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

表 目 錄

圖 目 錄

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（transparant）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的資料庫，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

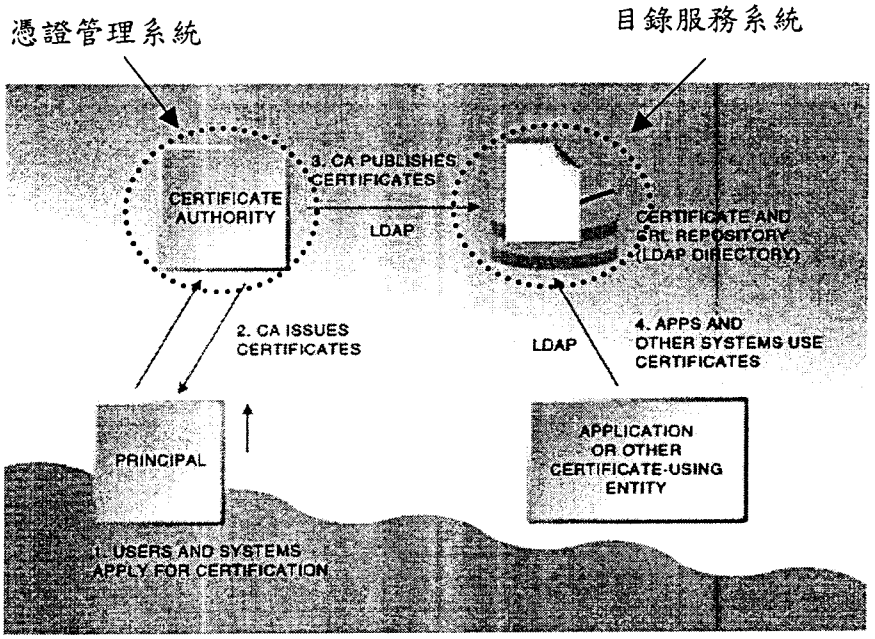
- 憑證管理系統（CA, Certificate Authority）

  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

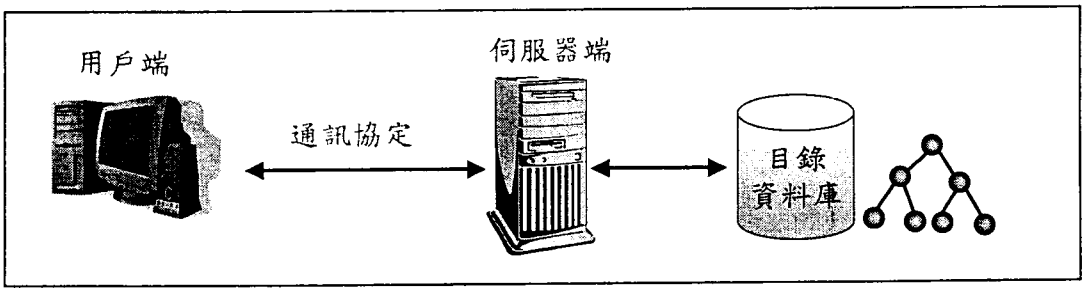
目錄服務為一個特殊的資料庫，其將資料組織並儲存起來，提供一個快速的搜尋機制讓使用者獲得所需的資訊。早在 1986 年，Banyan 便推出目錄服務，而 Novell 也於 1993 年於其 Netware 作業系統附上 NDS(Novell Directory Services)。Internet 上陸續也有許多公司，如：Yahoo、Bigfoot 等都有提供目錄服務，但各

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。