植基於屬性憑證之授權管理基礎架構

研 究 生 ： 汪清華　　指導教授：黃景彰 博士

劉敦仁 博士

國立交通大學

管理學院（資訊管理學程）碩士班

中文摘要

公開金鑰基礎建設（Public Key Infrastructure, PKI）是以公開金鑰密碼學技術為基礎而衍生的架構，以解決網路使用者身分鑑別的問題；「授權管理基礎建設」（Privilege Management Infrastructure, PMI），X.509v4 中對 PMI 定義為「一種能夠支援權限管理，而用以支持廣泛的授權服務（簽發及管理屬性憑證），並與公開金鑰基礎建設相關連的基礎建設」，而 PMI 是在 PKI 的基礎上解決使用者授權控管的問題。

本研究主要是在網路環境運作架構中解決組織資源存取權限控管問題，我們以空軍總部架構為範例，運用屬性憑證（Attribute certificates, AC）設計整體授權管理架構，而授權連結的體係是以「業務」為主體，而不是以階層式的設計建置 PMI，憑證的授權運作是由業務憑證管理中心執行（Independent Business Certificates Unit, IBCU）。授權模式區分組織內部及外部，組織內部的授權管理是基於職位（Role）為主體的模式，經由職位的指派而間接賦予相對映的權限；組織外部則以是用戶端（Client）為主體，經授權管理者直接賦予資源存取權限。

此授權模式架構的設計可彈性的配合組織架構而修改，以職位指派間接賦予工作權限，在管理上獨立授權作業，可有效的提昇組織資源管理的安全性，運用屬性憑證區分授權管理作業與資源管理作業，分工明確可以提昇授權管理的運作效能，以達成一致性的身分鑑別及資源執行權限控管，使組織 PMI 更完整。

關鍵字：公開金鑰基礎建設、授權管理基礎建設、鑑別、屬性憑證、授權政策

Design of Privilege Management Infrastructure based on attribute certificates

Student：Wang, Ching-Hua　　Advisor：Dr. Jing-Jang Hwang
Dr. Duen-Ren Liu

Institute of Information Management

National Chiao-Tung University

ABSTRACT

Public Key Infrastructure, a framework derived from the Public Key Cryptography technology, is to solve the problem of the authentication among network users. Privilege Management Infrastructure is defined in X.509v4 as「The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a public key infrastructure.」 So PMI is designed to solve the problem of user privilege management on the basic of PKI.

This study is focused on solving the problem of the management of accessing organization resource privilege among the framework of networks operation, using Attribute Certificates to design the CAFHQ management framework of whole organization privilege.The object of privilege chain is「Independent business」, not hierarchy PMI structure. IBCU, Independent Business Certificates Unit, controls the operation of certificates privilege. The models of privilege management are divided into interior and exterior—the interior model is basic on the Role, and the exterior model is basic on the Client.

According to different organizations, the designs of privilege frameworks can be revised resiliently. Giving the privilege indirectly by assigning roles and exercising the operation independently in management can efficiently improve the security of organization's resource management. The clear division of labor can advance the efficiency of privilege management. Through this, the unity of user identification and resource access control can be achieved, and make the PMI of organization more perfect.

Keywords：Public Key Infrastructure, PKI；Attribute Certificate,AC；Privilege Policy；Authentication；Privilege Management Infrastructure,PMI

誌謝

本論文得以順利完成，首要感謝的是我的指導老師黃景彰博士，在與老師的求學過程中，除了吸收專業領域的知識外，對於人生未來的規畫與做人處事的經驗教導，更是受益良多，深深的一鞠躬，謝謝您的提攜與照顧。

此外感謝交通大學資訊管理研究所羅濟群老師及劉敦仁老師、長庚大學資訊管理研究所蔡榮隆老師於百忙中抽空擔任口試委員，對我的指正及教誨，使得本論文能更臻完善；以及感謝資管所的老師、所辦、交大的同學及長庚大學資管所資訊安全實驗室的學弟妹們，在求學過程有了你們的指導、協助與陪伴，才造就今天的我，謝謝你們。

在工作上我要非常感謝我的署長何屏東將軍，對我及我家人的照顧，使我能兼顧工作與學業，讓我第一次感受到好長官的風範與慈愛；以及單位內所有的長官及同仁對我的鼓勵與支持，你們都是我的貴人。

最後要感謝我爸、媽及丈母娘的照顧與支持，及老婆大人二年的書童日子，過著極度無趣的生活，真是辛苦您了。還有所有的家人及親朋好友，因為有你(妳)們對我的全力支持，我才得以全心投入，並順利完成學業。

在此致上我最深的謝忱

目　錄

表 目 錄

圖 目 錄