通信情報保護學會誌
第7卷 第3號, 1997. 9

SET 기반의 전자 지불 시스템과 보안 기술

Electronic Payment System and Security Technology based on SET

송 병 열*, 조 현 규*, 송 유 진**, 이 경 호*, 함 호 상*

요 약

SET은 인터넷과 같은 개방형 통신망에서 안전하고 효율적인 신용카드 기반의 전자 결제를 수행하기 위해 개발된 전자 지불 표준 프로토콜이다. SET을 기반으로하는 전자 지불 시스템은 크게 카드를 소지하고 있는 고객(Cardholder), 상품을 판매하고 대금 결제를 요구하는 상인(Merchant) 기존의 은행과 연동하기위한 지불 게이트웨이(Payment gateway)로 구성되며 부가적인 요소로 인증기관(CA)을 포함하고 있다. SET은 고객과 상인, 상인과 은행간의 안전한 거래를 지원하기 위해 여러 가지의 강력한 암호화 알고리즘을 채용하고 있으며 이러한 SET의 보안성은 전자 상거래의 보급에 커다란 기여를 할 것으로 예상된다. 본 논문에서는 기존의 전자 지불 방식을 특성별로 분류하여 그 기능과 구성에 대해 검토하고 SET에서 사용된 보안 기술과 SET을 기반으로하는 전자 지불 시스템의 기능과 특성을 검토·분석한다.

1. 서 론

인터넷과 같은 개방형 통신망을 통한 전자 상거래를 실현하기 위해 가장 큰 문제라고 하면 안전한 전자 지불 시스템의 구축이 선행되어야 한다는 것이다. 잘 꾸며진 전자 상점에서 물건을 선택하고 나서 구매하기 위해 다시 은행으로 가서 자금을 이체하거나 또는 신용카드 번호를 전화로 알려주는 등으로 구매하는 방식들은 시간적, 공간적 제약을 벗어나는 전자 상거래의 커다란 이점을 포기하게 하며 금융 사기의 위험성마저 가지게 한다. 따라서 진정한 의미의 시간적, 공간적 제약을 벗어난 전자 상거래가 성립되기 위해서는 안전한 전자 지불 체계가 구성되어야만 한다.

전자 지불의 초기 단계에서는 웹 홈페이지에서 이용자가 직접 신용카드 번호를 입력하는 방법과 전자 우편(email)을 통해 신용카드 번호를 전송하는 방식등을 이용하였다. 그러나, 이 방식은 신용 카드 번호가 암호화되지 않은 채 네트웍상에 그대로 전송되므로 악의를 지닌 해커에 의해 도용될 위험이 높아 그다지 많이 쓰이지 않았다. 그 외의 또 다른 방

* 시스템 공학 연구소
** 동국대학교 정보산업학과

법으로 웹 홈페이지에서 선택한 상품을 전화 또는 전자 우편으로 주문하고 지불은 은행에 가서 직접 대금 이체하는 방식이 있으나 이런 방식은 전자 지불이라 할 수 없다.

전송되는 지불 정보가 해커에 의해 도용 당하는 것을 방지하기 위한 방법으로 제시된 것이 SSL[1], SHTTP[2]등과 같이 전송되는 데이터를 암호화하는 보안 프로토콜을 사용하는 것이다. 보안 프로토콜로 보호되는 홈페이지에서 입력된 신용카드 번호와 같은 지불 정보는 암호화되어 안전하게 상인에게 전송된다. 이 방식은 사용되는 암호화 키의 크기에 따라 그 안전성이 결정되는 방식으로 큰 비트의 암호화 알고리즘을 사용하는 경우 높은 안정성이 유지되어 현존하는 많은 상거래 서버 시스템이 이 방법을 사용하게 되었다. 특히 SSL은 Netscape사가 개발하여 자사의 Commerce Server에 적용하였으며 그 외 OpenMarket, IBM, Microsoft등의 상거래 서버에도 채택되었다. 그러나, 이 방법은 전송되는 모든 데이터가 암호화 되므로 지불 정보만이 보호될 필요성이 있는 전자 지불 처리에서는 지불 정보를 제외한 다른 정보까지 암호화되어 시스템의 효율을 떨어뜨리는 문제점을 가지고 있다. 또한 이 방식은 앞서의 암호화를 하지 않는 지불 방식과 같이 쇼핑몰을 운영하는 상인에게 신용카드번호가 공개되므로 나쁜 의도를 지닌 상인이라면 도용당하여 사기의 피해를 입을 수 있으므로 안전하고 믿을만한 전자 지불의 해결책이 되지 못한다.

2. 전자 지불 시스템

인터넷 상에서 전자 지불 시스템이 해결해야만 될 문제점으로 대표적인 것이 앞서 언급한 지불 정보의 보호를 들 수 있으나 완전한 지불 시스템을 구성하기 위해서는 그외에 거래 부인 방지, 거래 당사자의 인증, 기존 금융체계와의 호환성등의 문제를 해결해야만 하며 따라서 지불을 목적으로하는 전자 지불 시스템의 개발을 요구하게 되었다.

전자 지불을 구현하기 위한 연구는 기업, 은행, 학계, 정부기관등에서 다양하게 진행되었고 그 결과로 등장하게 된 것이 Digicash 사의 E-cash[3]와 Mondex사에서 개발한 IC카드형의 전자 화폐인 Mondex Card[4]로 대표되는 전자 현금 시스템과 First Virtual사의 Green Commerce 모델[5], IBM의 iKP[6]등을 포함하는 신용카드 전자 지불 시스템 그리고 USC의 NetCheque[7]와 같이 수표를 이용하는 전자 수표 시스템등이 있으며 특별히 개발된 프로토콜은 없으나 유망한 전자 지불 방법의 하나로 Security First Network Bank의 전자 자금 이체(EFT: Electronic Fund Transfer)[8]방법 등이 있다. 표1은 기존의 대표적인 전자 지불 시스템을 지불 매체에 따라 열거해 보았다[9].

표 1 지불 매체별 전자 지불 시스템

지불매체	프로토콜
전자현금	E-cash(Digicash), NetCash(NetBank), CAFE(CAFE), Mondex(Mondex), PayWord, MicroMint, Millicent(DEC), MPTP(W3C)
신용카드	iKP(IBM), Green Commerce(First Virtual), SEPP(MasterCard), STT(Microsoft, VISA)
전자수표	NetCheque(USC), NetBill(CMU)
EFT	SFNB

다음으로 대표적인 전자 지불 프로토콜을 메커니즘 측면에서 전자 현금 방식과 지불 브로커 방식으로 분류하고 그 기능과 특성을 검토·분석한다.

2.1 전자 현금 방식

전자 현금 방식은 그 이용 방법에 따라 네트워크형과 IC카드형으로 나눌 수 있으며 지불 액수에 따라 다시 중·고액형과 소액형으로 구분된다. 전자 현금은 이용되는 매체가 실제 통화와 동일한 가치를 지니는 것으로 고도의 암호화 기술을 필요로 하며 가장 이상적인 전자 지불 방법이라 할 수 있다. 그러나, 실제 현금과 같은 지불자의 익명성 보장이나 위조·복사 방지와 같은 해결해야만 될 많은 기술적 문제가 여전히 남아있으며 현실 세계에서 통용되기 위해서는 거쳐야만 될 많은 사회·경제적인 문제가 남아 있다.

다음은 대표적인 전자현금 방식인 E-Cash, Mondex, Millicent을 소개하고 그 특징을 기술하였다.

(1) E-Cash

네트워크형 전자 현금의 대표적인 것으로 네덜란드의 DigiCash사에 의해 가장 먼저 서비스되었으며 David Chaum의 은닉 서명(blind signature)[10]을 사용하여 지불자의 익명성을 보장한다. 현재 Mark Twain Bank에서 실제 화폐와 일대일 교환 가능한 서비스를 실시하고 있다. 그림 1에는 E-cash를 기반으로하는 전자 지불 시스템의 구성을 보였다.

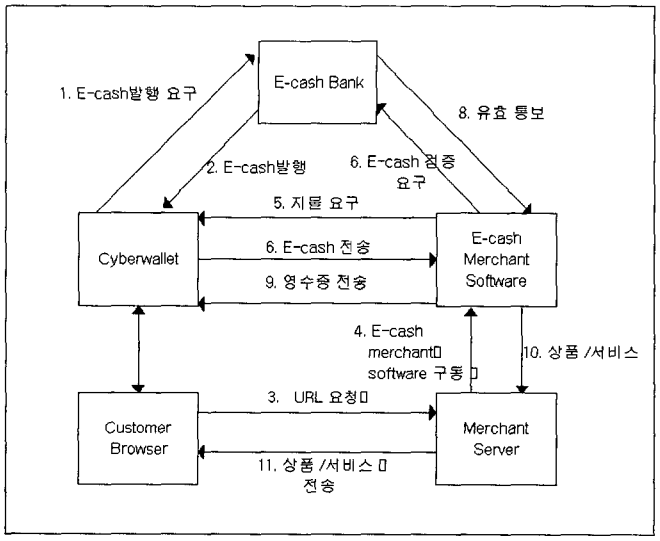


그림 1 E-cash 전자 지불 시스템

(2) Mondex

Mondex는 신용 카드 전자 지불 방식과 함께 가장 실현성이 높은 것으로 주목받고 있는 스마트카드(IC 카드)를 이용한 전자 지불 방식으로 영국의 National Westminster 은행과 Midland은행이 주도되어 현재 영국의 Swindon이라는 곳에서 실용 실험을 실시중이다. Mondex의 특징은 은행으로부터 그림 2와 같은 모양의 IC카드를 이용한 전자 지갑에 직접 화폐가치를 이전하여 실제 화폐와 같이

사용할 수 있다는 점이며 이용에는 전용 단말기가 필요하다는 점이다.

그림 2 Mondex Card

Mondex의 운용방식은 먼저 은행구좌에서 ATM(현금자동인출기)이나 전용 전화기를 사용하여 Mondex 카드에 전자 현금을 이전하고 전용 단말기가 설치된 상점이나 주차장, 또는 공중전화등에 사용한다. Mondex 카드로 대금을 지불하면 개인의 Mondex 카드안에 있던 전자 현금이 실제의 현금이 이동하는 것과 같이 상점의 단말기로 이용하여 개인의 Mondex 카드에 있는 전자 현금은 지불한 액수만큼 금액이 줄어들고 상점의 단말기에는 지불받은 액수만큼 금액이 늘어나게 된다. 이렇게 해서 개인의 Mondex 카드의 잔고가 바닥나게 되면 다시 ATM등을 이용하여 전자 현금을 이전하여 사용하며 개인용 단말기로 카드간 금액 이전도 가능하므로 실제의 통화와 같이 사용가능하다.

(3) Millicent

네트웍상에서의 소액지불을 구현하기 위한 대표적인 전자 지불 시스템으로 DEC에서 제안하였다.

Millicent의 기본적인 개념은 Millicent의 매체가 가지는 화폐가치가 매체의 암호화를 깨는데 드는 비용보다 적게 한다는 것으로 지불 브로커가 전자 화폐의 일종인 스크립(scrip)을 발행하고 전자 화폐에 대한 유효성 확인은 분산시킴으로서 화폐 처리에 소요되는 비용을 줄여 소액지불을 가능하게 하였다.

2.2.2 지불 브로커 방식

지불 브로커 방식은 신용카드를 이용한 전자 지불 방법이 가장 대표적이며 지불 정보의 보호하기 위한 암호화 기술과 함께 은행망과 같이 기존 금융 시스템과 연동하기 위한 구체적인 체계를 필요로 한다. 지불 브로커 방식에서는 지불 정보가 지불 게이트웨이나 지불 대행 기관을 통해 금융망과 연동되어 처리됨으로써 거래가 성립된다는 점에서 전송되는 매체 자신이 가치를 가지고 있는 전자 현금과 구별되며 실제의 금융거래와 함께 연동된다는 점에서 현실성이 높다. 그러나, 전자 현금에 비해 지불 정보가 전송되고 처리되는데 드는 비용이 비교적 높아서 소액 지불에는 적합하지 않은 방법이다.

(1) iKP

IBM에서 제안한 신용카드 기반의 전자 지불 프로토콜로 공개키 암호화 방법을 기반으로 고객의 신용카드 번호와 PIN 번호를 보호하고 거래 부인 방지를 제공한다. iKP의 기본 구조는 그림 3과 같으며 공개키의 소유 방식에 따라 1KP, 2KP, 3KP로 구분된다.

1KP : 은행의 지불 게이트웨이만이 공개키 쌍을 가지고 인증 기관의 역할을 하며 판매자와 구매자에 대한 거래 부인 봉쇄는 제공하지 못한다.

2KP : 은행의 지불 게이트웨이와 판매자가 공개키 쌍을 가지는 방식으로 판매자가 전송하는 메시지에 대한 거래 부인 봉쇄 서비스를 제공하며 인증서의 확인을 통해 쇼핑몰의 정당성을 확인할 수 있다.

3KP : 판매자와 구매자, 은행 지불 게이트웨이 모두 공개키를 가지는 방식으로 모든 거래 메시지에 대한 부인 봉쇄 서비스를 제공하며 쇼핑몰 및 구매자의 정당성을 확인할 수 있다.

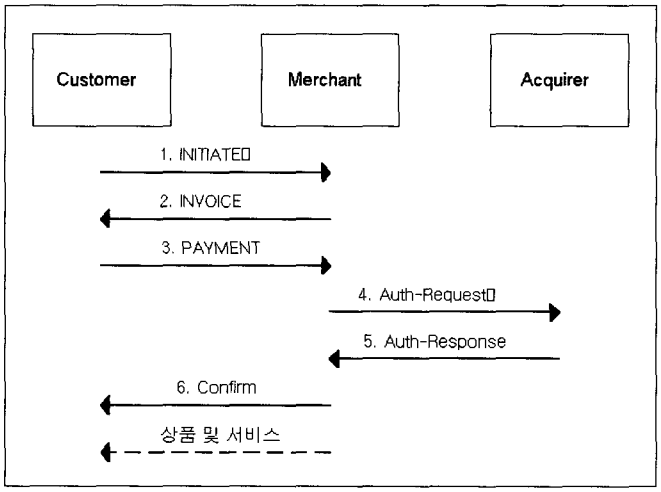


그림 3 iKP의 기본 구조

(2) Green Commerce

FV(First Virtual)의 Green Commerce 모델은 인터넷상에서 구현된 최초의 전자 지불 기술의하나로 이 기술은 기본적인 WWW 브라우저와 전자 메일만을 이용해 전자 지불 시스템을 구축했다는 점에서 다른 시스템과 구별되며 개개의 상품에 대한 지불을 거부할 수 있는 절대적인 권한을 고객에게 주어 믿을 수 없는 상인으로부터 고객을 보호한다는 것이 특이점이다.

Green Commerce 모델에서 구매자는 먼저 FV에 계정을 신청해야만 한다. 이때 필요한 정보는 이름, 주소, 전자 메일 주소이며 FV에서는 email로 FV의 전화번호와 12자리의 등록 신청번호를 전송한다. 구매자는 전화로 신용카드번호와, 유효기간을 FV에 알리고 email로 Virtual PIN이라고 불리우는 일종의 계정 ID를 받는다.

Virtual PIN을 이용한 실제의 구매 행위는 그림 4와 같이 FV의 Green Commerce Server를 중심으로 이루어진다.

(3) NetCheque

앞서의 iKP와 Green Commerce 모델이 신용카드를 기반으로하는 지불 브로커 방식의 전자 지불 기술이라면 캘리포니아 대학에서 개발 중인 NetCheque는 현실 세계에서 사용되고 있는 수표를 그대로 인터넷 상에서 구현한 전자 수표 시스템이다.

NetCheque는 분산된 복수의 서버를 도입하여 처리 비용을 낮추고 사용자 수를 극대화할 수 있는 방법으로 분산된 서버사이의 사용자 인증을 위해 MIT의 Kerberos[11]를 가반 기술로 채택하고 있다.

NetCheque의 전자 수표를 쓸 때 서명을 하거나 받은 수표에 배서할 때 Kerberos 티켓의 일종인 proxy를 사용하며 비밀키(secret key)를 사용하는 관용 암호화 방식을 사용하므로 공개키 암호화 알고리즘에 비해 효율적인 시스템이나 Kerberos 시스템이 가지는 한계[12]를 그대로 갖게 된다는 문제점이 있다.

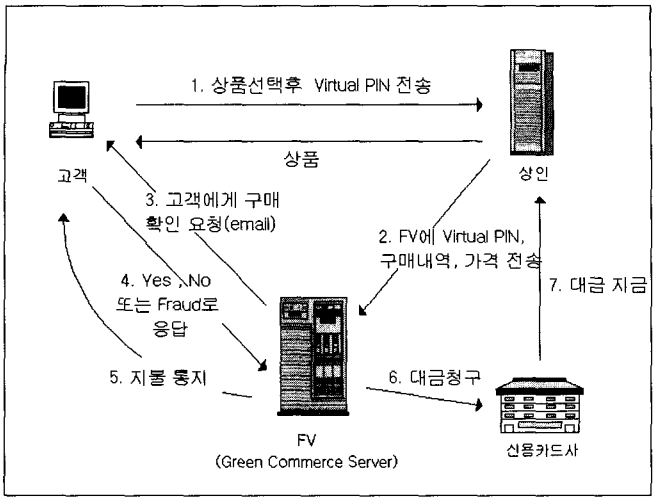


그림 4 Green Commece 모델

3. SET의 기능과 구성

최근 VISA와 MasterCard에 의해 발표된 인터넷을 통한 신용카드 전자 지불 프로토콜의 표준인 SET은 현실세계의 신용카드거래를 기반으로 모델링되어 기존 금융 시스템과의 연동이 용이한 구조이며 RSA의 암호화 기술을 기반으로 전송되는 지불 데이터를 보호하고 이중서명(dual signature)이라는 방법을 통해 상인에 대한 지불 정보의 투명성을 보장한다. 특히 신용카드회사의 80%를 점유하고 있는 VISA, MasterCard에서 표준으로 채택된 프로토콜이라는 점에서 다른 프로토콜에 비해 더욱 높은 이용 가능성을 지니고 있으며 실제로 SET을 지원하는 전자 지불 시스템의 개발이 미국, 일본등 세계 각국에서 진행되고 있다. 국내에서도 학계, 기업 및 연구 기관에서 SET을 기반으로하는 전자 지불 시스템에 대한 연구가 시작되고 있다.

3.1 SET의 기본 기능

전자 지불 프로토콜로서 SET은 보안 문제점이 금융기관, 상인, 고객 모두의 이익에 어떤 문제도 끼쳐서는 안된다는 원칙을 기본으로 하며 다음과 같은 기능적 요구 사항을 만족하도록 설계되었다.

(1) 정보의 기밀성 제공

인터넷을 통한 개인의 신용카드 번호등의 지불 정보와 지불 정보와 함께 전송되는 구매 정보등 상거래 정보의 유출을 막기위해 메시지 암호화를 통해 정보의 기밀성을 유지한다.

(2) 정보의 무결성 제공

지불 정보가 전송중에 변조되지 않았다는 것을 증명하기위해 전자 서명을 사용하여 보낸 메시지와 받은 메시지가 정확히 일치함을 보여줌으로써 정보의 무결성을 제공한다.

(3) 고객에 대한 인증

카드를 가지고 거래를 하는 고객에 대한 인증은 고객이 인증기관에서 발급받은 인증서와 전자 서명을 사용하여 해당 고객이 유효한 신용카드 사용자임을 확인한다.

(4) 상인에 대한 인증

고객의 입장에서 볼 때 자신이 거래하는 상인이 해당 브랜드의 카드를 수용할 수 있는 권한을 지니고 있는지 확인하기 위해 전자 서명과 함께 상인이 인증기관에서 발급받은 인증서를 사용한다.

(5) 최상의 보안성 제공

전자 거래의 모든 정당한 구성원을 보호하기 위해 효율적이면서도 강력한 보안성을 제공하기 위해 공개키 암호화 알고리즘과 관용 암호화 알고리즘 및 전자 서명, 전자 봉투(digital envelope), 이중 서명등의 보안 기술을 사용한다.

(6) 벤더(vendor) 독립성

기존 전자 지불 처리 기술과 달리 특정 벤더에 영향받지 않고 다양한 하드웨어와 소프트웨어에서 적용이 가능한 구조로 설계되어 다양한 응용 소프트웨어의 개발이 가능하게 하였다.

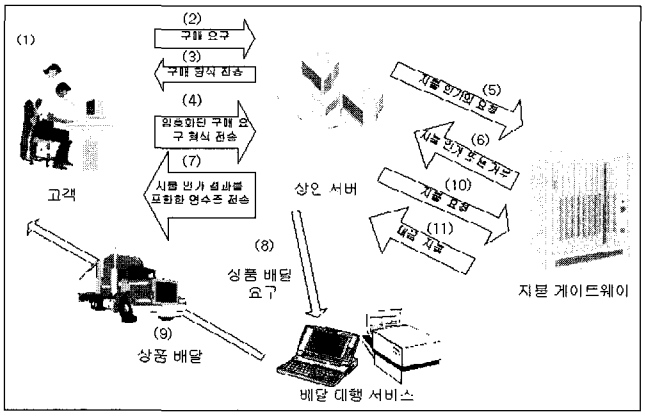


그림 5 SET 쇼핑 시나리오

3.2 SET의 쇼핑 시나리오

SET은 실제 세계의 신용카드를 이용한 우편 주문 및 전화 주문(MOTO:Mail order, telephone order)와 유사한 쇼핑 시나리오를 가지고 있으며 이와 같이 기존 쇼핑 환경과 유사하다는 점이 다른 전자 지불 시스템에 비해 더욱 일반 고객에게 친숙하게 느껴지게 한다.

그림 5는 SET이 모델링한 쇼핑 시나리오를 도시한 것으로 그 흐름은 다음과 같다.

(1) 고객이 상인의 웹 홈페이지에서 구매할 상품을 검색하고 선택한다.

(2) 선택된 상품에 대한 구매 요구가 상인 서버로 전송된다.

(3) 상인 서버는 접수된 구매 요구에서 고객이 선택한 물품에 대한 가격, 선적 요금등을 포함한 구매 형식을 고객에게 전송한다.

(4) 고객은 상인으로부터 받은 구매 요구 형식을 확인하고 지불에 사용할 신용카드의 정보와 함께 암호화하여 최종 구매 요구를 상인 서버로 전송한다.

(5) 상인 서버는 고객이 전송한 최종 구매 요구에 포함되어 있는 지불 정보를 지불 게이트웨이로 전송하여 지불 인가를 요청한다.

(6) 지불 게이트웨이는 상인으로부터 전송된 지불 정보를 은행망과 연동하여 지불 인가(authorization)를 요구하고 그 결과를 상인 서버로 전송한다.

(7) 상인서버는 지불 인가 결과에 따라 거래가 성립되었다면 지불 인가 정보를 포함한 전자 영수증에 해당하는 구매 확인서를 전송한다.

(8) 상인 서버는 성립된 거래에 대한 서비스를 수행하거나 배달 대행 서비스에 상품 배달을 의뢰한다.

(9) 접수된 상품 배달 요구에 따라 해당 고객에게 상품이 배달된다.

(10) 상인서버는 지불인가와 동시에 또는 일괄처리에 의해 정기적으로 인가 받은 지불에 대한 결재 요구를 지불 게이트웨이로 전송한다.

(11) 지불 게이트웨이는 상인 서버로부터 전송된 결재 요구를 금융망과 연동하여 수행한다.

3.3 SET 프로토콜의 범위와 구성

SET 프로토콜이 정의하는 영역은 전송되는 메시지에 대한 암호화 알고리즘의 적용 방법과 인증에 사용되는 메시지와 그 형식, 구매에 사용되는 메시지와 그 형식, 인가에 사용되는 메시지와 그 형식, 대금 결재에 사용되는 메시지와 그 형식 그리고 구성 요소들간에 주고받는 메시지등이다.

SET에서는 상품 검색이나 상품 배달, 상품 정보의 제공에 사용되는 메시지, 고객 및 상인의 신용도 관리나 상인에 의해 구성되는 웹 홈페이지의 구성과 신용카드 이외의 수단 및 고객, 상인, 지불 게이트웨이 시스템 자체에서의 방화벽등에 의한 시스템적 보안에 대해서는 정의하지 않았다.

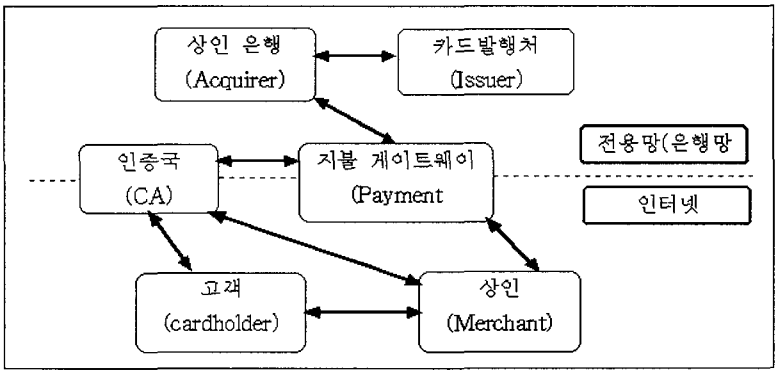


그림 6 SET의 기본 구조

SET은 OSI layer의 응용 계층에서 운영되는 프로토콜로 크게 고객(Cardholer), 상인(Merchant), 상인 은행(Acquirer), 카드 발행처(Issuer :은행 또는 카드회사), 인증국(CA)지불 게이트웨이(Payment gateway)로 구성된다. 그림 6은 SET을 기반으로한 전자 지불 시스템이 인터넷 상에 구현되었을 때의 구조를 보인 것으로 그림에서 화살표는 정보의 흐름을 나타낸 것이다.

고객은 카드 발행사로부터 발급받은 신용카드를 소지하고 컴퓨터를 이용하여 인터넷에 있는 상인의 홈페이지에서 상품을 선택하고 구매하는 당사자를 의미한다.

상인은 인터넷 상에 홈페이지를 개설하고 상품을 판매하거나 서비스를 제공하는 역할을 하며 신용카드를 취급하기 위해 은행과 관계를 맺어야 한다.

지불 게이트웨이는 상인으로부터 전송된 지불 정보를 은행망 쪽에 있는 상인 은행으로 전송하여 처리하는 일종의 대리인 역할을 한다.

고객, 상인, 지불 게이트웨이은 SET을 이용한 거래를 하기 위해 인증국에 등록하고 인증서를 발부받는다. 서로 메시지를 주고 받는 당사자들은 상대방에게 보낼 메시지를 암호화하는데 공개키가 실제로 상대방의 공개키가 확실한지 확인할 방법을 필요로 한다. 인증국은 공개키의 안전한 배포를 위해 믿을수 있는 기관에 설치되며 등록자들의 공개키가 들어있는 인증서를 전자 서명하여 인증한다.

카드 발행처와 상인 은행은 지불 게이트웨이로부터 전송된 신용카드 지불 정보를 기존의 신용카드 거래에서 수행되는 방식과 동일한 방법으로 처리하고 그 결과를 지불 게이트웨이로 전송한다.

4. SET 기반의 전자 지불 시스템

4.1 SET의 메시지 구성

SET의 메시지는 크게 인증서 관리를 위한 메시지와 지불 처리를 위한 메시지로 나눌 수 있다.[13]

인증서 관리를 위한 메시지는 CA와 고객간, CA와 상인간, CA와 지불 게이트웨이간의 등록 및 인증서 관리를 위한 메시지를 정의한 것이며 지불 처리 메시지는 고객과 상인간, 상인과 지불 게이트웨이간의 지불 처리를 위한 메시지를 정의한 것이다. 표 2는 SET에서 정의한 인증서 관리 메시지를 관련 구성 요소와 함

표 2 SET의 인증서 관리 메시지

분류	메세지 종류	관련 구성 요소
인증서 관리 메세지	• Cardholder 인증서 초기화 메시지 (CardCInitReq/ CardCInitRes)	Cardholder, CA
	• Merchant의 인증서 초기화 메시지 (Me-AqCInitReq / Me-AqCInitRes)	Merchant, CA Payment Gateway
	• Cardholder 등록 Form 메시지 (RegFormReq / RegFormRes)	Cardholder, CA
	• 인증서 요구 및 응답 메시지 (CertReq / CertRes)	Cardholder, Merchant, CA, Payment Gateway
	• 인증서 질의 메시지 (CertInqReq / CertInqRes)	Cardholder, Merchant, CA, Payment Gateway

표 2 SET의 인증서 관리 메시지

분류	메세지 종류	관련 구성 요소
지불 처리 메세지	• 지불 초기화 메시지 (PInitReq / PInitRes)	Cardholder, Merchant
	• 구매 요구 및 응답 메시지 (PReq / PRes)	Cardholder, Merchant
	• 질의 메시지 (InqReq / InqRes)	Cardholder, Merchant
	• 인가(Authorization) 요구 및 응답 메시지 (AuthReq / AuthRes)	Merchant, Payment Gateway
	• 대금 이체 요구 및 응답 메세지 (CapReq / CapRes)	Merchant, Payment Gateway
	• 인가 취소 메시지 (AuthRevReq / AuthRevRes)	Merchant, Payment Gateway
	• 대금 이체 요구 취소 메시지 (CapRevReq / CapRevRes)	Merchant, Payment Gateway
	• Credit 메세지(고객에게 환불하는 메세지) (CredReq / CredRes)	Merchant, Payment Gateway
	• Credit 취소 메세지 (CredRevReq / CredRevRes)	Merchant, Payment Gateway
	• 인증서 fetch 메세지 (P/G에서 인증서 획득) (PCertReq / PCertRes)	Merchant, Payment Gateway
	• 일괄처리 관리 메시지(Batch administration) (BatchAdminReq / BatchAdminRes)	Merchant, Payment Gateway

께 열거하였고 표 3에서는 SET의 지불 처리에 사용되는 주요 지불 시스템 메시지를 관련 구성 요소와 함께 기술하였다.

표 2의 인증서 관리 메시지중에서 인증서 요구 및 응답 메시지는 SET 지불 시스템의 구현시 반드시 구현되어야 하는 메시지이며 다른 메시지들은 구현하는 것을 추천하고 있으며 특히 CA의 경우에는 인증서 관리 메시지 모두를 수용할 수 있는 시스템으로 개발되는 것이 바람직하다.

SET 지불 시스템 메시지는 지불 초기화 메시지와 구매 요구 및 응답 메시지, 지불 인가를 받기 위한 인가 요구 및 응답 메시지, 그리고 인가받은 지불에 대한 대금 결재를 받는 대금 이체(capture) 요구 및 응답 메시지를 주요 지불 메시지로 하며 이외에 인가 및 대금 이체 요구 취소 메시지와 현재 진행 중인 지불 처리의 상태를 문의하는 질의 메시지, 고객의 환불 요구를 처리하기 위한 Credit 및 Credit 취소 메시지, 지불 게이트웨이의 인증

서를 지불 게이트웨이로 부터 받아오기 위한 인증서 fetch 메시지, 대금 이체의 일괄 처리를 위한 일괄 처리 관리 메시지등의 보조 지불 처리 메시지로 구성된다.

4.2 SET기반 전자 지불 시스템의 구성

SET을 기반으로 하는 전자 지불 처리 시스템은 cardholder로 표현되는 고객 소프트웨어(Cardholder software)와 Merchant로 표현되는 상인 서버 시스템, 신용카드 발행처(Issuer)와 상인 은행(Acquirer)와 연동하기 위한 지불 게이트웨이, 그리고 각 구성 요소들의 인증서를 발부해주는 인증 서버 시스템(CA)으로 구성된다.

(1) 고객 소프트웨어

고객 소프트웨어는 SET 프로토콜을 처리하기 위한 일종의 전자 지갑 소프트웨어로 웹 브라우저의 helper 프로그램으로 존재하며 지불 처리시 상인 서버에서 전송되는 구동 메시지에 의해 시작되는 것이 일반적이다. 고객 소프트웨어는 고객의 구매 및 지불 정보의 보호, 인증서 및 개인키 관리, 거래 내역의 관리, 상인 서버와 연동한 SET 전자 지불 처리를 주요 기능으로 한다.

(2) 상인 서버

상인 서버는 전자 상점 소프트웨어와 공존하거나 독립된 시스템으로 존재할 수 있으며 고객의 구매 요구 및 지불 명령을 처리한다. 주요 기능은 상인의 공개키 및 개인키를 관리, 거래 정보의 보호 및 거래 내역 관리, 고객의 주문 처리, 지불 게이트웨이에 대한 인가 요구 및 대금 이체 요구등이다.

(3) 지불 게이트웨이

SET 지불 메시지를 은행망과 연동하여 처리하기 위한 일종의 지불 대행 시스템으로 은행 자체에 존재하거나 믿을 수 있는 제 3 기관에서 운영될 수 있다. 지불 게이트웨이는 상인으로부터의 인가 메시지와 대금 이체 메시지를 은행망으로 전송하여 처리하고 그외 거래 사고의 방지를 위한 거래내역 관리, 신용도에 따른 인증 서버의 인증서 취소 리스트와의 연동, 상인 서버와의 연동등을 주요 기능으로 한다.

(4) 인증 서버 시스템

인증국에서 운영되는 인증 서버 시스템은 SET 거래에 참가하는 구성 요소들에 대한 등록과 인증서 발행을 주요 목적으로 하며 믿을 수 있는 기관에 의해 운영되는 방식이어야 한다. 인증서버의 주요 기능이라면 인증서의 발행 및 관리, 잘못된 인증서를 알리는 인증서 취소 리스트(CRL)의 운용, 은행망과 연동하여 고객 및 상인의 인증서 취소 또는 재발행, 다른 인증 서버와의 연동등이다.

5. SET에 사용된 보안 기술

SET에서 사용하는 주요 암호화 알고리즘은 DES로 대표되는 관용 암호화 알고리즘과 RSA로 대표되는 공개키 암호화 알고리즘이다. SET은 이들 암호화 알고리즘을 이용한 전자 서명과 전자 봉투, 이중 서명등을 사용하여 다양한 보안 요구를 만족시킨다.

5.1 전자서명(Digital Signature)

보통 공개키 암호화 방식에서 개인키(private key)로 암호화 된 것은 이에 대응하는 유일한 공개키(public key)에 의해서만 해

독될 수 있다는 알고리즘의 수학적 특성은 부인 방지에 사용될 수 있다. 그림 7은 전자 서명의 기본적인 흐름을 나타낸 것이다. 그림에서 M은 메시지, H는 해쉬 알고리즘을 나타내고 ER은 암호화를 DR을 해독을 나타낸다. Kpr과 Kpu는 각각 개인키와 공개키를 의미한다. SIGN은 메시지로부터 생성된 해쉬값을 개인키를 사용하여 암호화한 전자 서명 값을 의미한다. 전자 서명의 확인은 그림에서 보인 바와 같이 메시지와 함께 전송된 전자 서명 값을 공개키로 해독하고 그 결과값을 전송된 메시지의 해쉬값과 비교하여 수행하는데 그 결과 값이 동일하면 전송된 메시지의 무결성이 증명됨과 함께 전자 서명이 확인된 것이며 다르면 전송된 메시지가 변조된 것으로 전자 서명의 확인이 실패한 것이다.

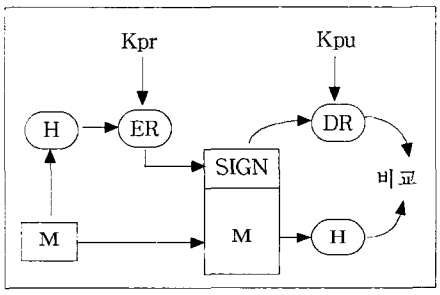


그림 7 전자 서명

5.2 전자 봉투(Digital envelope)

전자 서명의 문제점은 전송되는 메시지의 무결성은 제공하나 다른 사람에 의한 열람을 방지하는 기밀성을 제공해 주지 못한다. 전자 봉투는 이를 해결하기 위한 방법으로 제시된 것으로 전자 서명된 메시지를 관용 암호화 방식으로 암호화하고 여기에 사용된 비밀키를 다시 수신자의 공개키를 가지고 암호화하여 함께 전송하는 방식으로 메시지의 기밀성과 함께 무결성을 제공하는 방법이다.

그림 8은 전자 봉투 알고리즘을 간략히 나타낸 것으로 그림에서 SM은 서명된 메시지이며 Ks는 관용 암호화 방식에 사용되는 비밀키이며 Kpu는 공개키, Kpr은 개인키이다. ER과 DR은 각각 공개키를 사용하는 암호화와 해독을 나타내며 E와 D는 비밀키를 사용하는 암호화와 해독을 나타낸다.

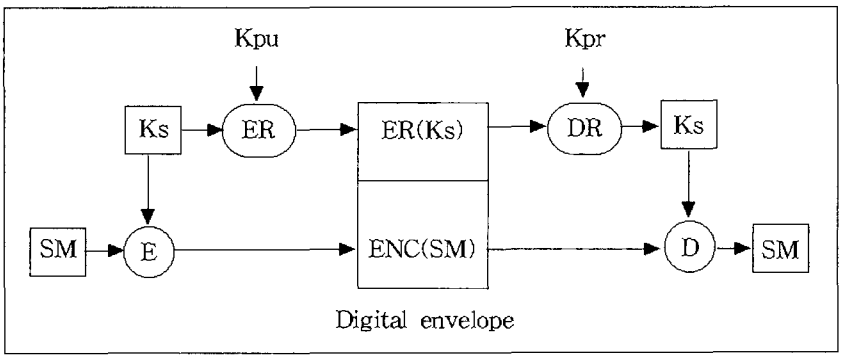


그림 8 전자 봉투

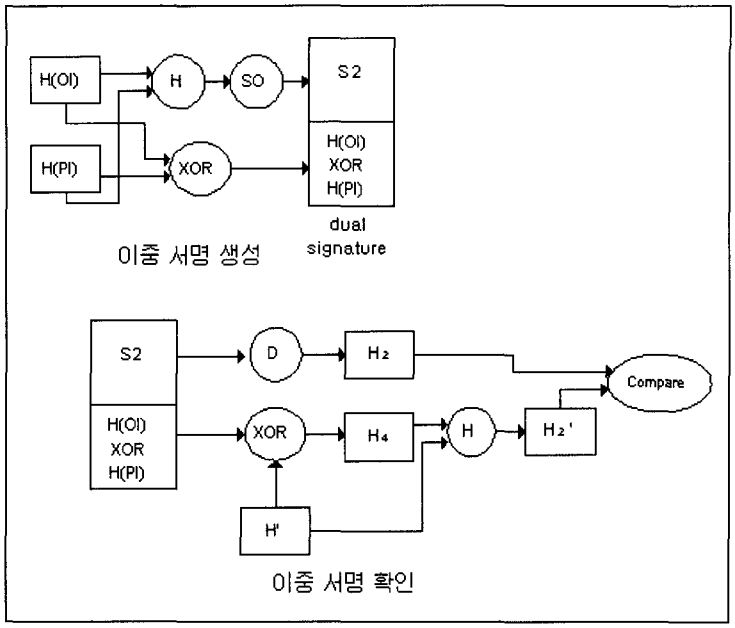


그림 9 이중서명 메케니즘

5.3 이중 서명(Dual Signature)

이중 서명은 상인에 대해서는 지불 정보의 투명성을 은행에 대해서는 구매 정보의 투명성을 제공하기 위한 것으로 서로 다른 공개키로 암호화된 지불 정보와 구매 정보를 연결하여 지불 정보의 실제 내용을 모르더라도 지불 정보의 무결성을 검사할 수 있는 방법을 제공한다. 그림 9에는 이중서명의 수행 및 확인 메커니즘을 나타내었으며 이를 사용하는 각 구성 요소에서의 자세한 동작은 다음과 같다.

(1) 이중 서명 방법

$H_2 = H(\{H(\mathrm{OI}), H(\mathrm{PI})\})$ (식 1)

$S_2 = SO_c(H_2)$ (식 2)

$SD_2(\mathrm{OI}, \mathrm{PI}) = \{S_2, (\mathrm{H(OI)\ XOR}\ H(\mathrm{PI}))\}$ (식 3)

(식 1)에서 OI와 PI의 해쉬를 연결하여 새로운 해쉬값 H_2를 생성하고 이것은 (식 2)에서와 같이 연산자 SO_c로 전자 서명하여 S_2를 얻는다. (식 3)에서 S_2는 다시 OI의 해쉬값 H(OI)와 PI의 해쉬값 H(PI)의 XOR 연산된 값과 함께 이중 서명 SD_2를 구성한다.

(2) 상인의 이중 서명 확인 방법

$H_3 = H(\mathrm{OI})$ (식 4)

$H_4 = H(\mathrm{OI})\ \mathrm{XOR}\ (H(\mathrm{OI})\ \mathrm{XOR}\ H(\mathrm{PI}))$ (식 5)

$H_2' = H(\{H_3, H_4\})$ (식 6)

$H_2 = D_c(S_2)$ (식 7)

상인은 자신의 개인키로 구매 정보를 해독하여 OI를 얻고 이에 대한 해쉬값 H_3를 (식 4)와 같이 얻는다. PI의 무결성을 검사할 해쉬값은 PI를 해독할 키를 가지고 있지 않은 상인으

로서는 PI로부터 직접 얻을 수 없다. 따라서 SD_2로 전송된 정보를 (식 5)와 같은 방법으로 직접 H_4=H(PI)를 얻을 수 있다. H4는 (식 4)에서 얻어진 H_3와 함께 (식 6)과 같이 H_2'을 생성한다. H_2'은 S_2를 (식 7)과 같이 개인키 해독 알고리즘인 D_c를 통해 얻어진 H_2와 비교하여 전송된 지불 정보와 구매 정보의 무결성을 확인하는데 사용된다.

(3) 지불게이트웨이의 이중 서명 확인 방법

$$H_5 = H(\mathrm{PI}) \quad \text{(식 8)}$$

$$H_6 = H(\mathrm{PI}) \ \mathrm{XOR}\ (H(\mathrm{OI}) \ \mathrm{XOR}\ H(\mathrm{PI})) \quad \text{(식 9)}$$

$$H_2'' = H(\{H_5, H_6\}) \quad \text{(식 10)}$$

상인으로부터 전송된 지불 정보가 해당 구매 정보와 관련된 유효한 지불 정보인지 확인하기 위해 지불 게이트웨이는 자신의 개인키로 상인으로부터 전송된 지불 정보를 해독하여 PI를 얻고 이에 대한 해쉬값 H_5를 (식 8)과 같이 얻는다. OI의 해쉬값 H_6는 (식 9)와 같이 SD_2로부터 얻은 H(OI)와 H(PI)의 XOR 값을 (식 9)와 같이 H(PI)와 XOR 연산하여 H_6=H(OI)를 얻는다. H_6는 (식 8)에서 얻어진 H_5와 함께 연결되어 (식 10)과 같이 이중 해쉬값인 H_2''을 생성한다. H_2''은 (식 7)을 통해 얻어진 H_2와 비교하여 지불 정보에 대한 해당 구매 정보가 유효한지 판단하는데 사용된다.

6. 결 론

인터넷 상에서의 진정한 전자 상거래를 구현하기 위한 필수 조건의 하나인 전자 지불 처리 기술은 전자 현금, 전자 수표, 신용카드 기반의 전자 지불 기술등으로 연구가 진행되어 왔으며 최근 개발되어 주목받고 있는 SET은 신용카드 시장의 80% 이상을 장악하고 있는 VISA와 MasterCard에 의해 표준으로 채택되었다는 점에서 가장 많이 사용될 가능성을 지니고 있다. 특히 SET은 전자 서명, 전자 봉투, 이중 서명등의 보안 알고리즘을 통해 신용카드 번호와 같은 지불 정보에 높은 보안성을 제공하며 상인에 대한 지불 정보의 투명성과 은행에 대한 구매 정보의 투명성을 보장하여 다른 지불 시스템에 비해 더 높은 만족도를 지니고 있다.

SET을 지원하는 전자 지불 시스템은 현재 미국, 일본등지에서 개발되고 있으며 우리나라도 예외는 아니다. 이러한 시점에서 볼 때 SET을 지원하는 전자 지불 시스템을 통해 안전하게 컴퓨터를 통해 인터넷 쇼핑을 하는 날이 곧 다가올 것으로 예상된다.

참고문헌

[1] SSL, http://home.netscape.com/newsref/std/ SSL.html

[2] Secure HTTP Description, http://www.eit.com/projects/s-http/index.html

[3] E-cash, http://www.digicash.com/ecash/ecash-home.html

[4] Mondex, http://www.mondex.com/mondex/home.html

[5] FV, http://www.fv.com/

[6] iKP, http://www.zurich.ibm.com:80/Technology/Security/extern/ecommerce/iKP.html

[7] NetCheque, http://nii-server.isi.edu/info/NetCheque

[8] SFNB, http://www.sfnb.com/

[9] Phillip M. Hallam-Baker, Electronic Payment Schemes, http://www.w3.org/Payments/roadmap.html

[10] D. Chaum, Blind Signatures for Untraceable Payments, Advances in Cryptology -Crypto82, Plenum Press, 1983, pp.199-203

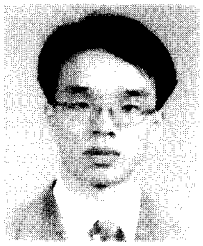
[11] J.G.Stenier, B.C.Neuman, and J.I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," in Proceedings of the USENIX UNIX Security Symposium, USENIX Association, Berkeley, CA, August 1988

[12] S.M. Bellovin, and M. Merritt, "Limitations of the Kerberos Authentication System," ACM Computer Communication Review, Vol. 20, 1990, pp.119 - 132.

[13] SET spec v1.0 , http://www.visa.com/cgi-bin/vee/nt/ecomm/set/downloads.html

[14] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc.

□ 著者紹介



송 병 열

1995년 전북대학교 전자공학과 졸업(학사)
1997년 전북대학교 전자공학과 졸업(석사)
1997년 ~ 현재 시스템공학연구소 연구원

※ 주관심분야: 분산처리, 네트워크 보안, 전자 상거래, 인공지능

조 현 규

1988년 한국외국어대학교 독일어학과 졸업(학사)
1990년 고려대학교 경영정보학(MIS) (석사)
1997년 한남대학교 경영정보학(MIS)전공 (박사)
1988년-1990년 현대해상 정보시스템부
1990년- 현재 시스템공학연구소 선임연구원

※ 관심분야: 동적 스케쥴링 시스템, shop floor control system, 전자 거래(EC) 관련 요소기술

송 유 진(회원)

1982년 한국항공대학교 졸업(학사)
1987년 경북대학교 대학원 졸업(석사)
1995년 일본 Tokyo Institute of Technology 졸업(박사)
1983년 - 1986년 공군 기술장교
1986년 - 1988년 금성정보통신
1988년 - 1996년 한국전자통신연구원
1996년 - 현재 동국대학교 정보산업학과

※ 관심분야 : 암호 이론, 부호 이론, CALS/EC 보안 응용, 전자 화폐

이 경 호

1987년 고려대학교 산업공학과 졸업(학사)
1990년 고려대학교 산업공학과 석사
1990년-현재 시스템공학연구소 선임연구원

※ 관심분야: Web서버기술, 전자거래보안기술, 전자화폐

함 호 상

1977년 고려대학교 산업공학과 졸업 (학사)
1982년 고려대학교 산업공학과 졸업 (석사)
1995년 고려대학교 산업공학과 졸업 (박사)
1983년 - 현재 시스템공학연구소 전자거래연구실장, 책임연구원

※ 관심분야: 객체지향 실시간 시스템, 전자거래 플랫폼 구축분야, 전자 거래 관련 기술 분야