行政院國家科學委員會專題研究計畫　成果報告

利用電子憑證來驗證開放式代理者電子化服務環境的可信度

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-004-014-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：國立政治大學資訊科學系

計畫主持人：胡毓忠

計畫參與人員：楊銘煇　唐朝緯　陳世庭

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 92 年 10 月 21 日

利用電子憑證來驗證開放式代理者電子化服務環境的可信度

(Trust Verification Through Digital Certificates for Open Agent E-Services Environment)

計畫編號： NSC 91-2213-E-004-014
計畫期限： 91/08/01 – 92/07/31
計畫主持人： 胡毓忠　　政治大學資訊科學系
計畫參與人員：楊銘煇、唐朝緯、陳世庭　　政治大學資訊科學

摘要

本研究的主要目的是利用電子憑証的使用，來驗証開放式代理者在進行電子化服務時的可信度。研究的重點包括：代理者系統的公鑰匙架構的建立及使用，利用語意網的技術來表達代理者間的資訊及知識並利用語意網的技術來表達代理者間資源控管的規則[1]。本研究初期將以傳統式的電子商務模式為主來進行分析及實作，未來將此概念應用在一個以代理者為主的電子化資訊網服務 （web services）上。在代理者之間的溝通協定是以抽象概念的交談協定為主，以便於具體化驗證本架構的可用性。代理者間的溝通則是建置一個具有可信度本體論 (trust ontology)供需要交談的代理者來參考，並配合代理者通訊語言 (Agent Communication Language, ACL) 的方式來完成具有語意能力的溝通，而資源控管的方式則是利用 RuleML 這一種表達規則的統一性的語言來制定資源控管的規則[3][5][7][10][11]。配合上述的各種技術以實現代理者軟體可以在語意網環境的資訊網服務的目的。

關鍵詞：軟體代理者、可信度、電子商務、電子化資訊網服務、語意網

一、　簡介

多代理者系統的安全和可信度的研究一直是本計畫主持人所領導研究團隊的主要研究方向。為了要落實代理者系統技術能夠被廣泛的使用在電子商務和電子化資訊網服務的應用領域之中，我們必須要有一套完整的機制來建構代理者系統的可信度的管理和驗證。實際上代理者在全球資訊網上的可信度研究可以從好幾個面向來探討，有的人是從心理學的角度來分析代理者在網路上進行各式各樣服務時的可信度驗證，有的則是從社會學的角度來加以分析。本研究群則一直是以安全的觀點來進行代理者可信度的分析。因此本研究的基礎是根據主持人發表在 2001 年於 Autonomous Agents, Montreal, Canada 的結果來加以擴充[8]，我們並將本計畫的部分研究成果發表在 2003 年的 The Seventh International Conference on Knowledge-Based Intelligent Information & Engineering Systems 的研討會上[9]。

二、　研究方法

我們的研究主要是承續過去在代理者系統的研究成果，首先先建立以代理者為導向

的公鑰匙架構 (Agent-Oriented Public Key Infrastructure)，目的是要先建立代理者與代理者之間的可信度關係，其中包含了系統架構的建立、憑證管理的機制、信任路徑的建立及信任程度的計算等。之後再利用語意網中本體論的技術建置一個可信度的本體論[11]。在本體論中我們定義包括：身份憑証、屬性憑証、授權憑証…等等與可信度相關的字彙來讓代理者使用。利用本體論的技術可以定義及規範各式各樣的詞彙與詞彙之間的關係以方便軟體代理者在進行自主式溝通時的語意上的瞭解。除此之外，為了確保整個可信度的可驗證性，我們定義資源控管的規則來規範可信度驗證的準則，當然有些規則將是以能夠平順的完成網路上的電子化服務為主[2][4]。為了確保這些規則的可交換性和整合，我們使用 RuleML 的旗標來表示上述相關性的規則，以確保網路上不同的推論引擎之間對於規則交換的處理能力。當然以本體論所定義的可信度詞彙再加以配合可信度規則，可以讓多代理者軟體進行具有語意層級的自主式溝通及驗證相互之間的可信度。

可信度驗證的步驟是由資源（服務）控管者啟動服務要求者的身份和屬性憑證的檢驗工作，如果通過此程序的檢驗則可以由資源（服務）控管者簽發授權憑證給服務要求者來進行各式各樣的授權，以取資源（服務)。我們分兩種模式來探討資源要求者和提供者的關係：封閉式及開放式。在封閉式的資源要求和提供的模式中，資源要求者的屬性憑證是由資源提供者所簽發，至於開放式的模式之中，則沒有此種限制。因為資源要求者和提供者皆為軟體代理者，因此我們設計了一些代理者程式間的溝通協定來描述上述的資源提供者與服務要求者之間的關係。至於規則憑證提出的目的則是為了提供資源提供者對於各式各樣資源要求者所做的規範，這些規範主要還是在對於相關身份和屬性憑證的設限條件。這些設限條件如果透過適當的表達和簽章將可以在網路上被交換及驗證，以達到條件交換、整合等目的，以方便於整個資源存取時的憑證準備和驗證的工作。

三、 未來研究

安全的議題包含甚廣，而在我們設計的設限規則內容中，主要都是圍繞在認證、授權等議題上加以發揮，然而規則在安全的應用還有許多發揮的空間，例如隱私權的規則設計，過濾電子郵件的規則，這些都是屬於安全規則設計的範疇，在未來我們希望可以納入這些議題，發展更全面的應用[2]。除了在安全規則及設計的延伸之外，擴展網路應用層面的安全議題，也是未來我們考量的重點之一，例如現在網路上所盛行的 P2P (peer to peer)網路服務的架構正在快速的興起卻也正面臨著很多安全的議題，未來我們也將著手進行這一方面的研究。

四、 結論

配合語意網的技術及代理者系統，我們成功的描繪出一個進行資訊網服務時的可信度檢驗的機制。一直以來代理者的可信度是一個備受關注的議題，因為如果無法明確的解決這個問題，使用者也不會放心的交付其代理者去代替他來執行任務。我們延續過去在電子憑証的研究以及多代理者系統的成果，利用電子憑証的管理及檢驗的機制來確保代理者之間的可信度。當然

這樣的模式建立其實只是達成可信度的最基本需求，完整的可信度達成可能還包括在進行資訊網服務時服務流程的可信度及其它安全的問題。我們的終極目標是要建立一個讓多代理者軟體可以自行使用的可信度驗證機制，以方便於代理者軟體可以自主的來進行相互之間的可信度驗證，而本研究中可信度建立則只是整體的資訊網服務的安全考量中的一個環節。

五、 參考文獻

[1] Adams, C., Burmester, M. et. Al., Which PKI (Public Key Infrastructure) is the right one? , *CCS'00 Conference, Athens,Greece*, 2000.

[2] Benjamin Grosof and Terrence Poon, Representing Agent Contracts with Exceptions using XML Rules, Ontologies, and Process Descriptions, *Proc. International Workshop on Rule Markup Languages for Business Rules on the Semantic Web*, Sardinia (Italy), June (2002).

[3] Foundation for Intelligent Physical Agents (FIPA), *http://www.fipa.org/*.

[4] Gerd Wagner, How to Design a General Rule Markup Language?, *Invited Talk, Workshop XML Technologien für das Semantic Web (XSW 2002)*, Berlin, June (2002).

[5] Harold Boley, Said Tabet, and Gerd Wagner, Design Rationale of RuleML: A Markup Language for Semantic Web Rules, Proc. SWWS'01, Stanford, (2001).

[6] He, Qi, Katia P. Sycara, and Timothy W. Finin. Personal Security Agent: KQML-Based PKI, *Proceedings of the Second International Conference on Autonomous Agents*, 1998.

[7] Hendler, J., Agents and the Semantic Web, *IEEE Intelligent Systems*, 16(2), (2001).

[8] Hu, Y. J., Some Thoughts on Agent Trust and Delegation, *The Fifth International Conference on Autonomous Agents (AA'01)*, May 28 – June 1, Montreal, Canada.

[9] Hu, Y. J. and C. W. Tang, Agent-Oriented Public Key Infrastructure for Multi-Agent E-Service, *Seventh International Conference on Knowledge-Based Intelligent Information & Engineering Systems (KES'2003)*, University of Oxford, UK.

[10] Jennings, N., Sycara, K. and Wooldridge, M., A Roadmap of Agent Research and Development, *Journal of Autonomous Agents and Multi-Agent Systems*, (1998).

[11] McGuinness, D. L., et al., DAML+OIL: An Ontology Language for the Semantic Web, *IEEE Intelligent Systems*, 17(5), (2002).