CA Live-CD：開放原始碼下中文化認證中心的設計與實現

鄭佩技 國立高雄師範大學資訊教育研究所

楊中皇 國立高雄師範大學資訊教育研究所

摘要

現今人們透過網路蒐集、交換各項資訊已成為擷取資訊的主要來源，網路商店的電子交易也大為興盛。然而在網際網路內進行交換資訊的同時，資訊安全愈形重要，如何保護重要資訊不被竊取、盜用，為網路安全的重要議題。在過去，以通行密碼的資訊系統容易遭人入侵也很難確實得知使用者身份的缺點，對商業金融等需要高度機密的單位，實是一大弱點。近年來公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)的興起，強化了使用者認證的機制，也提供了電子文件的電子簽章，達到資料的不可否認性及使用者身份的保護。

因此建制一個符合 PKI 的安全管理系統，將是刻不容緩的課題之一。在本研究中我們探討憑證中心之組織架構與實作憑證中心時的相關問題與解決方案。同時我們也以開放原始碼的的 OpenCA 系統為基礎，開發一個中文化的憑證管理中心系統，來有效加強網路傳輸的安全。我們也製作一個可攜式的憑證管理中心，結合 IC 卡的應用，以便快速有效的建置認證中心。

關鍵字：PKI、憑證管理、Live CD、電子簽章、數位簽章

1. 緒論

目前全球上網人口已達數億，各個行業的經營也越來越離不開電腦和網路系統。當企業或組織機構想要以網際網路來延伸業務範圍時，除了相關的程式要調整外，最重要的問題便是資訊安全方面的考量。目前網路電腦安全的系統中，主要的安全問題來自於使用者身份驗證，只要使用者身份驗證問題能解決，網路安全問題也可以迎刃而解。但是透過網路並不像人與人之間能互相面對面驗證身

份，所以必須依賴使用者與電腦之間共享的資訊來驗證身份 [8][12][18]。

本研究中，我們透過修改開放原始碼 OpenCA [5]，製成中文化的憑證管理系統，讓各行各業可擴展安全的網際網路業務。再者將之製成 Live CD 讓每個單位都可以快速的建置認證中心。同時配合我們開發的客戶端程式，結合 IC 卡 [14]的應用，讓企業可以更簡易且方便的應用憑證在各個資訊與網路安全領域中。

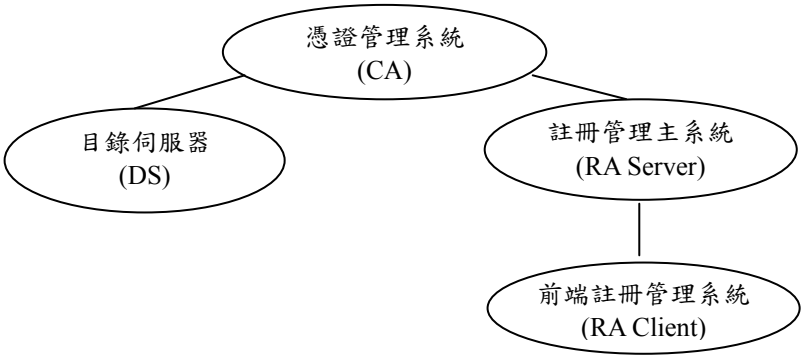
2. 文獻探討

2.1. 公開金鑰基礎建設

公開金鑰基礎建設 [1][3][7]是以公開金鑰密碼學技術為基礎而衍生的架構，運用公開金鑰及公開金鑰憑證以在電子訊息傳遞與交換過程中，確保訊息的身分鑑別（Authentication）、資料完整（Integrity）、不可否認性（Non Repudiation）與私密性（Private）等資訊安全四大需求功能。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 [17]之有效性及真實性，克服網路交易匿名性所造成的不信任感，交易雙方相互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，即可經由憑證管理中心核發的電子憑證 [1][6][13]確任彼此身份，提供資訊安全的保障。

2.2. 憑證管理服務

為使公開金鑰基礎建設 [15]能順利運作，需建立相當的資訊系統，用以管理使用者金鑰及憑證，憑證授權機構(Certificate Authority，簡稱 CA) [8][11][19]以具公信力第三者的身分，利用憑證管理資訊系統(包括：憑證管理系統、註冊管理系統、目錄伺服器)對憑證作業流程執行嚴密的管理，提供憑證管理服務。CA 服務項目包括：申請者註冊、憑證的簽發、廢止、管理、產生稽核記錄等。其架構圖如下：



圖一：憑證管理系統

2.3. OpenCA 憑證系統

2.3.1. OpenCA 計畫

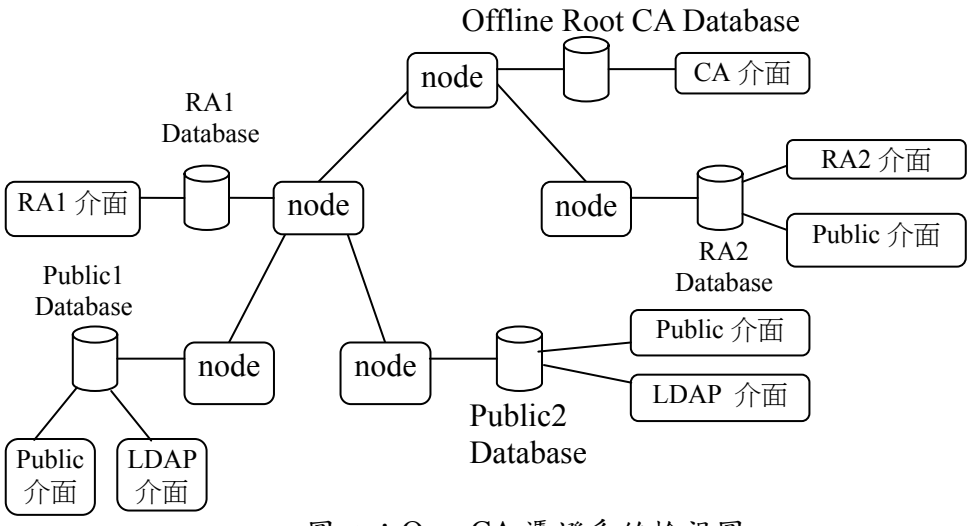
目前最被信賴的公開金鑰基礎建設存在一個很大的的問題，雖然它能強化應用程式的安全性，但是憑證及金鑰卻難以設定安裝，而且必須花費高昂的成本，才能夠使用。基於這樣的理由，OpenCA [5]開始發展。

OpenCA PKI 發展計畫起於 1999 年，致力於發展一個強健且全方位的開放原始碼程式。它是根據多個開放原始碼計畫，可以支援以下程式：OpenLDAP、OpenSSL、Apache Project、Apache mod_ssl，來結合各個應用。這個發展計畫分成主要兩個部份：研究及強化安全基模，確保最安全的憑證模型，及最方便的安裝及管理。

2.3.2. OpenCA 的基本架構

從 OpenCA 的基本架構來看，它的基本概念是每一個 X.509 [6]的 PKI 建設為一個強化的階層組織。因此在建置時，必須建立一個分散式的資料庫系統，利用資料庫來儲存管理使用者的所有資訊，如：憑證、金鑰、申請及註銷資訊...等。

而 OpenCA 在每一個資料庫之前都提供了一個管理的介面稱為 node(節點)，並提供網頁式的介面存取。OpenCA 分成三個主要的部份，以 Perl 做網頁介面，OpenSSL 做為後端的密碼技術，並利用 Database 來儲存管理使用者的所有資訊。系統管理者可利用這些介面依自己的所需來設定，並架設階層式的伺服器來分散流量負擔。一個完善的 OpenCA 憑證管理系統設計圖如下圖所示。



圖二：OpenCA 憑證系統檢視圖

2.4. Live CD

大多數的使用者都習於使用微軟的作業系統，不過近年來 X-windows 介面的設計已非常的完善，也漸漸帶動 Linux 的平台的興盛。伴隨著使用者不斷的增加，問題也隨之而來，雖然 Linux 為開放原始碼及免費使用，但其安裝設定卻不如微軟的方便。因此在自由的前提下，開始有人將 Linux 平台改寫成速成光碟版，讓使用者只需要將一片光碟置入，免安裝、而且無須硬碟就可以馬上直接在光碟上執行完整的 Linux 作業系統。這樣的 Live CD 既可以用來當桌上工作站用，也可以用來當網路伺服主機，十分方便。目前已有許多的 Live CD [9]釋出，較有名的如 KNOPPIX [4][20]、Mandrake Move、Fedora Live CD…等等，而微軟也推出 Windows PE [10]，更有進階版支援微軟系統掃毒的 avast! BART CD [2]出現。

2.4.1. KNOPPIX 介紹

KNOPPIX [4][20]是由德國程式設計師克勞斯(Klaus Knopper)設計的，以自由軟體 Liunx 的 Debian 套件為主要作業系統,利用特殊的壓縮技術將 GNU/Linux 的軟體收錄在光碟裡面，作為一個可開機的光碟。另外還透過一支內附的小程式，還可以將光碟上的系統安裝到硬碟中。

KNOPPIX 於 2000 年初步完成，可由網路上下載 ISO 檔自行燒錄成光碟，並且允許自由散佈與修改。KNOPPIX 可以用作 Linux 平台的展示、教學、急救系統、也可以自行客製化(Customization) [4][20]成自己所需的伺服光碟。

2.4.2. Windows PE 及 BART CD 介紹

微軟所推出的 Windows PE (Microsoft Windows Preinstallation Environment) [10]是一種精簡型 Windows 系統，以 Widnows XP Professional 和 Windows Server 2003 核心為主，提供有限的服務，讓 IT 專業人員的部署和修復工作省下更多時間，藉以提升生產效率。

同樣的 Windows PE 也可以做桌上型電腦和伺服器部署，微軟也與每個經過授權的 OEM 和 ODM 合作開發各種測試和診斷解決方案、支援工具組，以及零售應用程式。

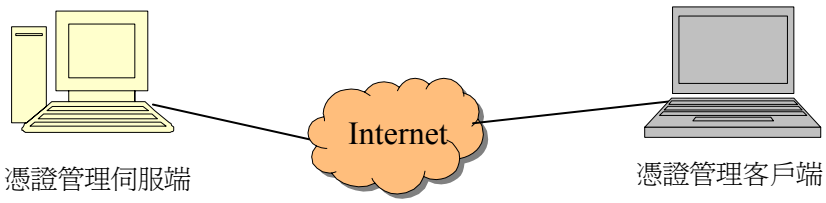
而 avast! BART (Bootable Antivirus & Recovery Tools) CD [2]除了給使用者開機的功能以外，更增加了偵測及清除病毒的能力，讓使用者可以快速的急救電腦

系統。但是 Windows PE 及 BART CD 都是屬於需付費且有版權的商業軟體，無法自由散佈及修改。

3. 中文化憑證系統實作

3.1. 系統架構

本研究所建立的憑證管理系統主要分成兩大部份，一為以 Linux 平台作為憑證管理伺服端，且將 Linux 平台製成 Live CD。二為以 C++ Builder [16]所開發的客戶端程式。其系統架構圖如下所示：



圖三：系統架構圖

為實現本研究的憑證管理系統設計，本研究分成以下三個步驟，來逐步完成：

一、我們在 Linux 平台下修改 OpenCA 的開放原始碼來架設中文化的憑證管理系統。

二、再以 KNOPPIX 為基礎將 OpenCA 納入光碟中，製成 CA 的 Live CD 光碟讓使用者可以輕易且快速的測試、使用憑證管理系統。

三、最後採用 Borland 公司的 C++ Builder 6.0 [16]做為開發客戶端軟體程式工具。客戶端軟體功能整合了憑證管理系統的主要功能：包含憑證/註銷申請、憑證/註銷憑證核准及發佈、下載憑證、辨識使用者私鑰身份，搜尋憑證及申請資料及資料庫備份。再將 IC 卡功能引進客戶端程式，使 IC 卡能記錄客戶的私鑰及他人的憑證，加強程式的安全性。

3.1.1. 憑證管理伺服端

本研究中憑證管理伺服端是在 Linux 平台上安裝並修改開放原始碼的 OpenCA 工具套件，結合 OpenSSL、Apache、mod-ssl、Perl5、MySQL 等套件完成系統的主架構。

OpenCA 架設啟動後，需透過瀏覽器連上使用，您可以看到 OpenCA 所使用

到的相關 Perl 模組套件及伺服器版本訊息(如圖四)。

圖四：憑證管理伺服器訊息

而 OpenCA 提供的介面主要有三個，讓使用者及 RA/CA 管理者可以連上網路進行申請憑證、管理系統的動作，三個介面分述如下：

1. Public 介面：提供一般使用者的操作介面(如圖五)，用來建立瀏覽器的憑證簽發請求(CSRs)。可以做客戶端申請要求及個人私鑰、取得伺服器端的 PEM 格式的 PKCS#10 請求、註銷憑證、註冊憑證註銷清冊、支援兩種註銷方式、搜尋憑證、瀏覽器線上測試使用者憑證。

2. RA 介面(如圖六)：提供處理使用者提出申請作業的要求，包含編輯申請、核准申請、建立使用者的私密金鑰、刪除錯誤的申請，及寄電子郵件給使用者。管理者在此審核申請者的資料，再批准審核通過的資料，送到最上層的 CA 伺服器來處理。

圖五：Public 介面

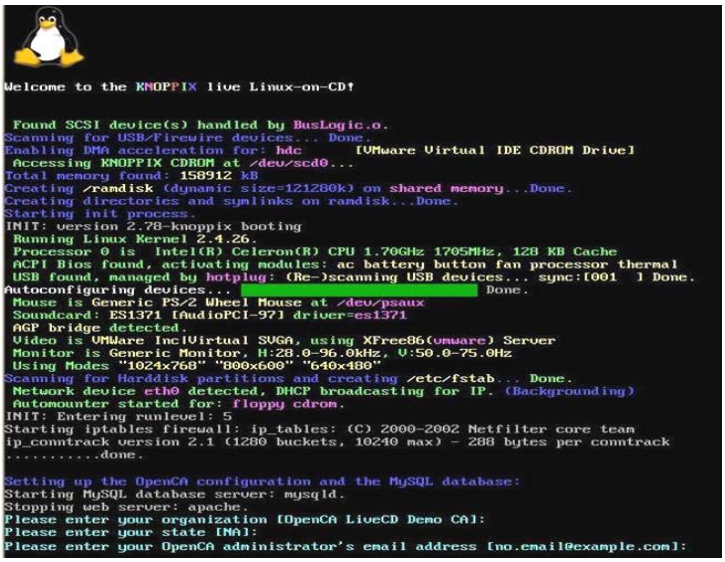
圖六：RA 介面

3. CA 介面(如圖七)：為系統最主要的部份，提供建立 CA Server 及使用者的憑證及憑證註銷清冊、改變系統設定及提供批次處理系統，讓管理者可以進行各項憑證作業。

圖七：CA 介面

3.1.2. CA Live CD 客製化

本研究以 KNOPPIX 的光碟作為基礎，新增中文化套件，以提供中文的作業系統介面及中文字型、中文輸入功能。由於中文化後，會佔用許多空間，因此也必須移除不必要的程式，以節省空間，才能再製成符合一般光碟的容量。然後再將 OpenCA 納入到 KNOPPIX 系統中，並加入開機執行檔，該使用者在開機時，可以依自己所需設定憑證系統名稱及管理者的電子郵件。最後再以其壓縮技術，將修改過的 KNOPPIX 重製成中文的 CA Live CD，如此一來便可輕易的架設一台憑證管理系統伺服器了。(如圖八)



圖八：CA Live CD 啟動畫面

3.1.3. 憑證管理客戶端

本研究利用 C++ Builder 來開發 CA 整合系統，使得憑證申請/註銷流程更為簡便。本研究所開發的 CA 客戶端之主程式(如圖九)用來整合憑證管理系統功能，提供一個單一的介面來進行各項憑證系統作業，避免使用者及管理者得不斷的切換網頁介面來操作各項功能。

圖九：憑證管理系統

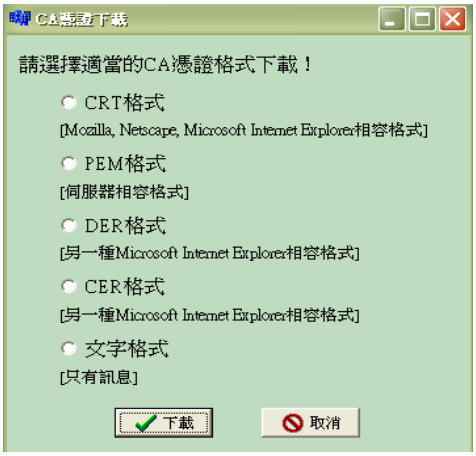
程式設計主要分成四大部份：申請作業、憑證作業、RA 管理及 CA 管理。為了確保系統安全，因此前兩項作業設定為任何人都可以使用，後兩項則須經由身份認證後確認為 RA/CA 管理者才能分別使用其功能。

申請作業主要有憑證申請(如圖十)、註銷申請(如圖十一)，提供給客戶做簡易申請資料。客戶只要在申請表填入適當資料，按下送出便可以將申請資料送往 RA 伺服端，讓 RA 管理者來進行審核使用者身份。另外，也可以利用查詢申請狀態的功能來瞭解目前個人的憑證及註銷的申請進度。

圖十：憑證申請表

圖十一：註銷申請表

而憑證作業則包含下載適當格式的 CA 憑證(如圖十二)、下載使用者憑證(如圖十三)、匯出憑證等。在通過 RA 管理者審核及 CA 管理者發佈憑證後，使用者便可以透過這項作業，將自己所需憑證及個人私鑰下載至個人的資料中，再利用匯出憑證的功能將資料儲存於 IC 卡或 USB 裝置中。



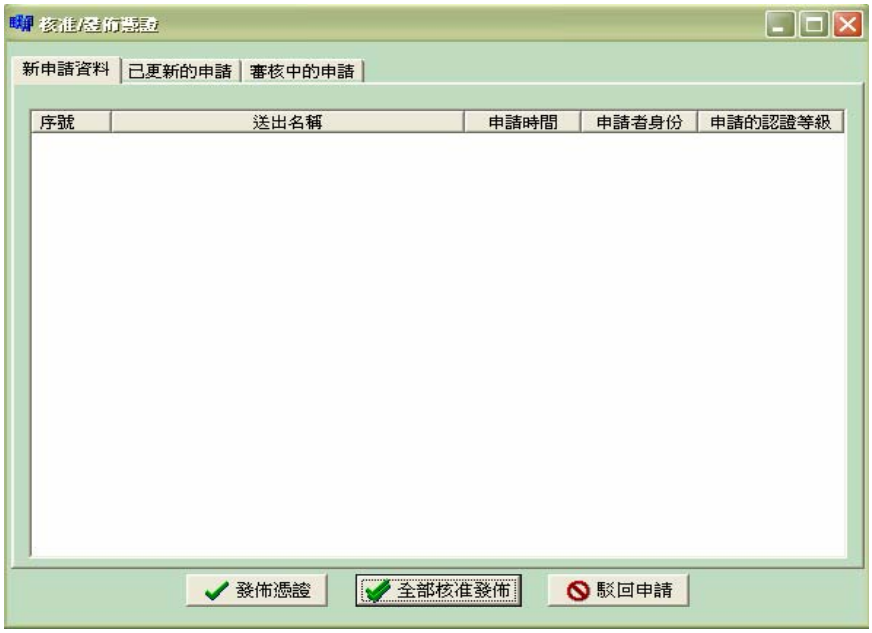
圖十二：下載 CA 憑證

圖十三：下載使用者憑證

RA 管理部份主要做為 RA 管理者審核使用者的申請用，來確認使用者身份是否正確。因此 RA 管理者必須在通過身份認證確認後，方可透過統一的介面看列表檢視內目前待審核的資料(包含新申請、更新申請)，做批次核准申請(如圖十四)，當然也可以單獨點選個別資料檢視每一筆申請資料的詳細內容，再做核准或刪除使用者的申請，最後將資料送往 CA 伺服器，由 CA 管理者來做最後的憑證發佈作業。

圖十四：審核申請

CA 管理部份主要是做為核准發佈使用者憑證(如圖十五)、核准註銷使用者憑證以及建立憑證註銷清冊。同樣的，想要使用 CA 管理功能也得先通過身份認證確認後才能使用。



圖十五：核准申請

除了以上四大功能外，我們還提供了資料庫備份及還原的功能，以儲存資料庫內的的資料。此項功能僅提供給 CA 管理者使用。

4. 結論

在 OpenCA 計畫提到希望能達到最方便的安裝管理，但由於它結合了相當多的自由軟體套件來完成其系統的建置，因此其安裝步驟及後續的設定步驟實在是相當的繁瑣。所以我們將使用者介面中文化，並利用 KNOPPIX 的特性將整個系統重製成 CA Live CD 後，使用者可省略在系統架設與設定上的困擾。

而管理及使用上，OpenCA 伺服端的主程式雖已提供了相當多的功能及介面讓使用者來使用，但需不斷的切換網頁來進行資料申請、審核及核准發佈的動作，使用起來有許多不便之處，所以我們開發客戶端程式，來整合 OpenCA 的所有介面的主要功能，讓使用者的作業能更簡化，也讓 OpenCA 更易於使用，成為各資訊系統使用的利器。

5. 參考文獻

1. Andrew Nash, William Duane, Celia Joseph, and Derek Brink, PKI: Implementing and Managing E-Security, 2002, McGraw-Hill.
2. avast! BART CD, http://www.avast.com/eng/avast_bart_cd.html, 取得時間 2005/3/15。
3. Dartmouth PKI Lab, http://www.dartmouth.edu/~pkilab/, 取得時間 2005/3/15。
4. KNOPPIX, http://www.knoppix.org/, 取得時間 2005/3/15
5. OpenCA Labs, http://www.openca.org/, 取得時間 2005/3/15
6. R. Housley, W. Ford, W. Polk, and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt, 1999.
7. Shashi Kiran, Patricia Lareau, and Steve Lloyd, PKI Basics-A Technical Perspective,http://www.pkiforum.org/pdfs/PKIBasics-Atechnical_perspective.pdf , Nov 2002, 取得時間 2005/3/15。
8. Stallings W., Cryptography and Network Security Principles and Practices, 2002, 3/e, Prentice Hall.
9. The Live CD List, http://www.livecdlist.com/, 取得時間 2005/3/15。
10. Windows 預先安裝，http://www.microsoft.com/taiwan/whdc/system/winpreinst/default.mspx，取得時間 2005/03/10。
11. 行政院研究發展考核委員會，http://www.pki.gov.tw/，取得時間 2005/03/10。
12. 陳澤雄、林國任，『公開金鑰基礎建設之研究』，中華民國資訊通訊學會通訊，2001 年 3 月，第四卷，第一期，pp.43-56。
13. 陳淑鈞、游原龍，『數位證書登出及驗證之研究』，中華民國資訊通訊學會通訊，2002 年 3 月，第五卷，第一期，pp.89-98。
14. 黃瓊瑩、陳正鎔，『公開金匙憑證的標準與應用』，資訊安全通訊，1996 年 6 月，第二卷，第四期，pp.6-14
15. 楊中皇，『密碼學演算法於 IC 卡上的具體實現』，資訊安全通訊，2002 年 6

月，第八卷，第三期，pp.8-17

16. 蔡孟凱、雷穎傑、黃昭雄、陳錦輝、陳正凱，C++ Builder 6 完全攻略，2003 年，初版，台北：金禾資訊。

17. 樊國楨、方仁威，『電子簽章法及其應有之安全規範芻議』，資訊安全論壇，2002 年 4 月，第五期，pp.20-35。

18. 劉燦雄、樊國禎、方仁威，『密碼學與憑證機構互通簡介』，資訊安全論壇，2002 年 4 月，第五期，pp.7-19。

19. 賴溪松、韓亮、張真誠，近代密碼學及其應用，2003 年，初版，台北：旗標出版股份有限公司。

20. 謝法安，行動 Linux─KNOPPIX 改造手冊，2003 年，上奇科技。