行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ **電子商務預付卡安全交易系統** ※
※ **之研究與製作（II）** ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：個別型計畫

計畫編號：NSC 89－2213－E－009－145－

執行期間： 89 **年** 8 **月** 1 **日至** 90 **年** 7 **月** 31 **日**

計畫主持人：曾文貴 教授

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 資訊科學系

中 華 民 國 90 **年** 7 **月** 31 **日**

電子商務預付卡安全交易系統之研究與製作（II）

Research and implementation of a secure transaction system for pre-paid cards in electronic commerce（II）

計畫編號：NSC 89-2213-E-009-145
執行期限：89 年 8 月 1 日至 90 年 7 月 31 日
主持人：曾文貴 教授 交通大學 資訊科學系
執行機構：國立交通大學 資訊科學系
E-mail: tzeng@cis.nctu.edu.tw

一、中文摘要

我們提出一個預付卡式的電子商務付款機制。台灣人口稠密，便利商店發達，預付卡可以透過一般的零售商店，很容易地到達大部份人的手中，因此，預付卡式的付款方式，應當很適合台灣的線上購物環境。這套預付卡付款系統，特別適用於小額的交易。透過實作出這套系統的雛形，我們希望能夠技轉商家和發卡公司，由於發卡公司及商家所需的資本與技術皆不高，只要兩者能夠搭配 PKI 的建構即可付諸實行。本系統不需要人人都有電子憑證，因此有機會在台灣本土成功地推廣開來，促進電子商務的發展。

關鍵詞：電子商務、安全付款機制、小額付款、預付卡

Abstract

In this project we developed an electronic payment system based on pre-paid cards. This system is suitable for the transactions of small amount. We hope that we can transfer related technologies to the related companies so that they can develop commercial products and introduce them to small WWW vendors.

Keywords: electronic commerce, secure payment system, small amount transaction, pre-paid card

二、緣由與目的

隨著電腦的普及與網際網路的高度發展，每天上網看看網頁、寫寫電子郵件變成我們生活中不可或缺的一部份，而伴隨著電子商務的推行，更讓我們可以透過網路，來進行購物、納稅等多種的消費行為。

然而，原本蔚為流行的 .com 風，在最近網路事業泡沫化的影響下，多家網路公司紛紛歇業倒閉，使得電子商務的運作模式也在跌跌撞撞中不斷的轉變。很明顯的，並不是只要推行電子商務，就一定會賺錢，因為整個配套的措施仍然在摸索的階段，雖然能夠成長的空間還相當的大，但是，如何能夠找到一個最為大眾所接受的運行方法，依然是目前大家所關注的重點。

電子商務包含行銷、物流、財務、整合與趨勢等方面，而安全的電子付款系統是不可或缺的一環。本計畫提出以「預付儲值卡」為支付工具的安全交易系統，來做為網路購物之用，希望利用台灣這個便利商店發達、人口稠密的環境，配合目前推行效果不錯的手機門號預付卡的概念，來發展出另外一種付款方式的系統。期望在 SET 與電子錢幣之外，提出一套適合我國消費習慣的網路安全交易系統。

在我們的系統中，消費者到零售商店購買一定面額的〔儲值預付卡〕後，當需要透過網路進行消費行為時，只需鍵入預付卡上的密碼，發行儲值預付卡的發卡公司就會將交易金額從該卡中扣除，商家也可以據此向預付儲值卡的發卡公司請款，來完成交易，一旦該卡的金額消費完畢，隨即就失去效用。

以預付儲值卡為支付工具的網路交易系統有下列的優點：

1. 符合我國消費者的消費習慣且使用方便：我國的便利商店林立，所以對於預付儲值卡的銷售非常方便，消費者可以隨處購買到所需的預付儲值卡。而預付卡式的系統早已廣泛的被使用，例如一般及行動電話儲值預付卡、捷運儲值卡等，對於消費者而言，以相同的方式來從事網路購物，應該不會是件難事。

2. 具有匿名的優點：以目前消費者的消費習慣來看，大多都是以匿名消費為主，所以，本系統也具有匿名消費的特性，可以讓消費者不用去適應不同的消費方式。再者，也無須擔心信用卡被不肖的商家或駭客盜用，因為即使有損失發生，也只有該卡額度的損失。
3. 本土的系統，技術掌握在自己受中：這樣可以不受到國外大公司的控制，也方便整套系統的維護與問題解決。
4. 適用範圍廣、潛在消費者多：預付卡的適用範圍廣，除了購物消費之外，還可以繳納各項的費用，例如考試的報名費、訂閱雜誌、交通罰款、資訊使用費等。
5. 適合小額消費：除了安全性的要求滿足外，更確保了交易雙方的權益，而不會因為小額消費而降低任何方面的要求。
6. 不需要電子憑證(Certificate)相關的資訊基礎建設，系統簡單：目前完整的電子憑證基礎建設，還待普及，而且電子憑證必須存在電腦或 IC 卡上，使用上的不方便，也會影響到消費者使用的意願。我們以預付卡式的系統來進行網路消費，將可以簡化交易的流程，使得開發的成本降低，更能加速系統的普及。
7. 沒有倒帳風險、交易成本低：一般而言，信用卡遭到盜用及消費者倒帳的風險很高，造成交易的成本無法降低，而一般信用卡公司的費用是交易金額的 3%-5% 如果利用預付卡，可以大大的降低這方面的損失，使得交易的成本降低。
8. 聯合廣告、節省成本、促進競爭：將來可以有多家預付除值卡的發卡公司，透過聯合推廣的方式，來達到節省成本的效果。對於商家而言，選擇是否接受某一發卡公司的預付儲值卡，可以造成發卡公司間彼此的良性競爭。

三、結果與討論

本預付卡付款系統主要有三個參與者，分別是消費者（Customer）、商家（Merchant）與發卡公司（Card issuer），再配合 PKI 的環境來架構整套系統。成果我們分為下面數個部份來討論：

1. 預付儲值卡的編碼方法：因為預付儲值卡是以卡的密碼作為辨識的依據，消費者最直接的攻擊為猜中「合法」的密碼，除此之外，消費者還可能從預付卡的密碼猜出發卡公司的「編碼密碼」，再自己編出密碼，因此如何設計編碼的方法就極為重要。我們以密碼學中的 Message Authentication Code (MAC)來處理這方面的問題。
2. 預付儲值卡交易流程：我們參考了 SET 及各類電子錢幣系統的做法，從網路購物安全交易系統中各參與者要注意的事項中，設計一適合以預付儲值卡為付款工具的網路購物安全交易系統。並設立網站來模擬測試交易的情形。
3. 傳輸的安全研究：當消費者將預付儲值卡的密碼鍵入網頁瀏覽器時，如何將預付卡的密碼安全的送到商家及發卡公司，及商家及發卡公司間的安全傳輸是要注意的，這便是傳輸的安全。我們以現有的各類加密演算法，如 DES，AES 等來作資料的加密，我們也使用公開金鑰的方法來作通訊金匙(session key)的建立，並配合 SSL 的使用來增加網頁瀏覽的安全性。
4. 使用者介面的設計與製作：當消費者從事網路購物時，如果消費者決定使用預付儲值卡來付款，他就按下商家網站的預付儲值卡 icon，這時輸入預付卡密碼的畫面會出現，消費者電腦也會下載一些相關的 Java 程式(必須是認證過的)，當消費者輸入密碼後，安全交易的流程就開使啟動，密碼加密過後送給商家，商家經過「驗證」之後再送給發卡公司，發卡公司處理之後，送出確認信息給商家和消費者完成交易。
5. 商家相關軟體的設計與製作：商家的交易軟體包含預付儲值卡密碼的驗證，與發卡公司的安全傳輸、與發卡

公司的相互身分認證、與發卡公司對交易訊息的確認、及向發卡公司請款等軟體的研究、設計與製作。我們以 IC 卡作為商家處理秘密資料(如商家的電子憑證、私密金匙等)的儲存及計算的工具。

6. 發卡公司相關軟體的設計與製作：發卡公司的軟體包含預付儲值卡的密碼編碼程式、與商家及消費者的安全傳輸、與商家的相互身分認證、對商家的交易發出確認的信息、處理商家請款的功能等。

因為在設計這套系統時，考慮到在目前的網路架構下，為了維持消費者購物匿名的原則，便限制了消費者只能夠與商家連線溝通，因為如果消費者直接與發卡公司或一個第三公正的單位連線的話，可能會破壞匿名的原則，為了提高效率，我們不考慮設立第三公正單位的情況，所以整個付款系統的流程架構大致就是：消費者↔商家↔發卡公司，這樣的一個架構。

簡單的來說，我們設計出一套以預付卡為基礎的安全交易協定，而這個協定具有消費者匿名、不需要下載安裝額外的軟體、較有效率等優點。並且實作出整套系統中消費者、商家及發卡公司所需要的相關軟體。最後並且設立一個簡單的實驗購物網頁，配合我們開發的軟體，實際進行整個網路消費的過程。

相關的論文與軟體資料可以到下列的網頁查詢下載：

http://infosec.cis.nctu.edu.tw

四、計畫成果自評

這是一個為期三年的計畫，有下列預期的目標：

1. 一套預付儲值卡的編碼方式（第一年）
2. 一個預付儲值卡網路購物交易系統的流程（第一年）
3. 一個預付儲值卡使用者介面，與相關的軟體（第二與第三年）
4. 一個預付儲值卡的商家軟體 prototype （第二與第三年）
5. 一個預付儲值卡的發卡公司軟體 prototype （第二與第三年）
6. 讓參與計畫的學生學習到密碼學、智慧卡與網路購物安全交易系統的技術與知識，對於整合性的電腦安全問題，能夠有深入的了解，期望培養目前社會上所急需的人才。

由於不斷的努力，我們以兩年的時間把整個為期三年的研究計畫提前完成。本計畫除了學術上的研究外，我們也著重於整體系統實作上的設計與研發，在相關軟體的配合下，整個電子商務購物消費的流程都是確實可行的，除了顧及到安全性及消費交易各方面的權益外，更因為便利性與預付卡消費方式的特性，讓整套的系統更具實用的價值，我們也相信在推廣進入真正的市場運作上，會輕易的為商家或消費者接受。

我們也訓練了多名的碩士生，透過整個計畫的研究與系統實作的過程中，讓他們對於相關的知識有充分的了解，相信經過這段時間的訓練，他們可以在社會上的相關領域有所貢獻。

五、參考文獻

1. Douglas R. Stinson. “Cryptography: Theory and Practice” CRC Press 1995.
2. W. Stalling. “Cryptography and network security: principles and practice, 2nd Ed.” Prentice Hall, 1999.
3. Kiyoon Sung. “Analysis and Design of the Internet Based Payment System.
4. DigiCash, http://www.digicash.com/.
5. CyberCoin and CyberCash, http://www.cybercash.com/cybercash/services/.
6. SET, http://www.setcom.org.
7. Sung—Ming Yen, Jong-Ming Lee, Liang-Tai Ho, Jack G. Lee. “PayFair: A Prepaid Internet Micropayment Scheme Promising Customer Fairness” Proceedings of the Ninth National Conference on Information Security.
8. Dos attack, http://webopedia.internet.com/Networks/Security/DoS_attack.html.
9. Security in Java,

http://java.sun.com/docs/books/tutorial/security1.2/index.html.
10. Signed applet, Microsoft SDK for JAVA Documents.
11. Scott Oaks. “Java Security” O’Reilly & Associates, 05/1998.
12. Jonathan Knudsen. “Java Cryptography” O’Reilly, 05/1998.
13. The SSL Protocol, Version 3.0. http://hme.netscape.com/eng/ssl3/ssl-toc.html.
14. David Wagner, Bruce Schneier. “Analysis of the SSL 3.0 protocol” The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 1996, pp. 29-40. http://www.counterpane.com/sssl.html.
15. Tatsuaki Okamoto, Kazuo Ohta. “Universal Electronic Cash” Crypto 1991.
16. Daniel R. Simon, “Anonymous Communication and Anonymous Cash”, Crypto 1996.
17. Jean Claude Pailles. “New Protocols for Electronic Money” AsiaCrypt 1992.
18. Simson Garfinkel, Gene Spafford. “Practical Unix and Internet Security” O’Reilly, 1996.
19. Charlie Kaufman, Radia Perlman, Mike Speciner. “Network Security: PRIVATE Communication in a PUBLIC World” PTR Prentice Hall.
20. Donal O’Mahony, Michael Peirce, Hitesh Tewari. “Electronic Payment Systems” The Artech House computer science library.