일회용 신용정보를 이용한 전자지불 시스템의 설계 및 구현

신 종 철[†]·박 종 열[††]·이 형 효[†††]·이 동 익[††††]·윤 석 환[†††††]

요 약

최근, 인터넷의 급속한 발달은 개인의 업무에 많은 변화를 주었다. 새로운 환경에서 개인의 전자거래는 시장의 요구사항과 산업적 경향에 따라서 변화와 발전을 거듭하게 되었고 그 결과 전자지갑, 전자화폐, 전자수표와 같은 안전한 지불수단이 필연적으로 등장하게 되었다. 하지만 지금까지 새롭게 제안된 시스템들이 안전성은 뛰어나지만 널리 사용되지 못하고 있다. 그 이유는 각 시스템들이 안전성을 위해서 사용자의 편의성을 많이 희생하기 때문이다. 반면 신용카드는 안전성은 낮지만 사용이 편리하여 대중화되어 있다. 따라서 신용카드 기반의 안전한 지불 방법이 요구된다. 이 논문에서 "지불정보는 항상 새로워야 한다", "기존 신용카드 시스템의 사용이 가능해야 한다", "사용자에게 별도의 시스템을 요구하지 않는다"와 같은 보안성과 편의성을 가지는 신용카드 기반의 지불 시스템을 설계/구현한다.

Design and Implementation of the Payment System using One-time Credit Information

Jong-Cheol Shin[†]·Jong-Youl Park[††]·Hyung-Hyo Lee[†††]
Dong-Ik Lee[††††]·Seok-Hwan Yoon[†††††]

ABSTRACT

Recently, personal business styles have been rapidly changed into e-business due to the rapid progress and deployment of Internet. As a result of the change, new and safe ways of payment such as electronic wallet, electronic money and electronic check have been developed and introduced. In this paper a secure and user-friendly payment method is addressed. One of most important reasons why newly developed safe payment methods are not widely used in e-business is lack of convenience for the users. On the other hand credit card based payment, which is traditional one, is the most prevailing due to the user-friendliness. However this payment also has some problem in sense of security. In this paper, we design and implement a secure credit card-based payment system using one-time credit information. The main features are "payment information must be new", "can use the old credit system", and "do not require client software".

키워드 : 전자지불 시스템(electronic payment system), 신용카드(credit card), 일회용 신용정보(one-time credit), 일방향 함수(one-way function), 시점확인 서비스(time-stamp service)

1. 서 론

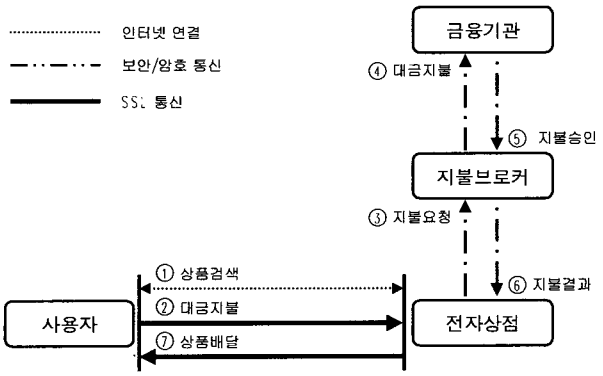
인터넷 사용자의 급속한 증가는 실생활에서의 많은 변화를 가지고 왔다. 그 중에서 상거래에서는 사용자가 공간 및 시간 제약을 받지 않고, 물건을 쉽게 구입할 수 있는 기회를 제공하였다. 또한 상거래를 위해서 필요했던, 전시공간 및 관리비용을 절약하여 저렴한 구매를 가능하게 하였다. 전자상거래는 기존의 "돈"으로 표현되던 가치정보를 가상공간에서 표현해야 했고, 필연적으로 전자지불 시스템이 등장하게 되었다.

† 정 회 원 : 송우아이엔티㈜ 기술연구소장
†† 준 회 원 : 광주과학기술원 대학원 정보통신공학과
††† 정 회 원 : 원광대학교 정보·전자상거래학부 교수
†††† 종신회원 : 광주과학기술원 정보통신공학과 교수
††††† 종신회원 : 정보통신연구진흥원 책임연구원
논문접수 : 2001년 12월 31일, 심사완료 : 2002년 5월 13일

전자지불 시스템에서 신용카드를 이용한 전자지불 시스템들은 그 편리성 때문에 널리 사용되고 있다. 2002년 3월 통계청 집계에 따르면 온라인 쇼핑몰에서 신용카드를 이용한 결제가 2002년 1월 전체의 71.5%를 차지하여 전년대비 5.3% 증가를 보인 반면, 온라인 입금은 25.1%로 작년 대비 -5.2%를 기록했다[1]. 그러나 인터넷 이용자중에서 75%가 인터넷 서비스 업체의 안전성과 보안성을 불신하고 있으며, 79%가 신용카드 결재시에 위험부담을 느끼고 있는 것으로 나타났다[2]. 실제로 전체 인터넷 사용자의 약 30%에 해당하는 900만명의 개인정보가 유출되고, 온라인상에서 카드번호가 도용되어 개인의 재산권을 침해하는 사건들이 발생해서 신용카드 기반의 안전하고 편리한 전자지불 방법이 절실히 요구되고 있다. 특히 기존 상거래는 대면거래인데 반해 전자상거래는 가상공간에서 이루어지는 비대면 거래이

기 때문에 더 안전한 방법이 제공되어야만 한다[3].

가장 널리 사용되고 있는 신용카드 기반의 전자지불 방식은 SSL(Secure Socket Layer)를 이용한 지불 시스템이다. 이 방식은 사용자와 전자상점 사이의 안전한 전송을 위해서 SSL을 사용하는 방법으로 (그림 1)과 같은 구조를 가진다. 사용자는 상품검색 후 지불에 필요한 카드번호와 유효기간을 전자상점에 전달하고 전자상점은 이 정보를 이용하여 상품 대금을 청구하는 방식이다. (그림 1)에서 사용자 → 전자상점 → 지불브로커 → 금융기관까지 모두 안전한 통신망을 사용하므로, 과거처럼 도청에 의한 신용정보의 유출은 적어졌다. 그렇지만 사용자의 신용정보는 전자상점을 거쳐 지불되기 때문에 악의를 가진 전자상점에 의해서 신용정보가 유출될 가능성이 있다.



(그림 1) SSL을 이용한 지불 시스템

본 논문에서는 SSL을 이용한 신용카드기반의 지불 시스템이 가지는 개인 신용정보의 유출 가능성을 차단할 수 있는 방법으로 지불 시 실제 카드번호와 다른 일회용 신용정보를 사용하는 전자지불 시스템을 제안한다. 이 지불 시스템은 보안성을 향상시키고 기존의 신용카드의 장점을 그대로 살리는 특징을 가진다. 그러기 위해서는 사용자에게 추가적인 프로그램의 설치를 요구하지 않아야 하고 기존 신용카드의 "마그네틱 카드를 그대로 사용", "대금지불을 후불로 결제"와 같은 장점을 그대로 살릴 수 있어야 한다.

논문의 구성은 다음과 같다. 2장에서는 기존의 전자지불 방식들을 소개하고, 간단한 특징들을 설명한다. 3장은 신용카드 기반의 전자지불 시스템의 문제점을 분석하고 4장에서는 본 논문에서 제안하고 있는 일회용 신용정보를 이용한 전자지불 시스템에 대해서 알아본다. 5장에서는 제안된 시스템의 구현에 관한 내용을 정리하고 6장에서는 결론을 내린다.

2. 관련 연구

전자상거래의 발달과 더불어 많은 전자지불 시스템들이 연구되어 왔다. 또한 안전성의 향상을 위해서 많은 시스템들이 물리적 혹은 전자적인 방법들을 연구하고 있다. 특히 암호학적 연산을 이용한 시스템들이 등장하면서 많은 발전을 이룩하였다.

이러한 전자지불 시스템은 가치정보의 저장위치에 따라 전자지갑형과 네트워크형으로 크게 나뉘어 발전해 왔다. 네트워크형은 다시 전자화폐, 신용카드, 전자수표, 온라인이체(인터넷뱅킹)로 분류되며 다음과 같다.

2.1 전자지갑

전자지갑은 사용자가 화폐가치를 가지는 정보를 은행으로부터 발급받아 개인 PC혹은 IC카드에 저장하는 가치 저장형으로 영국의 Mondex[4], 벨기에의 Proton[5], Visa 카드사의 Visa Cash[6]등이 대표적인 시스템이다. 이러한 전자지갑시스템은 현금을 대신하는 시스템으로 실세계의 현금을 대신한다. 장점으로는 익명성, 안전성, 불추적성 등의 특징을 가지지만 사고 발생시 불추적성으로 인해 분쟁해결이 어렵고, 분실 및 시스템 오동작으로 가치정보를 상실할 가능성이 크다.

2.2 전자 화폐

네트워크형 전자화폐는 온라인으로 지불에 필요한 정보를 전송하여 지불을 수행하는 방식으로 eCash[7], MiliCent[8]가 대표적인 시스템이다. 특징으로는 이중사용이 방지되고 안전성이 뛰어나며 불추적성을 가진다. 발행은행의 온라인 확인과정이 필요하여 많은 시간이 소요되고 이용수수료가 비싼 것이 단점이다.

2.3 신용 카드

일상생활의 신용카드를 인터넷으로 구현한 방법이며, 후불식 방식으로 SET 프로토콜[9], Cyber Cash[10], First Virtual[11]이 대표적인 시스템이다. 후불식 방식을 취하고 있어, 지불에 관련된 분쟁이 발생했을 경우 분쟁해결 능력이 뛰어나고, 지불과정이 간단하여 가장 널리 사용되고 있는 지불 방식이다. 단점으로는 시스템이 복잡하고 일부 시스템에서는 "이중지불"과 "신용카드 정보의 유출"로 인한 사고의 위험이 있다.

2.4 전자 수표

기존의 수표를 전자화한 시스템으로 수표의 배서 부분을 전자서명으로 구현한 방법이다. 전자서명은 거래은행의 인증서를 기반으로 서명을 생성/확인 하는 시스템이다. 대표적인 시스템으로는 Echeck[12], Netcheque[13] 시스템이 있으며, 안전성이 뛰어나고 이중사용이 방지되며, 불추적성의 특징을 가진다. 단점으로는 인증서 관리 및 서명을 위한 별도의 프로그램을 설치해야 하는 문제점을 가지고 있다.

2.5 온라인 이체(인터넷뱅킹)

특정 금융기관과 상점이 협약하는 경우 혹은 금융기관과 전자지불 시스템을 운영하는 회사가 상호 협의한 경우, 인터넷뱅킹을 이용하여 계좌이체를 수행하고 수행된 결과를 전자상점에 보고함으로 해서 전자지불을 수행하는 방식이다. 장점으로는 기존 시스템을 그대로 이용할 수 있어 수수료가 적고, 전자상점은 빠른 입금 확인과 현금지급이 가능하다는 점이다. 단점으로는 정해진 시간(인터넷뱅킹이 가능한 시간)에만 지불이 가능하며, 계좌이체는 현금과 같이 바로 지불되는 방식으로 분쟁이 발생하는 경우 사용자를 보호할 방법이 없다.

위와 같이 많은 전자지불 시스템이 뛰어난 보안성을 가지고 있지만, 널리 이용되지 못하고 있다. 반면 SSL을 이용한 신용카드 기반의 지불 방식은 통신보안을 제외하고는 어떠한 암호학적 보안장치도 없지만, 가장 널리 사용되고 있는 방식이다. 하지만 분쟁이 발생했을 경우 이를 해결하기 위해서는 지불 부인방지 및 신용정보의 유출을 막을 수 있는 장치들이 필요하다.

3. 신용카드 기반 지불 시스템의 문제점

SSL을 이용한 신용카드 기반의 전자지불 시스템은 구조상 사용자의 신용정보에 대한 취약점이 노출되어 있으며, 사용자가 지불(구매행위를) 부인을 하는 경우 분쟁해결이 어렵다. 즉 신용카드 기반의 지불 시스템은 악의를 가진 전자상점 혹은 악의를 가진 사용자에 의해서 문제가 발생할 수 있다. 다음은 이러한 문제점들을 자세히 알아본다.

3.1 악의를 가진 전자상점

신용카드 기반의 전자지불 시스템은 신용정보가 전자상점을 거쳐 은행에 지불되기 때문에 악의를 가진 상점의 개입이 가능하다. 이는 SSL이 전자상점과 사용자 사이의 통신만을 보호하기 위한 암호학적 연산으로, 모든 개인 신용정보가 전자상점에게 모두 노출되어 있는 구조이기 때문이다. 일부 공개키 기반의 전자 지불 시스템은 은행의 공개키로 암호화하고 이를 다시 상점의 공개키로 암호화 하는 이중암호화를 통해 전자상점이 지불에 필요한 정보를 직접 볼 수 없도록 만들었지만 SSL기반의 지불시스템은 그러한 기능을 가질 수 없다.

만약 악의를 가진 전자상점 혹은 전자상점의 직원이 사용자들의 신용정보를 이용하여 다른 전자상점에서 물건을 구입하는 경우, 정당한 사용자가 물건을 구입한 것인지 도용된 것인지 판단하기 어렵게 된다. 특히 영세한 상점이나 잘 알려지지 않은 상점의 경우 소비자들이 안전성에 의문을 제기하고 외면하는 문제가 발생할 수 있다.

3.2 악의를 가진 사용자

현재 사용중인 SSL을 이용한 방법은 정당한 사용자가 지불을 요청한 것인지, 구매자가 다른 사람의 신용카드 번호와 유효기간(예를 들면 악의를 가진 상점에 의해서 유출된 정보)을 이용한 것인지 정확히 구분할 방법이 없다. 특히 분쟁이 발생하는 경우, 전자 상점이 가지는 법적인 근거는 전무하다. 만약 악의를 가진 사용자가, 물건을 구매하고 신용카드 회사에 자신이 구매하지 않았다고 말한다면, 전자상점에서 제시할 수 있는 근거가 없기 때문에 시간적 금전적 피해를 보게 된다. 최근에 이러한 문제를 해결하기 위해서 일부 시스템의 경우 신용카드 소유자임을 증명 하기 위해서 몇 가지 방법이 제안되었다.

- **물리적인 증명** : 신용카드 외에 고객 고유의 CD-ROM을 이용하여 본인임을 증명하는 개인 식별 방식으로 사용자 인증을 위한 비밀정보를 CD-ROM에 보관하여 지불에 사용한다[14]. 이와 유사한 방법으로 IC 카드를 이용한 인증방법과 OTP(*One Time Password*)를[14,15] 이용한 방법이 있다.
- **비밀번호** : 신용카드의 4자리의 비밀번호 중 2자리를 입력하여 지불 시 한번 더 확인하는 방식이다[16].

이러한 시도들은 사용자의 지불을 증명하기 위한 방법들로 악의를 가진 사용자의 지불거부를 방지하기 위한 방법들이다. 물리적인 증명은 이를 위해서 CD-ROM, IC 카드, OTP 생성기와 같은 특별한 하드웨어를 요구하는 단점이 있다. 비밀번호를 이용하는 방법은 법적인 근거를 가지기 어렵고 비밀번호 4자리 중에서 2자리를 상점에 알려주기 때문에 악의를 가진 상점이 비밀번호를 알 수 있다.

3.3 전자거래에 의한 분쟁

전자상거래과정에서 "악의를 가진 상점", "악의를 가진 사용자" 외에도 많은 분쟁의 소지를 가지고 있다. 이러한 분쟁을 해결하기 위해서는 분쟁 해결을 위한 근거 자료가 필요하다. 즉 전자상점과 사용자 사이에 거래가 성립되었음을 증명할 방법이 필요하다. 이것은 신용카드 정보를 인터넷에서 사용하고 있지만 전자상점 사용자의 주문내역을 쉽게 복사 혹은 변형할 수 있기 때문이다. 물론 신용카드 회사에서 사후 분쟁 조정을 할 수는 있지만, 많은 시간과 노력이 필요하다. 이러한 시간과 노력은 결국 전자 상거래를 위한 관리비용으로 들어가고 시스템의 전체 운영비를 높이게 된다.

사용자의 대금지불 요청을 증명하는 방법으로 전자 서명을 많이 사용한다[17]. 전자 서명은 특정한 누군가에 의해서 작성된 전자적 문서가 변하지 않았음을 증명하는 것으로 전자거래를 증명할 수 있는 근거 자료가 된다. 법원에서 증명서류를 발급 받을 때, 발급일과 유효 날짜를 찍는 것과

같이 문서에 전자 서명을 할 때 정확한 시간 정보를 추가하게 된다. 이 시간 정보는 전자상점이나 사용자에 의해서 결정되는 것이 아니라 인증기관으로부터 발급 받아야 한다[18]. 이렇게 발급된 증명서는 전자거래의 "누가, 언제, 어디서, 무엇을, 어떻게, 했는지"를 증명하게 되며 사용자와 전자상점 사이에 계약서와 같은 역할을 한다. 이는 사용자와 전자상점 모두에게 거래가 성립되었음을 증명할 수 있는 근거를 제시하는 것으로 전자상거래에서 생기는 분쟁을 해결할 수 있는 역할을 한다.

4. 일회용 신용정보를 이용한 전자지불 시스템

앞에서 언급한 것과 같이 SSL을 이용한 신용카드 지불 시스템은 많은 보안상의 문제점은 안고 있다. 그러한 문제들의 원인은 다음과 같은 구조 때문이다.

- 사용자의 신용정보가 전자상점에 아무런 보호 없이 전송된다.
- 전자상점과 합법적인 사용자 사이의 거래를 증명할 법적 근거를 가지고 있지 않다.

사용자의 신용카드 정보를 안전하게 금융기관까지 전송하는 방법은 다음의 세 가지가 가능하다.

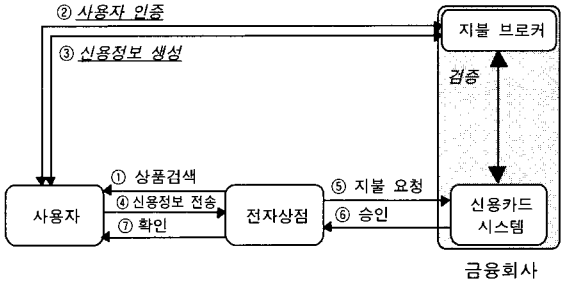
1. 신용정보를 전자상점을 거치지 않고 직접 금융기관에 전송 : 이 방법은 전자 수표 혹은 인터넷 뱅킹의 확장된 형태로 시스템 자체는 매우 안전하다. 하지만 대금 지불 과정이 물건 구입과 별도로 운영되는 구조를 가지고 있어 전자상점과 금융기관 사이의 통일된 통신 규약이 필요하다.
2. 공개키 기반구조(PKI)에서 이중암호화 : 개인 신용정보를 금융기관의 공개키로 암호화하고 다시 전자상점의 공개키로 암호화하여 전송하는 방법으로 사용자 신용정보를 전자상점에게 전송하지만 볼 수 없도록 하는 방법이다.
3. 일회용 신용카드 정보를 사용하는 방법 : 전자상점이 받은 신용카드 정보를 실제의 신용카드 정보가 아닌 가상의 일회용 신용정보로 변환하여 지불에 사용하고 한번의 거래에서만 사용이 가능하도록 만든다.

위의 세 가지 모두 사용자의 신용정보를 보호하는 기능을 가지고 있다. 하지만 신용정보를 금융기관에 직접 전송하는 경우 전자상점의 상품주문자와 은행의 대금 결재자가 같은 사람임을 증명할 방법이 추가 되어야 한다. 공개키 기반구조에서 이중암호화는 "암호화", "공개키 관리", "전자지불"을 위한 별도의 프로그램을 요구한다. 반면 일회용 신용카드를 이용한 지불은 별도의 프로그램도 요구하지 않으며, 기존의 SSL을 이용한 신용카드 지불 시스템에 그대로 연동이 가능하다.

한편, 전자상점과 합법적 사용자 사이의 거래내용을 증명할 수 있는 방법으로 전자서명을 사용한다. 전자서명은 사용자와 전자상점의 공개키를 이용하는 경우가 많아 공개키 기반 구조에서 가능하다. 하지만 SSL을 이용한 신용카드 지불시스템은 사용자가 공개키를 가지고 있지 않다. 그래서 본 논문에서는 사용자의 전자서명 대신 일회용 신용정보를 이용하고, 전자상점은 자신의 공개키를 이용하여 전자서명하고 공증기관[18]으로부터 공증을 받는 구조를 채택한다.

4.1 일회용 신용정보

일회용 신용정보를 이용한 전자지불 시스템은 신용정보 생성을 위해서 일방향 해쉬함수를 사용한다. 일방향 해쉬함수란 주어진 메시지 x에 대해서 $y=f(x)$를 계산하는 것은 쉽지만, 역함수인 $x=f^{-1}(y)$를 계산하는 것은 불가능(computationally infeasible)한 함수를 말한다. 이는 안전한 일회용 신용정보의 생성/검증은 용이한 반면 합리적인 시간 내에 이를 복원하는 것은 불가능함을 의미한다.



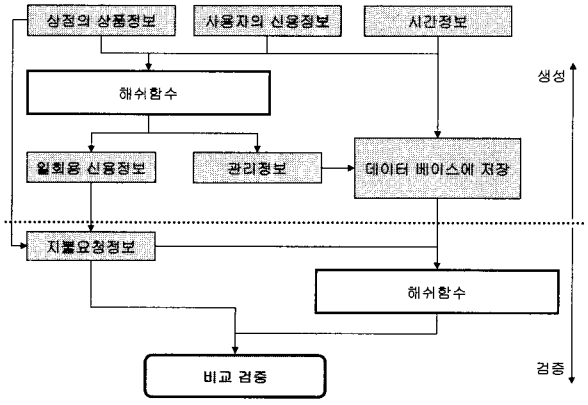
(그림 2) 제안한 지불 시스템(Proposed payment system)

본 논문에서 제안하는 일회용 신용정보를 이용한 지불 시스템은 (그림 2)와 같은 구조를 가진다. 즉 기존의 SSL을 이용한 신용카드 지불 과정에서 이탤릭체로 쓰여진 "②사용자인증", "③신용정보 생성", "검증"의 3단계가 추가된다.

사용자는 전자상점에서 물건을 검색(그림 2-①)하고 구매를 진행한다. 전자상점은 대금 지불 방법으로 일회용 신용정보를 선택하는 경우, 지불 브로커에 연결(그림 2-②)하고 사용자는 연결된 지불 브로커에서 일회용 신용정보를 발급 받아(그림 2-③) 전자상점에 입력(그림 2-④)한다. 전자상점은 입력된 신용정보를 이용하여 기존 신용카드 승인절차(그림 2-⑤)를 거치게 되며 금융기관은 신용카드 지불 과정에서 일회용 신용정보가 입력되면 이 정보를 지불 브로커에 검증을 요구한다. 지불브로커는 발급된 내용이 정당한지를 검사하여 신용카드 시스템에 결과를 알린다. 신용카드 시스템은 이를 바탕으로 지불을 승인 혹은 거절(그림 2-⑥)하게 되며, 상점은 지불 결과(그림 2-⑦)를 통해 물건을 배송한다.

이 과정에서 지불 시스템은 다음과 같은 기능이 필수적으로 필요하다.

- **안전한 신용정보 생성/검증** : (그림 3)은 신용정보의 생성 및 검증과정을 나타낸다. 지불 브로커는 사용자가 지불 브로커에 미리 등록한 자신의 신용정보와 구매하고자 하는 상품정보, 시간정보(time stamp)를 이용하여 일회용 신용정보를 생성한다. 또한 지불 브로커가 발행한 신용정보는 지불브로커 외에는 생성할 수 없어야 하며, 쉽게 검증되어야 한다. 이러한 문제의 해결을 위해서 일방향 함수를 사용하였다. 이렇게 생성된 신용정보는 매번 새롭게 생성되고, 함수의 일방향성 때문에 안전하다. 하지만 생성된 정보는 지불브로커에서 쉽게 확인할 수 있는 기능이 필요하다. 또한, 전자상점에서 지불이 요청된 경우 일회용 신용정보 생성에 필요한 정보들과 지불 시 요청된 데이터를 이용하여 신용정보를 검증하고 카드 승인을 하게 된다



(그림 3) 신용정보의 생성/검증(Generation and verification of a one-time credit)

- **사용자 인증** : 현재 지문인식과 같이 생체인식에 의한 인증 방식과 서버에서 제공한 난수 이미지를[1] 이용하는 방식 등 다양하고 강력한 인증 방식들이 제안되고 있다[19, 20]. 본 논문에서 사용자 인증 기능은 금융회사에서 제공하는 것으로 가정한다[19].
- **공증기능** : 공증기능은 시점확인 시스템[21-25]을 이용하며, 특정 시간에 문서 혹은 사건의 발생을 증명한다. 즉 사용자가 특정 시간에 지불브로커에게 지불을 의뢰하였음을 증명하기 위해서 시점확인 서버와 전자서명이 연동되어야 하며 자세한 내용은 다음절에서 설명한다.

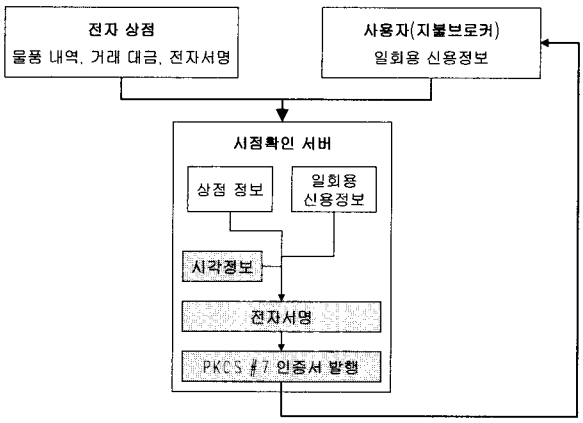
위에서 설명한 일회용 신용정보를 사용하면, 다음과 같은 장점을 얻을 수 있다.

- o 지불에 사용된 정보는 매번 새롭게 생성되어 개인 신용정보의 유출 가능성이 없다.
- o 지불에 사용된 정보는 일회성으로 이중 사용이 불가능하다.
- o 기존의 신용카드 기반의 지불 시스템과 연동이 가능하다.
- o 사용자에게 추가적인 소프트웨어의 설치를 요구하지 않는다.

위의 특징 중에서, 기존의 신용카드 기반의 지불 시스템에 그대로 적용 가능함은 상점의 입장에서 기존 시스템과 거의 동일한 구조를 가짐을 의미한다. 즉 기존 전자지불 시스템에 몇 가지 추가적인 기능 외에는 큰 변화가 없음을 의미하며 금융회사의 신용카드 시스템과 지불브로커에서 많은 기능이 추가되어야 한다.

4.2 거래내역의 공증

사용자와 전자상점 사이의 거래 내역을 증명하기 위해서 전자서명을 이용한다. 하지만 공개키 기반구조가 아닌 이상 사용자는 공개키를 가지고 있지 않다. 특히 서명을 위해서 사용자에게 별도의 프로그램을 요구하지 않기 위해서는 공개키에 의한 전자서명 방식을 이용할 수 없다. 본 논문에서는 사용자의 전자서명 대신 일회용 신용정보를 이용하여 공증기관으로부터 전자서명을 받는 방식을 제안한다. (그림 4)은 시점확인 서비스를 이용한 공증 과정을 나타낸다.



(그림 4) 시점확인(TimeStamp) 서버를 이용한 인증서 발행

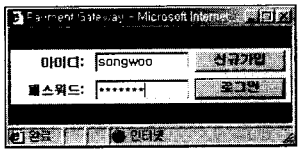
사용자가 구매를 하는 경우 전자상점은 상품 정보와 함께 자신의 서명을 제시하여 사용자에게 결제를 요구한다. 사용자는 상점의 지불 창에서 일회용 신용정보를 선택하고 지불브로커에 로그인 하면, 지불브로커는 상점에서 제공한 정보와 사용자의 신용정보를 이용하여 일회용 신용정보를 생성하고 생성된 신용정보와 상점의 서명을 이용하여 (그림 4)와 같이 시점확인 서버[25]에서 발행한 인증서를 받아서 저장한다. 시점확인 서버는 전자상점과 사용자로부터 받은 정보를 기반으로 지불 브로커에게 인증서를 발행한다. 시점확인 서버는 공인 인증기관에서 제공하는 서비스로서 법적인 효력을 가진다.

1) 난수를 일그러진 이미지로 전송하여 파일을 보고 읽은 사용자만 난수를 알 수 있는 이미지.

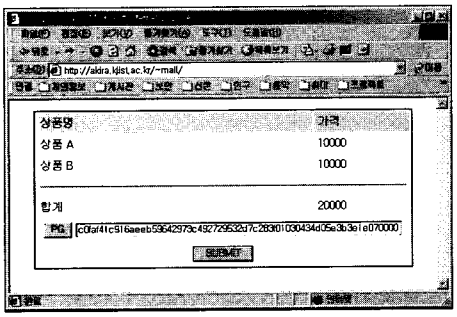
5. 구 현

신용카드 번호를 대신한 일회용 신용정보를 생성하기위한 방법으로는 "MAC 알고리즘을 이용하는 방법"이 있다. 이 방법은 MD5, SHA-1, RIPEMD 160 해쉬함수를 사용하는 HMAC 알고리즘을 이용하여 신용정보를 생성하는 방법으로 SSL 내부에 포함된 기본 기능으로 별도의 암호 알고리즘 혹은 라이브러리를 추가하지 않아도 된다.

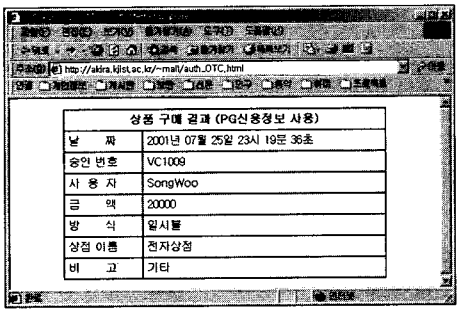
프로그램은 전자상점, 지불브로커, 신용카드 시스템으로 구성되며 각각 관리 기능과 감사기능과 데이터베이스를 가진다. 전체 시스템에서 신용정보의 생성/검증과 시점 확인 서버의 연동을 제외하고는 전부 통신과 데이터베이스에 관련된 모듈이다. 이중에서 사용자가 상점에 접속하여 대금을 지불하는 경우 지불브로커로 연결이 되는데 상점의 정보(상품정보, 지불금액)를 지불브로커에 전달하기 위해서 쿠키를 사용하였으며 구현 언어로는 자바 애플릿을 사용하였다. (그림 5)는 사용자가 지불을 요청 받아 지불 브로커에 로그인(그림 5) (가)하고 일회용 신용정보를 생성 받아 지불을 요청(그림 5) (나)하고 그 결과를 수신한 화면(그림 5) (다)을 보여주고 있다.



(가) 인증화면



(나) 일회용 신용정보를 이용한 지불 요청



(다) 일회용 신용정보를 이용한 지불요청 결과

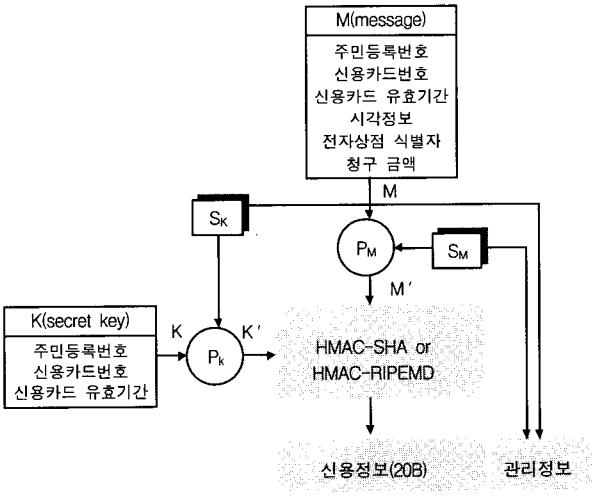
(그림 5) 일회용 신용정보 지불(One-time credit payment)

다음은 본 논문에서 제안한 일회용 신용정보 생성/검증과 시점확인 서버 연동에 관련된 구현내용이다.

5.1 신용정보 생성 알고리즘

신용정보는 일정 길이 이상이어야 한다. 일반적으로 암호 알고리즘에서 해쉬함수가 안전하기 위해서는 출력정보의 길이가 128비트 이상, 입력정보의 길이는 출력정보 길이의 최소 2배로 설정해야 하며[26, 27], 본 논문에서 제안된 일회용 신용정보 생성과정은 (그림 6)과 같다. 그림에서 secret key 부분과 message부분은 HMAC함수의 입력이며 사용자의 주민등록번호, 신용카드 번호, 유효기간, 시각정보, 전자상점 식별자, 청구금액을 사용한다. HMAC의 처리 과정에서 자동 생성된 S_k 와 S_m 은 관리정보로 사용자 정보와 함께 보관하게 되며, 일방향 함수인 HMAC-SHA나 HMAC-RIPEMD를 이용하여 일회용 신용정보를 생성하게 된다. 생성된 정보는 신용정보(20바이트) 와 관리정보(12바이트)로 나뉘어 지는데 신용정보는 지불에 사용되는 일회용 신용정보이며 관리정보는 사후 검증 시 필요한 정보이다((그림 3) 참조).

HMAC함수의 입력인 secret key 부분과 message 부분에 중복되는 정보를 가지고 있지만, 내부에서 각각 치환(Permutation) P_m과 P_k 과정을 거치면서 완전히 다른 값으로 변경되기 때문에 안전성의 문제는 발생하지 않는다.



(그림 6) 신용정보 생성 함수(Generation mechanism of a credit information)

여기서 message부분을 보면 시각정보가 있는데, 이 시각정보는 지불브로커가 생성한 시간이며, 이 시각정보와 발급받은 신용정보 그리고 상점의 전자서명을 해쉬하여 시점확인 서버의 공증을 받는다.

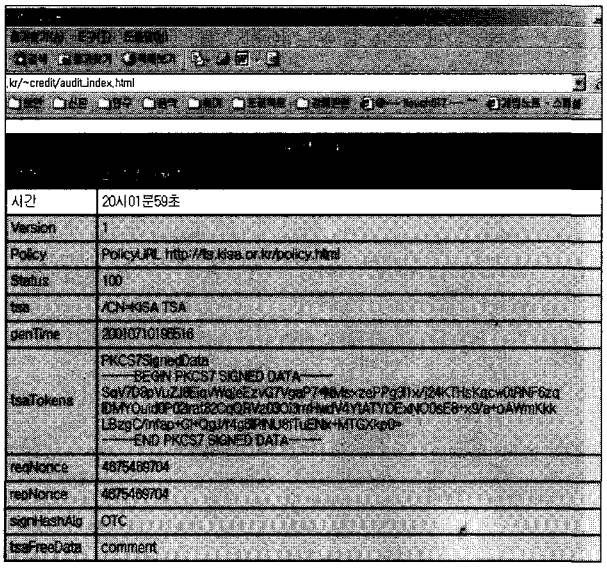
5.2 신용정보 검증

전자지불에 사용된 일회용 신용정보는 20바이트의 정보로 전송된다. 이 정보는 신용카드 시스템에서 지불 브로커

로 검증을 요구하게 되고 지불 브로커는 이 정보를 기반으로 일회용 신용정보 생성에 사용된 정보들을 검색한다. 발행된 일회용 신용정보의 유효기간과 기사용 여부를 검사한다. 아직 유효한 일회용 신용정보라면 청구된 금액과 상점 식별자를 보고 해쉬함수를 다시 수행하여 지급 요청된 일회용 신용정보가 맞는지 확인하게 된다. 이 과정은 (그림 6)과 동일하며 입력 값인 "관리정보", 주민등록번호, 신용카드번호, 신용카드 유효기간, 시각정보는 지불브로커에 저장된 내용을 사용하고 전자상점 식별자, 청구금액은 검증 시 전자상점으로부터 제공받는 정보를 사용한다.

5.3 시점확인 서버와 연동

시점확인 서버와 연동하기 위해서 제안된 표준 통신규격을 따라 설계하였다[24]. 그리고, 일회용 신용정보 생성/검증 시스템과 시점확인 서버간 교환되는 자료의 무결성 보호를 위해 시점확인 요청 메시지에 대해서는 SHA-1 해쉬함수가, 신용정보와 상점 정보에는 MD5 해쉬함수를 적용하였다. 아래 (그림 7)은 이러한 표준을 따라 서비스를 요청하여 받은 응답 메시지의 내용이다.



(그림 7) PKCS #7 인증서(Certificate)

6. 결 론

전자지불 서비스는 전자상거래의 시장에 비례하여 증가하고 있다. 2005년 약 2000억원 이상의 시장을 형성할 것으로 예상[2]하고 있으며, 현재 사용중인 SSL 기반의 신용카드 지불방식의 문제점인 "사용자 신용정보의 상점 유출"을 방지하고 신용카드 기반의 장점인 "후불식 지불"과 "분쟁 조정 기능"을 그대로 살릴 수 있는 시스템을 제안/구현하였다. 특히 비밀키나 공개키 암호방식이 일정 기간이 지난 후 개인키를 새로 발급(혹은 인증서) 받아야 하는 불편함이 있지만 제안된 시스템은 사용자에게 별도의 키 관리가 필요하지 않아 시스템 구축 후 관리비용이 저렴하다. 또한 사용자의 입장에서 추가적인 프로그램도 요구하지 않으며, 기존의 방법보다 안전한 지불 방법을 제공하고 있다.

특히 전자지불 시스템에서 분쟁이 발생하는 경우를 대비하여 독립된 인증 기관인 시점확인 서버를 연동하여 전자지불 시스템의 분쟁 해결을 위한 법적 근거를 마련하였다. 물론 법적근거를 마련하기 위해서는 공인 인증기관의 인증을 받거나 공인 인증기관의 서비스를 이용해야 하지만, 본 시스템에서 기존 시스템과 연동이 가능하다.

2) 엔더슨 컨설팅 '99

참 고 문 헌

[1] 통계청 서비스업 통계과, "전자상거래통계조사결과 (2002년 1월 사이버 쇼핑몰 조사-B2C)," http://www.nso.go.kr/report/data/suec0201.htm, 2002.
[2] 신철균, "<열린마당> 전자결제 보안 구멍", 전자신문, 2001.
[3] N. Asokan, Phillipe A. Janson, Michael Steiner and Michael Waidner, "State of the Art in Electronic Payment Systems," IEEE Computer, Vol.30, No.9, pp.28-35, 1997.
[4] Mondex, http://www.mondex.com/.
[5] Proton, http://www.element.be/.
[6] Visa cash, http://international.visa.com/.
[7] eCash, http://www.ecashtechnologies.com/.
[8] Milicent, http://www.milicent.digital.com/.
[9] SET Secure Electronic Transaction LLC, http://www.setco.org/set_specification.html.
[10] CyberCash, http://www.cybercash.com/.
[11] L. H. Stein, E. A. Stefferud, N. S. Borenstein, and M. T. Rose, "The green commerce model," Technical report, First Virtual Holdings Incorporated, http://www.fv.com/tech/greenmodel.html, October, 1994.
[12] Echecks, http://www.echeck.org/.
[13] NetCheque, http://www.isi.edu/gost/info/NetCheque/.
[14] http://www.cdcash.co.kr/index.asp.
[15] Neil M Haller, "The S/KEY One-Time Password System," Proceedings of the ISOC Symposium on Network and Distributed System Security, San Diego, CA, February, 1994.
[16] http://pgweb.dacom.co.kr/ECREDIT/.
[17] R. L Rivest, A. Sharmir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol.21, No.2, pp.120-126, Feb., 1978.
[18] http://www.rootca.or.kr.
[19] http://www.ehanvit.co.kr/.
[20] http://www.paypal.com/.
[21] RSA Laboratories, "PKCS #7 Cryptographic Message

Syntax Standard Version 1.5," Technical Note Version 1.5, Revised November, 1993.
[22] Adams, Cain, Pinkas, Zuccherato, "Internet X.509 Public Key Infra-structure, Time Stamp Protocol(TSP)," draft-ietf-pkix-time-stamp-12, Internet-Draft, 2000.
[23] ISO/IEC JTC1/SC27 N2107, "Guidelines on the use and management of Time Stamping Services(GUMTSS)," 1998.
[24] C. Adams, P. Cain, D. Pinkas, R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," ftp://ftp.rfc-editor.org/in-notes/rfc3161.txt, August, 2001.
[25] http://www.timestamp.co.kr/.
[26] L. R. Knudsen, X. Lai, and B. Preneel, "Attacks on fast double block length hash functions," Journal of Cryptology, Vol. 11, No.1, pp.59-72, Winter, 1998.
[27] Douglas R. Stinson, "Cryptography theory and practice," pp.233, CRC press, 1995.

신 종 철

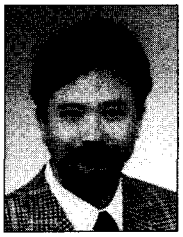
e-mail : sis@songwoo.co.kr
1976년 서울대학교 전기과 졸업(학사)
1994년 연세대학교 산업대학원(전자계산 전공) 졸업(석사)
2000년 충북대학교 전자계산학과 박사 과정 수료
1978년~1992년 현대엔지니어링 전산실/정보사업부
1992년~2000년 (주)송우정보 대표이사
2000년~현재 송우아이엔티(주) 기술연구소장
관심분야 : 개발방법론, 요구공학, 정보시스템 감리

박 종 열

e-mail : jypark@kjist.ac.kr
1996년 충남대학교 컴퓨터공학과 졸업(학사)
1999년 광주과학기술원 정보통신공학과 졸업(석사)
2001년~2002년 University of Utah, school of computing 객원 연구원
1999년~현재 광주과학기술원 정보통신공학과 박사과정
관심분야 : 전자지불, 이동코드, 인증시스템, 보안알고리즘, 분산 시스템 등

이 형 효

e-mail : hlee@wonkwang.ac.kr
1987년 전남대학교 전산학과 졸업(학사)
1989년 KAIST 전산학과 졸업(석사)
2000년 전남대학교 전산학과 졸업(박사)
1990년~1992년 삼보컴퓨터 기술연구소
1993년~1997년 한국통신 연구개발원
1995년 정보처리기술사(전자계산조직응용)
2000년 광주과학기술원 BK21 Post-Doc
2001년~현재 원광대학교 정보·전자상거래학부 전임강사
관심분야 : 정보보안, 보안모델, 통신망 보안관리, 전자상거래 보안



이 동 익

e-mail : dilee@kjist.ac.kr
1985년 영남대학교 전자공학과 졸업(학사)
1989년 Osaka Univ. 전자공학과 졸업 (석사)
1993년 Osaka Univ. 전자공학과 졸업 (공학박사)
1990년~1995년 Osaka 대학 전자공학과 문부교관
1993년~1994년 Univ. of Illinois at Urbana-Champaign 객원 연구원
2001년~2002년 Univ. of Utah 객원교수
1995년~현재 광주과학기술원 정보통신공학과 조교수, 부교수
관심분야 : 보안시스템, 에이전트시스템, 페트리 넷 이론 및 응용, 비동기 회로 CAD/설계 등

윤 석 환

e-mail : yoonsh@iita.re.kr
1982년 아주대학교 산업공학과 졸업
1984년 건국대학교 산업공학과 석사
1992년 품질관리 기술사 자격취득
1996년 아주대학교 산업공학과 박사
1986년~1997년 한국전자통신연구원 책임 연구원
1998년~현재 정보통신연구진흥원 책임연구원
1998년~현재 한국정보처리학회 이사 겸 학회지 편집위원장
2000년~현재 대전산업대학교 정보통신, 컴퓨터공학과 겸임교수
관심분야 : 소프트웨어공학, 품질공학, 개발방법론, 그룹웨어 등