통신 단말기를 이용한 전자상거래에서의 결제모델

(주)아이엠피비젼 안세호

1. 서 론

인터넷 등 네트워크를 이용한 전자상거래가 활성화되면서 상품구매, 서비스대금을 안전하게 상점에 지불할 수 있는 방법이 필요하다. 현재 가장 보편적으로 많이 사용되는 SET[1]는 지불수단으로 신용카드를 이용하고 있다. 또한 전자화폐, IC카드[2], 은행계좌이체 등을 이용하지만, 보안상의 문제와 사용의 불편함 때문에 전자상거래의 표준을 제시할 만큼 대중화되고 편리한 결제방법이 출현하지는 못한 실정이고, 다양한 지불수단이 실용화됨에 따라서 지불메카니즘의 불일치 문제가 대두되고 있다. 이를 해결하기 위하여 W3C 및 CommerceNet에서는 JEPI(Joint Electric Payment Initiative)[3]를 추진 중에 있다. 이는 상점과 고객간에 사전에 지불메카니즘을 협상하고 선택하게 해주는 프로토콜이다. 현재 여러 기업과 정부부처, 또 여러 벤처기업에서 IC카드를 포함한 새로운 전자화폐를 개발했거나 개발 중에 있지만, 전자화폐 사용을 위한 인식부족, 인프라의 부족 등으로 인해 대중화되지 못하고, 또한 너무나 많은 종류의 전자화폐를 생산함으로써 사용자로 하여금 혼란을 가져오게 하는 등 전자화폐 사용 활성화는 요원한 과제처럼 느껴진다.

본고에서는 이러한 상황에서 기존의 인프라와 시스템을 이용하여 가장 적절하게 전자상거래에서의 결제를 할 수 있는 2가지 비즈니스모델(IMTS I, II: Internet Mobile-phone Transaction System)을 제안하고, 구현 적용을 위한 방향을 제시하고자 한다. 본고는 2장에서는 신용카드와 연계된 이동통신 단말기를 사용한 결재의 모델로서 IMTS I을 제안하고, 3장에서는 은행 현금카드와 은행 직불카드를 이용한 결제모델인 IMTS II를 제안한다.

2. IMTS I

2.1 IMTS I 비즈니스 모델

1999년 말 현재 전국에 2,300만대의 이동통신 단말기가 보급된 상태이며, 신용카드도 현금 서비스를 제외하더라도 하루 750억원이 결제되고 있다. IMTS I에서는 이동통신 단말기와 신용카드라는 두 가지 인프라를 적절히 사용하는 방식을 취하고 있다. 이 비즈니스 모델은 신용카드 결제의 보안성을 높이고자 하는데 목적이 있다.

기존에 신용카드를 보유한 사용자가 전자상거래에서 결제를 하고자 할 경우 해킹에 대해 무방

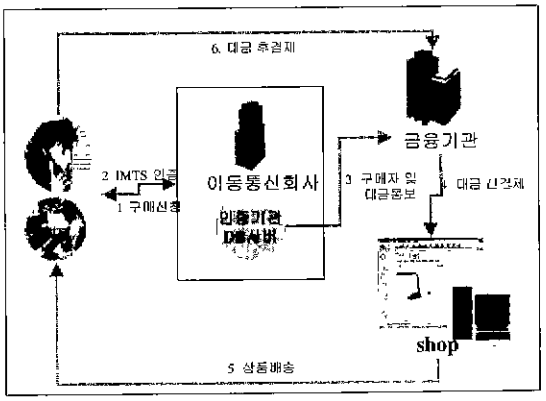

그림 1 IMTS의 개념도

비 상태였던 것과는 달리 이동통신 번호와 카드 번호를 연동하여 이동통신 번호값을 키로 하여 인터넷 상에서 물품을 구매하게 되고 이동통신 회사에서는 단문 메시지(SMS : Simple Message Service)를 해당 사용자에게 보냄으로 해서 거래에 대한 인증을 받을 수 있도록 되어 있다(그림1).

IMTS 모델은 다음의 3단계로 구현되어 진다.

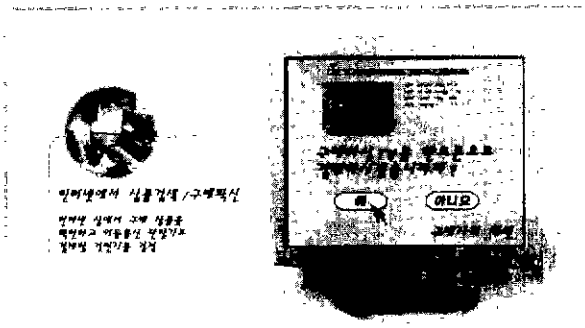

그림 2 인터넷에서의 상품검색 및 구매확신

단계 1 : 인터넷에서의 상품검색 및 구매확신 단계(그림 2)로서 신용카드를 보유하고 있는 사용자가 자신의 이동통신 단말기를 신용카드와 똑같이 사용할 수 있는 서비스(IMTS I)를 신청하면 자신의 신용카드와 연동되어 단말기로 사용할 수 있는 결제 한도액이 정해진다. 그리고 인터넷 상에서 상품 검색을 하고 핸드폰으로 결제할 것을 선택한다.

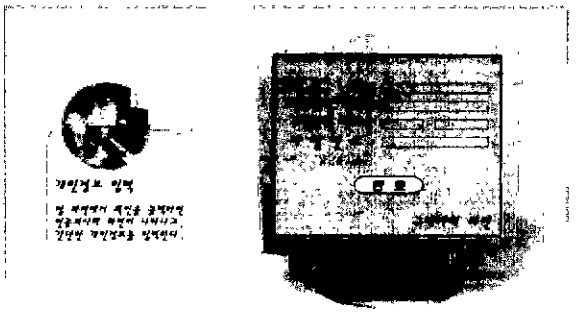

그림 3 개인정보 입력

단계 2 : 개인정보 입력단계로서(그림 3) 결제 방법을 이동통신 단말기로 선택하게 되면 Payment인증기관의 화면이 나타나게 되며 여기에 사용자의 개인정보를 입력하게 된다. 이 때 사용자의 이동통신 단말기 번호가 키값이 되므로 신용카드 번호를 입력할 필요가 없다.

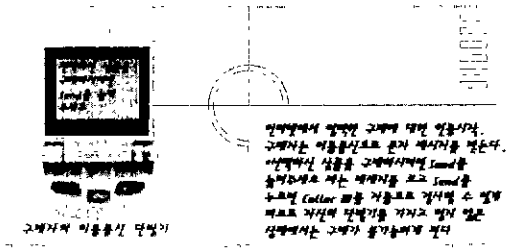

그림 4 이동통신 인증

단계 3 : 이동통신 인증단계(그림 4)로서 단계 2에서 입력한 개인정보는 Payment 인증기관으로 보내지고 인증기관에서는 동시에 이동통신 회사로 사용자의 이동통신 번호를 전송하고 이동통신 회사에서는 해당 사용자에게 위와 같은 단문 메시지(SMS)를 보내게 된다. 사용자가 거래를 확인하기 위하여 자신의 단말기의 SEND 버튼을 누르면 단말기 롬에 저장되어 있는 Caller ID가 이동통신 회사로 전송되며 이동통신 회사에서는 Caller ID가 등록되어 있는 사용자와 물품 구매를 위해 입력한 사용자 정보를 대조하게 된다.

즉, 일차적인 인증으로 Payment 인증기관에서 해당 사용자의 이동통신 단말기와 연계된 신용카드의 조회, 이차적으로 이동통신 단말기 사용자의 Caller ID와 입력된 개인정보의 대조를 통해 사용자가 개인정보와 이동통신 단말기를 동시에 분실하지 않는 한 타인에 의한 불법적인 결제가 불가능하도록 하는 것이 IMTS I이 추구하는 보안 모델이다.

이러한 과정을 거쳐 결제가 이루어지면 사용자의 신용카드 결제일에 이동통신 단말기를 이용하여 결제한 금액도 포함되어 청구된다. 최근에 이동통신 회사에서 대금 지급을 먼저 하고 이동통신 사용료 청구서에 전자 상거래 대금을 포함하여 청구하는 모델들이 나오고 있지만, 이는 현실적으로 불가능한 모델이다. 왜냐하면, 이동통신 회사는 사용자의 물품 구입대금을 선지급하는 여신업무를 할 수 있는 법적 근거나 허가가 없으며, 이동통신 사용료에 물품 구입대금을 포함시키려면 이동통신 회사의 요금고지 부분에 막대한

인적 물적 비용이 추가되기 때문이다. 그러므로 여신업무는 시스템과 인프라가 조성되어 있는 결제기관, 즉 신용카드 회사에서 행하는 것이 최상이며, 이동통신 회사는 이차적인 인증을 위해 이동통신과 통신 단말기와 관계된 부분을 수행하는 것이 본 비즈니스 모델의 흐름상 가장 적합하다.

IMTS I 모델에서는 이동통신 회사, 결제기관, 상품판매 회사, 그리고 구매자를 중개할 수 있는 기관이 있을 경우 데이터 전송 및 수신, 구매내역의 DB화 등을 더욱 효율적으로 할 수 있으리라 생각한다.

2.2 IMTS I의 수익성 측면

IMTS I은 현재 시행되고 있는 전자상거래의 신용카드 결제를 더욱 안전하게 할 수 있게 함으로써 시장을 확산시키고자 한다. IMTS I에 관계된 기관은 이동통신 회사, 결제기관, 인증기관, 중개기관이 있다. 이 4개의 기관이 지금까지와 마찬가지로 결제금액에 대한 일정 퍼센티지를 수수료 수입으로 잡는다면 보안이 보장된 신용카드 결제방법을 통해 확대되는 시장에 따라 수익구조도 개선되리라 본다.

3. IMTS II

3.1 IMTS II 비즈니스 모델

IMTS II와 IMTS I의 가장 큰 차이점은 IMTS I의 경우 이동통신 단말기를 매개체로 한 결제방법인 반면 IMTS II의 경우 통신 단말기는 결제의 보완수단이 된다. 그러나 두 경우 모두 카드 결제의 보안성을 향상시킨다는 특성이 있다. 그리고 IMTS I에서는 신용카드와 연계된 이동통신 단말기를 이용한 결제 모델이 중심이 되었지만, IMTS II에서는 현재 가장 널리 보급되어 있는 은행 현금카드와 은행 직불카드를 이용한 결제모델을 제시하고자 한다.

현재 어떠한 전자지갑이나 전자화폐보다 보급율이 높은 은행 현금카드와 은행 직불카드는 전자상거래에서의 결제수단으로 사용되지 못하고 있다. 그 가장 큰 이유로는 은행카드나 직불카드의 경우 신용카드와 달리 사용자 비밀번호 4자리를 입력해야 하는데 웹상에서 개인의 계좌 비밀번호이기도 한 카드 비밀번호를 입력할 경우 보안상의 허점으로 인하여 치명적인 결과를 초래할 수도 있기 때문이다. 본 개념도에서와 같이 Call Center를 통해 그 비밀번호를 입력한다면 웹상에서의 보안을 걱정하지 않고도 현금카드와 직불카드를 결제수단으로 이용할 수 있다(그림 5).

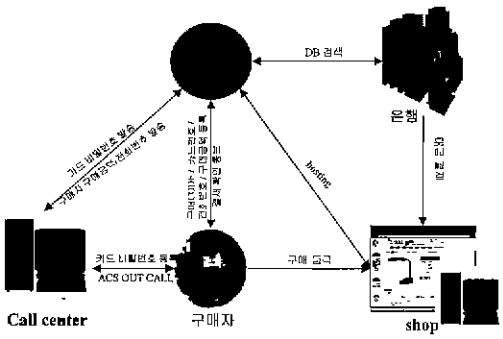

그림 5 IMTS II의 개념도

IMTS II 비즈니스 모델은 다음 2단계로 구현된다.

단계 1 : 결제방법 선택(그림 6)

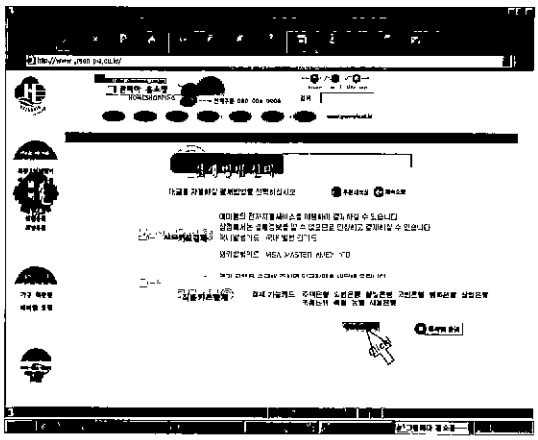

그림 6 결제방법 선택

은행 직불카드나 현금카드를 보유하고 있는 구매자가 구매 상품을 인터넷에서 선택하고 직불카드 또는 현금카드로 지불할 것을 결정하면, 일반 신용카드 결제와 마찬가지로 카드번호와 개인정

보를 입력한다. 직불카드와 현금카드는 비밀번호 4자리를 입력해야 하는 특성이 있는데 이를 웹상에서 입력할 경우 보안상 문제가 있을 수 있으므로 결제를 이원화하여 사용자가 개인정보 입력시 지금 현재 연락가능한 번호를 입력하면 ACS(Auto Calling System)을 통해 사용자에게 전화를 걸어 사용자의 비밀번호를 입력받게 된다.

단계 2 비밀번호 인증(그림 7)

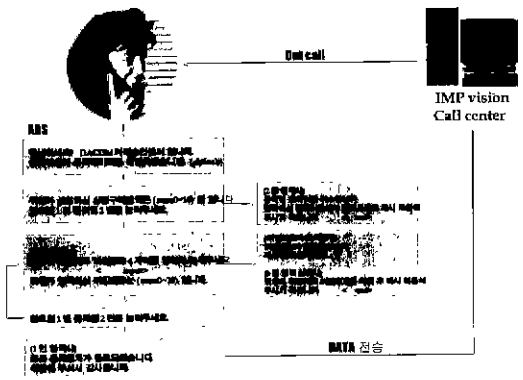

그림 7 비밀번호 인증

위와 같은 과정을 거쳐 비밀번호가 입력되면 이 정보는 인증기관의 Server로 보내지게 된다. Call Center에서 인증기관으로 비밀번호가 보내지는 과정에서 정보가 유출될 위험이 있으므로 Call Center와 인증기관의 Server는 같은 곳에 위치하게 하며, 내부라인을 이용함으로써 보안을 기할 수 있게 된다. 인증기관으로 온 정보는 해당 은행으로 보내져 조회가 되며 은행의 승인이 나면 거래 승인이 나게 된다.

이러한 모델을 이용할 경우, Call Center는 개인의 전화번호와 비밀번호만을 받게 되고 계좌번호를 모르므로 데이터 전송 중간에 정보가 유출되더라도 타인이 사용하기에 부적합한 정보가 되며, 직접적으로 현금이 빠져나가는 계좌를 보호하는 측면에서도 상당한 효과가 있으리라 믿는다.

3.2 IMTS II의 수익성 측면

현재 가장 문제가 되고 있는 인터넷 상에서의 소액거래시 유용한 지불 수단이 될 수 있는 것이 이러한 현금카드와 직불카드이며 다른 E-Cash와는 달리 이미 보급되어 있고, 전자화폐를 구매하지 않아도 된다는 장점이 있으며, 본 결제수단으로 인하여 소액 거래시장이 확장될 것이라 생각된다. 대규모 결제의 경우 할부 지급을 하지 못한다는 단점이 있지만 범용성이 있는 결제 수단으로 인정받을 수 있으리라 본다. 은행의 경우 거래대금 기준 약 2%정도의 수수료를 보장받을 수 있으며 인증기관과 Call Center 운용회사 간에도 적정 비율의 수수료를 부과할 경우 수익성을 예상할 수 있을 것이다.

4. 결 론

IMTS I과 II는 현재 가장 널리 보급되어 있는 신용카드, 은행 현금카드와 직불카드를 적은 비용과 노력으로 보안성을 높인 전자화폐화로 전환 시킬 수 있는 비즈니스 모델이다. 기존 신용카드에 대해서는 보안성을 높이고, 또 은행계좌를 가진 사람이면 대부분 직불카드나 현금카드를 새로운 인터넷상의 전자화폐 수단으로 만들 수 있는 방법이라 생각된다. 특히 직불카드와 현금카드는 대부분의 네티즌들이 추론 할 수 있으며, 이렇게 널리 보급되어 있으면서 현금 결제가 가능한 카드 형태의 지불 수단이므로 전자상거래시 최적의 결제수단이 될 수 있다.

현재 정부에서도 세수확대와 거래 투명성을 높이기 위해 신용카드 사용을 권장하고 있으며 전자 상거래시 정확한 근거가 남을 수 있는 지불수단이라면, 또 그것이 상용화되고 범용성을 가진다면, 또 지불수단을 개발하기 위한 노력과 비용이 천문학적인 현 상황에서 IMTS I과 IMTS II의 경우 현 상황에 적합한 전자지불 비즈니스 모델로서의 기능을 다할 것이라 본다.

참고문헌

[1] MasterCard and VISA Corporations, Secure Electronic Transaction(SET) Specification book 1, 2, 3, 1996, http://www.mastercard.com/set, http://www.visa.com

[2] ISO/IEC JTC1/SC11/WG4, WG8.

[3] CommerceNet Inc., eCo System:

CommerceNets Architectural Framework for Internet Commerce, http://www.commerce.net

안 세 호

1995.2 Corcoran Art College 대학교 광고디자인 유학중
1992.1~1993.9 Chicago Travel 관광가이드
1997.9~1998.8 (주)308 정보통신 ARS 팀장
1997.9~현재 서울지검 의사과 통역 자문위원
1998.9~현재 I.M.P Vision 대표이사
E-mail:impworld@impvision.com

• WAAC 2000 학술대회 논문 모집 •

- 응모분야 : 알고리즘과 계산이론에 관련된 모든 분야
- 일 자 : 2000년 7월 21 ~ 22일
- 장 소 : 일본 동경대학교
- 주 최 : 일본정보처리학회(IPSJ) SIGAL, 컴퓨터이론연구회
- 문 의 처 : 한국외국어대학교 컴퓨터공학과 김희철 교수
  E-mail:hckim@maincc.hufs.ac.kr, Tel. 0335-330-4267