

國防科技學術合作協調小組研究計畫成果報告

中華民國海軍目錄服務系統之建置

A Directory Service System for R.O.C. Navy

計畫編號：NSC91-2623-7-009-015

執行期間： 91年 1月 1日至 91年 12月 31日

計畫主持人：交大資管所 陳瑞順副教授

共同主持人：交大資管所 羅濟群教授

執行單位：交通大學資訊管理研究所

中華民國 91年 12月 31日

# 目 錄

一、計劃目標 .....	1
二、問題之背景、現況與需求定義 .....	2
三、研究方法與過程 .....	3
3.1 基本理論與假設.....	3
3.2 運用資料之範圍.....	3
3.3 蒐集資料之過程.....	4
3.4 分析資料之正確性與方法.....	4
四、研究成果 .....	5
4.1 公開金鑰基礎建設(PKI)相關技術探討 .....	5
4.1.1 公開金鑰基礎建設簡介.....	5
4.2 目錄服務(DIRECTORY SERVICE)相關技術探討 .....	7
4.2.1 X.500.....	8
4.2.2 DAP.....	9
4.2.3 LDAP .....	9
4.3 海軍目錄服務系統之建置.....	16
4.3.1 目錄服務伺服器- OpenLDAP Server 的架設.....	16
4.3.2 海軍認證中心目錄服務資料結構的建置.....	17
4.3.3 海軍認證中心目錄服務系統用戶端與伺服器端功能的說明,.....	19
五、海軍認證中心目錄服務系統範本流程 .....	21
5.1 憑證人員資料查詢與下載服務.....	21
5.2 憑證廢止清單下載服務.....	23
5.3 憑證上載服務.....	24
5.4 上載憑證廢止清單.....	26
5.5 憑證刪除服務.....	28
參考資料.....	31
附錄 A：目錄服務系統應用—人事資料目錄服務系統.....	33
A.1 資料結構說明.....	33
A.2 系統功能.....	33
A.3 使用步驟.....	33
附錄 B：使用收信者憑證寄送加密電子郵件範例.....	41

## 表 目 錄

表一、LDAP v3 相關標準文件 .....	15
-------------------------	----

## 圖 目 錄

圖一、公開金鑰基礎建設架構圖（資料來源: [4]） .....	7
圖二、X.500 目錄協定概圖 .....	8
圖三、LDAP 目錄存取協定演進概圖（資料來源: [9]） .....	10
圖四、LDAP 資訊模式示意圖 .....	12
圖五、LDAP 資料定義範例圖（資料來源: [11]） .....	14
圖六、LDAP 命名模式示意圖 .....	14
圖七、LDAP 訊息示意圖 .....	14
圖八、LDAP 安全模式協定示意圖（資料來源: [11]） .....	15

## 一、計劃目標

本計畫擬協助海軍總部建置公開金鑰基礎建設，所面臨目錄查詢的相關課題。將卓參目前所使用的目錄服務的資訊安全技術，歸納出一套適合海軍憑證管理中心作業所需的目錄服務架構，包括憑證資料查詢與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、以及與上層的資訊作業流程與目錄服務應用機制的配合等相關的技術問題也將進行深入的討論，從而加強「海軍公開金鑰基礎建設」憑證管理的效能與安全性。

## 二、問題之背景、現況與需求定義

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，然而通行密碼的安全系統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組織，實是一大弱點。

有鑑於此，海軍總部自 89 年 7 月 1 日至 90 年 12 月 31 日，即委託國立交通大學資管所進行「海軍公開金鑰基礎建設」相關研究與系統開發，以 ITU-T X.509 標準協定為參考，根據海軍的實際需求建立出一套適合海軍的「海軍憑證管理中心」雛形系統，目前皆已獲得初步的研究成果。然而，未來海軍要推動「公開金鑰基礎建設」中，除了憑證管理中心之外，目錄服務亦扮演相當重要的角色。憑證管理中心產生的憑證與憑證註銷清單提供了人們身份認證的服務以及驗證對方身份的機制，然而憑證查詢使用者如果不斷增加，對憑證管理中心造成極大的負荷；因此在 X.509 標準中，定義了目錄服務主要用來存放個人或單位機構的憑證與憑證註銷清單等相關資料，換言之，憑證管理中心所產生的憑證與憑證註銷清單透過目錄服務的方式提供使用者查詢，來減低以及分散憑證管理中心的負擔。

本計畫擬協助海軍總部建置公開金鑰基礎建設，所面臨目錄查詢的相關課題。將卓參目前所使用的目錄服務的資訊安全技術，歸納出一套適合海軍憑證管理中心作業所需的目錄服務架構，以增加海軍公開金鑰基礎建設系統的效能安全性。

## 三、研究方法與過程

### 3.1 基本理論與假設

隨著網際網路的蓬勃發展，資訊量一日千里，使得快速有效，擷取管理各類資訊的問題成為一重要課題，目錄服務需求也就應運而生。此處所談論的目錄，不單只有檔案系統，泛指各種物件，將各種不同物件的資訊儲存在各適當的目錄中，如此一來便可透過目錄得到所需的物件與這些物件所提供的服務。目錄服務最早在 X.500 標準中提出，主要為配合憑證管理中心（Certification Authority, CA）運作的網路資料查詢服務，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。目錄服務具有相當好的性質，提供快速的搜尋以及回應，而且樹狀性的資料結構也讓人能對整個目錄服務有整體性的概念，因而可以減低憑證管理中心維護的花費以及管理上的問題。此外，目錄服務所提供的內容可以進一步擴展所有網路應用軟體所需要的類型資訊，所以目錄服務的存在將可提供相同的介面取得各式不同的物件，這種通透性（transparent）將可大幅降低應用程式設計的複雜度，並可為網路服務、應用程式與使用資源的指導原則。

### 3.2 運用資料之範圍

目錄服務實際應用除支援憑證管理中心之外，另外還可以擔任網路存取資料庫，用來組織和索引資訊。因此具有多方面的用途，各用途分述如下：

1. 支援公開金鑰基礎建設：利用 LDAP，可以存放個人或單位機構的憑證與憑證註銷清單等相關資料。而這些資料，受憑證機構(CA)管理，LDAP 提供了可找到其他使用者認證的目錄服務，故可以輔助國家整個公開金鑰基礎建設系統的執行。
2. 電子郵件的位址簿：LDAP 服務之下，只要輸入關鍵字，如對方的姓名、職業別，工作組織等就可以輕易的查詢網路資料庫，得到對方的網站或是 email。這種直接由協定支援的網址定位，可以提供比現有的查詢介面

更快速而方便的服務。

3. 線上的企業電話目錄：LDAP 服務，每個 entry 不單只有個人資料，也可包含單位機構資料，因此企業電話、FAX 號碼等企業資料也可以放 LDAP 目錄服務資料庫。
4. 定位檔案伺服器、印表伺服器和其他網路服務：
5. 提供多群組、多地點單一使用名稱和密碼簽入(Log-in)功能：讓使用者或是管理者皆可獲致簡易和便利性的好處，對管理者而言，可將網路上所有 client 端的帳戶及密碼作統一的新增、刪除、修改等管理，不再需要逐一對分散於各處的使用者資料庫進行維護。因此其主要目標將針對中大型以上企業或使用單位，而多平台使用環境以及跨地區、國家的用戶將成為首要推展使用目標。

### 3.3 蒐集資料之過程

本計劃將參卓海軍總部自 89 年 7 月 1 日至 90 年 12 月 31 日，委託國立交通大學資管所進行「海軍公開金鑰基礎建設」相關研究與系統開發，根據海軍的實際需求建立出一套適合海軍的「海軍憑證管理中心」雛形系統，所獲得初步的研究成果。並廣泛收集國內外相關研究文獻與各標準規範進行研讀與比較。

### 3.4 分析資料之正確性與方法

1. 探討目錄服務協定標準，包括
  - X.500
  - DAP
  - LDAP
2. 探討「海軍憑證管理中心」下目錄服務整體架構與系統實作。
  - 目錄服務系統之規劃與建置
  - 目錄服務系統與金鑰基礎建設之整合應用

## 四、研究成果

### 4.1 公開金鑰基礎建設(PKI)相關技術探討

#### 4.1.1 公開金鑰基礎建設簡介

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[2][5]。

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。

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，而目錄服務主要是用來存放個人或單位機構的憑證與憑證註銷清單等相關資料，以供使用者查詢，來減低與分散憑證管理中心的負擔。

下圖一為公開金鑰基礎建設架構圖，其中左上角所圈選出的部分為憑證管理系統，而右上角所圈選出的部分為目錄服務系統

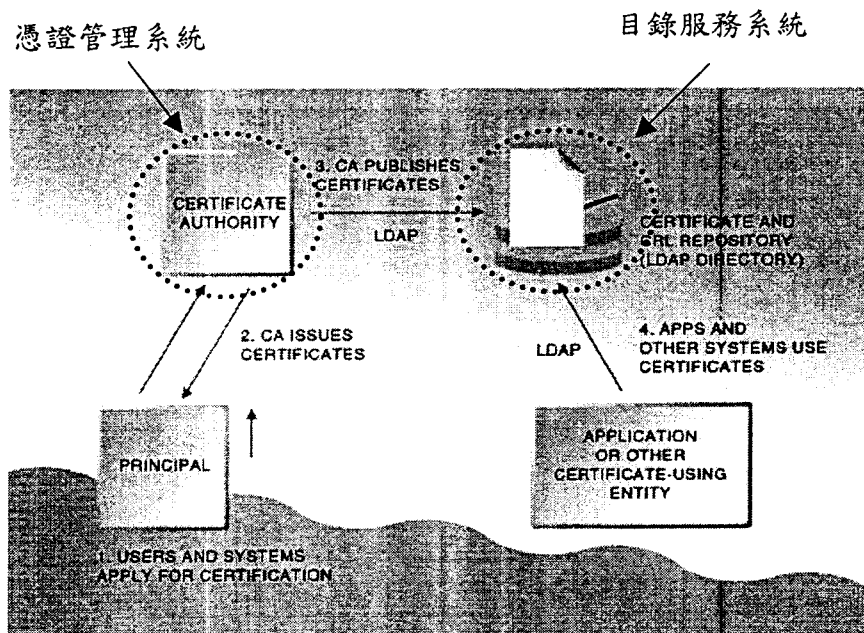
- 憑證管理系統 (CA, Certificate Authority)

指具公信力的第三者，提供認證與憑證簽發管理等服務。在海軍委託國立交通大學資管所進行「海軍公開金鑰基礎建設」相關研究與系統開發中，海軍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。

- 目錄服務系統 (Directory Service)

目錄服務系統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下載等服務。



圖一、公開金鑰基礎建設架構圖 (資料來源: [4])

本計劃所著重的部分即在規劃與實作可運用於海軍公開金鑰基礎建設的目錄服務系統，以增加海軍公開金鑰基礎建設系統的效能與安全性。

## 4.2 目錄服務(Directory Service)相關技術探討

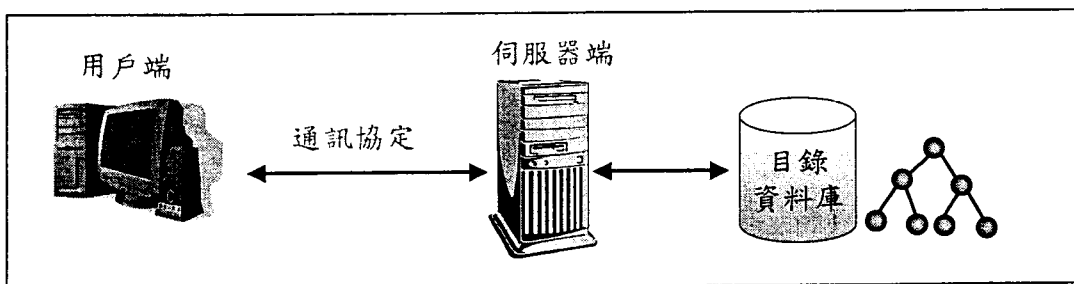
目錄服務為一個特殊的資料庫，其將資料組織並儲存起來，提供一個快速的搜尋機制讓使用者獲得所需的資訊。早在 1986 年，Banyan 便推出目錄服務，而 Novell 也於 1993 年於其 Netware 作業系統附上 NDS(Novell Directory Services)。Internet 上陸續也有許多公司，如：Yahoo、Bigfoot 等都有提供目錄服務，但各

家都用專屬的目錄系統，導致各個目錄服務間無法互通，因而有了將目錄服務標準化的概念[6]。

目錄服務包括「資料儲存的結構」與「擷取的協定」，而目前所採用的目錄服務標準有 X.500、DAP (Directory Access Protocol) 與 LDAP (Lightweight Directory Access Protocol) 三種，分別介紹於後。由於目前目錄服務系統大多採用 LDAP 標準，此章節我們將針對 LDAP 作較詳盡的說明。

#### 4.2.1 X.500

X.500 為最早提出目錄服務的標準，在八十年代中期，兩個不同的團體--CCITT 和 ISO，各自開始在目錄服務方面的研究工作。1988 年，這兩個國際性的目錄規範融合成一個，這就是 X.500。X.500 為一個分散式目錄服務標準[7]，它合併了階層性、物件導向的資訊模組、用戶端至目錄存取通訊協定、目錄服務之間系統通訊協定、與以公開金鑰加密為基礎的驗證機制。1993 年，X.500 的規格中增加了許多功能，支援目錄複製、目錄存取控制和架構發佈與發展[8]。許多廠商逐漸生產出符合 X.500 標準規格的產品；但由於 X.500 標準規格的複雜性，過於耗費系統資源使得實際運作表現並不好，因此沒有很多廠商願意配合加入，如：Microsoft、Netscape、Novell.....等並未支持 X.500 標準規格。



圖二、X.500 目錄協定概圖

X.500 實際上是指 X.500 至 X.521 的一系列標準，目的為建立一個跨平台、

分散式、範圍涵蓋全球的目錄服務。如上圖二所示，整個協定分為三大部分[9]：

1. 伺服器端：制定伺服器端目錄資料庫的規格
2. 用戶端：制定用戶端可具備的功能
3. 通訊協定：以 DAP 進行用戶端與伺服器端間的溝通

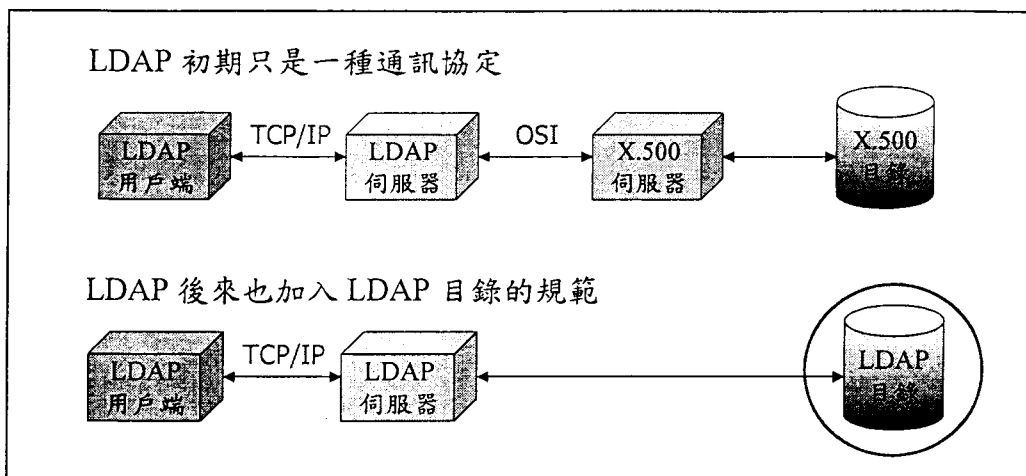
## 4.2.2 DAP

DAP 為 X.500 中所定義的目錄存取協定，其架構在完整的 OSI 七層通訊協定之上。X.519 中定義了目錄服務使用者端（DUA，Directory User Agent）與目錄服務系統端（DSA，Directory System Agent）之間訊息交換的通訊協定。

## 4.2.3 LDAP

### 4.2.3.1 LDAP 簡介

X.500 標準的複雜性使廠商實作出來的產品很少，IETF 的 OSI-DS 工作小組為改善此情況，進行了 X.500 的修正，將之簡單化成一個容易實作的協定，也就是輕量級目錄存取協定-LDAP，LDAP 提供了近 90%當初 X.500 所提供的功能，但卻只有 X.500 約 10%的資源耗用率[6]。LDAP 為 DAP 的精簡版，它簡化 X.500 的通訊協定，降低用戶端的複雜度。如下圖三所示，最初是把 LDAP 當作 X.500 的前端程式而已，後來則逐漸變成以 LDAP 伺服器為主與 LDAP 用戶端彼此相互溝通。在設計上 LDAP 用戶端向 LDAP 伺服器進行目錄資訊的存取；而 LDAP 伺服器則被設計為依據前端的目錄存取需求，向後端的目錄進行各種目錄資訊存取的操作，如：複製（Replica）、參照（Referral）等。如此不但可保留 X.500 的目錄的優點，還可降低整體管理的成本，讓各系統存取目錄服務時更簡便。



圖三、LDAP 目錄存取協定演進概圖 (資料來源: [9])

LDAP 是一個架構在 TCP/IP 上的目錄服務協定，X.500 實作上的困難使其應用範圍一直侷限在較小的部分，一直到 LDAP 的產生才成為目錄服務上廣泛應用的標準。1993 年 7 月，密西根大學開發了第一個 LDAP 規範，也就是 RFC1487，其簡化了 X.500 目錄標準，在功能性、資料表示、編碼和傳輸方面做了修改。目前 LDAP 的版本為第三版，此版本在國際化、命名、安全、擴展性等方面更加完善。LDAP 是由 X.500 所衍生而來，LDAP 與 X.500 中 DAP 間的差異為 LDAP 架構在 TCP/IP 之上，DAP 則是在 OSI 七層協定之上

- LDAP 僅涵蓋重要功能，省略 DAP 中重複或罕用的功能
- LDAP 大部分可使用字串的資料型態

LDAP 的設計以較少的資源就可以存取目錄資訊，其優點為[6][10]

### 1. 使用標準的協定

LDAP 是 IETF 所提出的標準協定，如同 TCP/IP、SMTP、NNTP、SNMP 一般，可與全球遵循此標準的目錄服務主機互通資料。

### 2. 有多種存取權限

LDAP 能選擇將使用者分類，並且提供不同的存取權限，如此可以讓在網路上的資料，既提供開放性，也有一定的保密性。

### 3. 具有編碼的安全功能

LDAP 可以將資料編碼，使得未授權者不能從主機隨意取得資料，藉此以保障使用者隱私權。

#### 4. 分散式架構

LDAP 提供分散式系統的功能，以達到負載平衡 (Load Balance) 與高妥善率 (High Availability) 的服務品質。

#### 5. 快速與簡便的查詢

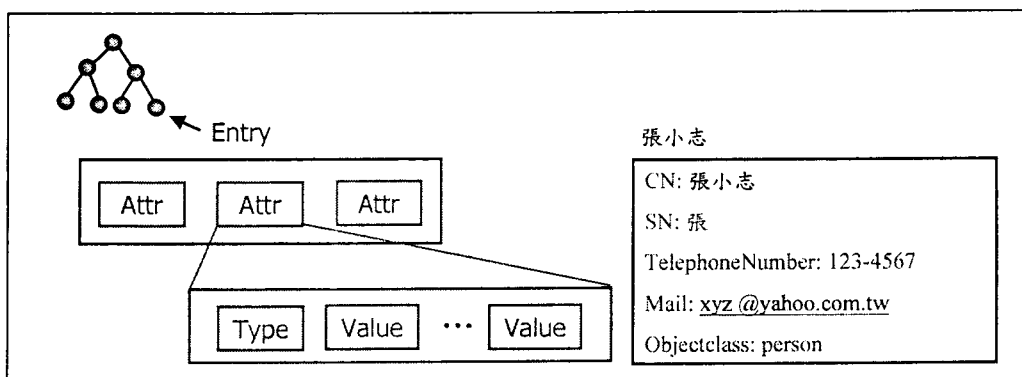
LDAP 提供比傳統資料庫更快速的查詢回應。

### 4.2.3.2 LDAP 標準規格說明

目錄服務為一個特殊的資料庫，以樹狀結構將資料組織並儲存起來，提供一個快速的搜尋機制讓使用者獲得所需的資訊。而 LDAP 提供了存取目錄服務的一個標準協定，它不只定義了存取的方式，也定義了一些資料的架構與格式。基本上 LDAP 內容共可分為四個模式 (model)，分別為資訊模式 (Information Model)、命名模式 (Naming Model)、功能模式 (Function Model) 與安全模式 (Security Model)，分別介紹於後。

#### ● 資訊模式 (Information Model)

資訊模式定義的是 LDAP 的資料架構，LDAP 的每一筆資料稱為一個 entry，而每個 entry 由多個屬性 (attribute) 所構成，而每個屬性則由一個型態 (type) 與多個數值 (value) 所組成，其關係如下圖四所示。



圖四、LDAP 資訊模式示意圖

RFC 2256 定義了 LDAP v3 可辨識的 55 種屬性種類 (attribute types)，以下

列舉其中數種：

- **cn** (common name)
- **sn** (surname)
- **giveName**
- **telephoneNumber**
- **title**
- **o** (organization)
- **ou** (organizational unit)
- **userCertificate**
- **serialNumber**
- **description**
- **objectClass**

RFC 2252 定義了 LDAP v3 的 33 種屬性型態的語法 (syntax)，以下列舉其

中數種：

- **Binary**
- **Bit String**
- **Boolean**
- **Certificate**
- **Telephone Number**
- **JPEG**

#### ● 命名模式 (Naming Model)

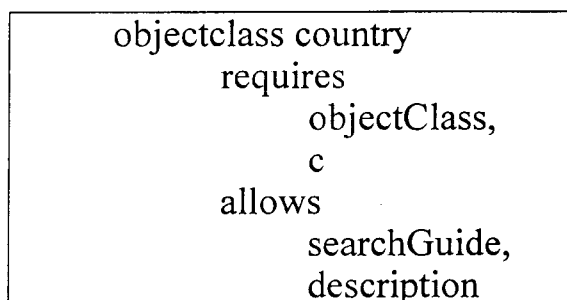
命名模式定義如何分辨出每一筆唯一的資料。LDAP 資料在邏輯上是以一個樹狀結構儲存，如下圖六所示，每一筆在樹狀結構中存在的資料有一個唯一的識別名稱 (DN, Distinguished Name)，每個 DN 最左邊的項目稱為相對識別名稱 (RDN, Relative Distinguished Name)，存取資料時以絕對路徑的方式存取，每個終端節點 (leaf node) 或非終端節點 (nonleaf node) 皆可存放資料。

LDAP 的每一筆資料會屬於一個特殊的物件類別 (object Class)，RFC 2256

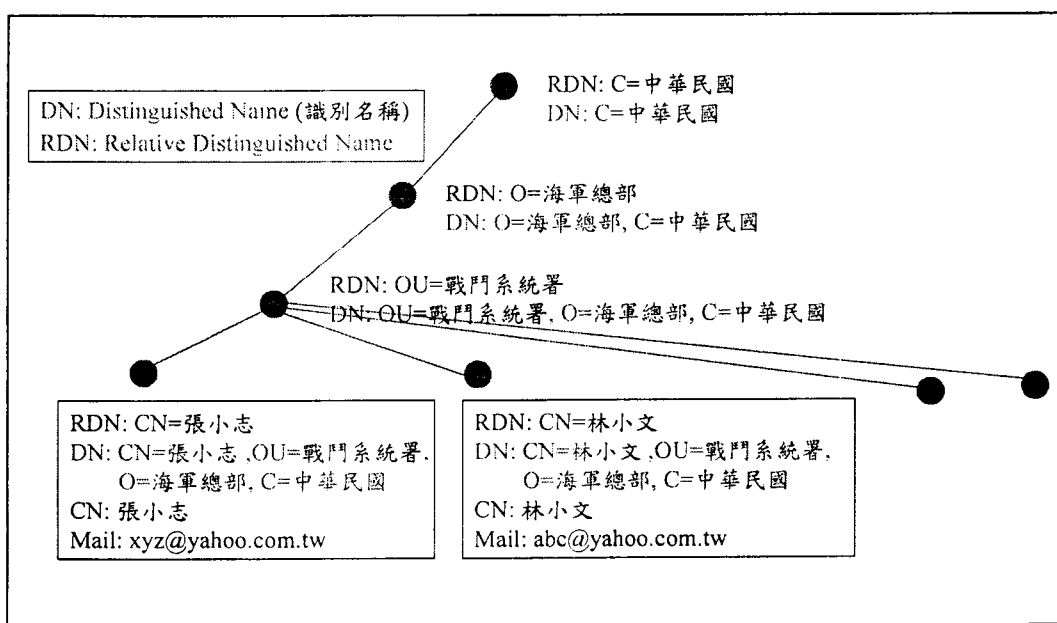
定義了 22 種物件類別 (object Class)，以下列舉其中數種：

- **country**
- **organization**
- **organizationalUnit**
- **person**
- **device**

依物件類別的不同，可以限制其應有的屬性，如：



圖五、LDAP 資料定義範例圖 (資料來源: [11])



圖六、LDAP 命名模式示意圖

- 功能模式 (Functional Model)

功能模式定義 LDAP 提供給使用者的功能，基本上可分為以下三類：

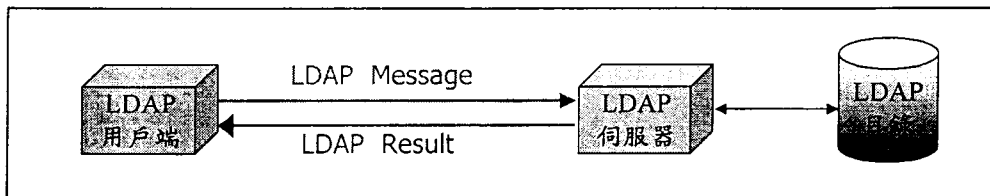
1. 查詢方面：Search、Compare



2.更新方面：Add、Delete、Modify、Modify RDN

3.認證方面：Bind、Unbind、Abandon

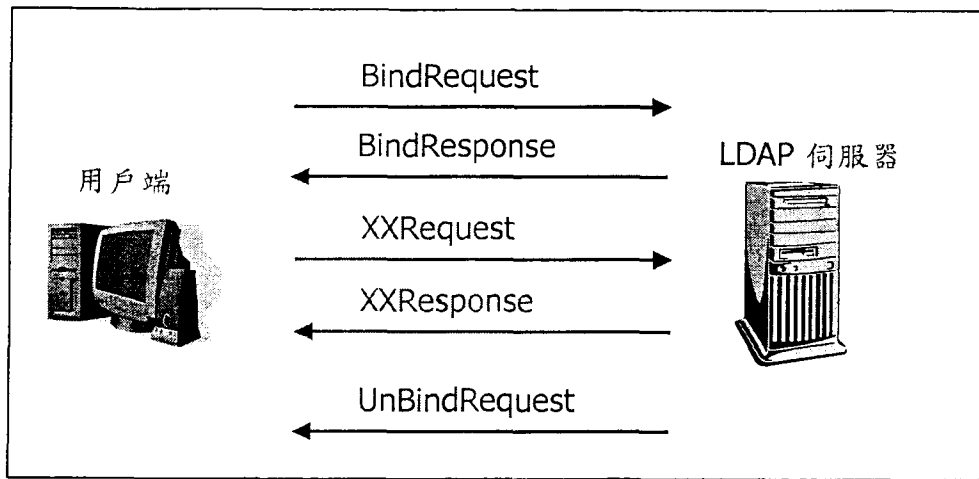
每種功能所定義的訊息通常有兩組，分別由 LDAP Message 與 LDAP Result 定義衍生而來，其訊息格式定義在 RFC 2251 之中。



圖七、LDAP 訊息示意圖

- 安全模式 (Security Model)

安全模式定義 LDAP 伺服器上的安全策略，對於資料作存取控制的機制。用戶端經過身分認證後，即可被授與相對的權利以執行相關的動作；如系統管理者與使用者可被授權而執行動作是不相同的。如圖七所示，用戶端在要求 LDAP 伺服器提供任何服務之前，必須先送出 **BindRequest** 訊息，伺服器在收到 **BindRequest** 訊息後，檢視自己的資料與完成使用者認證後，將 **BindResponse** 訊息回送給用戶端。用戶端在收到 **BindResponse** 訊息後，才真正送出服務請求訊息 **XXRequest**，直到收到服務的回應訊息 **XXResponse** 後，由用戶端送出 **UnBindRequest** 訊息結束此次通訊，使用者也可隨時送出 **Abandon** 訊息終止 LDAP 通訊[11]。



圖八、LDAP 安全模式協定示意圖 (資料來源: [11])

#### 4.2.3.3 LDAP 標準文件

LDAP 協定已被 IETF 接受為一種標準協定，LDAP v2 協定的主要內容規範在 RFC 1777 中，LDAP v3 的內容則規範在 RFC 2251 中，其它 LDAP v3 相關標準文件整理在表一當中。

表一、LDAP v3 相關標準文件

標準文件	內 容
RFC 2251	Lightweight Directory Access Protocol (v3)
RFC 2252	LDAPv3 Attribute Syntax Definitions
RFC 2253	LDAPv3 UTF-8 String Representation of Distinguished Names
RFC 2254	The String Representation of LDAP Search Filters
RFC 2255	The LDAP URL Format
RFC 2256	A Summary of the X.500 User Schema for use with LDAPv3
RFC 2829	Authentication Methods for LDAP
RFC 2830	LDAPv3 Extension for Transport Layer Security

### 4.3 海軍目錄服務系統之建置

## 4.3.1 目錄服務伺服器 - OpenLDAP Server 的架設

### 4.3.1.1 OpenLDAP 目錄服務伺服器軟體的取得

OpenLDAP 係由 OpenLDAP Project Group 所負責撰寫、維護，你可以在以下網址取得完整的程式原始碼：

<http://www.openldap.org/>

由於本系統建構於 Microsoft Windows 平台，故必須取得相對應的 Win32 Binary 版本。你可以自行編譯 OpenLDAP 的程式原始碼來取得，或者到以下網址取得已經編譯好的版本：

<http://www.fivesight.com/downloads/openldap.asp>

### 4.3.1.2 OpenLDAP 安裝步驟

在此我們假設你已取得 OpenLDAP 的 Win32 Binary 版本，無論你是經由以上網站取得、或是自行編譯程式原始碼，都可以依據以下步驟完成安裝動作。：

一、建立可供放置 OpenLDAP 軟體的目錄，例如：

C:\OpenLDAP

二、所有檔案複製到該目錄中

三、開啟 slapd.conf 檔案，進行以下修改動作：

1) 在 Global Setting 中，請將所有目錄資訊修改成目前 OpenLDAP 所在的目錄，例如：

```
pidfile    D:/WorkShop/OpenLDAP/slapd.pid
```

修改成

```
pidfile    C:/OpenLDAP/slapd.pid
```

注意：目錄中所有『\』字元皆必須改成『/』字元

2) 將你所要使用的 schema 加入 Server 設定。例如：

原本 OpenLDAP 只使用了 core.schema，其設定為

```
include    C:/OpenLDAP/schema/core.schema
```

今天我們決定要增加 cosine.schema 與 inetorgperson.schema，則必須修改為

```
include    C:/OpenLDAP/schema/core.schema
```

```
include    C:/OpenLDAP/schema/cosine.schema
```

```
include    C:/OpenLDAP/schema/inetorgperson.schema
```

3) 執行 slapd.exe，此舉將啟動 OpenLDAP Server

## 4.3.2 海軍認證中心目錄服務資料結構的建置

### 4.3.2.1 目錄服務資料結構的特性

在你準備使用目錄服務之前，必須先注意到：

- 一、 目錄服務的資料物件有 ObjectClass 與 Attribute，其中有些 ObjectClass 是有上下層之分的，譬如說，若你要在一筆資料中使用『organizationalPerson』這個 ObjectClass，則你也必須把它の上層 ObjectClass：『Person』也必須存在於這筆資料中。
- 二、 你所可以選擇的所有 ObjectClass 與 Attribute，其詳細的列表、資料與屬性都紀錄在前述的 schema 檔案中，你可以透過修改 OpenLDAP 的設定來增加新的 schema，亦可以自行發展出你自己的 schema 來。
- 三、 你可自由選擇你所要使用的 ObjectClass 與 Attribute，前提是這些 ObjectClass 與 Attribute 都已經包含在 OpenLDAP 所 include 的 schema 檔案之中。

### 4.3.2.2 目錄服務中新增資料的基本步驟

目錄服務的資料結構是樹狀結構，每個節點都必須存有資料。譬如說，你要新增這樣的一筆資料到空白 LDAP 資料集中：

```
dn: cn=海軍士兵 ou=MIS, o=NAVY, c=ROC
objectclass: top
objectclass: country
objectclass: organization
objectclass: organizationalUnit
cn: 海軍士兵
ou: MIS
o: NAVY
c: ROC
```

你新增這筆資料到空白 LDAP 資料集的步驟必須是：

- 一、新增這樣的一筆資料：  
dn: o=NAVY, c=ROC

```
objectclass: top
objectclass: country
objectclass: organization
o: NAVY
c: ROC
```

二、再新增這樣的一筆資料：

```
dn: ou=HeadQuarter, o=NAVY, c=ROC
objectclass: top
objectclass: country
objectclass: organization
objectclass: organizationalUnit
ou: HeadQuarter
o: NAVY
c: ROC
```

三、以上兩筆資料後，你才能新增你方才所指定的資料：

```
dn: cn=海軍士兵 ou=MIS, o=NAVY, c=ROC
objectclass: top
objectclass: country
objectclass: organization
objectclass: organizationalUnit
cn: 海軍士兵
ou: MIS
o: NAVY
c: ROC
```

### 4.3.3 海軍認證中心目錄服務系統用戶端與伺服器端功能的說明，

#### 4.3.3.1 開發工具

本系統採用以下程式開發工具：

一、**J2SDK v1.4.1**

功用：Java2 Software Development Kit, Standard Edition

下載地點：<http://java.sun.com/j2se/1.4/download.html>

二、**Sun ONE Directory SDK for Java 4.1**

功用：LDAP SDK 加上一堆好用的 lib

下載地點：<http://www.sun.com/software/download/developer/5175.html>

### 三、jspSmartUpload

功用：JSP/servlet 上傳檔案用的工具

下載地點：<http://www.jspsmart.com/>

#### 4.3.3.2 目錄服務系統用戶端功能

本系統對於目錄服務的用戶端提供以下服務：

##### 一、憑證人員資料查詢服務

提供使用者查詢資料之服務，使用者獲得查詢結果之後，可以進一步透過憑證下載服務來取得該筆資料的憑證檔案。

##### 二、憑證下載服務

提供憑證檔案的下載服務。

##### 三、憑證廢止清單下載服務

提供憑證廢止清單〔Certification Revocation List〕檔案的下載服務。

#### 4.3.3.3 目錄服務系統伺服器端功能

本系統對於目錄服務的管理提供以下服務：

##### 一、憑證上載服務

提供人員資料檔案與憑證檔案的上載服務，系統管理者可經由這項服務將人員的資料與憑證檔案存放在 OpenLDAP Server 中，以供使用者查詢、下載憑證。

##### 二、憑證廢止清單上載服務

提供憑證廢止清單的上載服務，讓管理者可以將 CA 所產生的憑證廢止清單存放在本服務系統中，以供使用者下載。

##### 三、憑證刪除服務

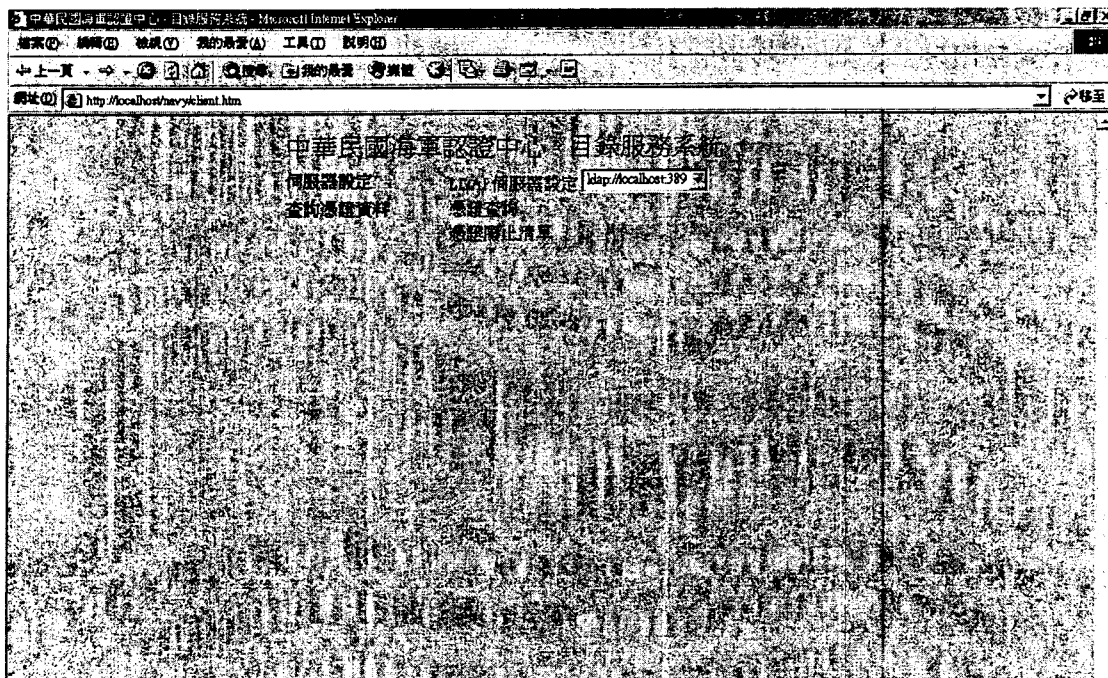
提供既存憑證資料刪除服務，讓管理者可透過本系統刪除已經存在 OpenLDAP Server 中的資料。

## 五、海軍認證中心目錄服務系統範本流程

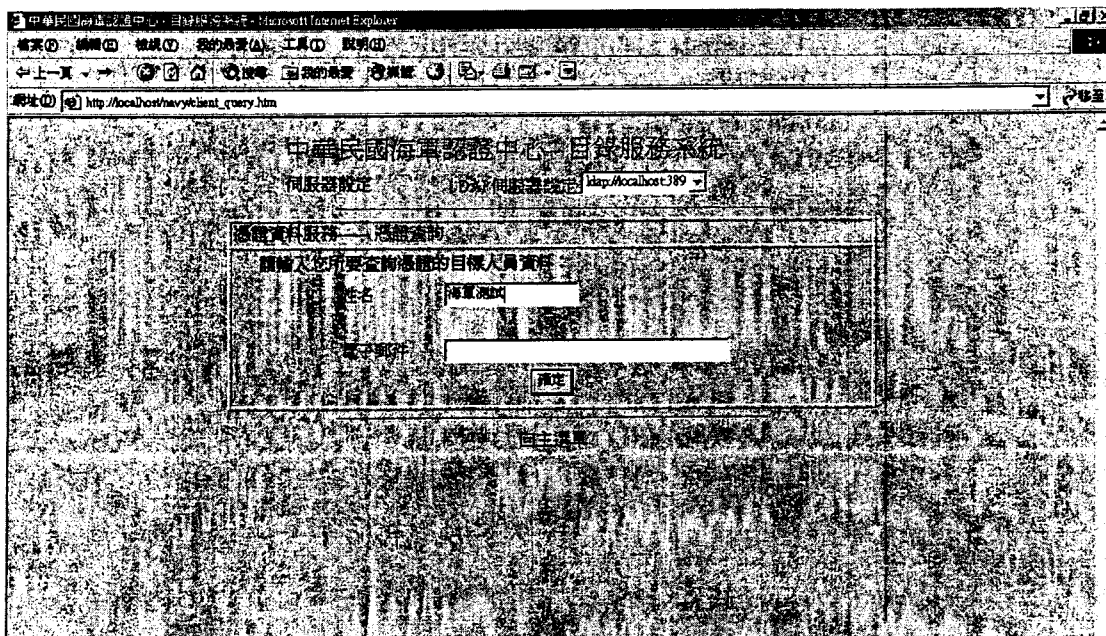
茲依據前述各項功能分別作使用流程說明：

### 5.1 憑證人員資料查詢與下載服務

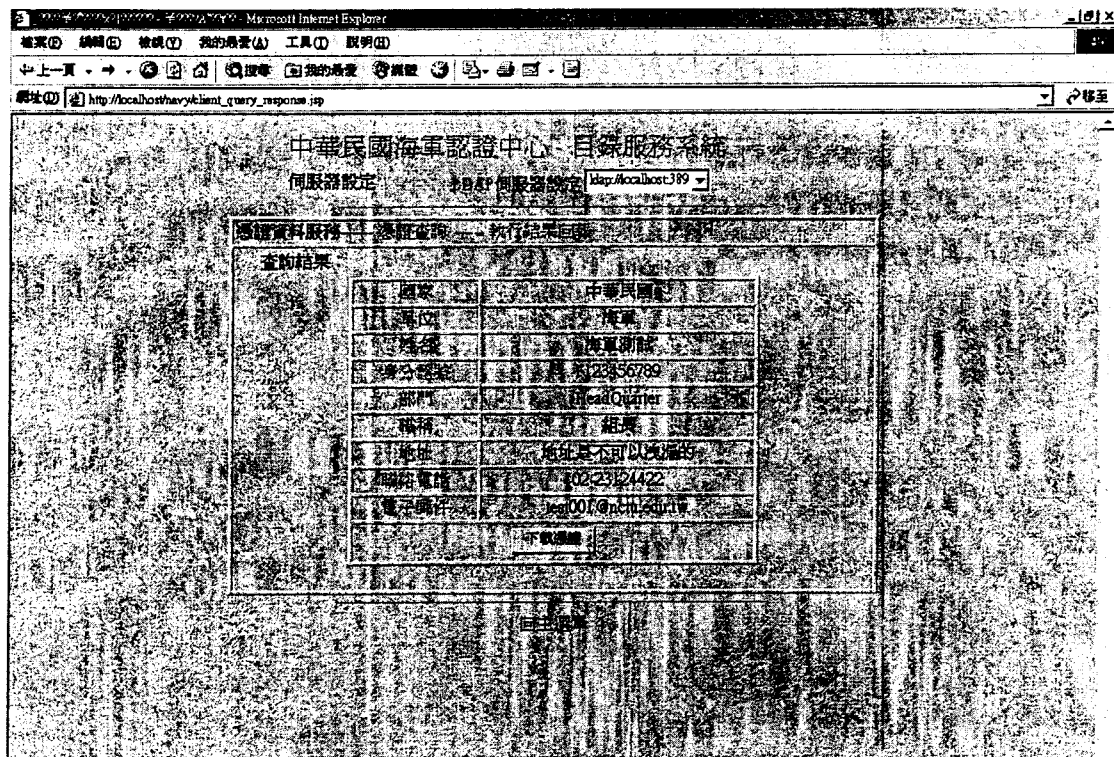
步驟一：連結到『目錄服務系統』首頁，選擇『憑證查詢』服務。網址為：  
<http://host/client.htm>。



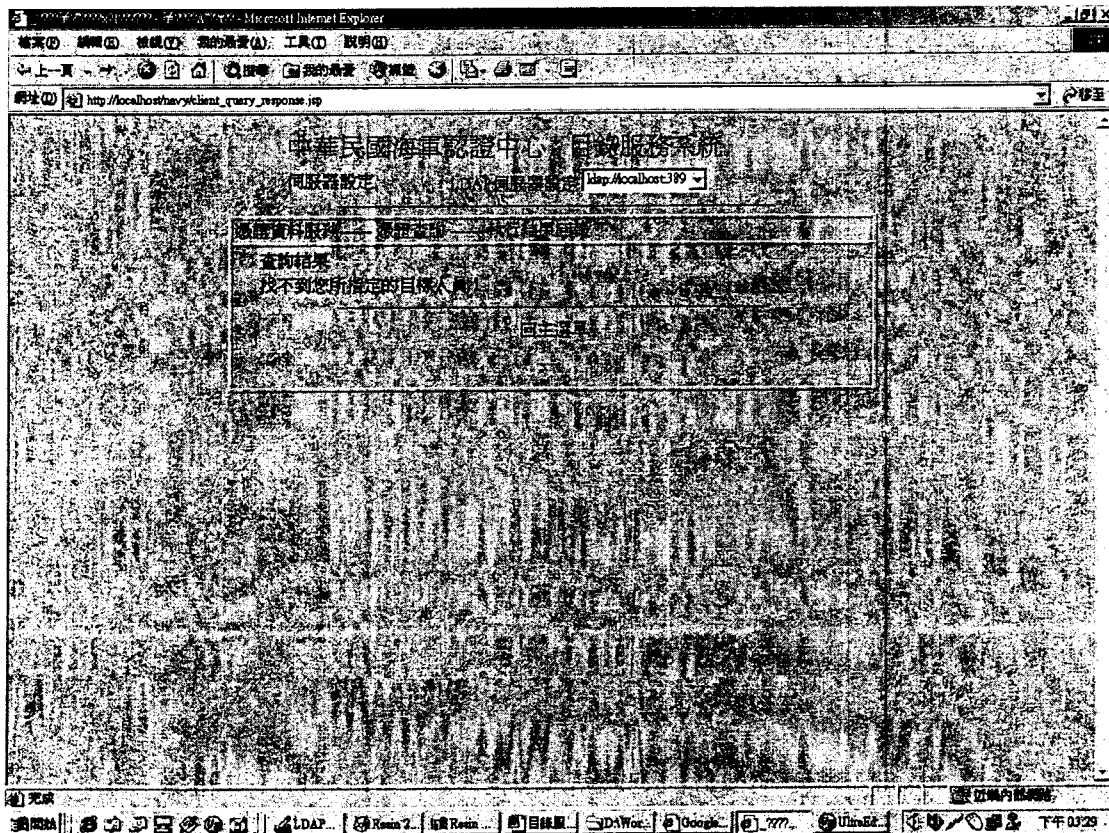
步驟二、輸入你的查詢條件之後，請按『確定』：



步驟三、系統將顯示出查詢結果。按下『下載憑證』的按鈕即可取得此人的憑證檔。



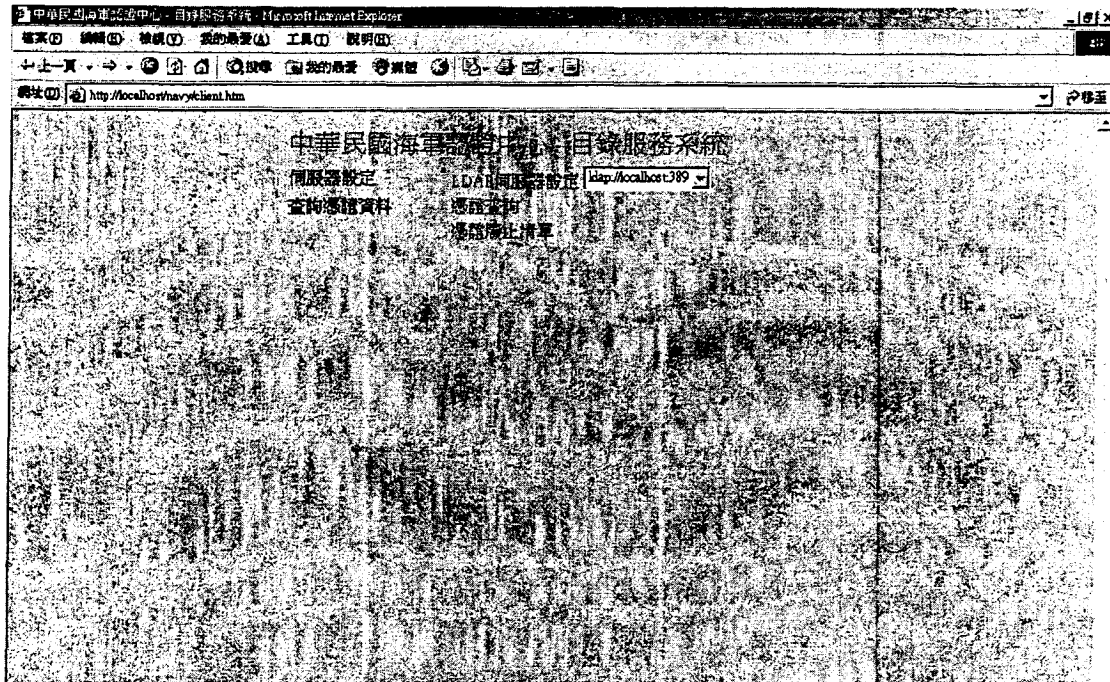
若系統未查詢到你所指定的人員，將會顯示以下訊息：



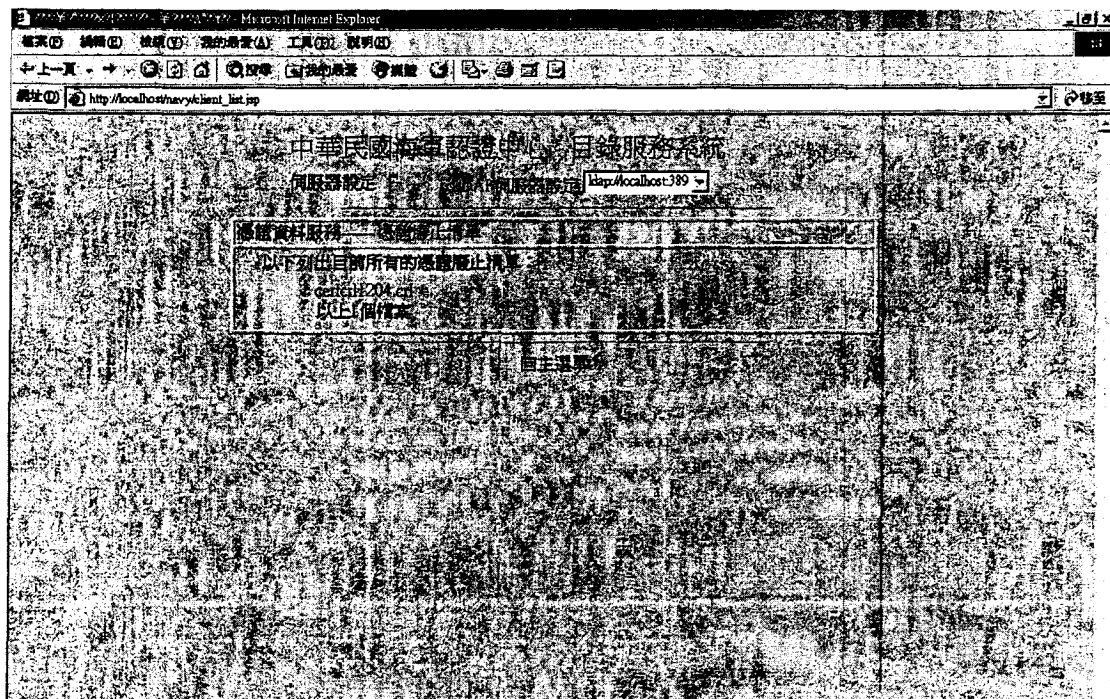


## 5.2 憑證廢止清單下載服務

步驟一、連結到『目錄服務系統』首頁，選擇『憑證廢止清單』服務。網址為：<http://host/client.htm>。

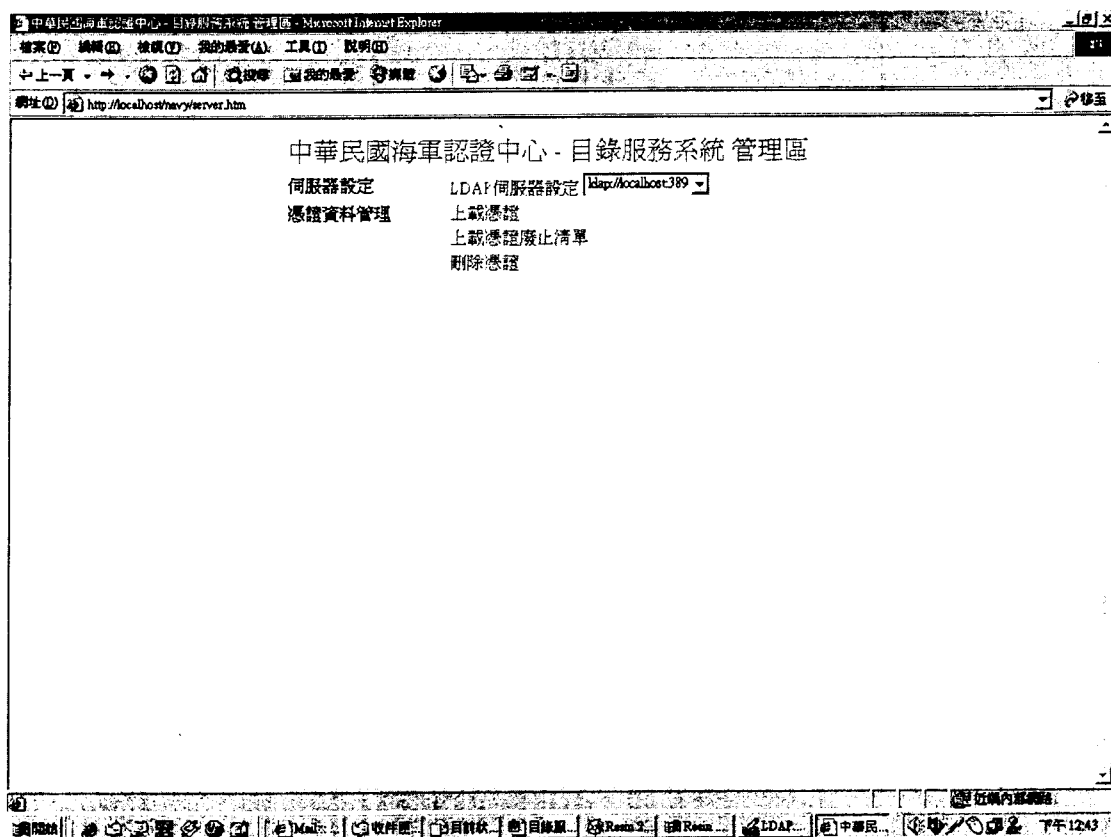


步驟二、系統將會列出目前存放的所有憑證廢止清單檔案。



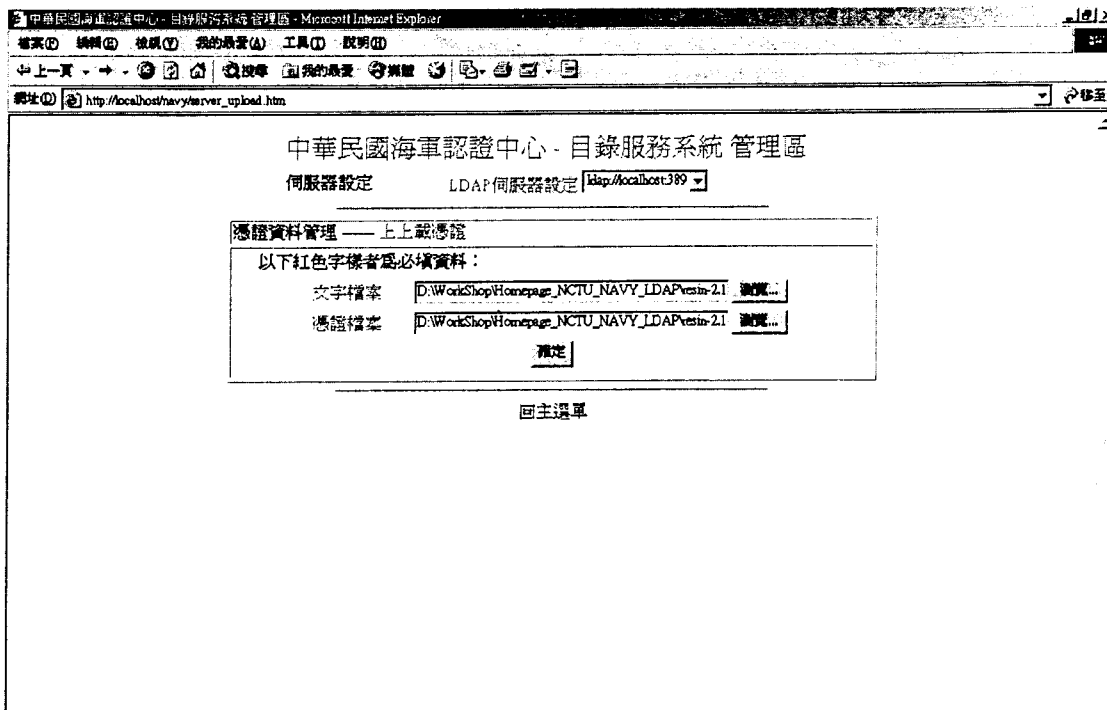
## 5.3 憑證上載服務

步驟一、連結到『目錄服務系統 管理區』首頁，選擇『上載憑證』服務。  
網址為：http://host/server.htm。

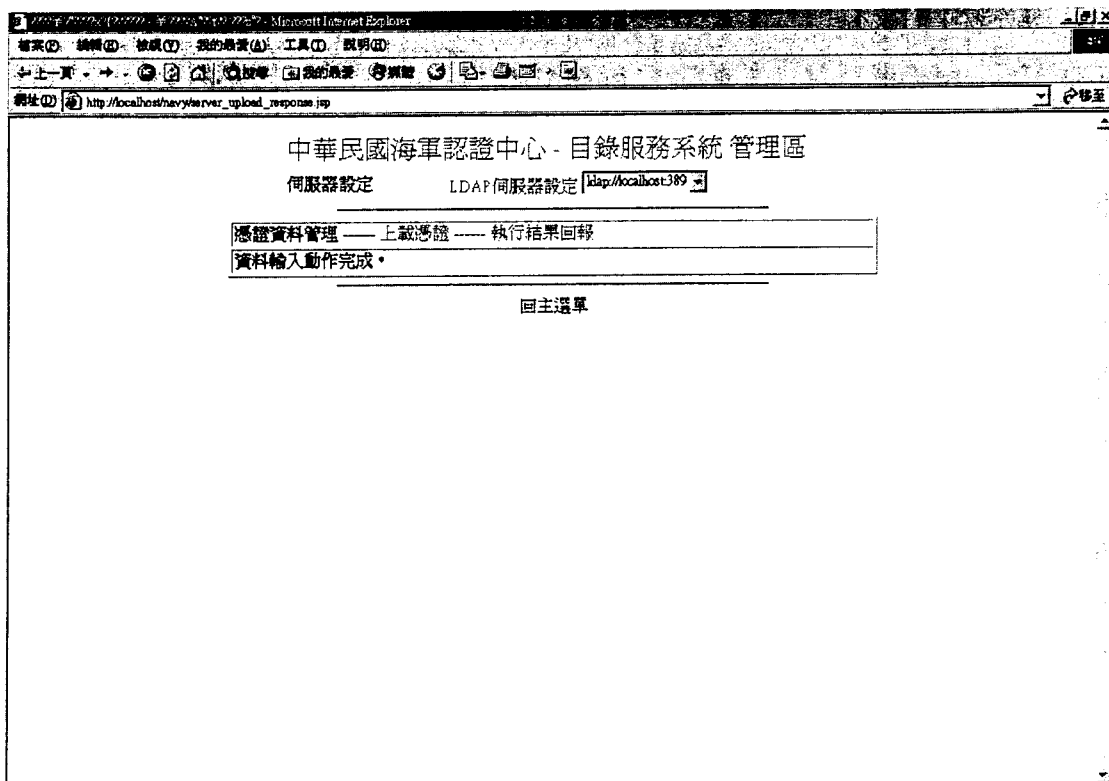


步驟二、請依據指示選取你的人員資料人事檔案與憑證檔案，人員資料人事檔案為既存的文字檔，其內容範例如下：

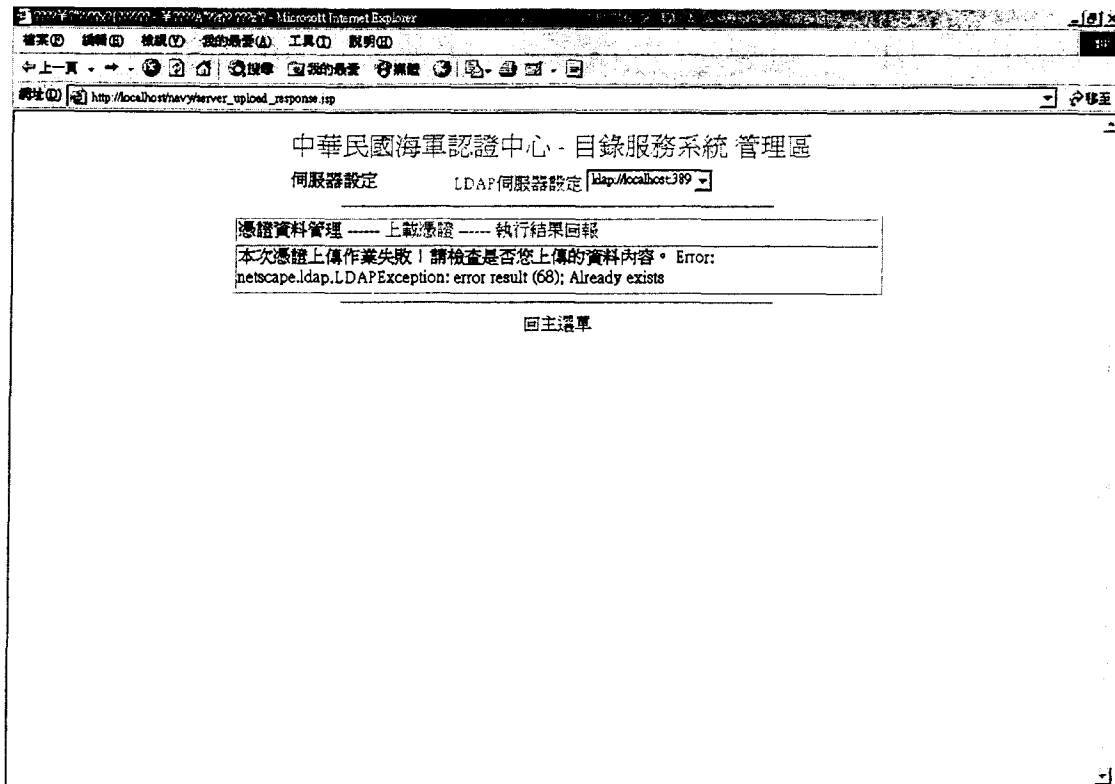
王大明,F123456789,1965-01-01,海軍,HeadQuarter,組長,中華民國,台灣,台北市大直,02-23124422,test001@nctu.edu.tw,1234



步驟三、點選『確定』，系統將為你處理文字檔案與憑證檔案。

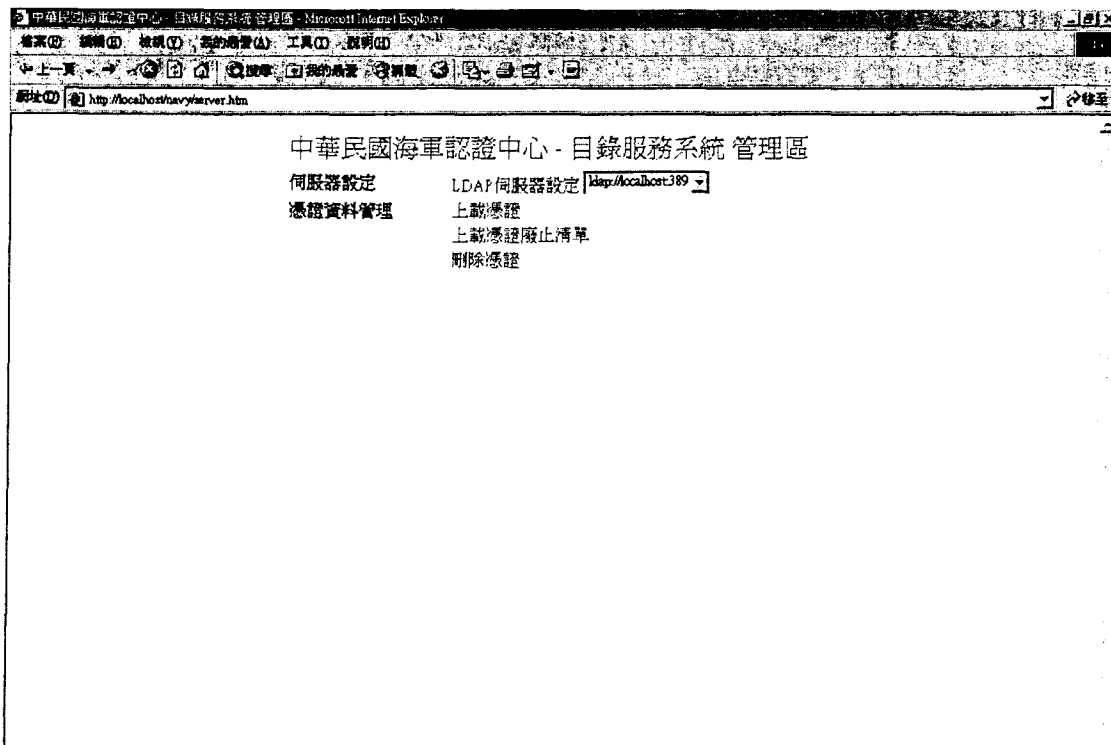


若你輸入的人員資料已經存在，則系統會給你錯誤訊息：

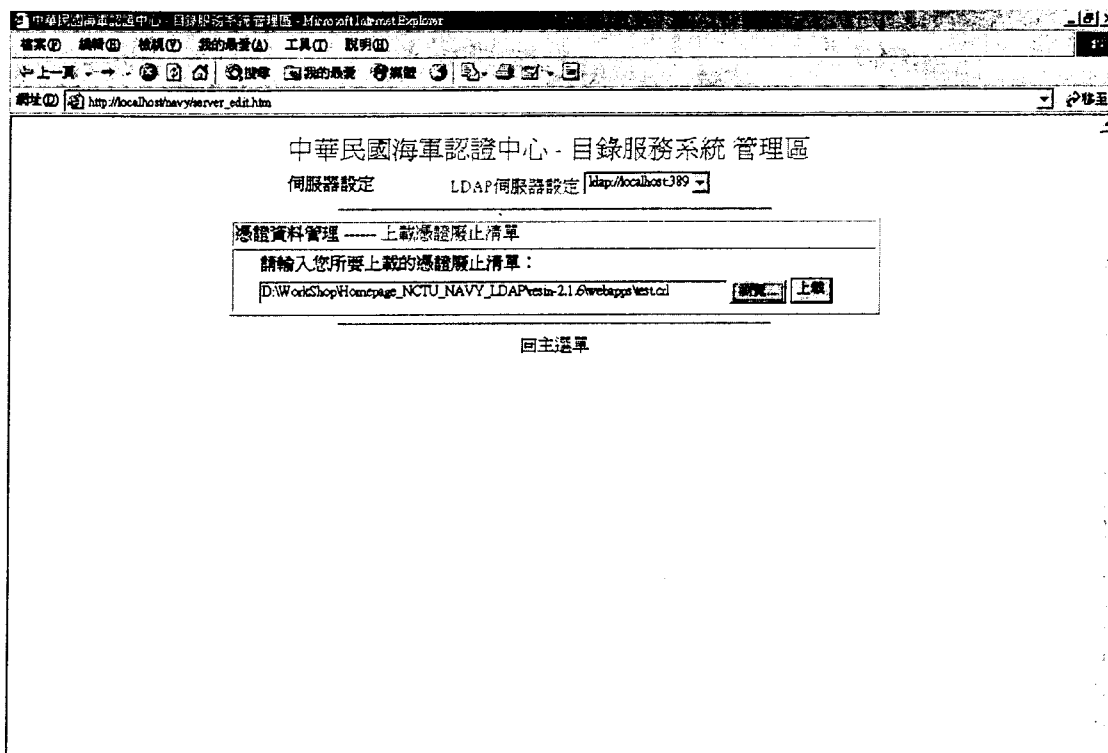


## 5.4 上載憑證廢止清單

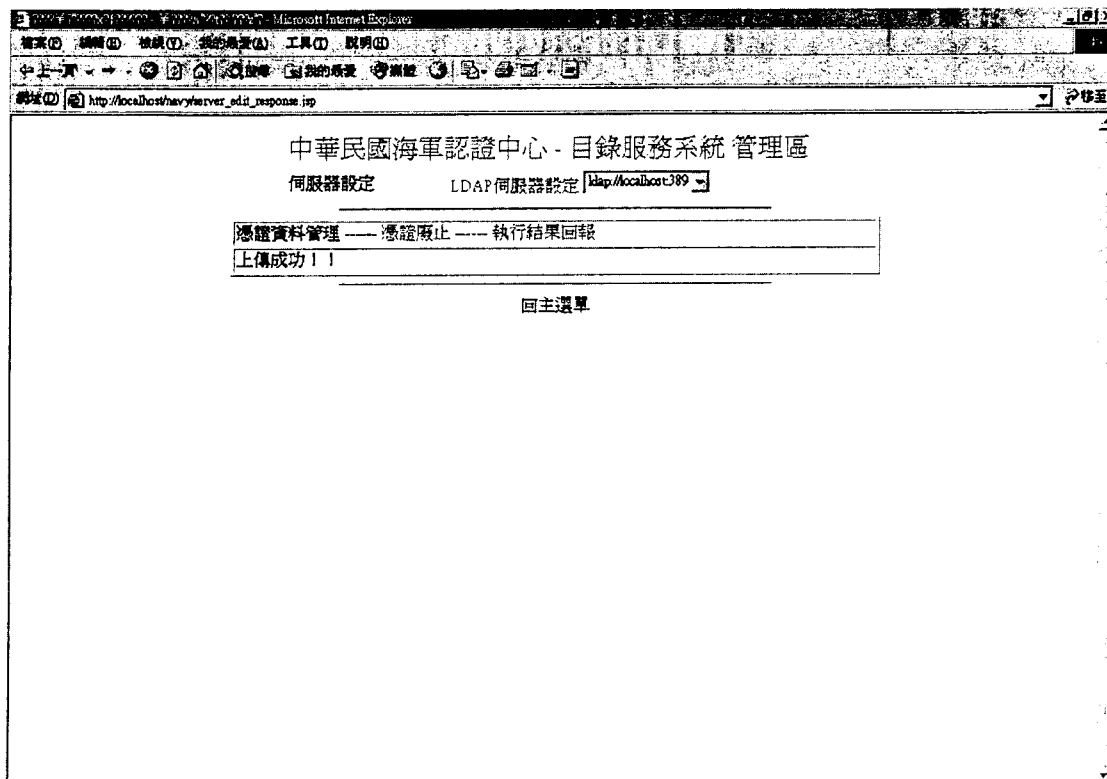
步驟一、連結到『目錄服務系統 管理區』首頁，選擇『上載憑證廢止清單』服務。網址為：http://host/server.htm。



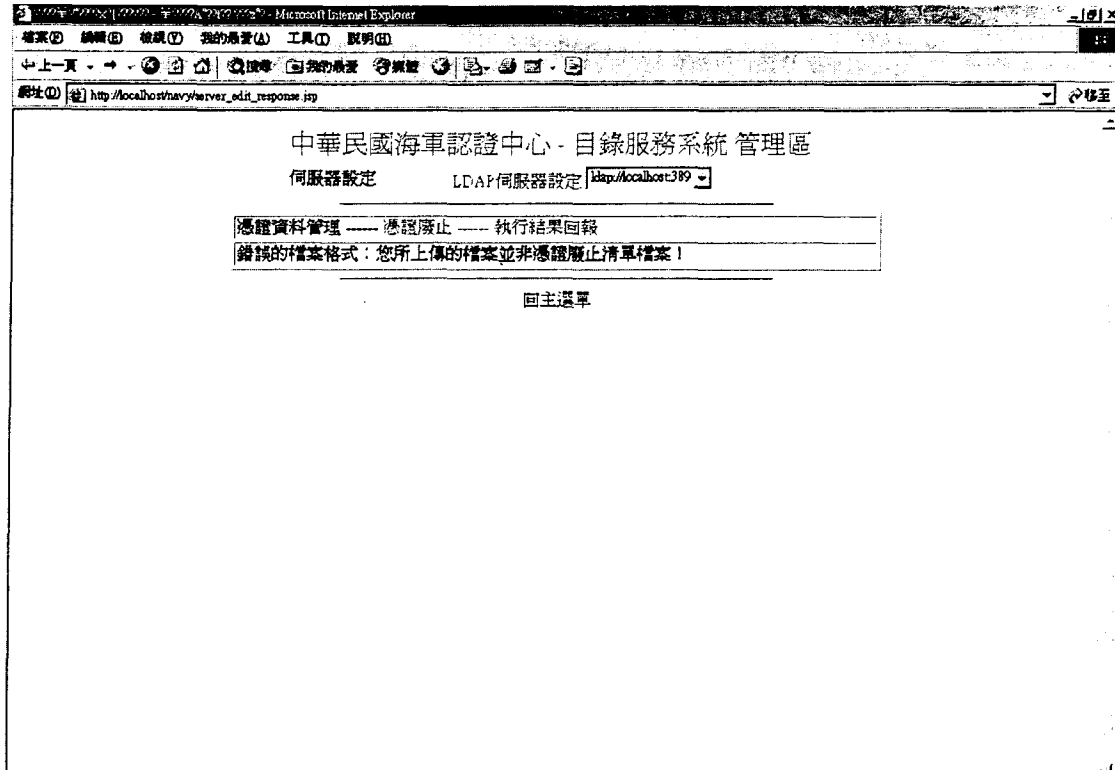
步驟二、請依據系統指示選擇你所要上載的憑證廢止清單檔案。



步驟三：若你上載成功，系統會給你這樣的訊息：

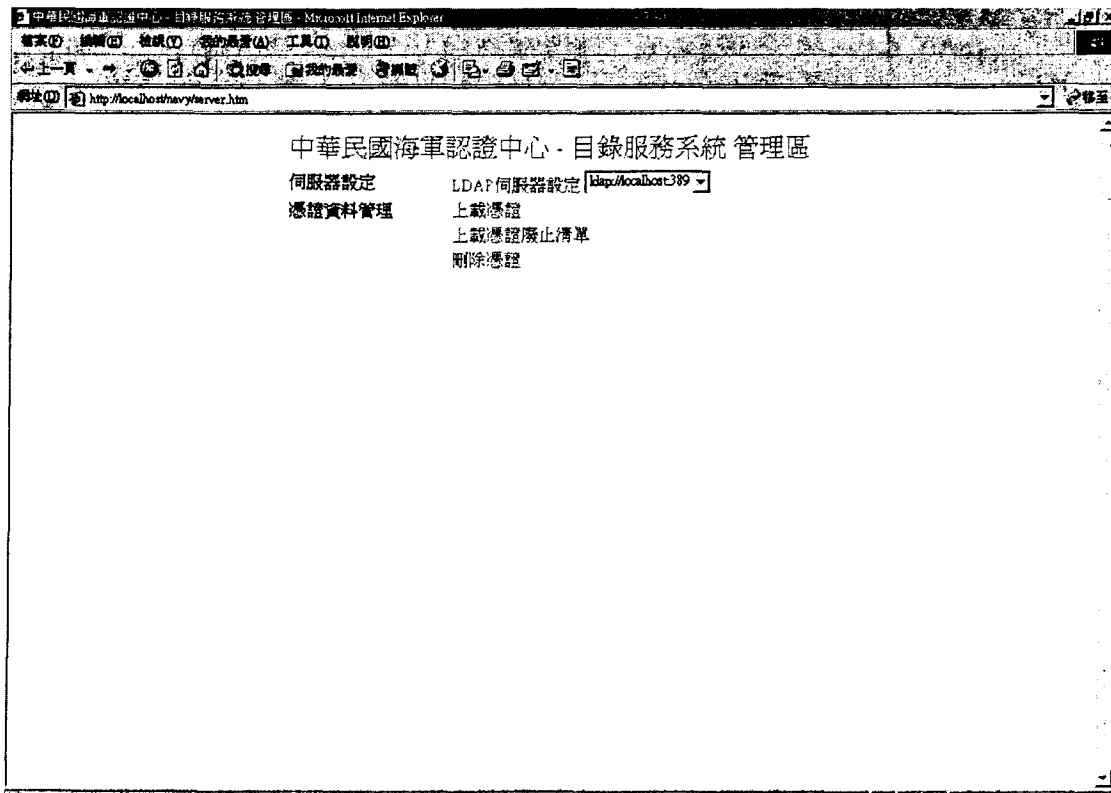


若上傳失敗，則會是：

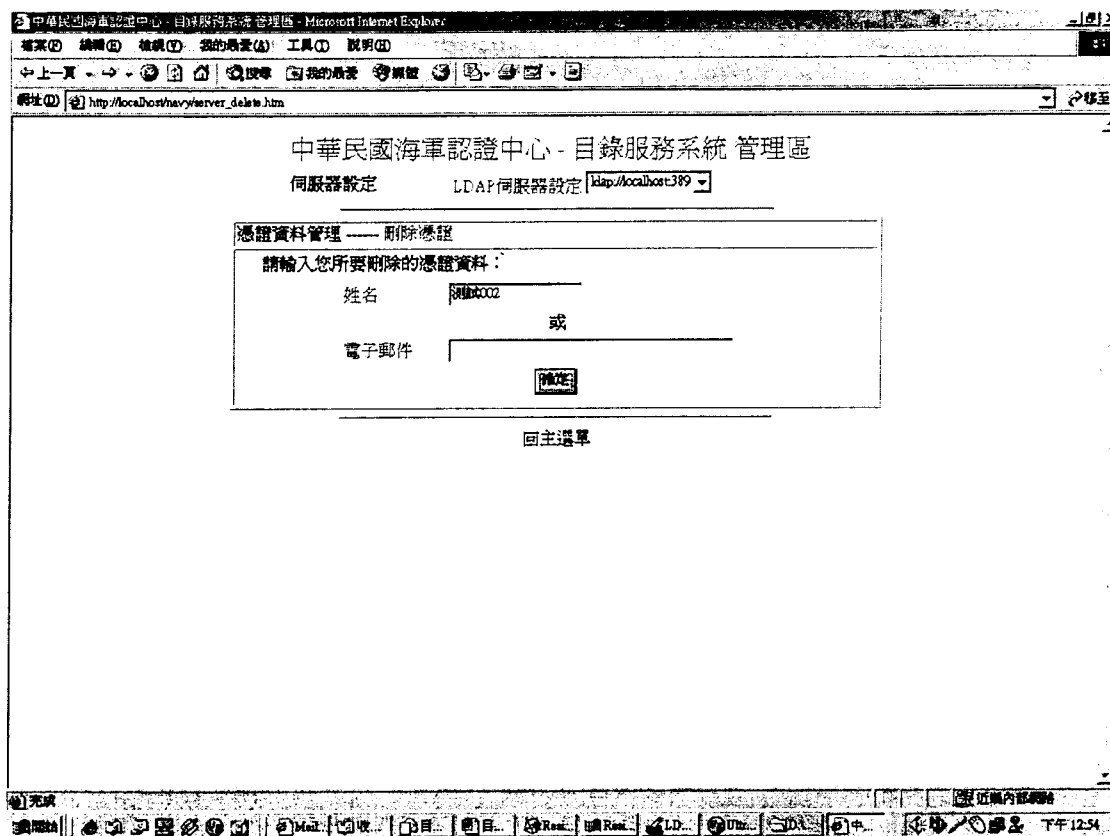


## 5.5 憑證刪除服務

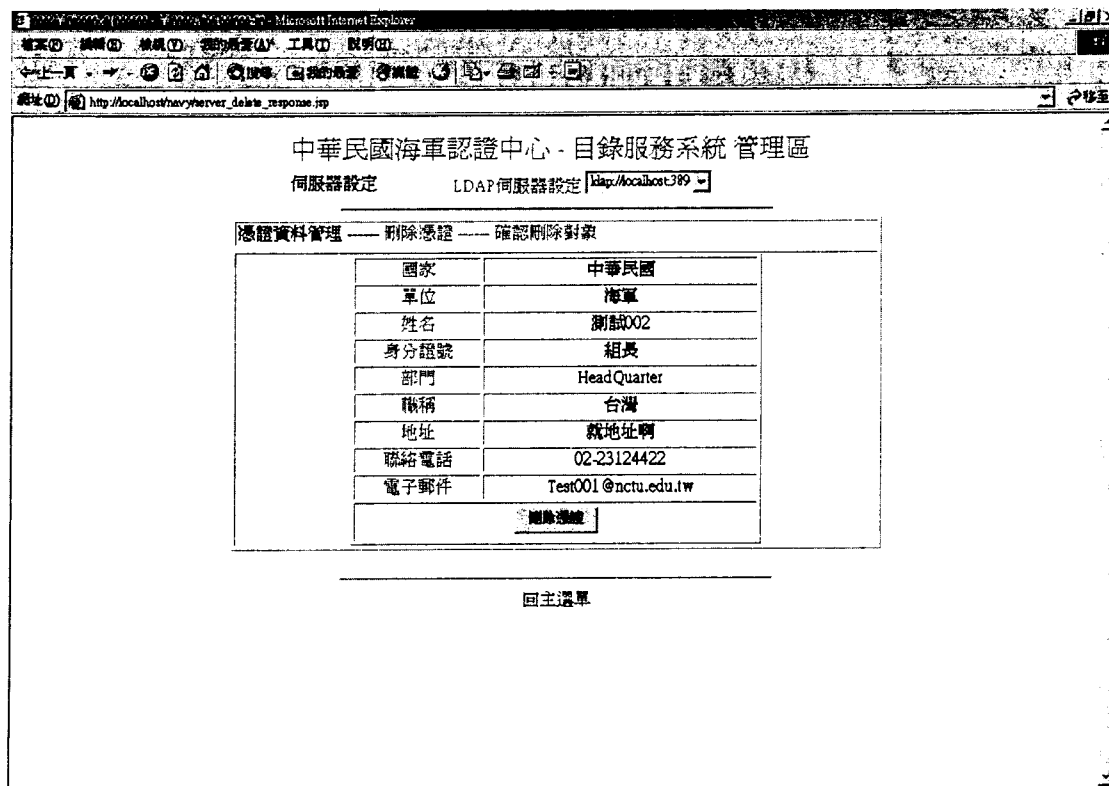
步驟一、連結到『目錄服務系統 管理區』首頁，選擇『上載憑證廢止清單』服務。網址為：`http://host/server.htm`。



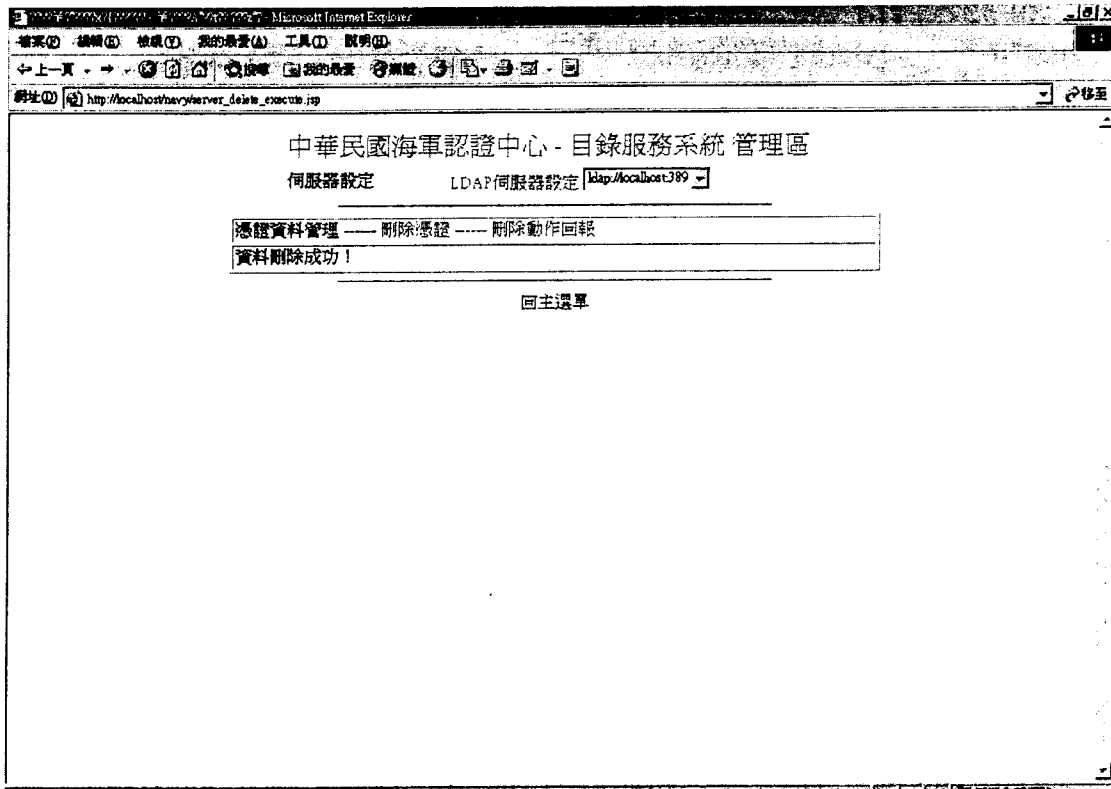
步驟二、請依據系統指示輸入你所要刪除的人員查詢條件。



步驟三、點選『確定』後，系統會為你將資料查詢出來，以供你確定是否刪除。



步驟四、若你確定要刪除該筆資料，請點選『刪除憑證』選項，系統會給你動作執行回報。





## 參考資料

- [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]. 謝文川、林國良、張永志，中華民國海軍認證中心離形系統之建置，2001 年，九十年度國防科技學術合作研究計畫
- [3]. 陳昱仁、林明華、張永志，中華民國海軍認證中心離形系統之建置，2001 年，八十九年度國防科技學術合作研究計畫
- [4]. Network Strategy Report , “Public Key Infrastructure Architecture”, vol. 9 Jul 1997
- [5]. [www.firsttaiwan.com.tw/stock/caqa.htm](http://www.firsttaiwan.com.tw/stock/caqa.htm) 張天杰，網路未來要角--LDAP，  
<http://mouse.oit.edu.tw/Hope/199908/CONTENT/ldap/LDAP.html>
- [7]. ITU-T Recommendation X.500 (ISO/IEC 9594-1) (1993 E), Information Technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models and Services.
- [8]. Daniel Blum 原著、廖裕康、陳仁泰編譯，認識 Active Directory Services 目錄服務，Microsoft，華彩軟體
- [9]. 施威銘研究室，Windows 2000 Server 系統實務，旗標出版社
- [10]. 中華電信網路及多媒體應用技術研究室研發成果，  
<http://www.chttl.com.tw/300/ldap>
- [11]. 陳彥學，資訊安全理論與實務，文魁資訊
- [12]. 陳俊良，訊息與目錄服務探究，網路通訊雜誌，1998 年 3 月號，p.72~77，  
資訊與電腦出版社
- [13]. 余政宗譯，LDAP 的精髓所在，網路通訊雜誌，1999 年 6 月號，p.130~135，  
資訊與電腦出版社
- [14]. Wengyik Yeong , Tim Howes and Steve Kille , Lightweight Directory Access Protocol, RFC 1777 , March 1995
- [15]. Mark Wahl , Tim Howes and Steve Kille , Lightweight Directory Access Protocol (v3) , RFC 2251 , December 1997

## 附錄 A：目錄服務系統應用—人事資料目錄服務系統

此部分說明將目錄查詢服務應用在人事資料系統時,人事資料目錄服務系統的資料結構、所提供的功能與使用方式。

### A.1 資料結構說明

本範例採用以下 ObjectClass 與 Attribute：

Schema： core.schema、cosine.schema

ObjectClass：country、organization、organizationalUnit、person

Attribute： cn、sn、c、o、ou、description、telephoneNumber、registeredAddress、postOfficeBox

### A.2 系統功能

本系統提供以下功能：

#### 1. 新增人事資料

你可透過此一功能新增人事資料到本系統的 OpenLDAP Server。

#### 2. 修改人事資料

提供你一個友善的介面，讓你可以透過此一介面修改目前已存在於 OpenLDAP Server 上的人事資料。

#### 3. 刪除資料

你可經由此一功能刪除任何你所指定的人事資料。

#### 4. 人事資料查詢服務

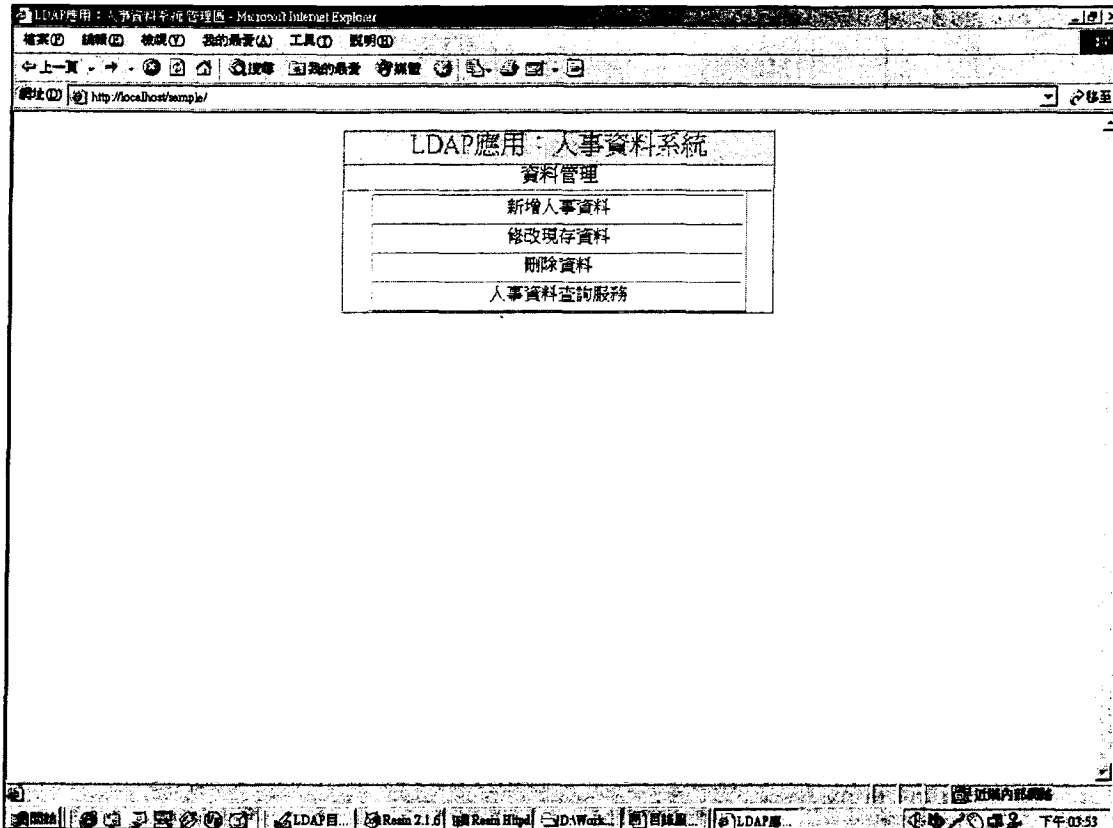
當然，我們提供了資料查詢服務，讓你可以透過這項功能來查詢你所儲存於本系統的人事資料。

### A.3 使用步驟

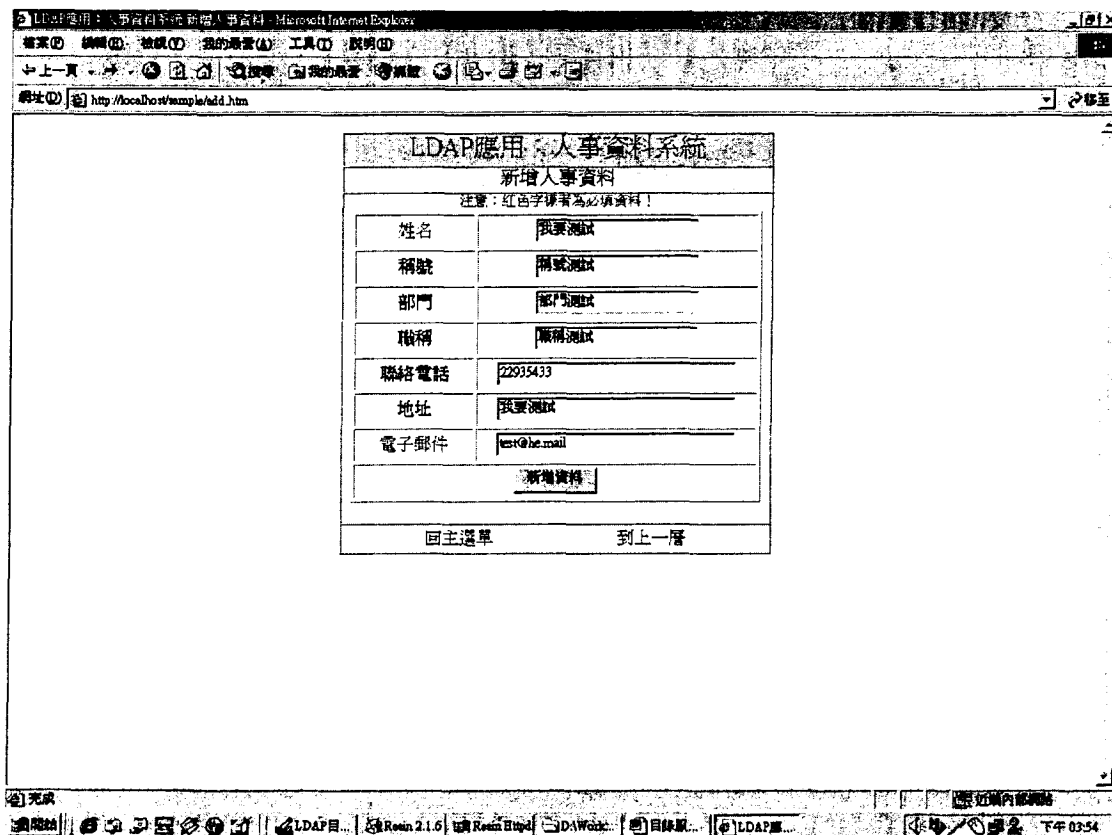
在此依據前面所提的四項功能分別以系統畫面說明：

#### 1. 新增人事資料

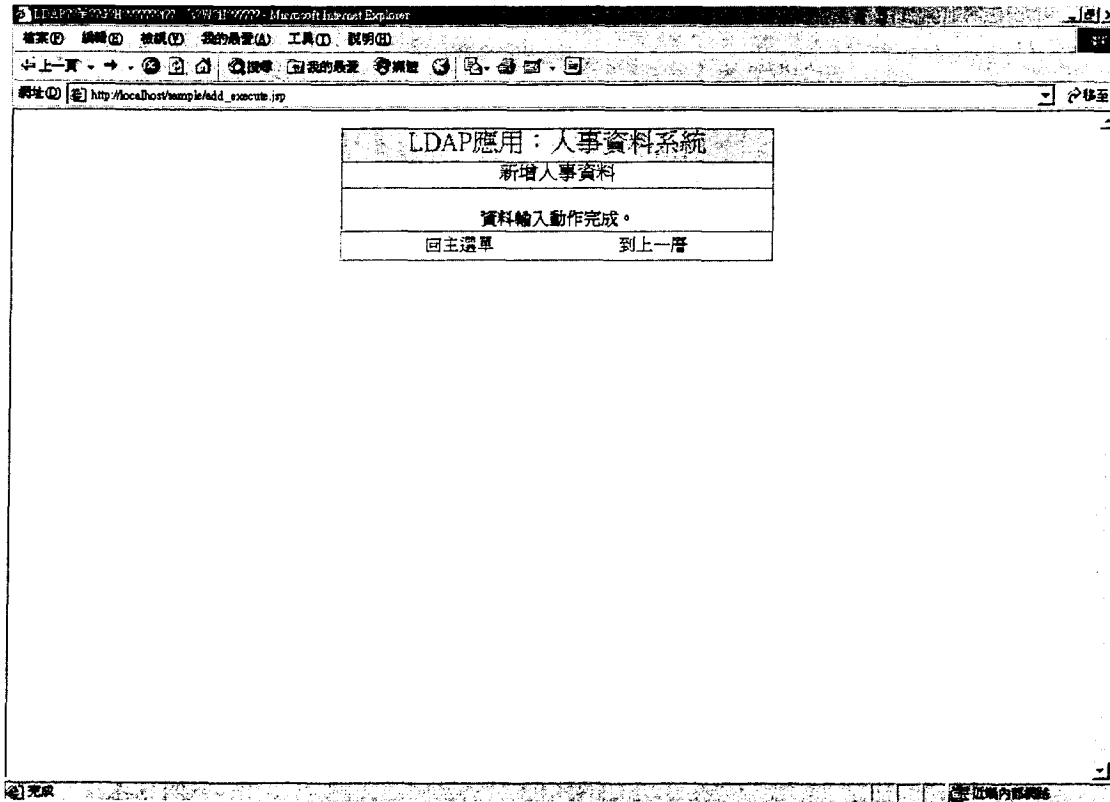
步驟一、進入本系統的服務首頁，點選『新增人事資料』功能。



步驟二、請填寫你所要新增的資料內容。

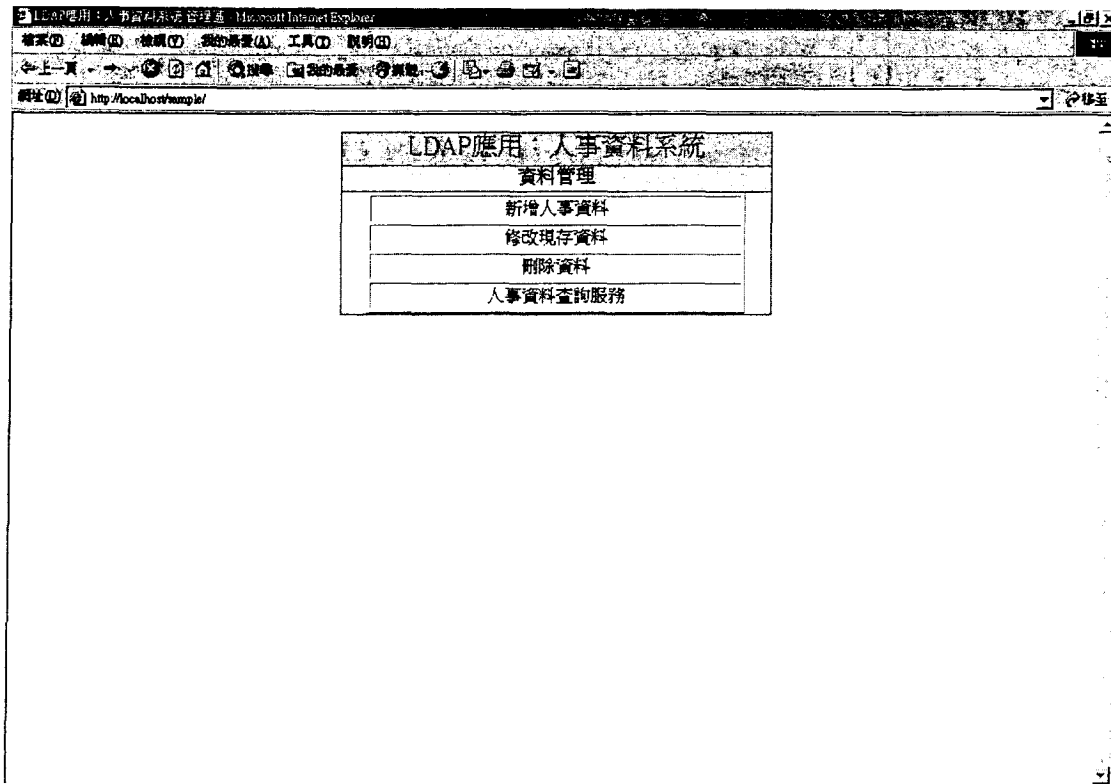


步驟三、填寫完成後，請點選『新增資料』按鈕，系統將會給你執行結果的報告。

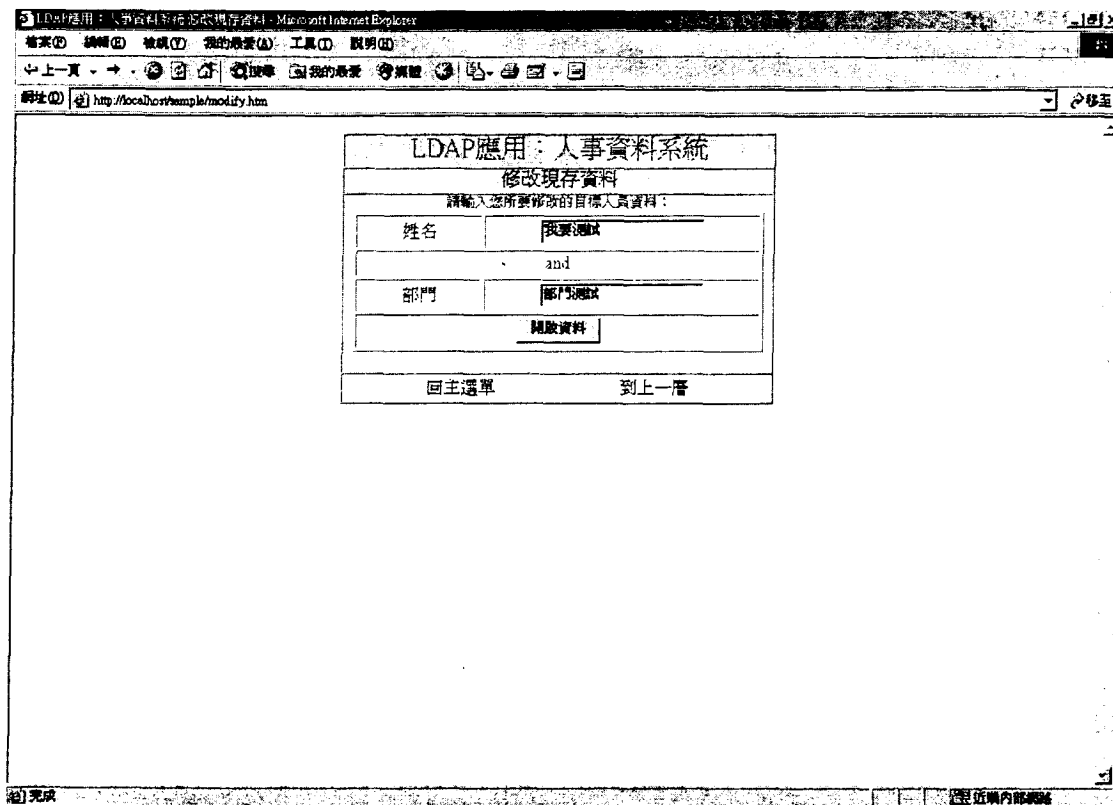


## 2. 修改人事資料

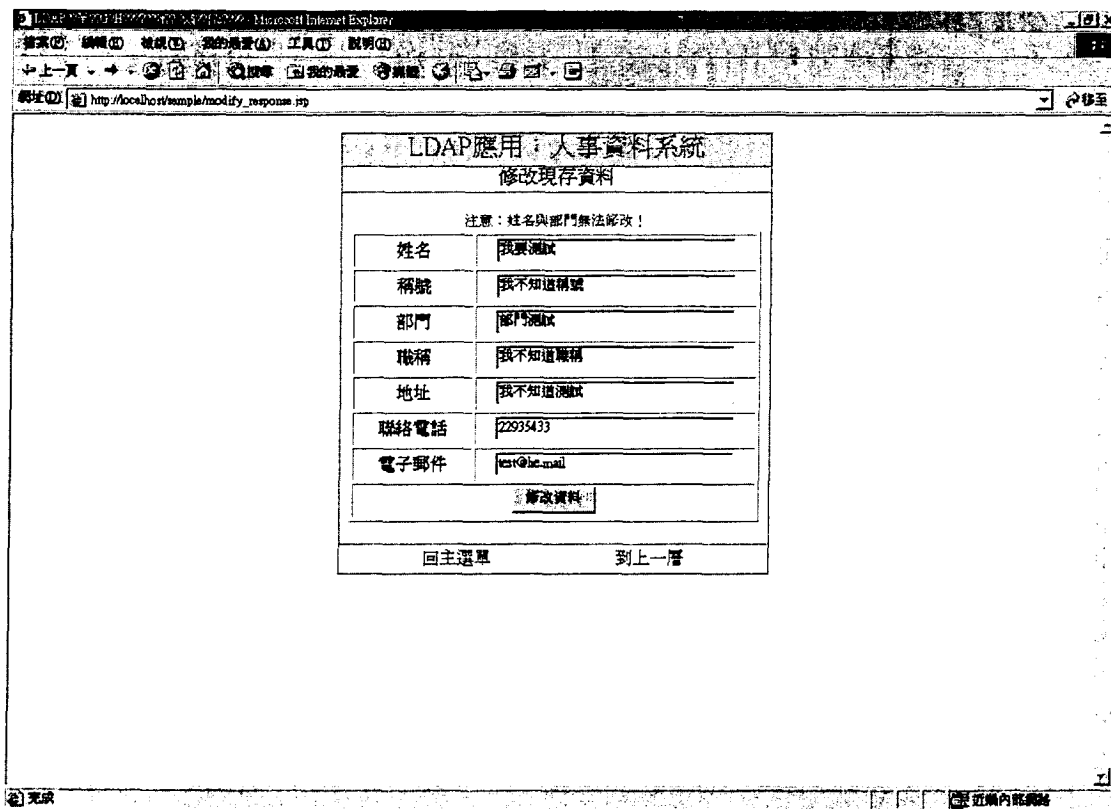
步驟一、進入本系統的服務首頁，點選『修改人事資料』功能。



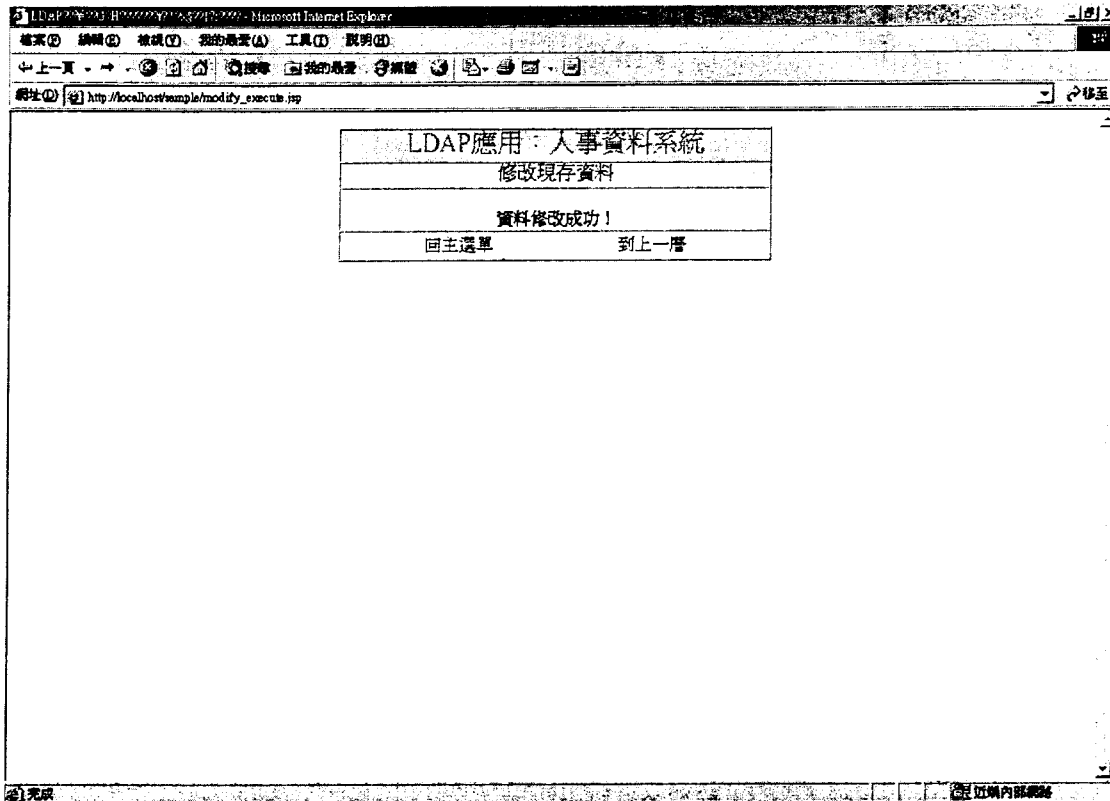
步驟二、請填寫你所要修改的人事資料，系統會幫你調閱出完整資料。



步驟三、請依據你的需求修改資料。

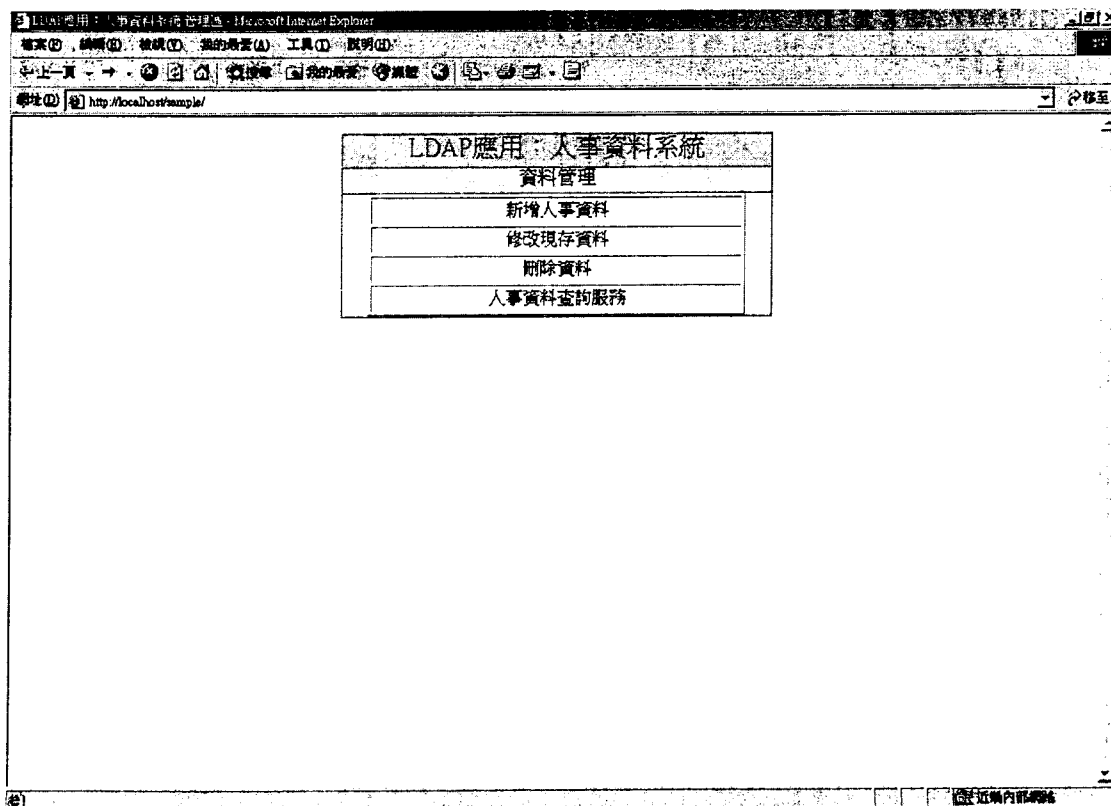


步驟四、按下『修改資料』按鈕，系統將會給你執行結果的報告。

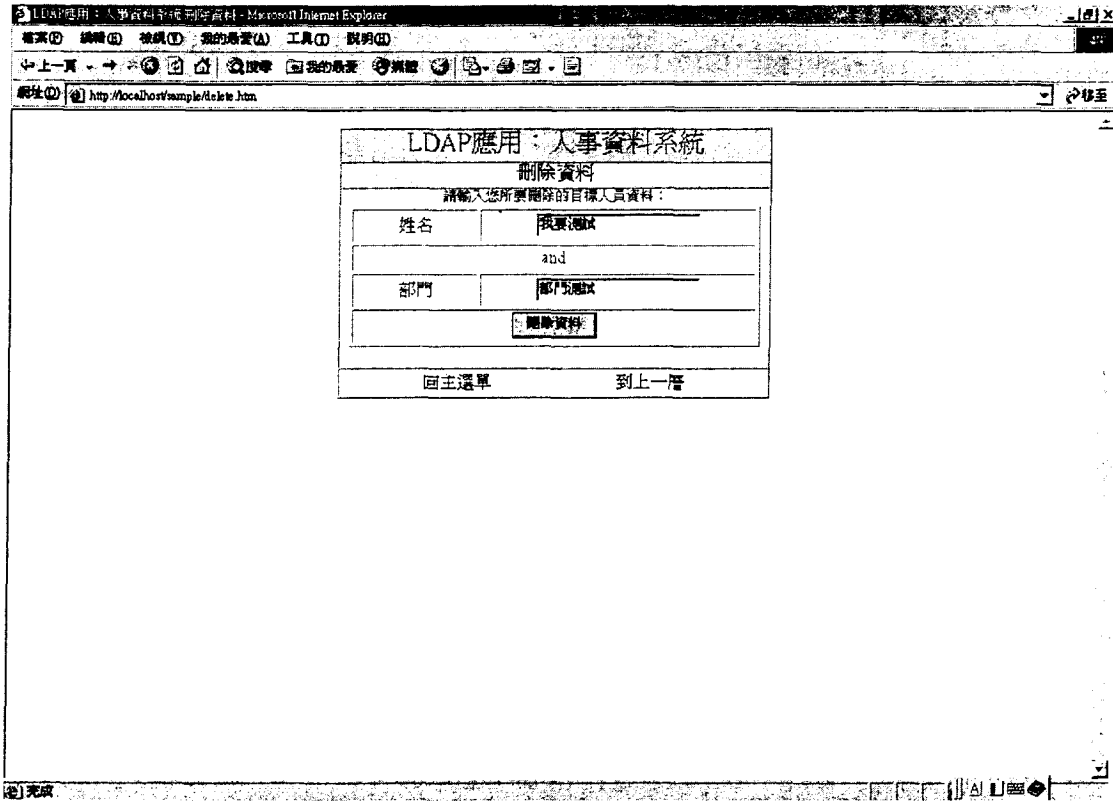


### 3. 刪除資料

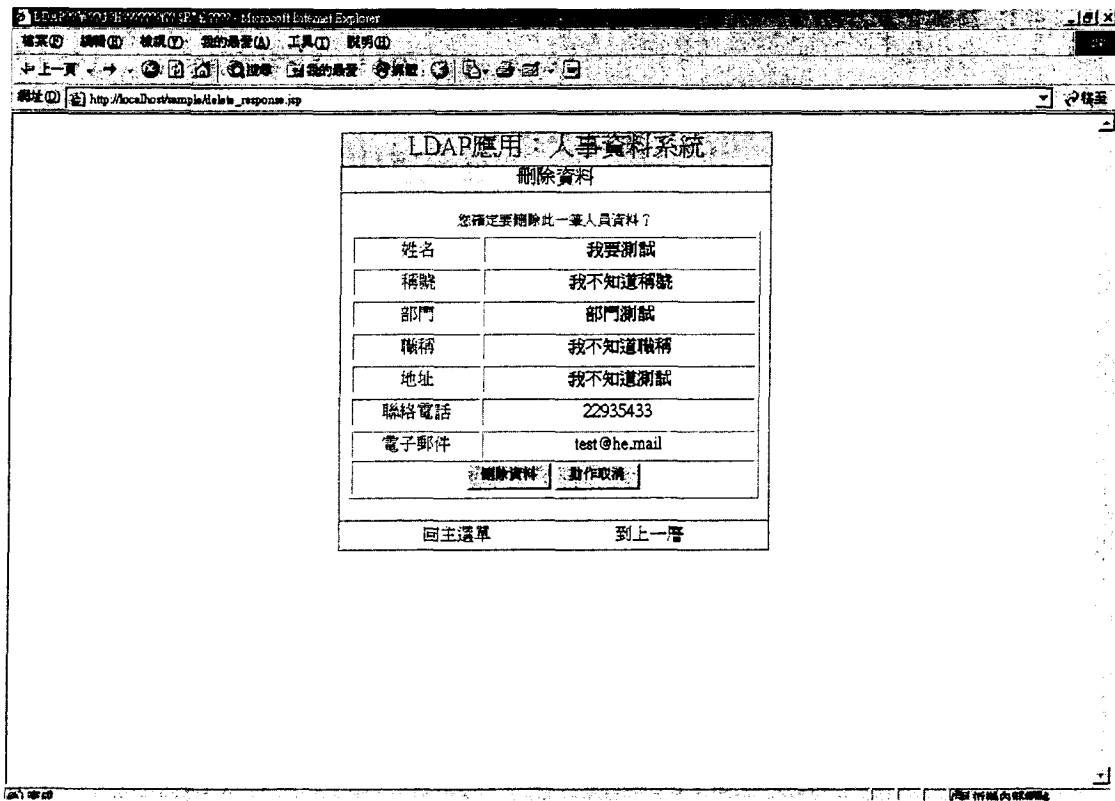
步驟一、進入本系統的服務首頁，點選『刪除資料』功能。



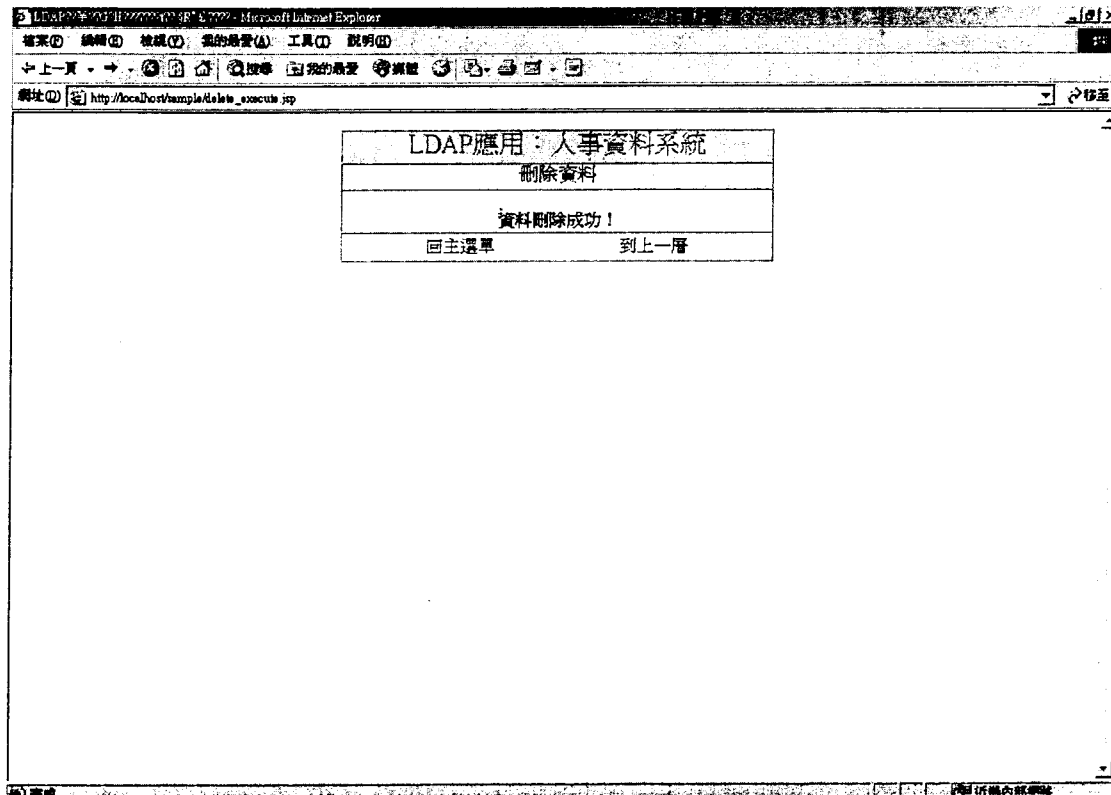
步驟二、請填寫你所要刪除的人事資料，系統會幫你將完整資料調閱出來供你確認。



步驟三、請確認這是不是你所要刪除的人事資訊。

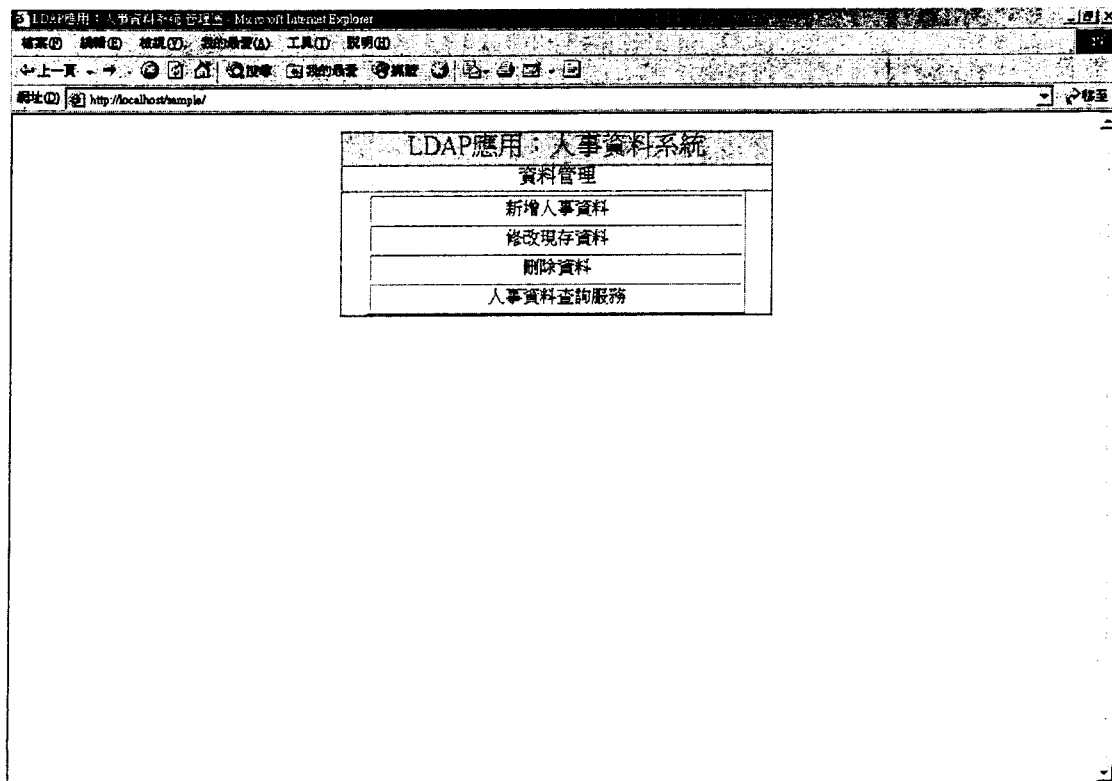


步驟四、若你確定要刪除這筆資料，請點選『刪除資料』按鈕，系統將會給你執行結果的報告。



#### 4. 人事資料查詢服務

步驟一、進入本系統的服務首頁，點選『人事資料查詢服務』功能。





步驟二、請輸入你的查詢條件。

LDAP應用：人事資料系統  
人事資料查詢服務  
請輸入您所擬查詢的目標人員資料：

姓名	再次測試
and	
部門	部門測試

開啟資料

重新查詢

步驟三、按下『開啟資料』後，系統就會為你到 LDAP Server 上查詢你所指定的資料，並給你結果回報。

LDAP應用：人事資料系統  
人事資料查詢服務  
查詢結果：

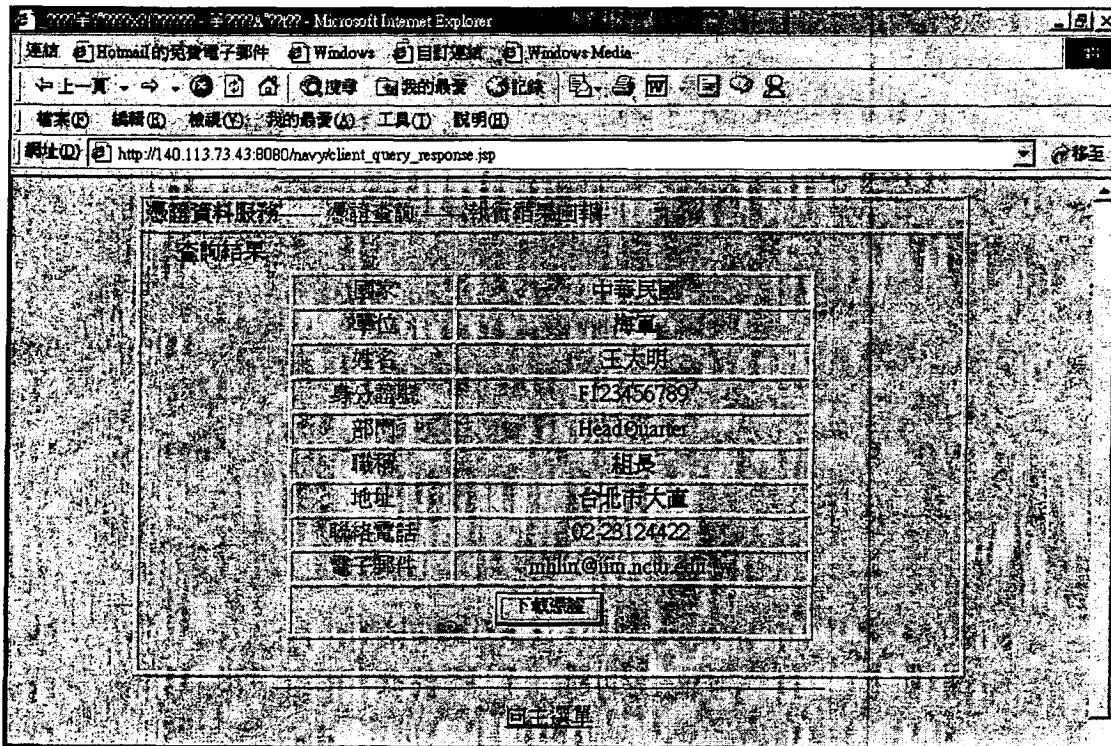
姓名	再次測試
稱號	再次測試稱號
部門	部門測試
職稱	再次測試職稱
地址	再次測試地址
聯絡電話	3353253
電子郵件	oh@not.again

重新查詢

## 附錄 B：使用收信者憑證寄送加密電子郵件範例

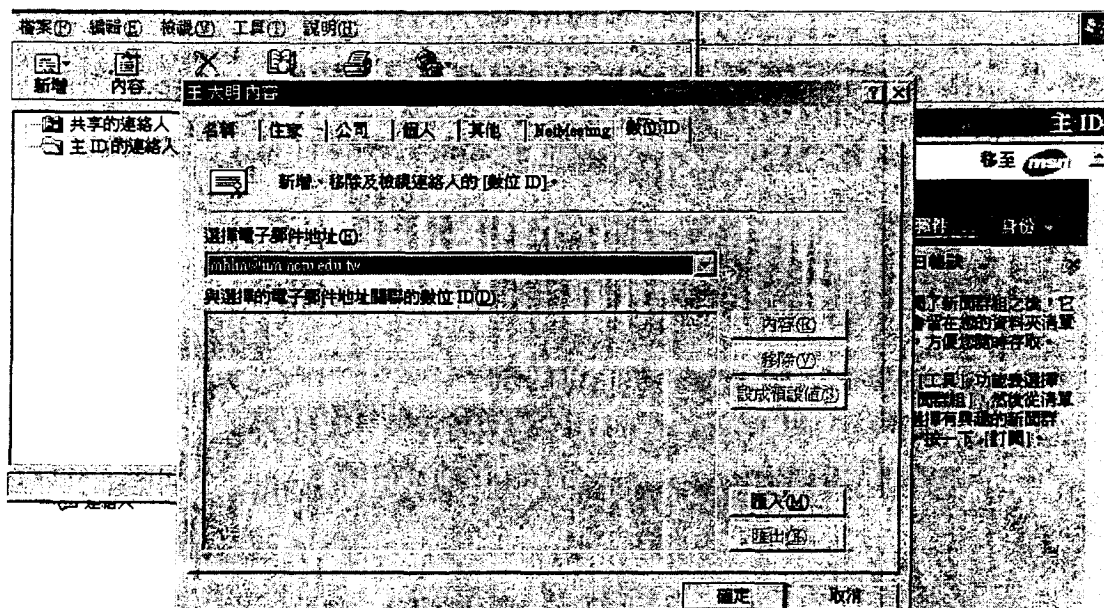
此部分說明如何在電子郵件寄送軟體 Outlook Express 中，將從目錄服務系統查詢下載所得的憑證，用在寄送加密的電子郵件上。其使用流程如下：

步驟一、請連線到目錄服務系統上，查詢並下載收信者的憑證，若收信者為「王大明」，則查詢結果如下：

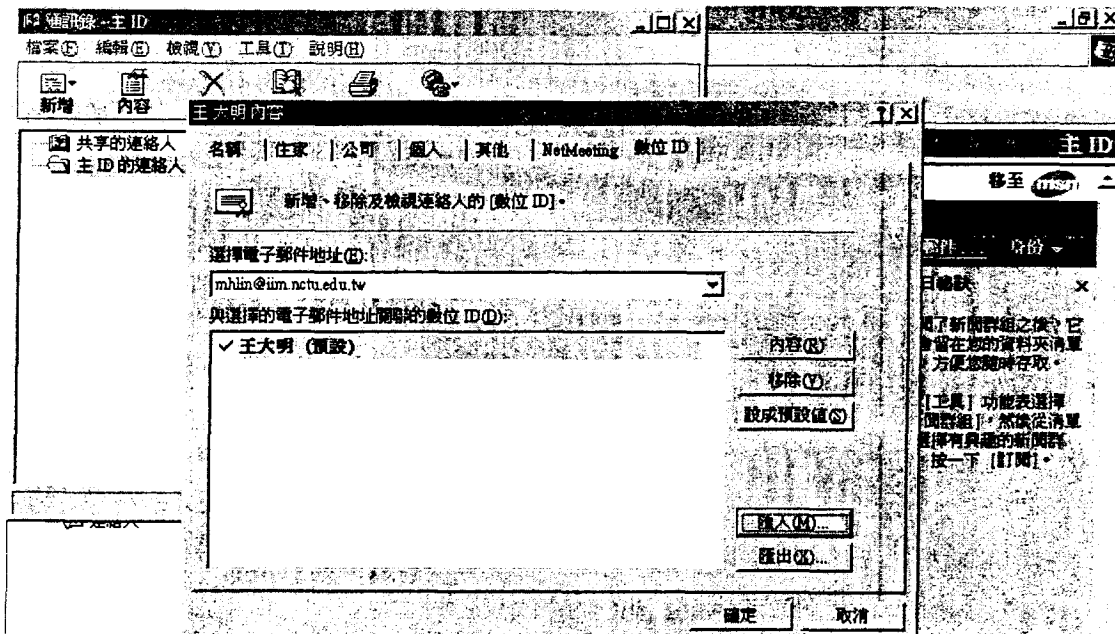


按下『下載憑證』按鈕，將所查到的憑證檔案下載到電腦中。

步驟二、在 Outlook Express 通訊錄中，找出「王大明」這個聯絡人，切換到『數位 ID』頁籤，畫面如下：

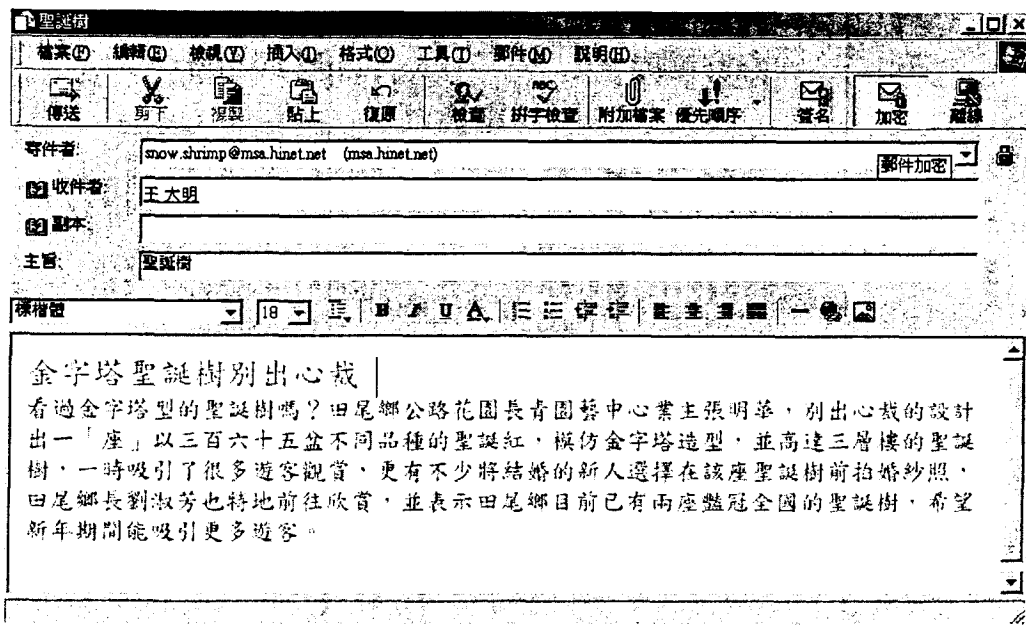


步驟三、在『數位 ID』頁籤，利用『匯入』按鈕將步驟一所下載的憑證檔匯入，畫面如下：

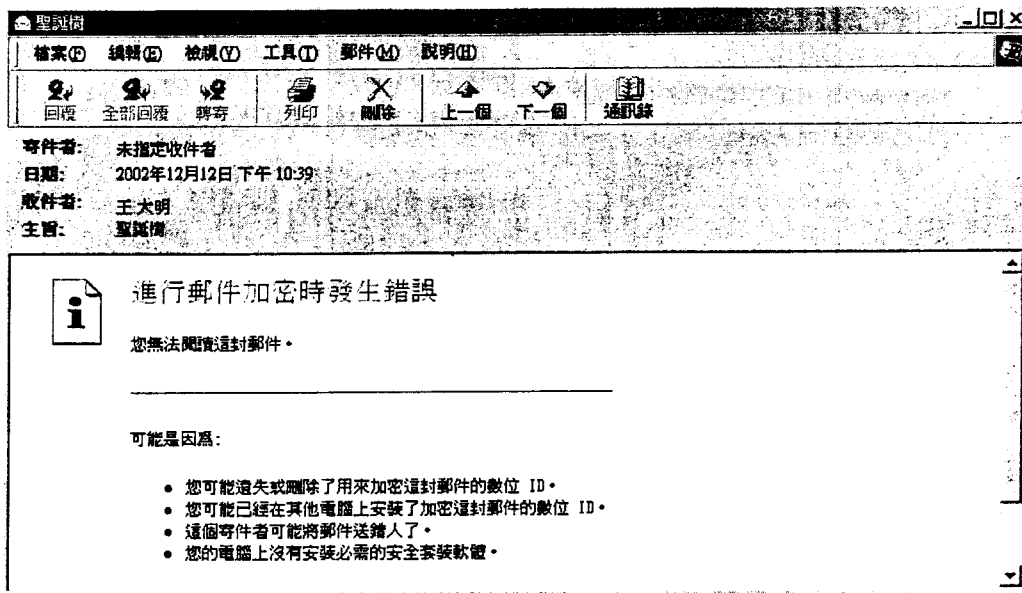


注意!! 通訊錄所記錄的電子郵件帳號，必須與收件者申請此憑證時所用的電子郵件帳號相同。

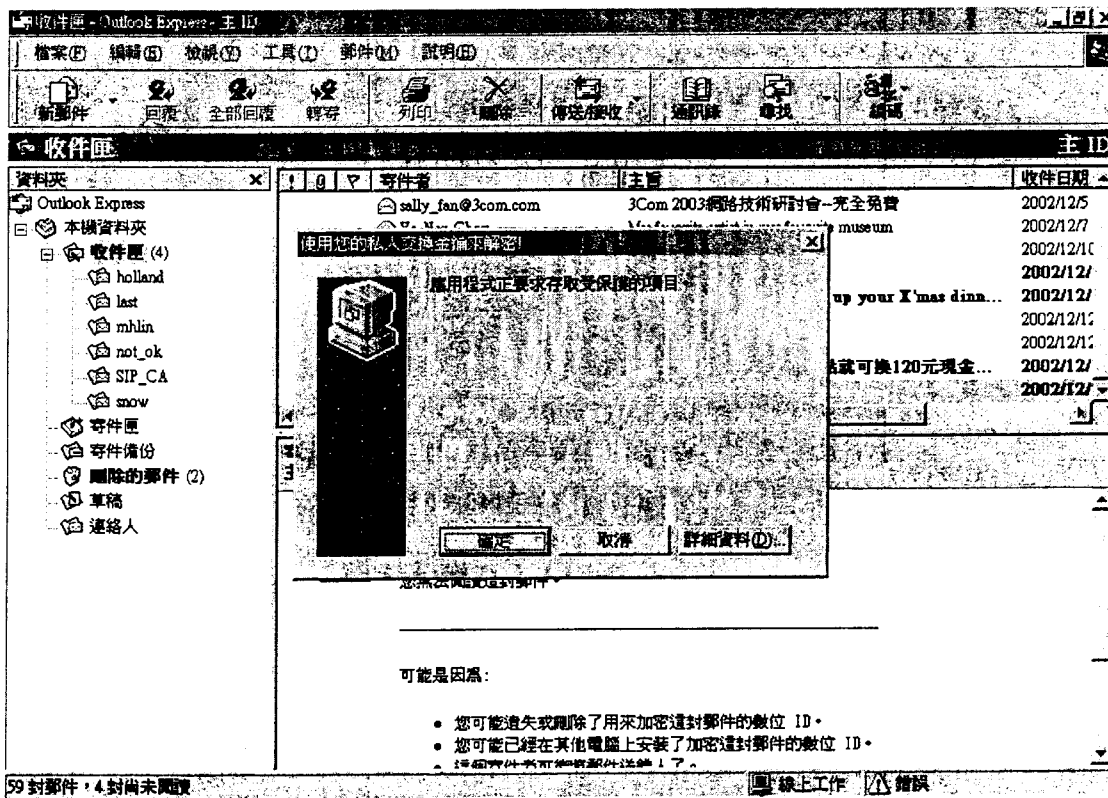
步驟四、經過以上的動作後，我們已經有了「王大明」的 Email 帳號及數位憑證了，我們現在就可以寄發加密後的電子郵件給王大明了。在 Outlook Express 撰寫一電子郵件，收件人為王大明，按下郵件右上角的『加密』按鈕，再按下『傳送』鈕便可以寄送加密的電子郵件了。因為加密是使用這個憑證內的公開金鑰，所以只有擁有私密金鑰的人才能夠閱讀這封加密後的電子郵件。



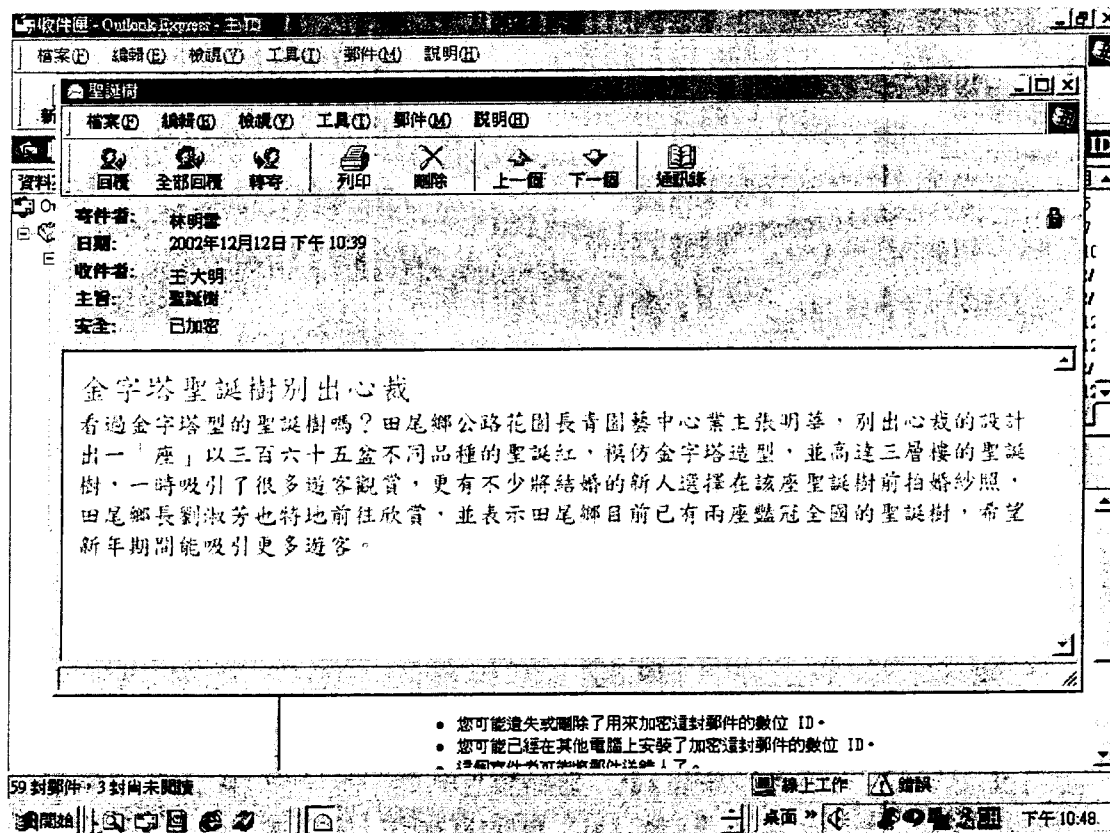
電子郵件的收件者若沒有可以解密的私密金鑰，會看到如下的畫面：



若收件者擁有私密金鑰則會出現如下畫面：



經過私密金鑰解密後，收信者即可看到正確的電子郵件了。



此外，在 Outlook Express 中設定目錄服務的帳號後，你也可以用 Outlook Express 通訊錄中所提供的『尋找人員』功能，到 OpenLDAP 目錄服務伺服器上尋找收件者的憑證來寄送加密的電子郵件。