行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ **電子商務付款機制公平性之研究** ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：¬個別型計畫　　□整合型計畫
計畫編號：NSC　89－2416－H－009－021－
執行期間： 88 **年** 08 **月** 01 **至**　89 **年** 07 **月** 31 **日**

計畫主持人：黃景彰
共同主持人：

本成果報告包括以下應繳交之附件：
- □赴國外出差或研習心得報告一份
- □赴大陸地區出差或研習心得報告一份
- □出席國際學術會議心得報告及發表之論文各一份
- □國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊管理研究所

中　華　民　國　89 **年** 10 **月** 31 **日**

行政院國家科學委員會專題研究計畫成果報告

電子商務付款機制公平性之研究

On the Fairness of Payment Schemes for Electronic Commerce

計畫編號：NSC 89-2416-H-009-021-
執行期限：88 年 08 月 01 日至 89 年 07 月 31 日

主持人：黃景彰　　國立交通大學資訊管理研究所
計畫參與人員：邵敏華　國立交通大學資訊管理研究所

一、中文摘要

本研究定義了一般付款交易的價值移轉活動與不可否認服務，並且有效連結電子商務後端的物流配送活動。在證據處理方面，我們嘗試以證據責任鏈的概念來設計，這減少了因實行安全機制所帶來的系統負荷，同時也遵循實務上法制機關偵辦不法情事的證據處理方式。此外，我們以專家系統的方式來設計證據的檢驗規則，並且使用易於理解的電腦語法，來表達交易糾紛事件、證據的提示、推論規則、及仲裁結果等活動。

關鍵詞：電子付款、公平交易、不可否認服務

Abstract

To study the fairness of payment systems, we have redefined a model of value transfer activities that include logistics activities conducted through distribution channels. Based upon this model, we have introduced an "evidence value chain" into the non-repudiation service design. The security mechanism doesn't downgrade system performance and it is concordant with the requirements of current law enforcement. In the model, we have formulated rules of presentation to express disputes, evidence contents, inference rules, and adjudications in terms of natural languages.

Keywords: Electronic Payment, Fair Transaction, Non-repudiation

二、緣由與目的

網際網路的蓬勃發展，提供了一種新形態的商業環境，形成了電子商務。由於交易個體並不是直接面對面進行交易，使得在虛擬世界中從事商業行為，一個可信賴的、公平的交易環境是必備要件。如果交易的公平性受到了質疑，可能導致使用者參與電子商務的意願降低而裹足不前，則推行網際網路商業活動的發展將窒礙難行。

尤其，在這種開放的網路作業環境中，進行資金移轉的付款活動，對於公平與安全的要求更需嚴謹。如果因為電子交易過程保護不足，損害參與個體的權益，輕則影響參與個體的隱私權或延後交易的完成，重則導致交易錯誤，造成參與個體的損失或買賣糾紛。

基於上述電子付款環境欠缺公平性可能導致的缺失，本計畫乃應用公平交換協定進行電子付款協定的比較分析，並且以 SET 為例，設計了一個不可否認服務的處理機制。

三、結果與討論

為了建構一個公平的電子付款機制，本計畫參考了一些現有的公平交換協定，釐清電子交易應具備的公平特性。我們將先就公平性的意義作一個定義與分析，然後說明本計畫所設計的 SET 不可否認服務機制。

（一）公平性在電子商務中的意義

公平性在電腦科學中的應用，主要有二個意義：一是，操作行為必須是正確的、適當的、合理的或可接受的；二是，系統或事件平均地影響每一個項目，並且依循規則運作[3]。其中公平性在電子化商業環境的研究，稱為「公平交換（fair exchange）」。以下整理了相關學者定義的線上交易公平性[1,3,15]。

Asokan (1998)	強勢公平		劣勢公平
Gärtner (1999)	強勢公平	最後的強勢公平	劣勢公平
Vogt (1999)	F_6	F_5, F_4	F_3, F_2, F_1

一個交易系統要能夠保障強勢公平，是需要投入大量的通訊或計算成本、犧牲作業效率等，縱使如此，還不一定能完全達到要求。此乃是一般公平交換協定為人所垢病之處，因此提供「最後的強勢公平」或「劣勢公平」保障，較能符合實際環境的需求。而這兩個部份透過系統內參與者或者系統外的公正仲裁者，一起合作來解決爭議實現交易公平性。為達此目的，必須在交易過程中針對被提出的事件或動作來產生證據，並予以收集、維護、提供使用、及檢驗其有效性，解決關於事件或動作發生與否的爭議；此為「不可否認服務」系統的工作目標。

（二）一般付款交易的不可否認服務

實務上存在各種付款工具，這些差異多屬於作業處理方式的不同，如交易發生與實際資金轉移的時間點等，但都是協助不同個體間的價值移轉活動[9]。Pfitzmann等人[1]針對一般的付款交易，定義三種價值移轉行為的集合，即價值扣減(value subtraction)、付款(payment)、價值要求(value claim)。然而，我們從網路商店紛紛與加盟店或 ISP 業者等合作，如安瑟與 7-11 的結盟等，充分顯示了目前消費者網路購物所顧慮的因素，不僅止於付款交易的安全，尚包括電子商務後端的物流配送活動。ISO/IEC [4,5,6,7]定義了四種主要的不可否認服務，其中送件證明(NRS)與傳遞證明(NRT)適用於有傳遞機構協助訊息的傳送。為了有效連結線上付款與物流活動，提供一個完整的爭議處理系統，我們加入商品所有權轉移的機制，即價值委託(value submit)、價值傳遞(value transport)，以及傳遞機構(delivery authority)的角色，如表一。而為了有效規範一般付款系統的交易類別，乃將付款方與收款方的金融機構以銀行角色替代。

表一　一般付款交易的不可否認服務

交易活動		交易事件	證據	證據當事者	證據使用者
Value_Subtraction		deduct	NRO_Subtraction	Payer	Bank
		allow	NRR_Subtraction	Bank	Payer
Payment		pay	NRO_Payment	Payer	Payee
		receive	NRR_Payment	Payee	Payer
Value_Claim		add	NRO_Claim	Payee	Bank
		allow	NRR_Claim	Bank	Payee
Ownership Delivery	Value Submit	submit	NRS	DA	Payee
	Value Transport	deliver	NRT	DA	Payee

系統中每一個活動都是經由事件所促發，不可否認服務工作必須針對每個被提出的事件或動作來產生證據。基本上，付款系統中的主要交易事件[1]，包括付款(pay)、收款(receive)、扣款(deduct)、取款(add)、及授權(allow)，加上物流配送活動的委託(submit)與傳遞(transport)事件。這些交易事件的啟動者與接受者，通常就是證據的當事者與使用者，而產生的證據所代表的意義以及證據間的關聯性，參考表二。

表二　付款交易的證據

證　據	意　義	關鍵參考項目 (Reference Key Items)
NRO_Subtraction	扣款請求的證明	TIDs, CID, AID, Amount, Time
NRR_Subtraction	扣款授權的證明	
NRO_Payment	付款承諾的證明	TIDs, MID, CID, DAID, Amount, Time, Order
NRR_Payment	交易確認的證明	
NRO_Claim	請求兌現的證明	TIDs, MID, AID, AuthID, Amount, Time, NRS
NRR_Claim	承諾兌現的證明	
NRS	委託運送的證明	MID, CID, DAID, TIDs, Time
NRT	商品寄達的證明	

符號說明：CID-消費者識別碼, MID-商店識別碼, AID-銀行識別碼, TIDs-交易識別碼, DAID-傳遞機構識別碼, AuthID-授權交易碼, Amount-交易金額, Time-交易時間, Order-訂購資訊

（三）SET 的不可否認服務機制

SET 為一個推行多年的信用卡付款系統，但在其公開的標準規格說明書第二本第四冊中[14]，直接指出「SET 沒有支援不可否認服務」。我們利用一般付款交易的價值移轉活動，來分析各交易階段參與者在系統中的角色及產生的證據，如表三。持卡人端的電腦與銀行的金融網路沒有直接連繫，兩者間的互動必須透過商店代為轉送，故交易事件同時促發兩個或兩個以上的價值活動，卻不代表實際取得證據的時機。SET 中有兩個價值活動就屬於這種情形(表中上標數字)，一是購買請求事件的價值扣減活動，銀行實際取得該證據的時間，是在商店向銀行請求該筆交易授權的時候；二是授權回覆促發的價值扣減活動，持卡人需等商店回覆購買訊息時才取得該證據。從 SET 的價值移轉活動中得知，付款交易活動缺乏對後續物流配送活動的連結，無法強制要求商店確實履行商品或服務的交付。

表三　SET 參與者在不可否認系統中的角色

交易階段		價值移轉活動	系統中的角色		
			持卡人	特約商店	銀行
購買請求	購買請求	Payment, Value_Subtraction	證據當事者	證據使用者 NRO_Payment	證據使用者 [1]
付款授權	授權請求	Value_Subtraction ,Value_Claim		證據當事者	證據使用者 NRO_Claim, [1]NRO_Subtraction
	授權回覆	Value_Claim, Value_Subtraction	證據使用者 [2]	證據使用者 NRR_Claim	證據當事者
購買請求	購買回覆	Payment	證據使用者 NRR_Payment, [2]NRR_Subtraction	證據當事者	
交易取款	請款要求	Value_Claim		證據當事者	證據使用者 NRO_Claim
	請款回覆	Value_Claim		證據使用者 NRR_Claim	證據當事者

(四) SET 的爭議處理規則

一個爭議事件通常會涉入四種角色，即原告(plaintiff)、被告(defendant)、仲裁者(adjudicator)、見證者(witness)。而見證者的角色通常是證據責任鏈中的關係人。一個不可否認服務系統可以視為是證據處理的專家系統，包含推論與判決引擎。推論引擎主要受理訴訟案件，遵循不可否認服務政策，收集證據責任鏈中的證據包括見證者的決定，分析證據並決定證據的有效性。判決引擎乃是根據推論引擎的分析結果裁判爭議的結果，即陳述可承認事實的部份、無法論定的部份、或事實錯誤的部份。這一階段的作法與法制環境有相當密切的關係，包括法律上要求仲裁者應為自然人，也就是資訊系統的判決不具有法律效力，但其結果可提供決策參考。因此以下仲裁者僅擔任證據驗證者的角色。

我們調整了 Asokan 等人所定義的付款爭議的宣告語言[2]，配合一般付款交易的不可否認服務，設計一個易於理解的電腦言法，規則格式如下：

claim **VALUE TRANSFER** activity　**plaintiff**, **defendant**, **witness**, **adjudicator**
VALUE TRANSFER EVIDENCE = { role: evidences }
Inference Rules
fact **VALUE TRANSFER** activity players={payer, payee, bank} events **yes**/**no**={players}

以下我們以付款價值移轉活動為例，說明爭議處理的規則，包括證據責任鏈。為了便於判決規則的說明，我們假設推論過程的檢驗都正確，故判決的結果將只呈現"yes"的部份，即陳述可承諾的事實。有關 SET 使用的符號與訊息的定義，請參閱 SET 標準規格說明書[11,12,13,14]。買方與賣方的交易行為稱為付款價值移轉活動，主要由兩個交易事件所促發，即買方向賣方承諾付款與賣方確認交易完成。故在此有兩個證據責任鏈需作處理，一是付款承諾的證據規則，另一是交易確認的證據規則。

¬　付款承諾的證明規則

由表三得知，付款承諾的證據使用者為商店（以 M 代表），證據的當事者為持卡人（以 C 代表）。當付款承諾發生爭議時，原告通常是受事件影響的一方即商店，被告則為證據的當事者也就是持卡人，而銀行提供資料佐證事實，也就是此事件的證人。至於仲裁者在此皆以驗證者代表。

claim **PAYMENT**　**plaintiff**=M, **defendant**=C, **witness**=Bank, **adjudicator**=verifier
NRO_Payment = { M: OIData[TIDs,HOD,ODSalt], HPIData, DS, S_A(AuthCode); Bank: PIHead) }
Inference Rule:
　if　H(H(OIData),HPIData) = E_c(DS)　/*check OIData integrity*/
　then
　　OIData is correct.
　　if　AuthCode≠"piAuthMismatch"　**and**　PIHead.TIDs = OIData.TIDs
　　/*TIDs,MID,HOIData are consistency between merchant's AuthReq and cardholder' PI*/
　　then　MID is confirmed.　**end if**　/*proof of payee identification*/
　　if　H(OIData.ODSalt,OD,PurchAmt) = OIData.HOD
　　then　OD and PurchAmt are correct.　**end if**　/*proof of purchase order*/
　　end if
fact **PAYMENT**　M, C　CIN,MID,TIDs,OD,PurchAmt　yes={Bank}

商店無法由持卡人所承諾的購買請求訊息中的 OIData，證明自己為該筆交易的收款者，必須透過銀行提供交易的付款資訊即 PIHead，來鑑別付款承諾的對象。其次，SET 的交易訊息中並沒有持卡人的識別碼 CIN，必須在檢驗雙重簽章時從憑證中取出。

¬　交易確認的證明規則

當持卡人收到商店的購買回覆時，表示商店確認交易協議內容，同時也取得銀行同意授權的付款金額。故此類爭議的原告為持卡人，被告對象則是商店。

claim **PAYMENT**　**plaintiff**=C **defendant**=M **witness**=Bank **adjudicator**=verifier
NRR_Payment = { C: S_M(TIDs,CompletionCode,AuthCode,AuthDate,AuthRatio), OD,PuchAmt,ODSalt; M or Bank: DS }
Inference Rule:
　if　AuthCode≠"piAuthMismatch"　/*gateway verify HOIData consistency from
　then　HOIData retrieved from E_c(DS).　merchant and cardholder*/
　　if　H(OIData) = HOIData
　　then　HOD is correct.　**end if**
　　if　H(OD,PurchAmt,ODSalt) = HOD
　　then　OD, PurchAmt are correct.
　　AuthAmt = PurchAmt✕AuthRatio
　　end if
　end if
fact **PAYMENT**　C, M　CIN,MID,TIDs,OD,PurchAmt,AuthAmt　yes={M or Bank}

在商店簽署的購買回覆訊息中，沒有註明買方的身份也就是持卡人的識別碼，以及買賣協議的內容包括商品的內容、金額等。雖然持卡人可提供購買請求的資料，但會造成球員兼裁判的現象，也就是如何擔保持卡人沒有捏造訂購資料。因此，必須由商店或銀行提供持卡人的雙重

簽章，檢驗持卡人提供的資訊；而由銀行擔任證人角色，則提供多一層的信賴保障。

四、計畫成果自評

資訊安全技術是否實用，除了本身提供的安全保障外，最重要的是執行時整體作業的成本效益，這攸關了市場接受的意願。公平交換與不可否認協定以維護網路上商業交易秩序為依歸，然而卻很少實際應用於市場上，歸究原因就出在不敷經濟效益而寧願承擔風險，例如一些小額付款系統。本研究以付款系統為主題，提供公平的不可否認服務。我們擺脫過去證據處理以單一使用者與事件的方式，採用以同類活動為主的管理，並納入證據價值鏈的想法，有效減少資訊系統的額外負擔。另外，關於爭議處理的不可否認服務機制，我們以專家系統的方式，設計推論引擎與判決引擎來輔助外在決策人員。同時，我們建立了一組簡單、易懂的電腦語法，以有系統的陳述這些爭議處理規則。由於不可否認服務是一種應用導向的功能，如此一來，我們可以很容易地將此設計應用在其它作業上，降低專業領域應用移轉的阻礙。本計畫已將 SET 部份的研究，發表於資訊安全通訊[16]，並進一步修改以投稿資訊管理學報[17]。此外，我們就此研究的內容準備了另一篇論文，將投稿於國際期刊[18]。

五、參考文獻

1. Asokan, N.(1998, May). Fairness in Electronic Commerce. PhD thesis, University of Waterloo.
2. Asokan, N., Herreweghen, E. V., and Steiner, M. (1998, Sep.). Towards a framework for handling disputes in payment systems. In Third USENIX Workshop on Electronic Commerce, Boston, Mass.
3. Gärtner, F., Pagnia, H., and Vogt, H. (1999). Approaching a formal definition of fairness in electronic commerce. Proceeding of the 18th IEEE Symposium on.
4. ISO/IEC. (1997). ISO/IEC 10181-4. Information Technology－Open Systems Interconnection－Security frameworks for open system: Non-repudiation framework.
5. ISO/IEC (1997). ISO/IEC 1388-1. Information Technology－Security techniques－Non-repudiation Part 1: General.
6. ISO/IEC (1997). ISO/IEC 1388-2. Information Technology－Security techniques－Non-repudiation Part 2: Mechanisms using symmetric techniques.
7. ISO/IEC (1997). ISO/IEC 1388-3. Information Technology－Security techniques－Non-repudiation Part 3: Mechanisms using asymmetric techniques.
8. Krause, M., Tipton, H. F. (1999). Handbook of information security management, Boca Raton, Fla. :Auerbach.
9. Peiro, J. A., Asokan, N., Steiner, M., and Waidner, M. (1998, Jan.). Designing a generic payment service. IBM Systems Journal, 1(37).
10. Pfitzmann, B., Waidner, M. (1996, May). Properties of payment systems: General definition sketch and classification. IBM Research, Research Report RZ 2823 (#90126).
11. Visa International and MasterCard International. (1997, May). SET secure electronic transaction specification: Business description (1.0 ed.), Book 1. Retrieved from World Wide Web: http://www.setco.org/.
12. Visa International and MasterCard International. (1997, May). SET secure electronic transaction specification: Programmer's guide－System design considerations (1.0 ed.), Book 2, Part 1. Retrieve from World Wide Web: http://www.setco.org/.
13. Visa International and MasterCard International. (1997, May). SET secure electronic transaction specification: Programmer's Guide－Payment System (1.0 ed.), Book 2, Part 3. Retrieve from World Wide Web: http://www.setco.org/.
14. Visa International and MasterCard International. (1997, May). SET secure electronic transaction specification: Programmer's Guide Appendices (1.0 ed.), Book 2, Part 4. Retrieve from World Wide Web: http://www.setco.org/.
15. Vogt, H., Pagnia, H., and Gärtner, F. (1999). Modular fair exchange protocols for electronic commerce. Proceeding of the 15th Annual Computer Security Application Conference.
16. **邵敏華、黃景彰，**"SET **使用的密碼學技巧：優缺點之評估，" 資訊安全通訊，第六卷第一期，八十八年十二月。**
17. **邵敏華、黃景彰，**"SET **技術特色的詮釋與安全評估"。（修改後將投稿於資訊管理學報）**
18. Min-Hwa Shao and Jing-Jang Hwang, " A Fair Payment Scheme with Non-repudiation for SET." (working paper, the institute of information management at NCTU in Taiwan.)