網路安全實作－憑證發行中心

洪傳榮、謝志騰、吳懿峰、黃國政
南華大學資訊管理系
周志賢副教授
jschou@mail.nhu.edu.tw
南華大學資訊管理系

摘　要

有鑒於網路駭客為數不少，加上我們對於這種方向感興趣，而選擇此題目。電子憑證主要之功能即在於證明電子文件簽署人之身分、資格。以電子簽章法所揭發之運作機制來說，因為憑證機構經過嚴格之身分驗證程序，確認數位簽章使用人之身分真實性，本於其驗證之感知，憑證機構始簽發電子憑證，以證明數位簽章使用人之身分真實性。

關鍵詞：憑證、憑證授權單位（CA）、公開金鑰基礎架構（PKI）

壹、緒論

■ 個人數位憑證就如同您的 Internet 電子護照，可以有以下的目的：

1. 電子郵件加密，該看的人才看得到，不該看的人無法閱讀。
2. 電子郵件簽名，如同您本人簽章，想假也假不了，想改也改不掉。

貳、相關文獻探討

一、憑證

與特定「主體」之「公開金鑰」有關、並經過數位簽署的一份聲明，而簽署者即爲該份憑證的「發行者」（所以「發行者」也必須握有另一對私密與公開金鑰）。您也可以把憑證稱爲「數位身分證」。

二、憑證授權單位

核發憑證的實體或服務，並扮演著驗證「主體」公開金鑰與其憑證內的身分資訊之間鏈結關係的「保證人」。

三、公開金鑰基礎架構

運用「公開金鑰密碼學」提供了一整套的服務和管理工具，以建立、部署、與管理植基於公開金鑰的應用程式。

參考文獻

【1】 布雷斯佛德/陳世訓/陳淳哲/Brelsford Harry M. 編著，「Windows 2000 Server 建構徹底研究」，臺北市/旗標/民 89

【2】 施威銘研究室著，「Windows 2000 Server 系統實務」，臺北市/旗標/民 89

【3】 羅塞爾 (Charlie Russel), 克勞福 (Sharon Crawford), 吉蘭德 (Jason Gerend) 原著/路德工作室譯著，「Microsoft Windows 2000 Server 超級管理手冊」，臺北市/文魁資訊/2003[民 92]

【4】 張凱傑編著，「Windows 2000 Server 系統安裝與管理」，臺北市/知城數位科技/2003[民 92]

【5】 施威銘研究室著，「Windows Server 2003 架站實務」，臺北市/旗標/民 92

【6】 陳彥學編著，「資訊安全理論與實務」，臺北市/文魁資訊/2001[民 90]

【7】 王國榮編著，「Active Server Pages & Web 資料庫」，臺北市/旗標/民 88[1999]

【8】 徐世豪,吳宗穎,李逢春編著，「ASP & ACP 之網路程式設計」，臺北市/儒林/1999[民 88]

【9】 李勁編著，「精通 ASP 資料庫程式設計」，臺北市/文魁資訊/2001[民 90]

【10】 陳會安編著，「Active Server Pages 3.0 網頁設計範例教本」，臺北市/學貫行銷/2001[民 90]

【11】 史密斯(Steven A. Smith)等著/普悠瑪數位科技譯，「ASP.NET 實例導引」，臺北市/碁峰資訊/2002[民 91]

【12】 陳峰棋編著，「深入淺出 ASP.net 程式設計」，臺北市/知城/民 92[2003]

【13】 一心工作室編著，「網路資料庫程式設計實務」，臺中市/松橋數位科技/2001[民 90]

【14】 李勁,蕭顯勝編著，「資料庫系統理論與實務」，臺北市/文魁資訊/2002[民 91]

【15】 劉杰編著，「網頁資料庫整合精華錄」，臺北市/金禾資訊/2001[民 90]