一個具有強韌性代理者管理服務的安全式軟體代理者架構

胡毓忠　國立政治大學資訊科學學系
計畫編號：NSC-89-2213-E-004-002

本研究之適用廠商：1.電子商務公司(如網路銀行) 2.PKI 公鑰匙架構發展公司 3.資訊安全軟體開發公司

一、簡介

利用分散式資源控管架構如 SPKI/SDSI 及 X.509 的標準來建立一個以代理者（Agent）為導向的公鑰匙架構（PKI）是本研究的主要目的。因為利用並發展代理者系統使其成為網路仲介者將是未來的一個趨勢。因此一群代理者軟體將利用我們的 Agent 為導向的 PKI 來進行各式各樣的授權和認證。這些授權的機制將包含有：串連式授權，門檻式授權，及條件式授權。

現階段因為 FIPA 標準協會缺乏 Agent 安全式的管理標準來提供給 Agent 進行可信度的管理和授權並同時兼具有法定的保障功能，因此我們也提出一些簡單的代理者溝通時所用 conversation act 來滿足我們在利用 Agent 授權及可信度管理時的需求。具體的來說，本研究將藉助一個網路銀行來說明如何在以 Agent 為仲介者時透過 Agent 為導向的 PKI 架構來完成可信度及授權的管理和驗證。

總結來說，本研究是在以 Agent 為導向的 PKI 中利用多樣化可供代理者軟體使用的電子數位憑證（Digital Certificate or Digital Credential）並配合網路環境中的服務及資源的提供者的憑證驗證引擎來完成電子憑證的可信度及授權服務的管理和驗證。

本研究的成果已經發表於世界知名的 2001 年自主性代理者研討會（The 5th International Conference on Autonomous Agents, Montreal, Canada, May 28–June 01, 2001）中，我們希望對於未來能將此技術及概念提供給 FIPA Agent 協會於制訂 Agent 安全服務規範時的參考，並希望在本研究系統開發時能累積出如何建立一個以 Agent 為導向 PKI 架構的經驗，以做為國內有興趣開發此系統的廠商能透過技術移轉的方式來建立一套商業用的軟體工具，來提供給全世界知名電子商務公司在利用 Agent 為仲介者時能加強其授信服務的管理。

二、研究方法

電子憑證或者數位憑證將是未來研究網路服務及授

信管理者的一個非常重要的依據。最新的研究趨勢是把數位憑證區分為三大類：身份憑證（Identity Certificate, ID-Cert），屬性憑證(Attribute Certificate, AT-Cert)，及授權憑證(Authorization Certificate, AU-Cert)。

ID-Cert 主要目的是把憑證當事人可區別的真實姓名和其公鑰匙做一個連結(binding)因此 ID-Cert 是由具有法定效力 CA（Certification Authority）認證機構來簽發； AT-Cert 則是把憑證使用當事人的可區別真實姓名和其個人所具有可能權力的屬性作一個相連結，AT-Cert 的格式中並不包含當事人的公鑰匙，在此 AT-Cert 也是有具有法定效力 AA（Attribute Authority）認證公司來簽發；至於 AU-Cert 則是把當事人的公鑰匙和其真實權力作一個相連結，因此 AU-Cert 是由具有網路上具有任何透過直接或者間接授權獲得此項權力的個別使用者的相關 Agent 來簽發。

除此之外，我們認為應該還有一種憑證，那就是規則憑證（Rule Certificate, RU-Cert），在此 RU-Cert 乃是資源或者服務的提供者對於授權憑證和應有權力作一個相連結的一種規則憑證，這種規則憑證則是存在於服務及資權提供者的憑證規則推論引擎之中，因此它們是由具有資源及服務管理者的使用者及其 Agent 來簽發。倘若資源要求者對於其自身擁有的憑證使用方式有一些條件設限以便於保護其自身的隱私權時亦可以做相對應的規則憑證的設定。本研究的初期僅利用 ID-Cert 和 AU-Cert 二種來進行我們的授信及授權的管理和驗證。

傳統的 X.509 的憑證為我們的 ID-Cert 的主要參考依據，而我們的授權憑證則是利用 Rivest 和 Lampson 最新提出的 SPKI/SDSI 憑證格式。因為我們的電子憑證正式提供給對等式通信方法的 Agent 來使用因此整個憑證管理的 PKI 架構將會比一般提供給主從架構的憑證使用和管理複雜。我們同時設計了使用者的 ID-Cert 和 AU-Cert 及 Agent 的 ID-Cert 和 AU-Cert。就理論上來說 Agent 的 ID-Cert 應該要能和其使用者主人來相連結，以方便在異常狀況發生時能夠追查出使用者當事人的法定責任，這是因為 Agent 在整個真實社會中是不具有法定責任的。至於 Agent 的 AU-Cert 則是源自於其主人先前所擁有的權力範圍和有限時效為主。現階段我們尚未考慮使用 AT-Cert 憑證於我們的 Agent PKI 中。至於 RU-Cert 我們則是採取了把屬性憑證相對應於資源服務提供者中提供的服務和資源的使用權限以固定設定的方式來進行。

未來我們將同時融合了 AT-Cert 和 RU-Cert 兩種憑證概念於我們 Agent 的 PKI 架構中來讓 Agent 能更有彈性的來選擇及設定其權力屬性的欄位，如此一來，Agent 將從其主人由不同 Attribute Authority 所獲得的 AT-Cert 將能更有彈性的由 Agent 來整合並且以動態的方式來對應於資源提供者的控管規則之中。

我們之所以會利用 Agent 軟體程式來代替使用者來進行各式各樣的網路活動及完成具有法定行為責任的交易，主要是因為 Agent 本身就是一個活在虛擬網路社會（Cyberspace）中的生物，來用 Agent 本身多樣化的溝通方式及其本身所具有的自主性正可以把我們在虛擬網路環境中的行為作有效率的完成。因此以 Agent 為仲介者來執行網路上使用者所授權的行為，如電子商務的交易正是現階段非常熱門的研究課題。但是 Agent 可

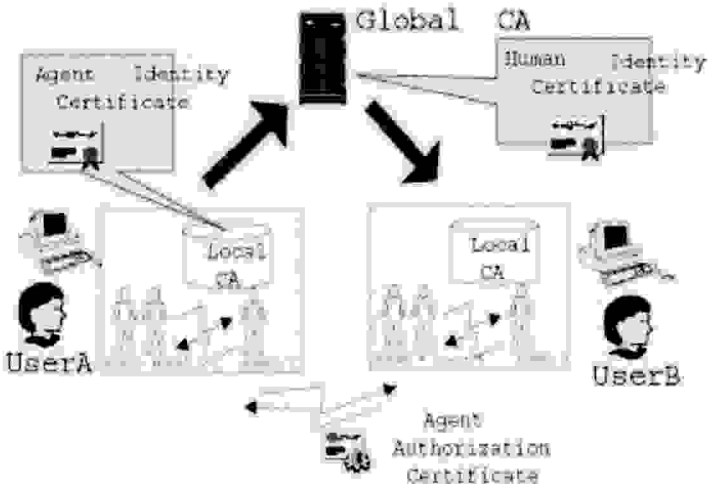
信度管理配合其由使用者的授信及授權問題倘若無法解決，則我們深信以 Agent 仲介者的研究當無法廣為大眾所接受，如此一來未來這項研究的成果成為實際商品化的情形將很難實現。因此這也是我們研究此項議題的主要原因。

基於我們是利用電子憑證的方式來進行 Agent 的可信度管理及其相關的授信及授權，因此憑證格式的設計及使用將會是一個首先需要解決的問題。我們因為只有 ID-Cert 及 AU-Cert 因此如何讓兩者之間能夠相關連並提供應該有的服務功能將是很重要的事情。在此我們並未從心裡及社會科學的角度來分析 Agent 的可信度和授權的管理。因此過去這方面的相關性研究只是提供我們當作背景資料來使用。一個以 Agent 為導向的 PKI 就架構圖可以如圖一所示。

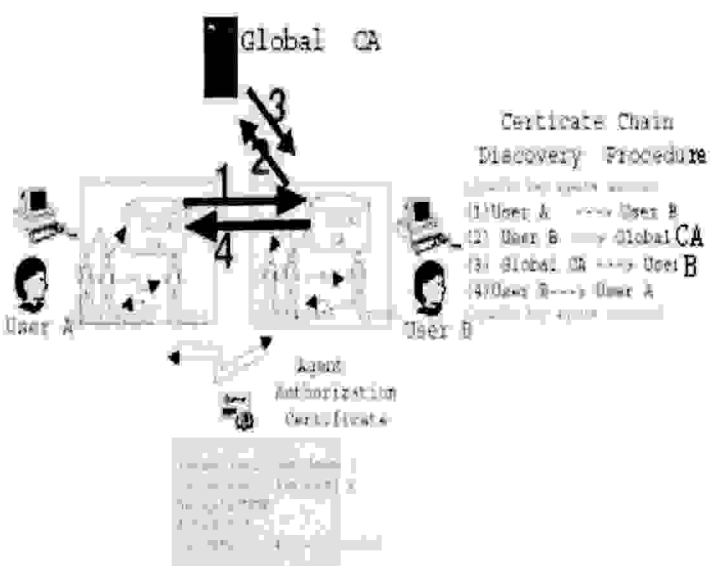
在這個以 Agent 為導向的 PKI 架構中，使用者的 ID-Cert 是存放在 global CA 之中而 agent 本身的 ID-Cert 則是存放在區域性的各 Agent 的 CA 中。對於 AU-Cert 而言，使用者對於 Agent 的 AU-Cert 是直接在使用者的電腦平台中完成，而 Agent 和 Agent 之間的授權則是可以彈性的在網路上透過相互之間的交換而來完成授權的動作。

因為 Agent 的授信及授權是以 AU-Cert 來進行，因此我們除非事先瞭解 Issuer 和 Subject Agent 的公鑰匙否則我們必須透過下列的查詢機制來完成 Issuer Agent 對於 Subject Agent 的公鑰匙查詢，如圖二所示。

在此圖二中很明顯的說明了一個使用者如何透過對方已知的唯一姓名來完成相對應其 Agent 的公鑰匙的查詢，以便完成接下來完成以公鑰匙授權和授信的動作。在整個授權機制上，我們使



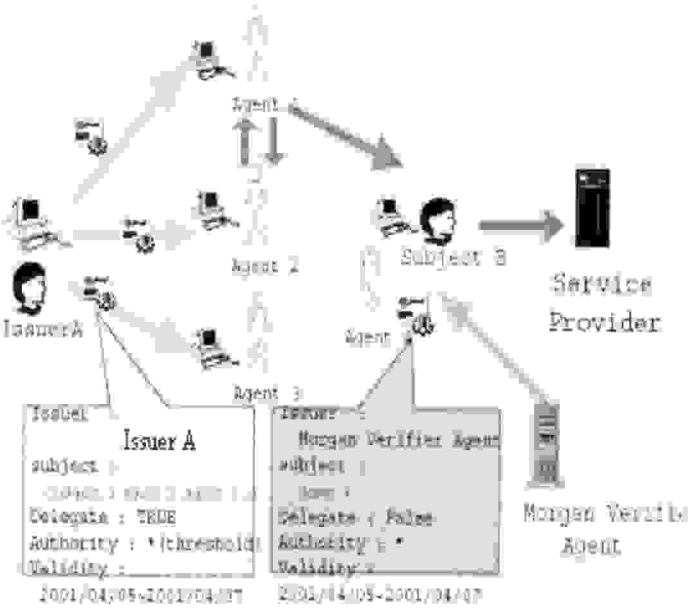
圖一　以 Agent 為導向的 PKI 架構圖



圖二　Agent 公鑰匙的查詢

用了：串連式授權，門檻式授權，及條件式授權三種方式來進行 Agent 和 Agent 之間的授權。而這三種授權的機制也可以加以混和使用形成一個 Agent 授權及授信網路（如圖三所示）以達到 Agent 授權的最大彈性。

除此之外，我們使用 Lampson 早期所提出的認證邏輯理論如完全授權的 speak-for 和部分授權的 speack-for with role constraints as 等來顯示 human 和 Agent 以及 Agent 和 Agent 之間的授權表達。例如當使用者說到我的 Agent 可以在任何的情況及條件下來代表本人時就是一個完全的授權方式；至於我所我的 Agent 只能在某個條件下來執行我的某些權力時就是部分授權的方式。至於完全授權和部分授權的表達我們都可以利用本人或者 Agent 所簽署的 SPKI/SDSI 電子憑證來表示在何種條件下誰授權給誰。



圖三　Agent 授權及授信的網路圖

三、結果

基於上述設計的理念和邏輯，我們以一個實際網路銀行的使用範例來展示我們的 Agent 導向的 PKI 架構該如何來被使用，並由相關性的 Agent 來做各式各樣不同型態的授權動作，已滿足由 Agent 代替使用者來進行網路銀行的存提款及轉帳的動作。

在此我們假設有一個公司的總經理 Bob 在 Morgan 網路銀行有一個存款的帳號，Morgan 網路銀行容許自己的客戶對自己銀行帳號的存提款做在授權的行為。因此，我們按部就班的表示 Bob 如何利用門檻式授權來授權自己的屬下來進行 Bob 帳號的存提動作。配合 Morgan 銀行內部驗證引擎的運作及整個授權過程中所有 AU-Cert 電子憑證的傳送及存放，我們可以看到我們是否允許某一個 Bob 屬下的經理來對 Bob 的帳號做提款的動作。

因為現階段 FIPA 標準對於 Agent 安全的規範還在起始的階段，因此毫無疑問的提供給 Agent 使用的電子憑證的 PKI 架構將會有一段時間來探討，因此我們也提供一些電子憑證管理的 conversation acts 給 FIPA 協會來做參考，配合 XML 及 XML/RDF 來對 Agent 的通訊外在及內在語言的使用趨勢，我們用一個簡單的範例來描述 Agent 和 Agent 之間該如何來對電子憑證作存提、查詢、及驗證的動作。希望在不久的將來能夠看到 Agent 研究的社群能夠在此方面的研究有一些具體的進展。本研究成果的詳細內容可以由 ACM 電子數位圖書館所提供的數位電子檔來做深入的瞭解（http://www.acm.org/pubs/contents/

proceedings/series/agents/)。

四、可應用範圍

本研究成果可以應用的範圍主要是以 agent 為導向的電子商務環境系統，因此舉凡電子商務系統該開發公司，Agent 系統開發公司，資訊安全軟體開發公司等，將會是有機會大量來使用本研究的技術和理念。

作者簡介

胡毓忠
國立政治大學資訊科學學系副教授兼系主任
美國密蘇里大學資訊科學博士
專長：安全式代理者系統架構；軟體代理者系統；網際網路安全
電話：(02)29387620
傳真：(02)22341494