스마트카드를 이용한 보안성 높은 전자지불시스템 제안

-A Proposal of Secure Electronic Payment System Using Smartcard-

박필승 남길현
국방대학원 전자계산학과
khnam@kndu.ac.kr

요 약

전자상거래의 활성화를 위한 전자지불시스템은 보안성과 통용성의 양면을 만족해야한다. 현재 서비스중인 전자현금이나 전자화폐는 디지털정보가 직접 화폐가치를 지니고 있기 때문에 인터넷에서 분실시 복구가 불가능하다. 또한 전자수표나 가상은행을 이용한 계좌이체방식은 인터넷 통용성이 약하며, 신용카드를 이용한 전자지불시스템은 통용성은 양호하나 신용카드번호 노출의 위험이 있고 수수료 등 트랜잭션 비용이 소요되므로 소액지불에는 불리하다. 전자지불시스템의 활성화를 위해서는 신용카드와 같이 휴대 가능하고 실세계에서의 통용성이 우수한 시스템이어야 하며, 직접지불이 가능하고 소액지불도 가능한 체계이어야 한다. 본 논문에서 제안하는 새로운 지불시스템 "스마트-Pay"는 모든 사람들이 은행을 사용하고 있다는 점을 착안하여 은행계좌기반이면서 실세계 및 인터넷에서 직접지불이 가능하도록 설계한 것이다. 본 지불시스템의 안전도는 발행기관, 은행, 고객으로 이어지는 인증사슬에 의한 강력한 인증과 스마트카드에 의한 전자서명에 의존하며 기밀성, 무결성, 부인봉쇄를 제공하므로 안전하다고 평가된다.

1. 서 론

전자상거래를 활성화하기 위한 전자지불시스템에 대한연구는 전 세계적으로 활발하게 진행되고 있으며 전자현금, 전자화폐, 전자수표, 가상은행에 의한 계좌이체방식, 신용카드기반 전자지불시스템이 있다. 전자지불수단을 인터넷에서 안전하게 사용하기 위해서는 고도의 암호기법과 상호인증 등의 기술적방법과 전자상거래 법, 제도의 제정을 통하여 보안의 기본요건인 기밀성, 무결성, 부인봉쇄를 반드시 달성하여야한다. 또한 전자상거래에서 널리 사용되기 위하여 신용카드와 같이 휴대성을 부여하여 대중 속에 널리 통용될 수 있어야 한다. 그러나 기존의 신용카드를 이용한 결재시스템은 신용카드번호노출로 의도된 범죄에 대한 대응력이 약하며 수수료나 트랜잭션 비용 때문에 소액결재는 곤란한 측면이 있어, 현재는 기존의 신용카드와 같은 플라스틱 카드를 자체 메모리 및 연산능력이 우수한 스마트카드로 대체하여 보안성을 높이고 트랜잭션비용을 줄이려는 노력이 진행되고 있다.

본 논문은 전자상거래 및 전자지불수단의 보안요건과 보안기술을 알아보고 현재까지 개발된 각종 전자지불시스템의 작동 메커니즘과 장. 단점을 비교한 다음 그 단점을 해소할 대안으로 스마트카드를 이용하여 실세계와 인터넷에서 동시에 통용이 가능한 안전하고 편리한 새로운 전자지불시스템을 제안한다. 이를 위한 논문구성은 총 5장으로서 제2장은 전자상거래 보안 및 전자지불시스템의 보안고려사항, 안전한 전자지불시스템을 구축하기 위한 암호화방식 등의 보안기술을 고찰하고, 제3장은 기존의 전자지불시스템을 분류하고 기존 전자지불시스템의 구조 및 기능에 대하여 고찰하며 장. 단점을 비교한다. 제4장은 2, 3장을 토대로 기존 전자지불시스템의 단점을 보완한 새로운 전자지불시스템 "스마트-Pay"를 제안하고 평가 및 분석하며, 제5장은 결론 및 발전방향을 제시한다.

2. 전자지불시스템 보안

2.1 전자상거래와 보안위협

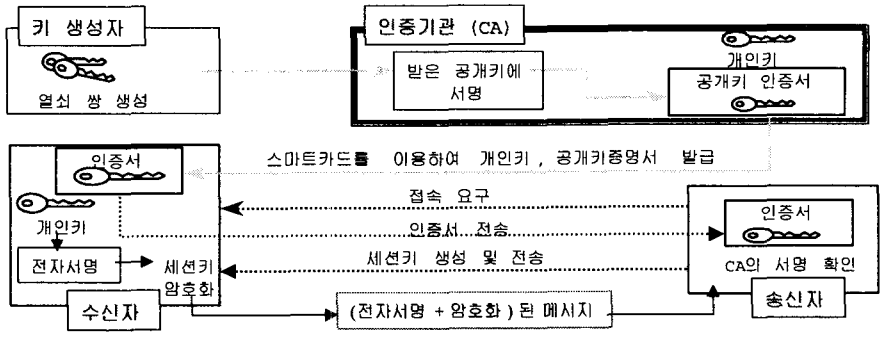
전자상거래의 거래과정 중에 일어날 수 있는 보안위협은 인터넷에서는 통신장애로 지불정보를 분실할 우려가 있으며, 거래당사자인 고객이나 상점도 불순한 의도를 가지고 있다면 거래부인, 지불정보의 재사용 등 전자상거래에 보안위협을 줄 수 있다. 특히 해커나 범죄자들의 침입이나 도청에 의한 지불정보나 데이터사취, 데이터위조, 개인정보수집, 고객의 신원 및 주소에 대한 사칭, 신용카드번호 대한 재사용, 극단적인 서비스방해 등은 전자상거래에 가장 큰 위협이 되고있다.

2.2 전자상거래 보안 고려사항

전자상거래를 고객들이 신뢰하며 사용하기 위해서는 전자지불시스템의 보안이 최우선적으로 보장되어야 한다. 전자상거래에 있어 기본적인 보안요구는 보안의 속성에 따라 다양 할 수 있지만 크게 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 3가지로 나누어 볼 수 있다. 전자지불시스템 보안 고려사항은 개인의 신상정보에 대한 개인 프라이버시보호, 전자현금 등과 같은 지불정보에 대한 이중사용과 같은 사기 및 위조 방지, 상호간의 거래에 대한 부인봉쇄, 분실이나 전송실패시 대응방안, 신뢰성 및 효율성 등이다.

2.3 전자지불시스템 보안기술

전자지불시스템의 보안성을 위하여 적용 할 메커니즘으로는 대표적으로 암호화방식이 있으며 그 외 스마트카드와 같은 위조방지장치를 적용하고 불법지불을 방지 할 수 있도록 지불정보에 대한 사용시간 및 사용한도를 제한하는 등의 기술적, 제도적인 제약을 가하는 방법이 있다.



<그림 2-1> 스마트카드를 이용한 키 분배 및 사용

암호화방식에서 키는 모든 정보보호 시스템의 가장 중요한 부분으로 암호 등을 사용하여 보호되어야한다. 관용암호시스템을 사용하더라도 문자 및 숫자를 혼합한 128bits이상의 키를 사용하는 것이 보통이므로 인증기관(CA)에서 키와 인증서를 <그림 2-1>과 같이 스마트카드와 같은 물리적 수단에 저장하여 분배하고, 스마트카드가 개인키 역할을 하여 스마트카드에 비밀번호를 입력하면 스마트카드 내에서 혹은 외부로 개인키가 인출되어 전자서명이나 암호화 등에 사용하는 방식이 키 분배 및 사용에 있어 효과적인 방법이다.

3. 전자지불시스템 구조 및 기능

3.1 전자지불시스템 분류

전자지불시스템은 <표 3-1>과 같이 분류 할 수 있다.

<표 3-1> 지불시스템의 분류

분류기준	설 명	지불모형 및 예
거래수단	거래매체와 수단에 의한 분류	ㅇ가치기반 : 전자현금, 전자화폐(Stored Value Card) ㅇ은행계좌기반 : 전자수표, 자금이체 ㅇ신용카드기반 : 신용카드
실제자금의 이체시점	거래시점과 지급시점의 관계	ㅇ선지불형(직접지불형): 전자화폐 ㅇ동시지불 : 자금이체, 직불카드 ㅇ후불형(지불지시형) : 신용카드, 전자수표
On-Line/ Off-Line	가용성 여부를 즉각확인/ 차후확인	ㅇOn-Line : 신용카드, 전자수표, 전자현금 등 ㅇOff-Line(현금처럼 사용) : 전자화폐

3.2 기존 전자지불시스템 고찰

인터넷에서 현재 서비스되고 있는 전자지불시스템으로 네트워크형 전자현금, 오프라인형 전자화폐, 전자수표 및 신용카드기반 지불시스템을 비교 연구한다.

1) E-cash

1995년 부터 미국의 마크트웨인 은행에서 서비스를 시작했으며 인터넷에서만 사용이 가능한 전자현금이다. 블라인드서명 형태로 화폐를 발행하여 완전 익명성과 불추적성을 달성하였으나 분할사용이 불가능하고 사용시에는 거래 도중 화폐발행서버로 지불정보가 되돌려져 이중사용여부를 확인받아야한다.

2) Mondex

1993년 부터 영국 내셔널 웨스트민스터 은행이 제공하기 시작한 IC카드를 이용한 오프라인 전자화폐시스템으로 개인간 이체가 가능하고 다국적 통화를 저장할 수 있으며 다양한 단말기를 개발하는 등 사용의 확산을 위하여 노력하고 있다. 가치저장카드(Stored Value Card)로서 오프라인 거래가 가능하며 위조 및 이중사용여부는 거래완료 후 발행은행으로 전송되면 확인된다.

3) FSTC의 E-Check

FSTC(Federal Services Technology Consortium)은 1993년 설립된 전자상거래를 위한 협회로 1995년 부터 Electronic Check이라는 전자수표 프로젝트를 진행중이다. E-Check는 발행은행의 개인키로 서명된 전자수표책을 PCMCIA카드에 보관하고 지불시에는 여기에 수령인정보 및 금액을 기록하여 수표발행인의 개인키로 전자서명한 형태로 전자수표를 제시하면 기존금융망을 통하여 결재가 이루어진다. 최종 자금이체시까지는 수표확인을 위한 시간이 소요된다.

4) SET

1996년 부터 비자와 마스터카드가 협력하여 인터넷에서 안전한 신용카드거래를 지원 할 수 있도록 공동 개발한 전자지불프로토콜이다. SET에 참여하는 개체는 고객, 상인서버, 지불게이트웨이, 인증국, 신용카드회사 및 전표매입회사이다. SET에서는 개인정보보호, 지불정보의 기밀성 및 무결성을 보장하기 위하여 개체 간 인증 및 암호화통신을 한다. 특히 전자봉투형식의 지불정보와 구매정보가 분리된 암호화와 이중서명으로 기밀성 및 무결성을 보장하고 있다. SET은 신용카드가 인터넷 상거래의 대부분을 차지하는 현실에서 보안성이 우수한 프로토콜로 사용이 점차 확산되고 있으나, 구현기술의 복잡성으로 상호운용성이 미비한 실정이다.

3.3 기존 전자지불시스템 비교분석

현재 인터넷에서 사용되는 전자지불시스템의 장. 단점을 비교하면 <표 3-2>와 같다.

<표 3-2> 각종 지불수단 비교

전자지불수단	장점	단점(제한점)
전자현금 전자화폐	ㅇ 익명성 보장 ㅇ 직접지불 (디지털신호가 직접 재화가치가 있음) ㅇ 실세계 통용성(전자화폐)	ㅇ 고액결재에 부적합 ㅇ 대규모 데이터베이스 소요 ㅇ 인터넷에서 분실시 대책미흡 ㅇ 오프라인 사용불가(전자현금)
전자수표	ㅇ 고액지불가능(대금은 지불처리까지 은행에 안전하게 보관) ㅇ 수표의 전자적 처리	ㅇ 익명성 미 보장 ㅇ 특수한 하드웨어 필요 ㅇ 수표 확인시간 필요 ㅇ 오프라인 사용 불가
신용카드기반 (SET)	ㅇ 실세계 통용성 ㅇ 국제적 통용성 ㅇ 신용카드번호 노출방지	ㅇ 익명성 미 보장 ㅇ 트랜잭션 비용(소액결재에 부적합) ㅇ 신용카드확인을 네트웍 구성필요 ㅇ 신용카드번호 노출시 재사용가능

제 4 장 스마트카드 기반의 전자지불시스템(스마트-Pay) 제안

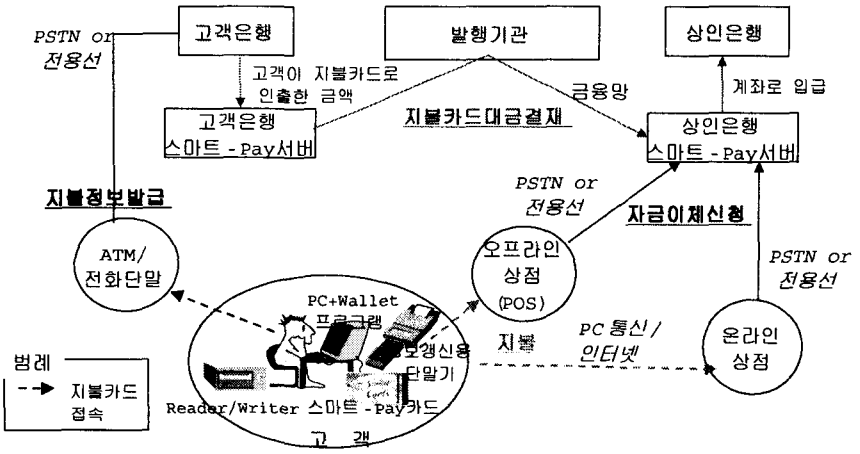
4.1 새로운 전자지불시스템(스마트-Pay)의 요구사항

지금까지 검토한 기존의 전자지불시스템의 단점을 해소하여 인터넷에서 사용시 안전하고 편리한 지불을 하기 위한 새로운 전자지불수단의 요구사항은 고객과 상인 간 제삼자의 개입 없는 직접지불성, 인터넷에서 지불정보 분실시 복구대책, 이중사용이나 카드번호 재사용공격 봉쇄, 실세계통용성이다. 본 논문에서는 위 요구조건을 만족시키는 새로운 전자지불시스템으로서 전자서명용 스마트카드를 "스마트-Pay카드"로 사용한 "스마트-Pay"를 제안한다.

4.2 스마트-Pay시스템의 운용개념

본 논문에서 제안하는 새로운 전자지불시스템 "스마트-Pay"는 유효기간 안에 스마트-Pay카드의 잔액한도 내에서 고객계좌에서 판매대금을 인출하여 상인계좌로 이체할 수 있도록 고객의 개인키로 전자서명된 수표형태의 지불지시서를 전송하여 지불을 완료하는 지불지시형으로 실세계 및 인터넷에서 고객과 상인 간 일대일 직접지불이 가능하다. 스마트-Pay시스템은 기존의 전자수표가 은행 및 개인이 동시에 이중서명 하던 것을 고객의 단일서명으로 수정하여 데이터분량을 최대한 축소하여 스마트카드에 적합하도록 설계하였으며 단말과의 통신은 스마트카드 인증절차를 응용하였고, 인터넷 지불 프로토콜은 SSL의 인증 및 전자봉투개념을 적용하였다.

새로운 전자스마트-Pay카드를 중심으로 연관된 관련개체는 고객, 상인(온라인, 오프라인 상점), 은행의 스마트-Pay서버, 발행기관으로 설정한다. 스마트-Pay시스템의 운용개념은 <그림 4-1>과 같다.



<그림 4-1> 스마트-Pay시스템 운용개념

스마트-Pay시스템을 표현하기 위한 기호체계는 다음과 같다.

<표 4-1> 정보표현을 위한 기호체계

ㅇ I, C, S, Bc, Bs : 발행기관, 고객, 상인, 고객은행 스마트-Pay서버, 상인은행 스마트-Pay서버
ㅇ IDc, IDs, IDtn, CIDc, CIDs : 고객, 상인, 단말의 ID, 고객카드, 상인카드의 카드 ID
ㅇ PK_I, PKc, PKs, (SK_I, SKc, SKs) : 발행기관, 고객, 상인의 공개키(개인키)
ㅇ Kss, K_{IB}, K_{BcC}, K_{BsS} : 세션키,발행기관-은행, 고객은행-고객, 상인은행-상인 간 공통키
ㅇ 키 K에 의한 메시지 M(암호문 X)에 대한 암호화 EK(M), 복호화 D(X) = DK(EK(M))
ㅇ Cert(I,Bc), Cert(Bc,C), Cert(I,Bs), Cert(Bs,S) : **I, Bc, I, Bs**에서 Bc, C, Bs, S를 인증한 인증서
ㅇ DBL(Bc,C), DBL(Bs,S) : 이중암호화된 은행 및 개인계좌정보 (ex) DBL(Bc,C)=(EK_{IB}(Bc), EK_{BcC}(C))
ㅇ Edate, Idate/Vdate : 인증서 유효일, Balance의 발급일/유효일
ㅇ Ms, Mc, Mtn : 상인, 고객이 발행한 지불정보, 단말의 지불정보발급 요청정보

은행에서 고객에게 스마트-Pay카드를 발행시에는 각종 암호키, 암호알고리즘, 인증서 및 데이터를 입력하여 발행하는데 그 내용은 <표 4-2>와 같다.

<표 4-2> 고객 지불카드의 보유정보

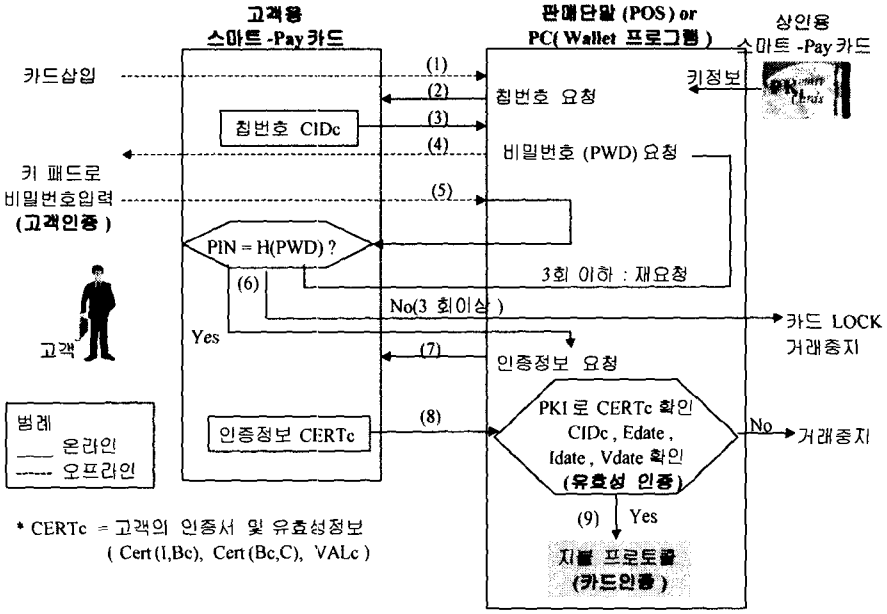
구분	정보표현	설명(사용용도)	접근방법
비밀영역	SKc PIN	고객의 비밀키 사용자 식별번호(Personal ID Number)=H(Password)	갱신불가/ 접근불가
접근통제	Balance TransNo	카드내부에 있는 잔액(Update는 은행과 접촉시만 가능) 서명시마다 1씩 올라가는 트랜잭션번호	비밀번호입력으로 읽기가능
공개영역	PK_I Cert(I, Bc) Cert(Bc,C) VALc	발행기관 공개키 발행기관에서 은행을 인증한 인증서 (DBL(Bc, C), IDc, CIDc, PKc, Edate)$_{SKBc}$ (IDc, Idate, Vdate)$_{SKBc}$: Balance 갱신시 고객은행의 비밀키로 전자서명한 유효성 정보 * CERTc=(Cert(I,Bc), Cert(Bc,C), VALc) : 인증정보	은행을 통하여 갱신/ 외부에서는 읽기만 가능
	CIDc IDc	칩 번호, 카드번호 은행이 고객에게 부여한 유일한 개인인식번호	갱신불가/ 읽기만 가능

4.3 스마트-Pay시스템의 각종 프로토콜

스마트-Pay시스템을 위한 프로토콜은 인증 프로토콜, 지불정보발급 프로토콜, 지불 프로토콜, 최종 지불정보처리로 구분 할 수 있다.

4.3.1 인증 프로토콜

스마트-Pay시스템에서 **카드와 오프라인 단말 간의 인증**은 <그림 4-2>와 같다. 카드인증(카드의 개인키 인증), 고객인증(PIN 인증), 유효성인증(카드 사용가능여부 인증)을 실시하되, 카드인증은 지불 프로토콜시 지불정보가 개인키로 전자서명되므로 이때 실시한다.



<그림 4-2> 카드 - 단말 간 인증절차

인터넷에서 상거래를 위하여 인증을 할 때에는 스마트-Pay카드는 Reader/Writer를 통하여 PC와 <그림 4-2>와 같이 인증을 하고, PC와 상인서버와 인터넷에서의 인증은 인증서를 상호교환함으로써 상호인증을 실시하며 순서는 다음과 같다.

1) 고객은 인터넷에 연결 후 웹 부라우저를 통하여 상인서버(가상쇼핑몰)에 접속하고 상품을 검색하여 선택한다.

2) 상인서버는 고객이 선택한 상품에 대한 정보를 고객의 웹 부라우저로 보내고, 고객이 화면상에서 구매를 결심하면 고객 PC내의 월릿(Digital Wallet)이 플러그인 형태로 작동된다. 월릿프로그램은 PC에서 스마트-Pay카드를 제어하여 인터넷에서 상인서버와 지불처리를 하는 프로그램으로 인증서 검색, 세션키생성 및 교환, 공통키 암복호화, 지불정보 전송 역할을 한다.

3) 월릿은 고객에게 스마트-Pay카드를 Reader/Writer에 삽입하기를 요청한다. 고객의 스마트-Pay카드를 PC와 연결된 Reader /Writer에 삽입하면 월릿은 <그림 4-2>와 같이 카드를 인증하고 카드정보를 읽어 PK_I, CERTc(=(Cert(I,Bc), Cert(Bc,C),VALc))를 기억한다.

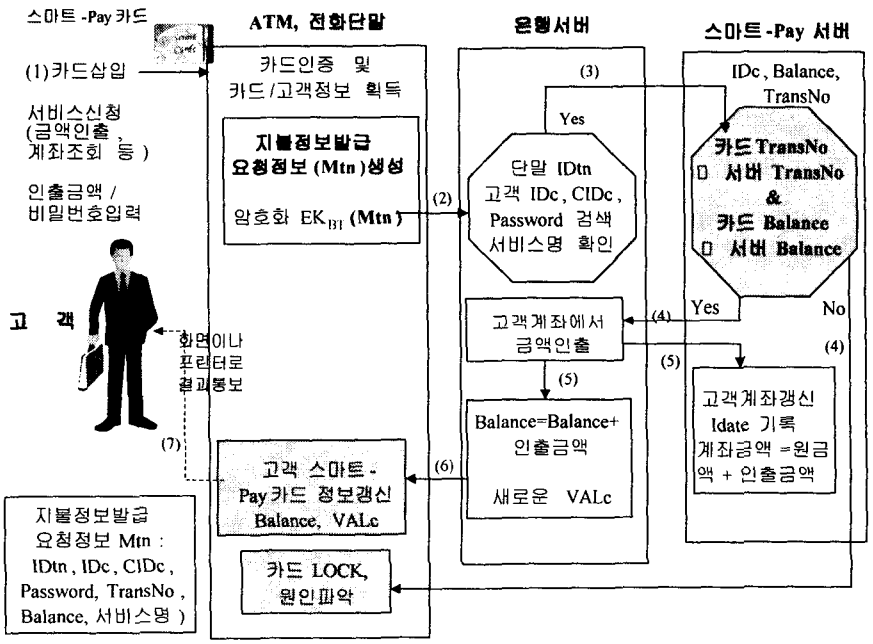
4) 고객 PC(월릿)은 상인서버로 인증정보(CERTs=Cert(I,Bs), Cert(Bs,S),VALs)를 요청한다.

5) 상인서버는 CERTs를 고객 PC로 전송하고 고객은 이를 검증한 후 상인의 공개키 PKs를 획득한다.

6) 고객 PC는 DES로 세션키 Kss를 생성하고 상인서버의 공개키로 암호화(EPKs(Kss))하고, Kss로 암호화한 CERTc와 함께 상인서버로 전송하며, 이후의 통신은 공통키방식의 암호화통신이 되도록 한다.

4.3.2 지불정보발급 프로토콜

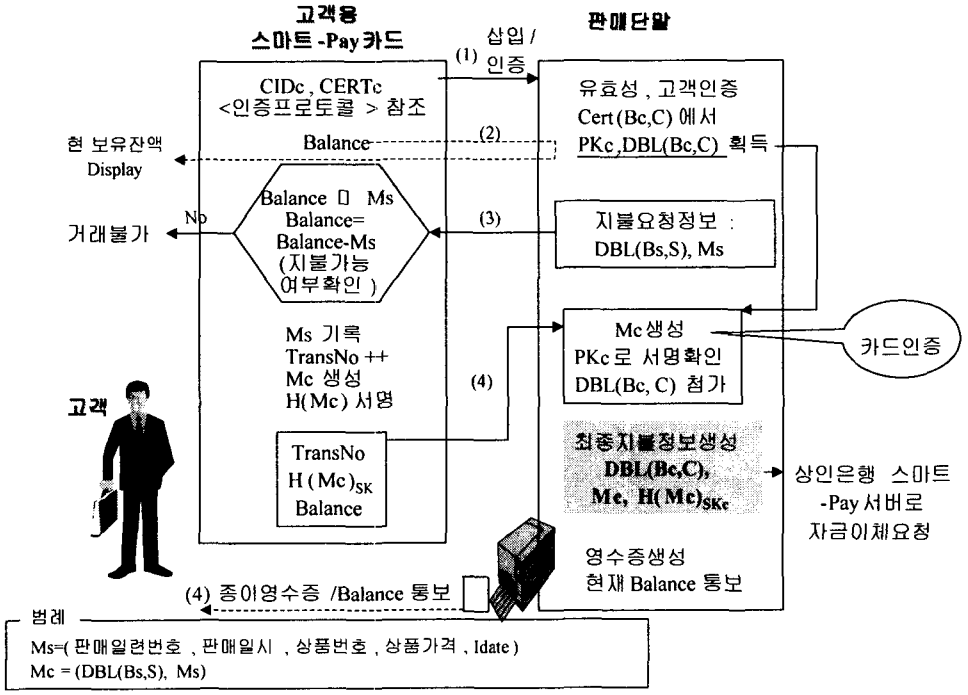
고객은 스마트-Pay카드를 ATM, 전화단말 등을 통하여 은행서버와 온라인으로 연결하여 금액인출이나 계좌조회 같은 서비스를 요청하면 은행서버는 스마트-Pay카드의 Balance와 유효성정보 VALc를 갱신한다. 지불정보발급을 위한 프로토콜은 <그림 4-3>과 같다.



<그림 4-3> 지불정보 발급 프로토콜

4.3.3 지불프로토콜

고객이 상품이나 서비스에 대한 대금을 지불하는 경우, 스마트-Pay카드는 판매단말에 접속되어 있는 상태로 <그림 4-2>와 같이 인증을 하고 지불프로토콜을 진행한다. 이때 지불정보에는 고객 및 상인의 인증서 내에 있는 DBL(Bc, C), DBL(Bs, S)가 포함되는데, DBL(Bc, C)는 EK_{IB}(Bc , EK_{BcC}(C))와 같이 발행기관과 은행간의 공통키 K_{IB}와 은행과 고객의 공통키 K_{BcC}로 각각 은행 및 개인계좌정보를 암호화하여 상인은 고객의 은행 및 계좌정보에 대하여 알 수 없고, 상인은행 스마트-Pay서버와 발행기관은 고객의 계좌정보를 알 수 없도록 하여 개인 프라이버시를 보호하기위한 것이다. 오프라인 거래시 지불프로토콜은 <그림 4-4>와 같다. <그림 4-4>에서 보듯이 지불정보의 전자서명은 $H(Mc)_{SKc}$로서 판매단말은 PKc를 이용하여 무결성을 확인 할 수 있으므로 이때 인증프로토콜에서 언급한 카드인증도 완료된다.



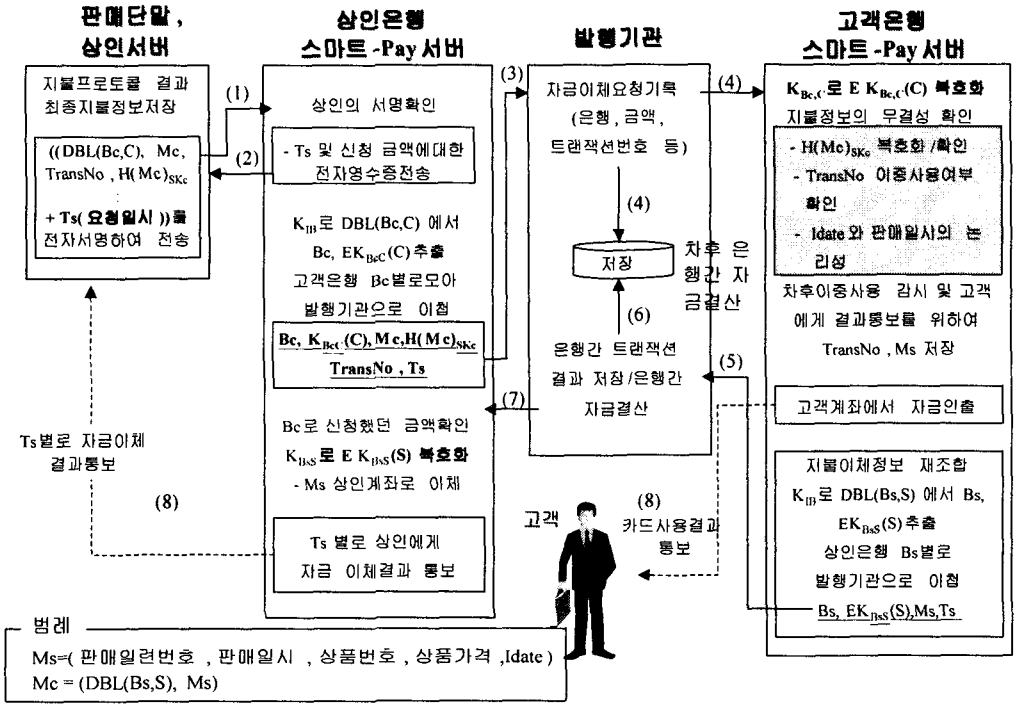
<그림 4-4> 오프라인 지불 프로토콜

고객이 인터넷에서 전자지불 할 때를 보면, 4.2.1 인증 프로토콜에서 스마트-Pay카드와 고객 PC는 <그림 4-2>와 같이 인증하고 고객 PC와 상인서버 간 인터넷에서 인증서 교환을 통하여 상호인증하였으며 고객 PC는 통신을 위한 세션키 Kss를 전송하였다. 이후 지불프로토콜은 Kss에 의하여 암호화된 형태의 통신으로 오프라인 지불프로토콜과 동일하게 이루어진다. 단 지불정보에 대한 전자서명은 PC에서 확인되고, 스마트-Pay카드로 전송되어 이루어진다.

고객이 네트워크 상에서 지불정보를 분실하여 상인서버 측으로부터 전자영수증을 받지 못하는 경우에는 우선 상인서버로 반복하여 전자영수증을 요청 할 수 있고 상인서버에서 반응이 없는 경우에는 지불정보의 분실이나 위장된 상인서버에 지불정보를 도난 당했을 경우로 판단 할 수 있다. 이 경우에는 분실된 일시, 웹 주소 등의 정보를 은행으로 전송하여 분실된 지불정보에 대한 은행 측의 지불을 중지하고, 스마트-Pay카드 유효성 정보 VALc의 유효일 Vdate가 만료된 후 상인의 자금이체가 완료된 후 스마트-Pay카드서버의 계좌잔액과 카드의 잔액을 조정하여 되돌려 받을 수 있겠다.

4.2.4 최종 지불정보 처리

최종 지불정보처리는 판매단말이나 상인서버에서 상인은행으로 판매대금에 대한 자금이체를 요청함으로써 시작되며 고객 스마트-Pay서버, 발행기관, 상인 스마트-Pay서버간 자금이체로 종결된다. 최종 지불정보 처리절차는 <그림 4-5>와 같으며 과정에서 각 개체는 공중망 혹은 전용망을 통하여 상호인증 및 암호화통신을 한다. <그림 4-5>에서는 개체 간의 인증 및 암호화과정은 생략하고 지불정보의 흐름 만 도식하였다.



<그림 4-5> 최종 지불정보 처리과정

4.3 제안된 지불시스템의 평가 및 분석

1) 보안성 : 본 논문에서 제시하는 스마트-Pay카드의 고객전자서명의 안전성은 발행기관, 은행, 스마트-Pay카드로 이어지는 인증사슬에 의존한다. 발행기관과 은행의 인증키의 길이를 1,024비트로 가정한다면 고성능의 컴퓨터에서 10^{10}년을 계산해야만 풀 수 있다는 결론이 나온다. 따라서 스마트-Pay카드의 개인키를 위조하기 위해서는 발행기관에서 은행을 인증하는 인증서와 은행이 스마트-Pay카드를 인증하는 인증서를 위조해야하기 때문에 불가능하다고 할 수 있다. 또한 본 시스템은 은행에서는 고객이 Balance를 갱신 할 때마다 유효성정보 VALc를 발행하고, 고객이 지불시에 이를 제시해야하기 때문에 전자서명 만으로 완벽히 지불정보를 위조 할 수 없으며, 따라서 스마트카드에서는 512비트의 비교적 짧은 키를 사용하더라도 안전하다고 판단되어 스마트카드의 보안성에 크게 의존하지않는다고 볼 수 있다. 상인 측에서 개인키를 위조한다 할 지라도 지불정보처리과정에서 은행과 상호인증을 해야하고, 더욱이 고객이 사용중인 지불카드의 현재의 Idate와 TransNo를 알아야하기 때문에 불가능하다. 또한 스마트-Pay카드는 스마트카드를 이용하여 구현됨으로 카드분실시에는 PIN으로 보호받을 수 있으며, 지불지시형으로 구현되어 인터넷에서 지불정보가 분실되더라도 일정한 기간 후에는 분실금액을 복구 할 수 있다. 고객의 프라이버시 노출방지를 위하여 지불정보에는 이중암호화된 은행 및 계좌정보(예 : DBL(Bc,C))를 제공하여 상인으로부터 고객은행 및 계좌에 대한 접근을 방지한다.

2) 효율성 : 스마트-Pay카드는 인증서와 100% 지불을 확신 할 수 있는 잔액을 갖고 있으며, 고객의 스마트-Pay카드의 전자서명은 상인이 제공한 판매정보를 서명하여 제공하기 때문에 상인이 믿을 수 있고 따라서 제삼자의 개입 없는 직접지불이 가능하다. 직접지불이 가능하므로 브로커와의

통신이 필요하지 않아 비용이 절감되고 인터넷에 연결된 서버만을 운영하는 소규모상점도 설치가 가능하여 전자상거래를 활성화시킬 수 있다.

3) 사용의 편리성 : 스마트-Pay카드라는 물리적수단을 제공하여 사용자 친숙성을 제공하고 실세계 및 인터넷에서 동시에 통용가능하며 기존 금융서비스(신용카드, 직불카드)등을 수용 할 수 있으므로 대중화하는데 유리하다.

제안된 스마트-Pay시스템은 직접지불이 가능하면서 분실시 복구가 가능하고 재사용이 불가능하여 기존의 전자지불시스템 보다 보안성이 높고, 인터넷 전자상거래에 적합하다고 평가된다.

4) 제한점 : 아직까지 공개키기반 스마트카드는 대중화되지 못하였으므로 본 시스템을 구현하는데 아직까지는 다소 제약이 있다고 판단되나 전자서명이 가능한 스마트카드는 새로운 기술과 알고리즘의 개발에 따라서 빠른 시간내 양산될 것이다.

5. 결 론

스마트-Pay시스템은 신용카드기반 지불시스템과 비슷하지만 카드 내의 유효성을 확인 할 수 있는 정보와 잔액을 포함하여 별도로 개인의 신용정보를 확인할 필요가 없으며 은행에 있는 자신의 계좌에 입금된 금액을 이용하므로 소액사용도 가능 할 만큼 트랜잭션 비용도 절약 할 수 있다고 판단된다. 또한 지불정보 내부에는 고객과 상인을 증명 할 수 있는 충분한 정보가 암호화되고 고객의 개인키로 서명되어 기밀성, 무결성을 제공한다. 최종적으로 개인계좌에서 대금을 인출하는 고객은행 스마트-Pay서버까지 전자서명된 지불정보가 전송되어 무결성 및 이중사용여부를 확인 할 수 있으므로 금융부문에서 매우 안전하다. 이와 같은 전자지불시스템의 보급은 전자상거래 뿐만 아니라 실세계에서도 현금을 대처할 수 있을 만큼 사용의 편리성을 제공할 것이다. 범 세계적으로 통용가능하면서 완전한 오프라인 지불능력을 갖춘 지불시스템은 좀더 연구하여야 할 과제이다.

참고문헌

[1] Alice Richmond, "Enticing Online Shoppers to by-A Human Behavior Study, "Fifth International World Wide Web Conference, http://www.cwi.nl, May 1996.

[2] Bruce Schneier, Applied Cryptography, John Wiley & Sons INC., 1994.

[3] Chan, Siu-cheung Charls, "An Overview of Smartcard Security," http:// grus.hkstar.com /~alanchan#smartcard, Aug. 1997

[4] Steven H. Low 외 2명, "Anonymous Creditcards and it's Collusion Analysis," AT&T Bell Laboratories, ftp://ftp.research.att.com/dist/anocc, Oct. 1994

[5] 남상열 역, Isobe Asahiko 저, 전자머니와 오픈 네트워크 사회, 영진출판사, 1997. 6.

[6] 박성준 외 9명, 공개키인증 소프트웨어 개발 보고서, 한국정보보호센터, 1997. 12

[7] 송관호, 이임영 외 8명, "전자상거래 환경을 위한 기술조사 연구," 한국전산원, 1996. 10.

[8] 임차식, 김홍근 외 3명, 알기쉬운 웹보안기술,한국정보보호센터, 1997. 12

[9] 전주환, 남길현, IC카드를 사용한 디지털 서명 설계 및 구현에 관한 연구, 국방대학원 전산학과 석사학위논문, 1993. 12.