전자지불시스템에서 구매자인증을 위한 ISP / 3D-Secure 프로토콜에 대한 연구

백 은 정
㈜ 데이콤
xelern@chol.com

A study of ISP / 3D Secure Protocol for buyer authentication of the Electronic Payment System

Eunjung Baek
Dacom Corporation

요 약

인터넷의 발달로 점차 활성화 되고 있는 전자상거래는 기존 시스템의 결제 정보 도용에 따른 문제점을 개선한 새로운 전자지불 시스템의 필요성이 대두되었고 국민/BC카드사의 인터넷 안전결제(ISP)서비스, 비자 안심클릭 서비스를 전면 시행하게 되었다. 사용자 본인인증 강화를 위한 인증방안과 서비스모델을 분석하고 개선방향을 제시한다.

1. 서 론

인터넷의 발전에 따라 전자상거래가 활성화되면서 인터넷 쇼핑몰을 통해서 거래되는 거래규모도 급격히 증가되었고 그에 따라 신용카드 정보 도용에 따른 제 3자의 부정거래 발생이나 카드 정보 유출, 사용 부인등 구매자들의 피해도 커지는 상황이다.

인터넷 쇼핑몰을 중심으로 한 전자상거래에서는 결제수단의 70%이상을 신용카드로 결제하고 있는 상황이다. 현재 널리 사용되고 있는 SSL 에 기반한 신용카드 전자결제시스템은 전송되는 정보의 안정성은 보장하나, 결제시 사용자가 입력한 신용카드번호, 신용카드 비밀번호, 유효기간등의 개인 비밀정보의 유출로 인해 부정거래가 발생 할 수있다. 전자상거래 상의 도용문제가 사회적인 문제로 대두되면서 정부와 신용카드사 등 결제기관에서 소비자 보호 대책의 제도화를 추진하였고 안정적인 전자상거래를 위하여 전면적인 전자결제 시스템의 개선에 대한 필요성이 높아졌다.

이에 따라 국민/BC카드 회원을 대상으로는 인터넷 안전결제(ISP)서비스를, LG/삼성/외환 등 국내 비자/마스터카드 회원대상으로는 안심클릭(3D-Secure)서비스를 2004년부터 전면 시행하였다. 인터넷 안전결제서비스, 비자 안심클릭서비스를 간단히 표현하면 SSL방식의 신용카드 결제 프로토콜에 카드 소유자 본인확인기능을 부여한 사용자 인증 프로토콜이라고 할 수 있다. 기술적인 사양은 차이가 있지만, 카드 소유자가 사전에 카드 발급사에 사용자명과 비밀번호를 등록하고 온라인 전자결제시에 카드 발급사가 이것을 확인하는 방법으로 구현이 되었다.

본 논문에서는 신용카드 결제시스템에서의 구매자의 본인인증을 하기 위해 현 지불대행사(Payment Gateway)에서 적용하고 있는 서비스 모델에 대해 분석하고 향후 발전방향에 대해서 제시한다.

2. 신용카드 기반의 전자결제 시스템

전자지불시스템이란, 인터넷을 통한 상품 구입 혹은 서비스의 이용 후 해당 대금을 신용카드, 계좌이체, 핸드폰 결제 및 기타 결제수단으로 전자결제 할 수 있도록 하는 시스템을 말한다.

주요 결제 수단으로 사용하고 있는 신용카드의 서비스 제공방식을 살펴보자. 신용카드는 가맹점이 고객의 카드 정보를 네트워크를 통해서 VAN사에 전송하면 카드 발급사로 전달되고 발급사가 온라인 상에서 이를 승인하는 형태로 이용된다. 오프라인 가맹점에서는 카드 소유자가 카드를 제시하고 전표에 서명하는 방식이지만 비대면 거래인 온라인 거래에 있어서는 카드 소유자의 본인 확인과 거래 데이터의 보안이 필수적이다. 데이터의 보안을 위해 주로 사용하고 있는 SSL 기반 방식은 웹브라우저와 웹서버와의 상호 인증 및 데이터 암호화 만을 제공하며 구매자 본인에 대한 인증을 제공하지는 않는다.

안전한 신용카드 사용을 보장하기 위해서 비자와 마스터카드는 새로운 인증 프로토콜을 발표하였다. 인터넷 쇼핑몰에서 구매시 카드사가 직접 카드 소지자의 신원을 확인할 수 있는 기능을 제공함으로써 인터넷상에서 발생할 수 있는 카드의 부정사용 가능성을 최소화하고 카드 결제관련 주요 정보(비밀번호, 주민등록번호)등을 카드사 이외의 타기관(쇼핑몰 또는 지불대행사)은 저장할 수 없도록 고안된 보안 장치이다.

안전한 신용카드 기반의 전자결제 시스템의 대한 요구사항을 만족시키고 구매자 본인인증강화를 위해 국내에서 시행하는 두가지 방식에 대해 알아본다

3. 인터넷 안전결제 서비스(ISP)

ISP(Internet Secure Payment)서비스는 모든 거래에 대해서 암호화 통신을 시행, 거래 당사자 확인을 위한 전자인증서의 사용, 전자 결제 지불대행사 (PG)에서의 금융거래정보 저장 및 해독 금지, 금융기관과 PG업체의 접속은 전용회선을 사용하는 등 전자서명법 및 전자금융안전 대책 기준 권고사항을 충족하고 있으며 인터넷 안전결제(ISP)인증서 및 전자서명을 통해 보안요건을 충족하고 있다. 아래 표는 기존의 전자결제 방식과 ISP방식의 입력정보를 비교한 것이다 [1]

<표1> 신용카드 전자결제 입력 방식 비교

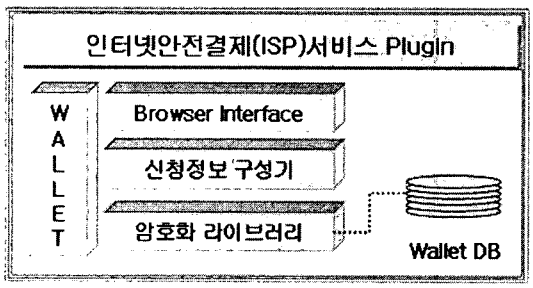
기존 Key In방식	ISP 서비스
신용카드번호	비밀번호(영숫자 6자리)
신용카드 유효기간	또는 공인인증서암호
카드 비밀번호(앞2자리)	
주민등록번호(뒤 7자리)	

신용카드 인터넷 결제시 카드정보를 전혀 입력하지 않음으로 인해 카드 정보에 대한 노출이 방지되었다.

3.1 핵심기술

ISP Plug-in은 개인정보 및 거래정보 관리, 제휴PG 및 ISP VAN사와 서버 연동 위한 Wallet 과 신용카드종류별 신청정보를 보관한 신청정보 구성기, RSA1024, SEED-CBC128, Triple-DES, Hash알고리즘 등이 포함된 암호화 라이브러리를 탑재하고 있다.

X.509 v3에 준한 PKI기반의 인증서 방식을 채택하여 전자서명 기능을 부여하였다. RSA 1024bit, SEED 128bit, SHA-1 등 국내외 표준 알고리즘을 적용하고 고객단에 설치된 Plug-in에서 암호화한 데이터로 송,수신 보안성이 높아졌다 [1]



<그림1> 인터넷안전결제(ISP) Plug-in 구성

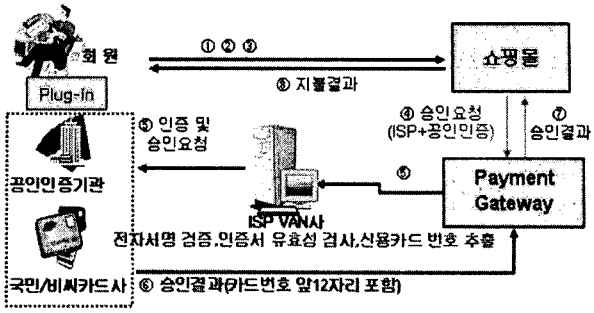
3.2 ISP 발급

ISP결제를 이용하기 위해서는 사전에 ISP 발급을 받아야만 한다. 카드사 사이트나 쇼핑몰의 결제화면에서 인터넷안전결제(ISP) 서비스를 신청한다.

카드번호,email, ISP비밀번호 등을 입력하고 발급요청을 하면 ISP발급대행기관에서 신청정보를 복호화한 후 해당 카드사로 심사요청을 하고 심사완료가 되면 사용자 PC에 사용자인증서를 설치하게 된다

3.3 ISP 결제

인터넷 안전결제를 적용했을 경우의 전자결제 Flow이다.



<그림2> 인터넷안전결제(ISP) 결제 흐름도 [2]

(1) 구매자가 인터넷쇼핑몰에서 상품을 구매 후 신용카드 결제를 할 때 KB/BC카드인 경우에 ISP 결제 화면 플러그인이 뜬다. 사전에 등록된 카드 리스트가 나타나며 ISP비밀번호를 입력하고 결제를 요청한다.

(2)10만원 이상인 경우에는 공인인증서 창이 뜨고 공인인증서 암호를 입력한다.

(3)ISP 결제 정보 및 전자서명을 암호화 하여 전송한다

(4)암호화된 ISP 정보와 공인인증정보를 PG를 통해서 ISP VAN사에 승인요청을 한다.

I(5)SP VAN사는 전자서명을 검증하고 인증서에 대한 유효성 검사, 신용카드 번호를 추출해 낸 후 해당 카드사에 승인요청을 한다.

(6)카드사가 VAN사로 승인결과를 전송한다

(7)PG는 쇼핑몰에 승인결과를 보내주고 카드 거래내역 조회 서비스를 위한 카드번호 앞자리 12자리를 보내준다

(8) 쇼핑몰은 구매자에게 지불결과를 보여준다

4. 비자 안심클릭서비스(3-D Secure)

비자의 3D-Secure는 온라인 거래시 카드사가 직접 카드 사용자를 인증하는 국제표준 프로토콜이다. 안심클릭 서비스는 기본적으로 3-D Domain 개념에 기반하고 있다 신용카드 거래 framework를 Issuer Domain(발급사영역), Acquirer Domain(매입사 영역), Interoperability Domain (상호운용영역)으로 구분하고 각 참가자들의 권리/의무관계를 명확히 하는 모델이다.

발급사(Issuer)는 카드소지자의 등록 및 온라인 거래의 인증을 책임진다. 인터넷 거래시에 온라인 브랜드 가치성을 높이고 발급사의 대 고객 관계가 강화되고, 구매 당시에 인터넷 거래에 대해 인증을 하므로 인터넷 거래를 온라인POS 거래처럼 보안을 강화할 수 있다.

매입사(Acquirer)는 가맹점의 신뢰 및 계약 여부 인증, 거래기반 기술을 확인하는 절차적 책임을 진다. 기존의 업무기반이나 시스템에 영향 없이 적용이 가능하다.

상호 운용영역 (Interoperability Domain)에서는 두 영역간의 거래교환을 돕는 책임을 진다 [3]

4.1 서비스 요구사항

3-D Secure 서비스를 적용하기 위한 요구사항이다.[4]

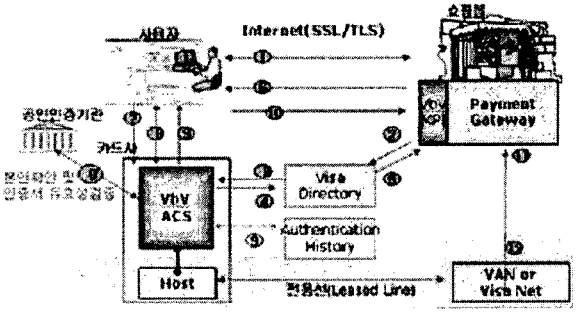
(1) 카드 소지자 사전 등록 (Enrollment)

3-D Secure 서비스를 이용하기 위해서는 카드 소지자는

사전에 발급사의 웹사이트에서 3-D Secure 비밀번호 또는 공인인증서를 개별적으로 등록해야 사용이 가능하다
(2) 구매 Flow 변경(Payer Authentication Processing)
카드 소지자가 인터넷 쇼핑몰에서 쇼핑한 후에 지불정보를 입력하면 MPI가 작동하여 사용자의 등록여부를 확인한다. 사전에 등록한 비밀번호로 인증 요청하면 발급사가 카드소지자 ' 본인임을 인증' 하고 가맹점은 카드 거래 승인을 위한 정보를 VAN으로 송부한다. 이때 CAVV가 적용된다. CAVV(Cardholder Authentication Verification Value)란 카드 회원의 인터넷 거래 관련 본인임을 증명하는 값으로 발급사 ACS에서 생성하여 카드소지자가 인증된 다음 가맹점의 지불승인 응답(PARes)에 포함하여야 하는 값이다.
(3) 온라인 가맹점은 MPI(Merchant Plug-in)을 결제 서버에 설치하여 3-D Secure사용을 가능하게 해야 한다.

4.2 3-D 적용 후 온라인 구매 Flow (국내)

비자의 본인 인증 서비스의 국내 서비스명이 "비자 안심클릭"이다. 모든 카드 브랜드 (Visa, MasterCard, Diners Club, American Express, 국내전용 등)가 국내 전자상거래에 지원 가능하도록 하며, 해외거래에서 국제 표준 규칙에 맞도록 재설계된 한국형 3-DS이다. 아래 그림은 3-D Secure기반의 공인인증서를 적용한 서비스 흐름도이다. [5]



<그림3> 비자 안심클릭 결제 흐름도
(1) 카드 사용자가 쇼핑몰에서 주문/배송정보를 입력하고, 결제정보(카드번호,유효기간)입력시 MPI 활성화된다
(2) 가맹점(자체 및 대행 PG)의 MPI가 3-D 인증이 가능한지 여부 확인을 위해 카드범위 체크 요청 메시지(VEReq)를 비자 D/S로 보낸다.
(3)비자 D/S는 카드범위와 Merchant의 참여 여부를 확인하고, 해당 카드사의 ACS로 VEReq 전송한다.
(4)카드사 ACS는 해당 카드번호가 3-D 인증 가능 여부를 체크하여 응답메시지(VERes)를 D/S로 보낸다.
(5)비자 D/S는 VERes를 해당 가맹점의 MPI로 전달한다
(6)가맹점 MPI는 VERes을 받아 들여 지불인증요청(PAReq)을 사용자의 쇼핑장치(지불 페이지 or Pop-up)를 통해서 카드사 ACS로 전송한다
(7)카드사 ACS는 PAReq을 받아 들여서,VEReq와 매칭 확인한다
(8)카드사 ACS는 사용자의 3D 암호, 공인인증서에 따라 적절한 화면으로 사용자 본인여부를 확인한다. 단, 공인인증서를 사용하는 경우에는 공인인증기관을 통해 본인 확인 수행.본인 확인 후 지불인증결과(PARes)와 전자서명(Signature) 메시지를 생성한다. 이때 CAAV 및 AAV를 생성한다
(9)카드사 ACS는 메시지를 재구성(PaRes)하여 쇼핑장치를 통해서 가맹점 MPI로 전송한다. 또한 비자의 AHS로 인증내역(PATransReq)을 보내고 응답을 받는다.
(10)가맹점 MPI는 PaRes를 받아 확인 한다.
(11)가맹점 MPI는 자체 또는 별도의 모듈을 통해 전자서명(Signature)을 검증한다.
(12)가맹점(자체 또는 대행 PG)은 VAN사을 통하여 카드사로 승인 요청을 한다.

5. 결론

인터넷상의 전자결제에 있어서 카드소지자와 결제자의 일치성, 거래의 유효성에 대하여 표준화된 인증방법으로 거래의 적법성을 인증할 수 있는 수단이 필요하다.
카드소지자의 본인인증을 카드사가 직접 수행 할 수 있는 인증방법으로 현재는 사전 등록된 비밀번호로 인증하거나 공인인증서로 인증처리를 한다. 고객과 카드발급사만 알 수 있는 전자거래용 별도의 비밀번호 시스템을 지원하지만 사용자 부주의에 의한 노출의 위험이 있다. 공인인증서는 인증서가 설치된 PC에서만 전자결제가 가능하다는 불편함이 있다. 인증수단으로 사용중인 비밀번호와 공인인증서 외에 다양한 인증수단에 대한 검토가 필요하고 IC카드, 전자지갑, 지문인식등 생체 인식기능등 이동성과 안정성을 모두 만족시키는 다양한 인증수단이 발굴되어 편리한 전자거래가 가능해지도록 되어야 할 것 이다.
신용카드 결제방식에 있어서 현재는 ISP,안심클릭 2가지 방식으로 본인 인증을 제공하고 있다. 카드사가 전략적으로 시장을 주도하기 위한 방안으로 동일한 모델로 통합되지 못하는 상황이고 계좌이체서비스 역시 SDT방식의 공인인증, 인터넷 뱅킹시스템을 이용한 공인인증, 이중암호화 방식 등 각자의 상황에 따라 다양한 방식으로 서비스를 제공하고 있다. 신용카드/계좌이체의 인증시스템 모두 비슷한 개념위에 개발된 플랫폼으로 결제정보를 제 3기관에서 알지 못하도록 발급사에서 직접 사용자를 인증하는 방식에 주문정보와 지불정보가 분리되어 처리가능한 구조이다. 전자지불시스템의 안정성과 확장성을 위해서 한국형 표준의 확립과 각 결제기관이 연합하여 동일한 지불시스템의 구조를 가져 갈 수 있도록 협력하는 일이 중요하다고 본다.

6. 참고문헌

[1] KVP, "인터넷 안전결제(ISP)서비스 소개자료, 2003.
[2] KVP, "인터넷 안전결제(ISP)서비스 모델, 2003.
[3] VISA Publication, "3-D Secure: Introduction", Version 1.0.2, 70001-01, pp.7-11, 2002
[4] VISA Publication, "3-D Secure: System Overview", Version 1.0.2, 70015-01, pp.15-25, 2003
[5] ILK Publication, "신용카드 기반의 전자상거래" , pp. 10-16, 2003.