公開金鑰基礎架構之憑證廢止清單相關技術探討

學生：蔡林彬　　指導老師：黃景彰 教授

羅濟群 教授

國立交通大學資訊管理研究所

摘　要

近幾年隨著公開金鑰基礎架構技術的演進逐漸已開始應用於資訊安全機密的保護與彼此相互信任的工作。公開金鑰基礎架構雖然並不是一項嶄新的技術，但經由不斷的改善後，已經可以滿足個人、企業與政府機關的需求。一般而言，目前公開金鑰基礎架構使用在機構之間的身份確認、機密資料傳輸與授權的行為與將這些概念與功能應用在網際網路的相關領域。

對公開金鑰基礎架構而言，最主要系統安全維護機制是憑證註銷清單。使用憑證註銷清單可以在憑證授權後，仍需持續監控與管理對憑證使用生命週期的狀態，以確保整個系統正常可用性。除此之外，還有一些問題包含信賴團體信任行為與憑證持有者權限等也都需要一併考慮到憑證註銷清單的範疇。因此，憑證註銷清單定期發行機制對公開金鑰基礎架構系統安全的重要性是不容忽視的。直到目前為止，仍然存在著一些效率與安全性議題需要去解決與深入探討的。

本論文重點主要是介紹公開金鑰基礎架構與其憑證註銷清單相關概念。而其他部分還包含各種憑證註銷清單定期發行機制的探討與個人在 P2P 方面的應用研究，探討其整合性概念說明公開金鑰基礎架構的憑證註銷清單與 P2P 架構整合

探討。另一方面，在附錄與論文相關憑證實作範例也以微軟伺服器 2003 作業系統所提供公開金鑰基礎架構與憑證註銷清單作說明。

關鍵字：公開金鑰基礎架構、憑證廢止清單、點對點對等連接

The related technologies about Certificate Revocation Lists of Public Key Infrastructure

Student: Lin-Pin Tsai **Advisor: Dr.** Jing-Jang Hwang
Chi-Chun Lo

Department（Institute）of Information Management
National Chiao Tung University

ABSTRACT

These years, Public Key Infrastructure has been developed to solve the rapid growth of security and trust assurances. Although Public Key Infrastructure is not new technology, it has already improved to satisfy with the requirement of individuals, enterprises and governments. In general, Public Key Infrastructure is used to support authenticated, secure communication and authorization between parties and the concept also allows these functions to be achieved over the Internet.

Certificate Revocation List is the primary protection system for Public Key Infrastructure. The certificate authorities keep tracking the status and managing the life cycle of certificate by Certificate Revocation Lists. Therefore, some issues need to be consider about communication between trust parties and certificate holders. The mechanisms about publish Certificate Revocation Lists periodically is also very important part for Public Key Infrastructure. Until now, there still exists some performance and security consistency problem need to be resolved.

The goal of this paper aims to introduce Public Key Infrastructure and Certificate Revocation Lists concept. The remaining part will focus on discussing the period public mechanisms of Certificate Revocation Lists and illustrate the concept and architecture about P2P integrated with the Certificate Revocation Lists of Public Key Infrastructure. Finally, try to create an environment to simulate Public Key Infrastructure in Microsoft Server 2003 and using the features within there to indicate how Certificate Revocation Lists work in this environment.

Keyword：PKI、CRL、P2P

誌 謝

交通大學師資與設備是我學習生涯中，資源最為豐富的教育環境。圖書館裡論文資料與內部相關書籍，是我學習之路中最好的書籍資料庫。而在資管所寶貴學習時間，接受學有專長與多年教學經驗教授們的教導，令我如沐春風般的學習與成長。在這短短幾年在交通大學學習，使我在探索知識與作系統化分析與自我研究與解決問題能力方面獲得精進。

在學習過程中，很幸運結識不少良師益友，除了在學習上互相砥礪，在生活上也彼此相互照顧。除了告別漫長的研究生生涯之外，更感謝在這段時間中幫助我體諒我的諸位貴人。尤其是在工作單位同事與主管間的相互體諒，使我在從事繁忙的產品研發軟體設計工作之餘，得以專心於論文研究撰寫工作。

本論文要特別感謝指導教授黃景彰老師的教導，帶領我進入密碼與網路安全的領域，瞭解公開金鑰研究領域並在學術研究與為人處事上使我有不少領略與成為學習楷模。促使個人得以應用相關的工作經驗與技術專長與此論文的資訊安全領域結合，完成此研究著作。

最後更要感謝拉拔我長大的父母，感謝您們多年的照顧與栽培。在我研究生與工作忙碌之中協助我處理生活瑣碎之事，使我不致分心去處理生活瑣事而缺乏時間作論文研究的工作。

要感謝的人真的很多，非簡短言語可形容。在此向所有曾經協助我的人，獻上我最誠摯的謝意。

目　　錄

表目錄

圖目錄