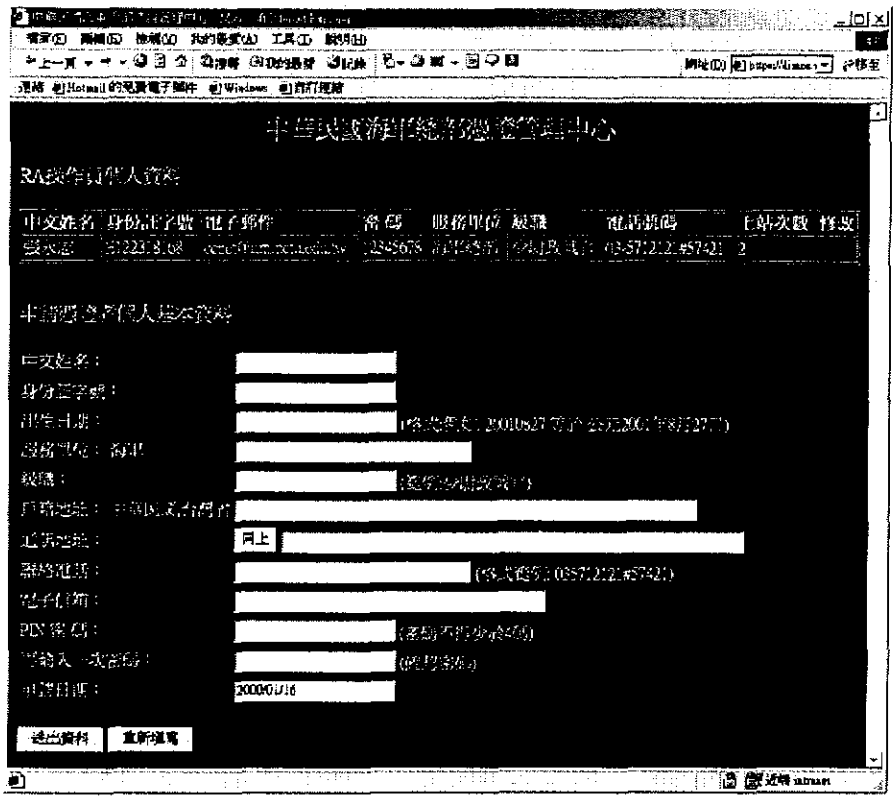


圖二、新增 RA 操作員資料庫 WEB 畫面

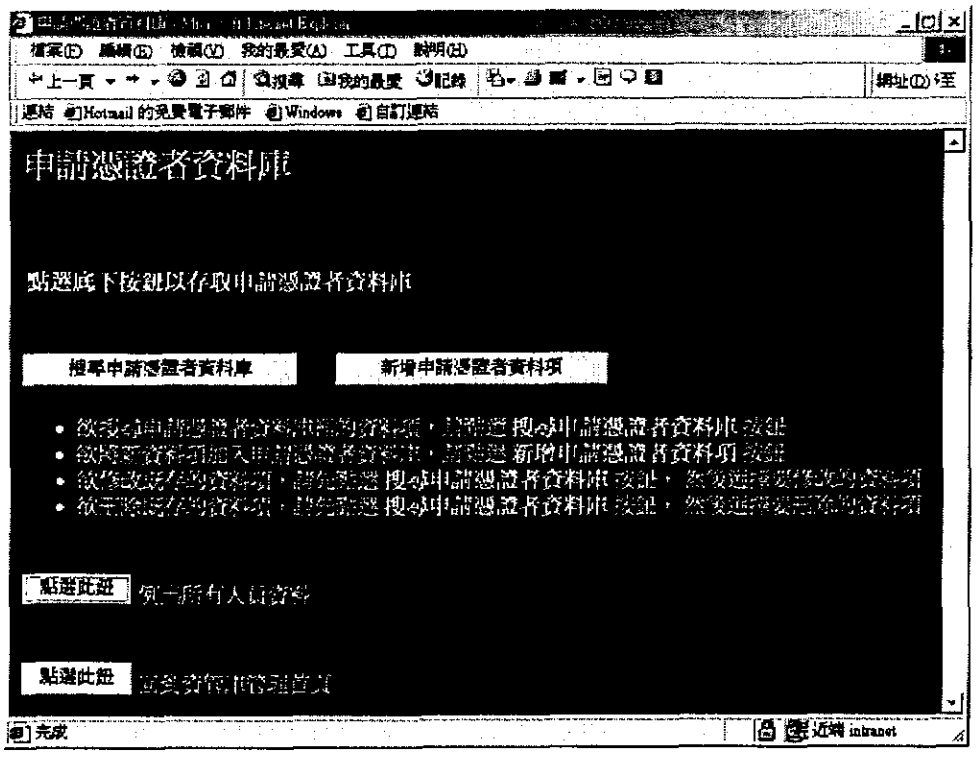
表三、申請憑證者資料庫設計（Table: ENROLL）

欄位	型態	NULL 支援	主要鍵	初始值	備註
PID	varchar(255)	YES		NULL	中文姓名
NAME	varchar(255)	YES		NULL	身份証字號
EMAIL	varchar(255)	YES		NULL	電子信箱
PASSWD	varchar(255)	YES		NULL	PIN
DEP	varchar(255)	YES		NULL	服務單位
POS	varchar(255)	YES		NULL	級職
TELEPHONE	varchar(255)	YES		NULL	聯絡電話
BIRTHDAY	DATE	YES		NULL	出生日期
HOME_ADDR	varchar(255)	YES		NULL	戶籍地址
COMM_ADDR	varchar(255)	YES		NULL	通訊地址
APPLY_DATE	DATE	YES		NULL	申請日期
ROWID	int(11)	NO	YES	NULL	auto_increment

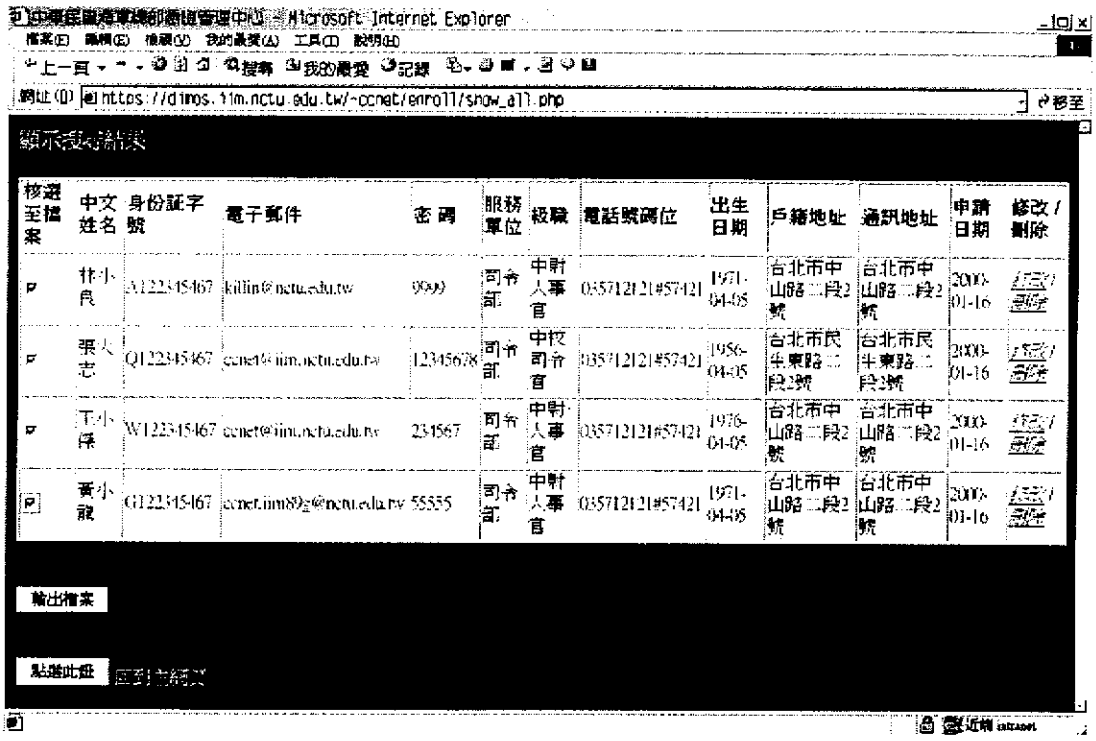
圖三、申請憑証者資料庫 WEB 輸入畫面—RAO 人員輸入資料



圖四、申請憑証者資料庫 WEB 管理畫面



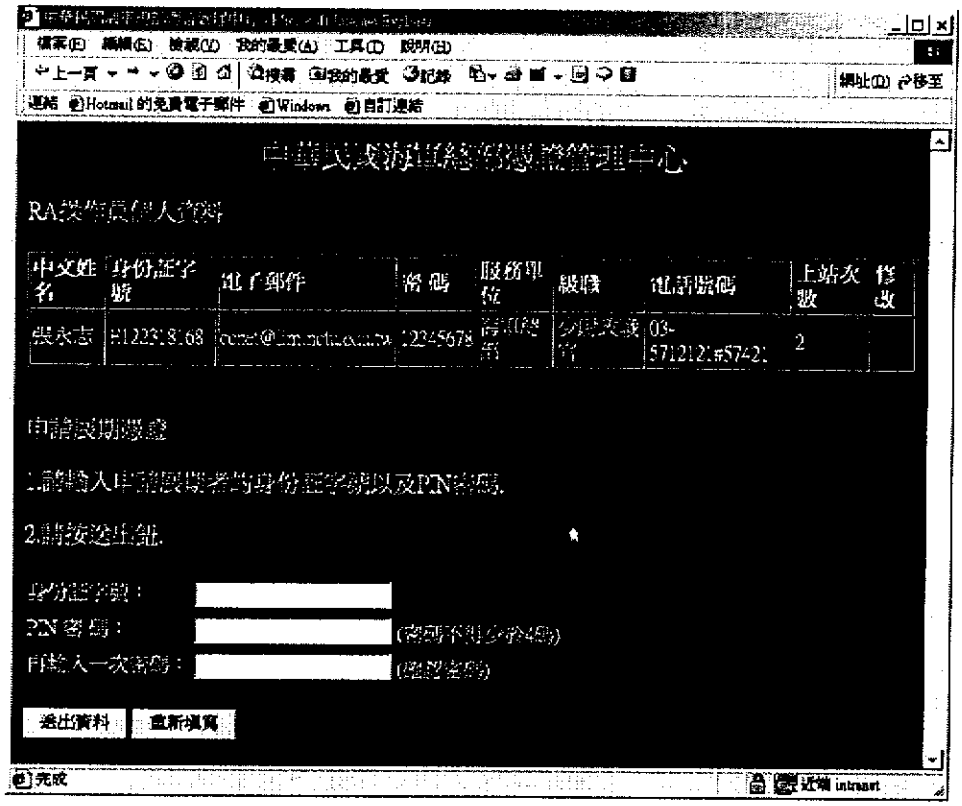
圖五、申請憑証者資料庫管理畫面—勾選人員資料輸出至 enroll.txt.



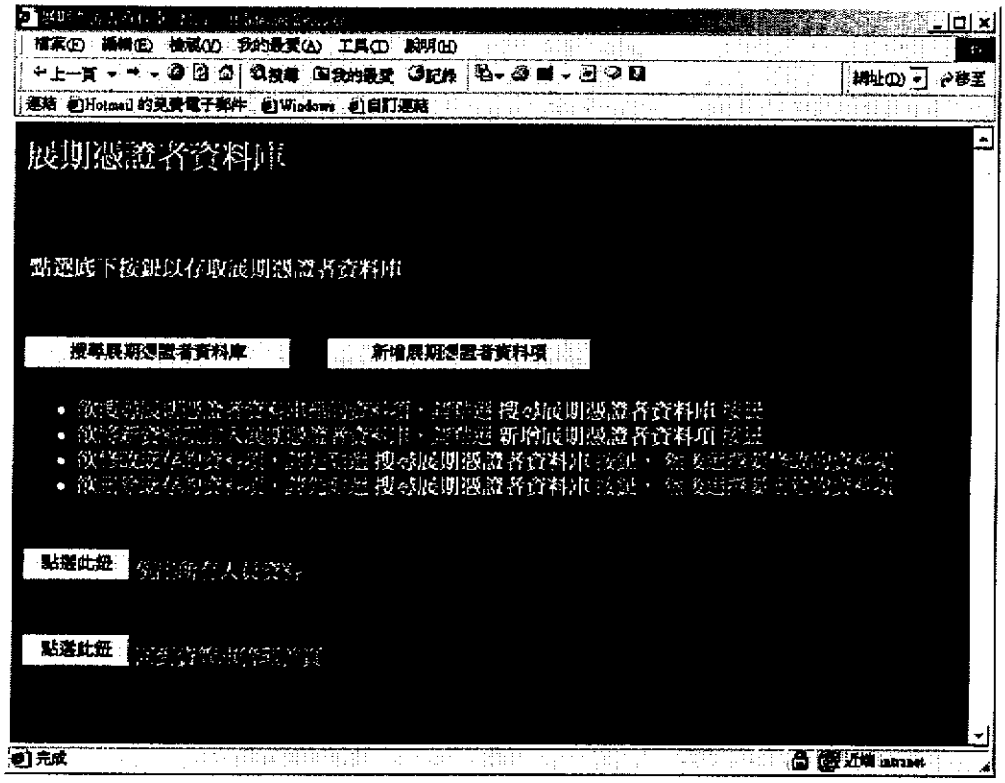
表四、申請展期憑證者資料庫設計（Table: RENEW）

欄位	型態	NULL 支援	主要鍵	初始值	備註
PID	varchar(255)	YES		NULL	中文姓名
NAME	varchar(255)	YES		NULL	身份証字號
EMAIL	varchar(255)	YES		NULL	電子信箱
PASSWD	varchar(255)	YES		NULL	PIN
DEP	varchar(255)	YES		NULL	服務單位
POS	varchar(255)	YES		NULL	級職
TELEPHONE	varchar(255)	YES		NULL	聯絡電話
BIRTHDAY	DATE	YES		NULL	出生日期
HOME_ADDR	varchar(255)	YES		NULL	戶籍地址
COMM_ADDR	varchar(255)	YES		NULL	通訊地址
APPLY_DATE	DATE	YES		NULL	申請日期
ROWID	int(11)	NO	YES	NULL	auto_increment

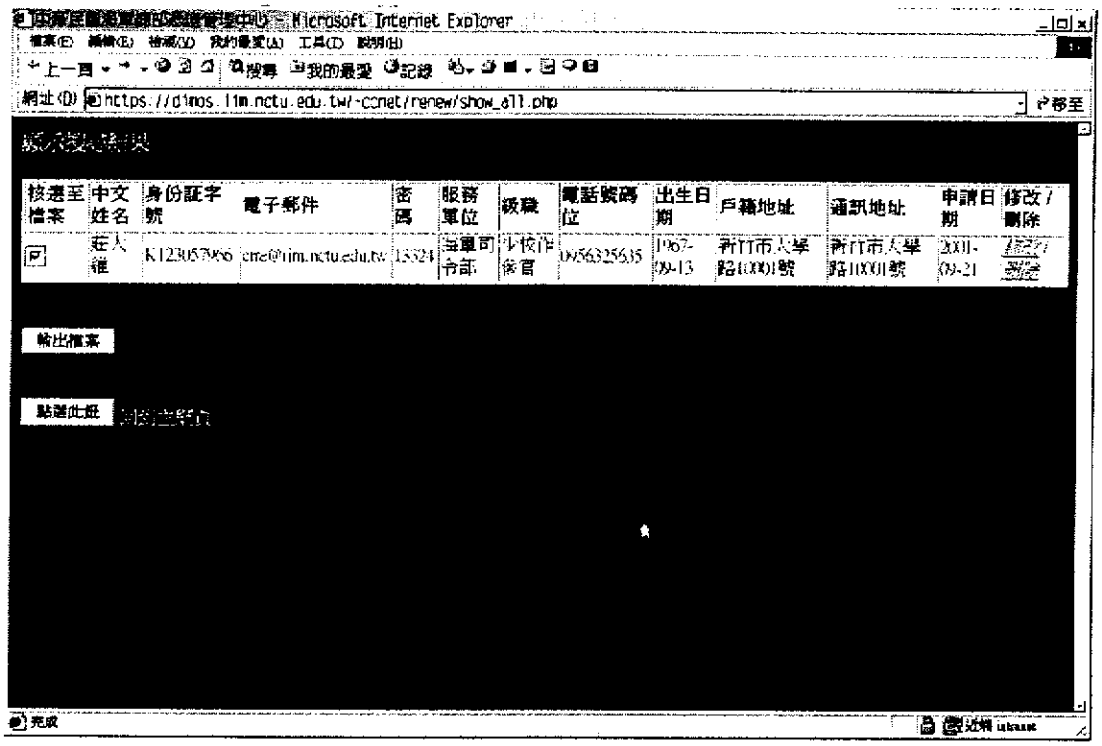
圖五、申請展期憑証者資料庫 WEB 輸入畫面—RAO 人員輸入資料



圖六、申請展期憑証者資料庫 WEB 管理畫面



圖五、展期憑証者資料庫管理畫面—勾選人員資料輸出至 renew.txt



表五、申請廢止憑證者資料庫設計（Table: REVOKE)

欄位	型態	NULL 支援	主要鍵	初始值	備註
PID	varchar(255)	YES		NULL	中文姓名
NAME	varchar(255)	YES		NULL	身份証字號
EMAIL	varchar(255)	YES		NULL	電子信箱
PASSWD	varchar(255)	YES		NULL	PIN
DEP	varchar(255)	YES		NULL	服務單位
POS	varchar(255)	YES		NULL	級職
TELEPHONE	varchar(255)	YES		NULL	聯絡電話
BIRTHDAY	DATE	YES		NULL	出生日期
HOME_ADDR	varchar(255)	YES		NULL	戶籍地址
COMM_ADDR	varchar(255)	YES		NULL	通訊地址
APPLY_DATE	DATE	YES		NULL	申請日期
ROWID	int(11)	NO	YES	NULL	auto_increment

圖七、申請廢止憑証者資料庫 WEB 輸入畫面-- RAO 人員輸入資料

圖八、申請廢止憑証者資料庫 WEB 管理畫面

圖五、廢止憑証者資料庫管理畫面—勾選人員資料輸出至 revoke.txt