특 집

CEPS 기반의 개방형 전자화폐 Teeni 시스템 개발

오 경 석*, 허 신**, 도 경 구**, 류 재 철***, 김 운****, 김 형 주*****

*노틸러스효성, **한양대학교 컴퓨터공학과, ***충남대학교 컴퓨터공학과,
****스마트카드연구소, *****서울대학교 컴퓨터공학과

요 약

최근 들어 컴퓨터 통신의 확산과 함께 인터넷의 사용이 전 세계적으로 급증함에 따라 인터넷의 용도는 지금까지의 학술 및 연구를 대상으로 한 정보 공유의 목적에서 인터넷을 마케팅의 대상으로 보고 이를 상업적으로 이용하려는 시도가 증가하고 있다. 이미 선진 외국의 경우에는 Mondex, Visa cash, Proton 등의 다양한 전자화폐 상품이 개발되어 사용되고 있으나 국제 호환성의 측면에서는 아직 미미한 형편이며 국제간 통용이 가능한 개방형 전자화폐 시스템 개발은 매우 필요하다.

소액지불 시스템의 국제 표준규격으로 인정받고 있는 CEPS(Common Electronic Purse Specification) 기반의 개방형 전자화폐 teeni 시스템은 EMV(Europay, Master, Visa)[1] 규격을 준용하고, PKI 기반의 보안기능을 채택하여 지불거래시 반드시 확보되어야 할 거래 데이타의 비밀성, 무결성, 부인방지 기능과 PIN(Personal Identification Number)를 이용한 사용자 인증을 제공하며 구매거래시 IC 카드와 가맹점의 구매 단말기(POS)와의 오프라인 동적 데이타 인증(Dynamic Data Authentication) 방식의 상호인증을 제공한다.

개방형 전자화폐 teeni 시스템의 구성 모듈은 발급, 충전, 구매, 정산, 인증시스템으로 구성되어 있으며, 웹기반의 사용자 인터페이스를 제공하고 DES, 3-DES, SHA-1, RSA, SEED 등 다양한 암호 모듈과 다양한 어플리케이션의 탑재가 가능한 Java Card를 기반으로 하고 있으며, VOP(Visa Open Platform) 2.0.1[2], Java Card API 2.1[3] 지원하는 시스템이다.

I. 서 론

최근 국내에서는 인터넷 PC 판매 등 PC의 보급 확대에 따라 인터넷, 전자상거래 이용 인구가 확대되고 있으며 전자거래 기본법 및 전자서명법의 시행으로 전자상거래를 위한 제도적 정비가 이루어지고 있어 보다 안전하고 편리한 사이버 지불 결제수단을 위한 경쟁이 더욱 치열해질 것으로 예상된다. 이미 선진 외국의 경우에는 Mondex, Visa cash, Proton 등의 다양한 전자화폐 상품이 개발되어 사용되고 있으나 국내에서는 아직 미미한 형편이며 특히 국내에서 개발되고 국제간 통용이 가능한 개방형 전자화폐 시스템 개발은 매우 필요하다. 특히 거래 문서의 위·변조, 개인 정보 누출, 신용카드 번호의 누출 또는 해킹의 위험성으로 인한 사용자들의 거부감을 해소하고 안전한 거래를 위하여 완벽한 보안 체계를 확보하여야한다. IC카드는 자체의 연산능력을 가진 IC칩에 암호화 기술이 결합되어 강력한 보안솔루션을 제공하므로, 자기띠 카드가 가지고 있는 취약한 보안성과 정보축적 한계를 한꺼번에 극복할 수 있는 가장 현실적이고, 이상적인 대안으로 현재 전세계적으로 각광을 받고 있다. 또한 IC카드 운용 서버 시스템에서도 카드와 단말의 인증을 구현하고, 거래 전문도 암호화 및 복호화 과정을

통해 송수신되므로 카드 보안뿐만 아니라 IC카드 시스템 전체의 강력한 보안기능을 지닌다. 특히 서구에서는 IC카드형 전자화폐 및 네트워크형 전자화폐 등이 속속 개발되고 있으며 EMV 등 IC 카드 관련 각종 표준이 등장하고 있다[4]. 국내에서도 최근 IC카드를 이용한 각종 서비스가 실시되고 있으며(서울시버스카드, 하나로 교통카드 등의 비접촉식 카드) I-Cash와 같은 네트워크형 전자화폐의 개발도 이루어졌다. 고객이 금융기관을 방문하여 입, 출금 등의 업무를 처리하는 전통적인 은행 창구 업무를 대체하며 전자금융으로 통칭되는 다양한 전자거래 업무는 조속한 시일내에 현실화될 것으로 예측되며 펌뱅킹, 홈뱅킹 등의 형태로 가시화 되고 있다. 특히 이러한 전자금융시대에는 은행업무에 대하여 기존의 은행뿐만 아니라 인터넷 뱅킹에 이미 참여한 마이크로소프트사, Manchester United 같은 연예오락 전문 회사, 통신망 업체, 인터넷 방송국, 소프트웨어 회사 등 여러 분야의 업체들이 인터넷을 통하여 은행업무에 참여할 것으로 예상되며 특히 이러한 일련의 변화들은 전자화폐가 기존의 실물화폐를 대체하게 될 수 있는 21세기에는 기존 금융환경의 변화도 필수적으로 수반될 것이다. 상기 언급한 바와 같이 시장 및 환경의 변화가 이미 일어나고 있으며, 이러한 변화에 대해 IC카드가 중요한 매체로 자리잡을 것이라는 점은 여러 석학들에 의해 지적된 바 있다. 이에 따라 구미 선진국에서는 현재 VISA카드社와 MASTER카드社를 양대 축으로 시장을 선점하려는 노력을 경주하고 있으며, 국내에서도 MONDEX시스템(MASTER카드社)이 이미 도입되어 시범운영을 계획하고 있는 실정이다. 이러한 시점에 국내 독자 기술로 세계시장의 흐름과 호환될 수 있는 시스템을 개발한다고 하는 사실은 국내 시장과 산업을 보호하고 이후 환경 변화와 기술 발전에 능동적으로 대처할 수 있는 기술 독립을 의미할 뿐만 아니라, 현재 그 가치가 날로 부각되는 개인정보, 소비 정보, 국가 기반 경제 활동 정보 등에 대한 국외 유출 방지에도 크게 기여할 것이다. 한편, IC카드를 이용한 전자화폐 시스템은 그 잠재력과 효용성에 비해 전세계적으로 초기 단계에 있는 것이 사실이고, 안정되고 검증된 시스템 솔루션은 아직 존재하지 않아 국내에서 안정된 시스템이 독자 개발될 경우 후발 국가에 많은 시장을 창출할 수 있다는 것을 의미하며 상기 언급한 시장 및 산업, 정보 보호라는 것의 반대 급부를 기대할 수 있을 것이다. 인터넷 사용자의 폭발적인 증가와 전자상거래용 쇼핑몰 사업자의 대거 등장으로 전자상거래 시장이 급속도로 확대되고 있어, 이에 상응하는 다양하고 안전한 결제시스템의 필요성이 대두되고 있다. 결제시스템은 경제 주체간의 금전적 교환이 신뢰할 수 있는 제3자를 통해 이루어지기 시작하면서부터 발전되어 왔으며 금융거래를 위해서는 무엇보다도 안전성 및 무위험성을 보장할 수 있는 결제 시스템이 구축되어야 한다. 전자화폐를 이용한 금융의 전자화 추세는 다양한 부가 서비스를 파생시키고 있으며 기존의 금융권 고유의 사업에서 머무르지 않고, 부가가치 통신회사는 물론 컴퓨터관련 회사들까지도 결제시스템을 개발하고 있다. 특히 SET, C-SET, OTP, S-UUTP, SSL 등 안전한 전자상거래를 위한 프로토콜이 속속 개발되고 있으나 현재 다양하게 등장하는 여러 정산 결제 시스템은 그 안정성과 보안성이 검증되지 않은 상태이고 외국의 기술에 의존하는 경우가 많은 현실이다. 따라서 안정성과 보안성이 검증된 전자화폐 시스템의 개발 및 국내 표준을 제정하는 일은 시급히 이루어져야 할 것이다. 본 논문에서는 CEPS[5]을 준용한 Teeni 전자화폐의 발급, 충전, 구매, 정산, 인증시스템별 구성도와 트랜잭션의 처리 절차를 설명한다.

II. 본 론

소액지불 시스템의 국제 표준규격으로 인정받고 있는 CEPS 기반의 개방형 전자화폐 teeni 시스템은 PKI 기반의 보안기능을 채택하여 높은 보안성을 제공하며 구매거래시 IC카드와 가맹점

의 구매 단말기(POS)와의 오프라인 동적데이타 인증(Dynamic Data Authentication)방식의 상호 인증을 제공한다.

개방형 전자화폐 teeni 시스템의 구성 모듈은 발급, 충전, 구매, 정산, 인증시스템으로 구성되어 있으며, 웹기반의 사용자 인터페이스를 제공하고 DES, 3-DES, SHA-1, RSA, SEED 등 다양한 암호 모듈과 다양한 어플리케이션의 탑재가 가능한 Java Card를 기반으로 하고 있다.

1. 전자화폐의 개요

1) Teeni 전자화폐의 개념

전자화폐는 IC칩이 내장된 신용카드 크기의 플라스틱 카드에 일정한 화폐 가치가 전자적 기호로 저장되어 이를 일반물품이나 서비스 구매에 일반화폐 기능을 수행한다. 기존의 국내 전자화폐와는 달리, teeni는 국내 최초로 PKI 인증 시스템과 Open Platform 기반으로 CEPS를 준용하여 개발되어 강력한 보안과 유연성, 국제적 호환성을 제공하는 전자화폐이다.

2) teeni란

t : 21세기형 현금(Twenty First Century Currency)

ee : 신속함을 추구하는 생활환경(Speedy Life-style)

n : 다양한 삶의 연결(Networked Society & Infrastructure)

i : 나를 대표해주는 카드(Individualism)

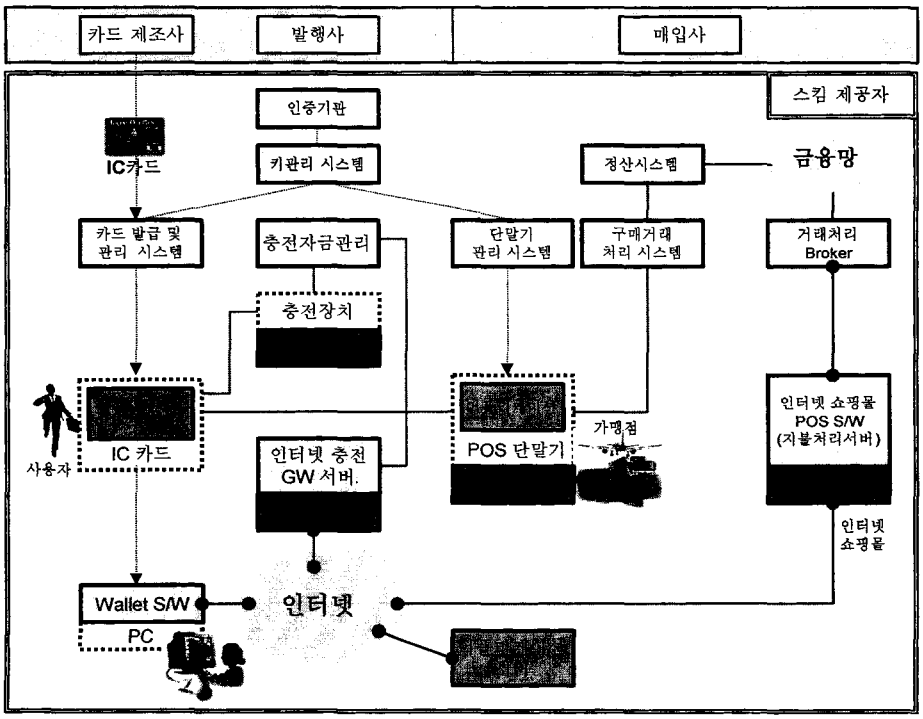
란 뜻으로 국제적 호환성, 높은 보안성, 다양한 응용성을 갖춘 전자화폐이다.

2. 전자화폐 시스템 전체 구성도

1) 구성요소와 역할

(1) 충전 단말기

충전 매입사에 의해 설치되는 충전기는, CEP



〈그림 1〉 전자화폐 시스템 전체 구성도

카드 발행사의 보안응용모듈(secure application module, LSAM) 사이의 on-line 통신 채널을 확립함으로써 CEP 카드에 새로운 잔액을 충전하거나 환전하는 서비스를 제공한다.

충전장치는 유인환경 및 무인환경 모두에 존재할 수 있다. 충전장치는 충전매입사의 전용 메시지 포맷 및 통신프로토콜을 사용하여 충전매입사 호스트 소프트웨어와 상호 작용한다.

(2) 충전매입사

충전 매입사는 충전단말기의 거래 데이터를 수집하여 해당 카드 발행사와 통신하는 역할을 한다. 또한, 타행충전시 카드 발행사와 자금 발행사 간의 정산에 참여한다.

(3) 발행사

발행사는 카드의 발급 주체로서, 충전/환불 거래의 인증에 책임이 있다. 카드 사용자 정보, 카드 정보를 관리하며 거래시 발생하는 채무의 책임이 있다. 또한, 발행사는 정산센터로부터 배치파일을 수신하고 수신된 배치파일의 총 건수와 총 금액, 배치파일 중복여부를 검사한 후 Fund-Pool 테이블에서 해당 카드의 잔액을 갱신하는 역할을 한다.

(4) 가맹점

구매 발생 시 Teeni 시스템의 정해진 format에 맞게 배치파일을 생성하여 정산센터에 전송한다.

(5) 정산센터

가맹점으로부터 배치파일을 수신하여 수신된 배치파일을 검증한 후 발행사별 또는 매입사별 결산파일과 정산파일을 생성하고 생성된 결산파일과 정산파일을 전송한다.

(6) 매입사

정산센터로부터 배치파일을 수신하고 수신된 배치파일의 총 건수와 총 금액, 배치파일 중복여부를 검사한 후 생성된 가맹점 입금 파일을 가지고 해당 가맹점에 정산 금액을 입금시킨다.

(7) 인증센터

카드 발행사 및 매입사의 인증서 요청에 따라 해당 발행사 및 매입사별 인증서를 생성, 배포, 관리하며 인증서 취소 목록을 생성하고 배포하는 역할은 한다.

(8) 자금 발행사

자금 발행사는 충전의 자금을 관리하고 제공하는 책임이 있다.

3. 전자화폐 발급시스템 구성도

전자화폐 발급시스템은 teeni 운영에 필요한 다양한 카드와 단말기의 보안모듈(SAM)을 발급하는 기능을 한다.

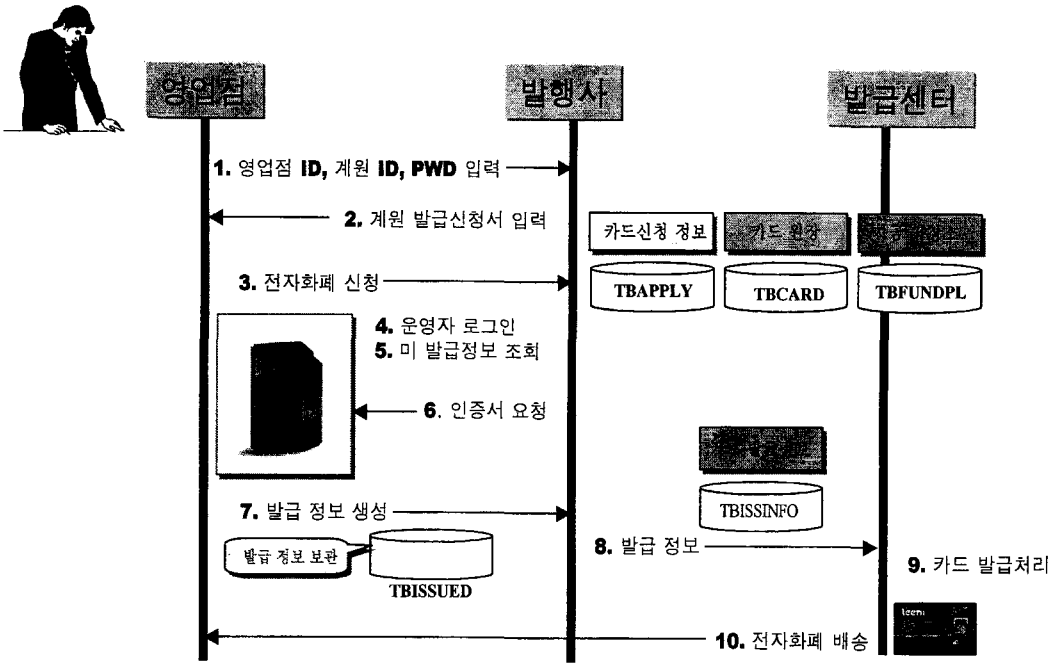
1) 발급흐름도

4. 전자화폐 충전시스템 구성도

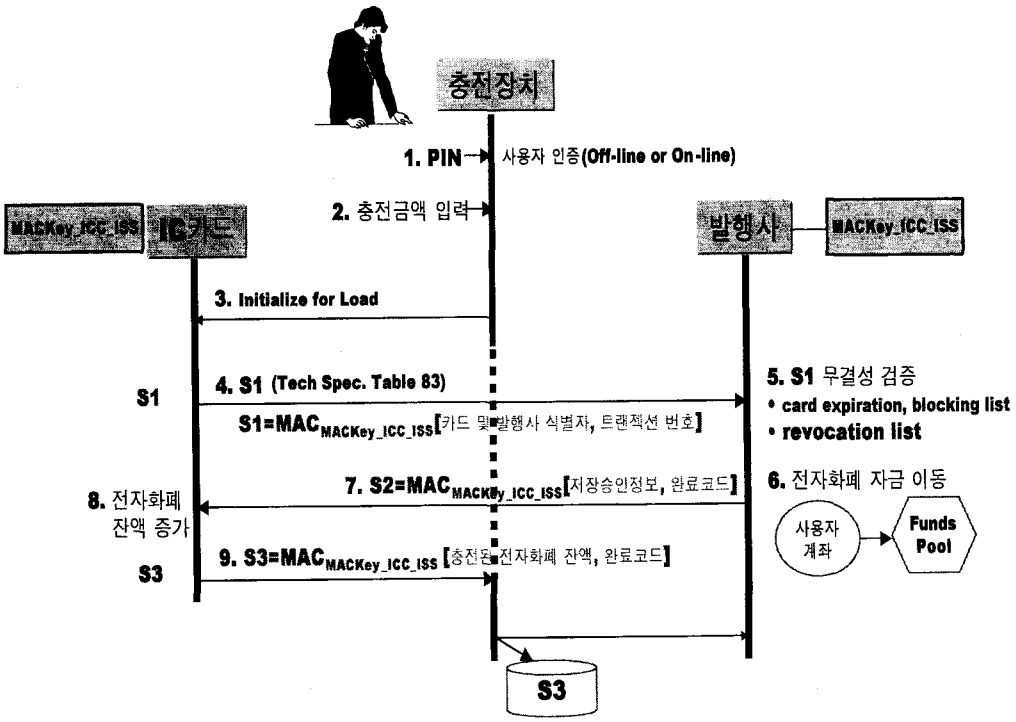
전자화폐 충전 시스템은 충전장치에서 시작되어 발행사의 호스트 시스템으로 전송되는 온라인 트랜잭션이다. 충전 트랜잭션은 CEP 카드로 자금을 추가시키는 과정이다. 두 가지의 충전처리 유형이 CEP 카드에서 지원된다. 발행사 금융기관이 소유한 계좌로부터의 linked 충전을 요구하는 발행사가 있을 수 있으며, 그렇지 않고 다른 자금 출처로부터의 충전을 허용하는 발행사도 있을 수 있다.

Linked 충전의 경우, 자금출처는 카드를 발행한 금융기관의 계좌로서 카드소지자가 보유한 모든 계좌가 가능하다. 발행사는 최종적으로 선택된 계좌에 대해 책임이 있다. 충전 트랜잭션에는 두 개의 명령이 사용되는데, 'Initialize for Load'와 'Credit for Load' 명령이 그것이다. 'Credit for Load' 명령은 반드시 성공적인 'Initialize for Load' 명령 수행이 선행되어야 한다(must).

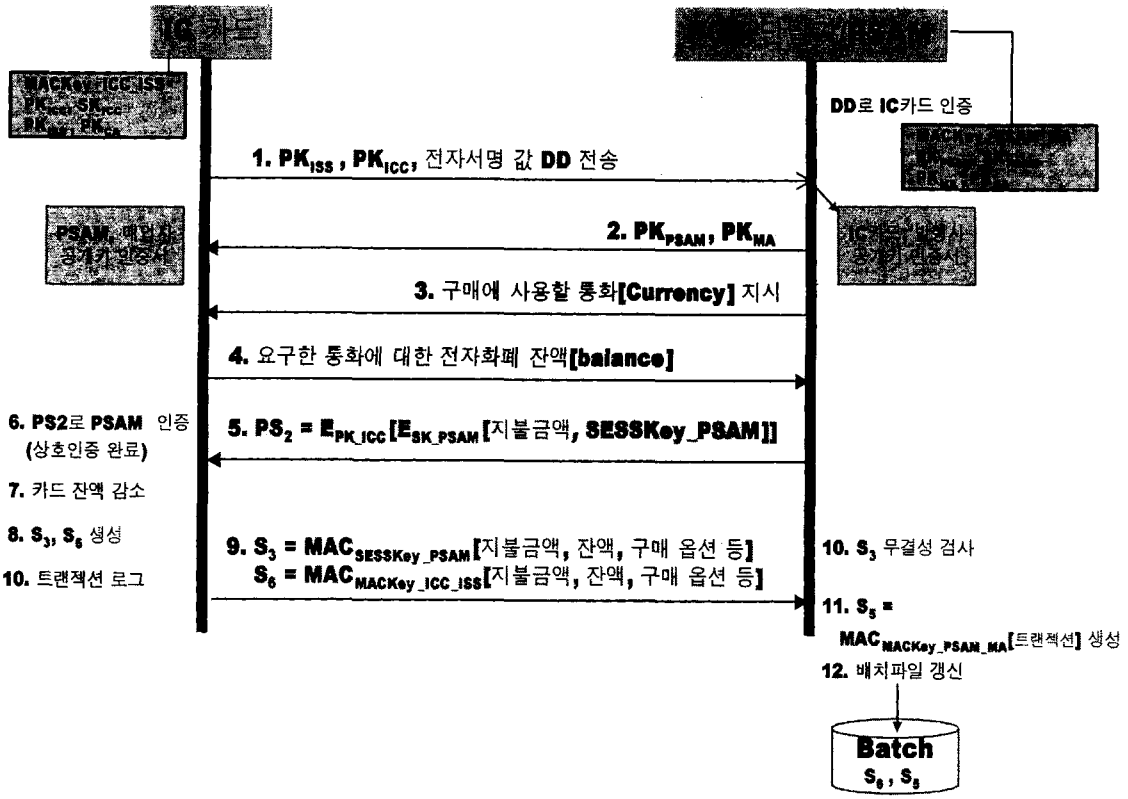
1) 충전 흐름도



〈그림 2〉 발급흐름도



〈그림 3〉 충전 흐름도



〈그림 4〉 구매 흐름도

5. 전자화폐 구매시스템 구성도

구매 트랜잭션은 POS 장치에서 시작되는 오프라인 트랜잭션으로서, 카드소지자로 하여금 CEP 카드에 저장된 전자화폐를 사용하여 상품이나 서비스를 구매할 수 있도록 한다. 전화기와 같은 POS 장치는 증분구매를 지원한다. 트랜잭션이 시작되면 CEP 카드는 초기증분금액을 지불한다. CEP 카드는 POS 장치에 투입된채로 시간 경과 혹은 해당 서비스의 지불기준에 기초하여 연속적인 증분구매 트랜잭션을 수행한다. 증분구매 트랜잭션의 연속구매 과정을 카드소지자가 받아들일 필요는 없으며, 카드소지자에게 추가적인 증분을 중단시킬 수 있는 수단을 제공해야한다. 구매 트랜잭션은, CEP 카드가 POS 장치로부터 배출되기 전에 CEP 카드로 구매취소(purchase reversal) 명령을 전송함으로써 취소될 수 있다. 증분구매의 경우에는 최종 증분에 대해서만 취소가 가능하다.

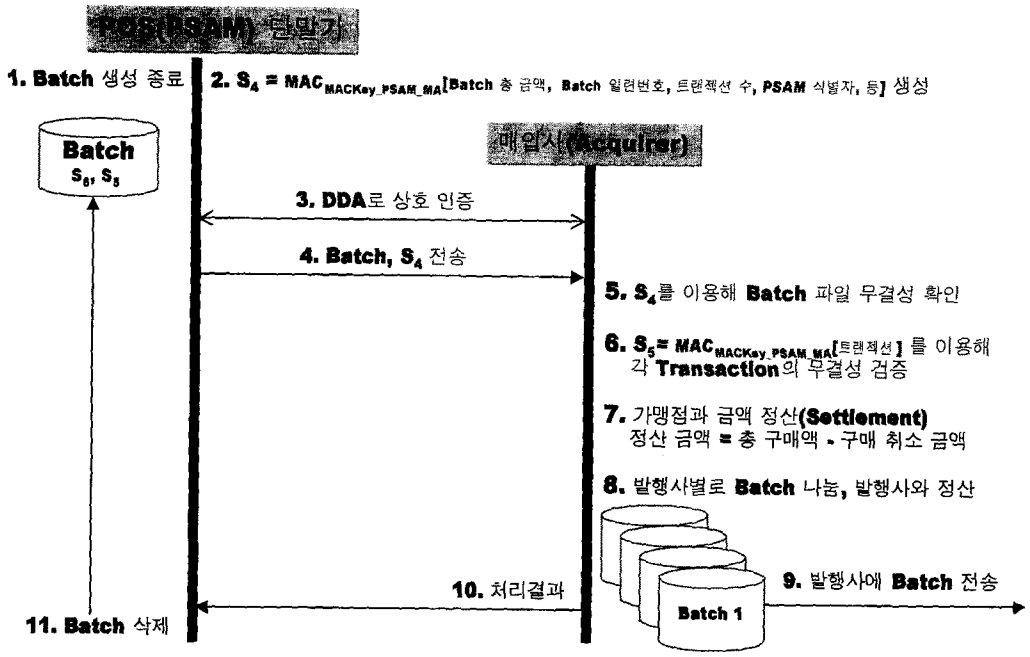
1) 구매 흐름도

6. 전자화폐 정산시스템 구성도

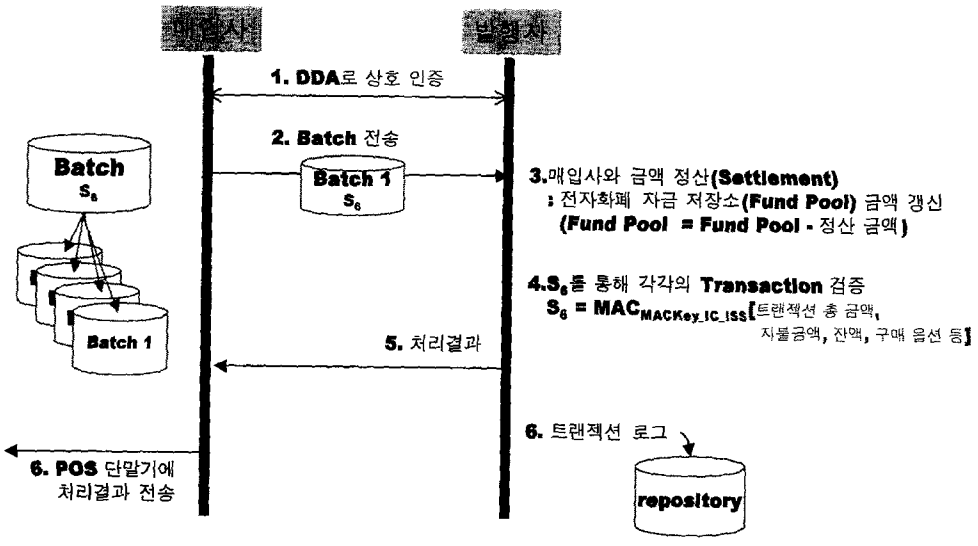
가맹점에서 일어난 모든 구매 거래에 대해서 정산센터, 매입사, 발행사에서 결산 작업을 하는 시스템이다.

1) 정산 흐름도

- 배치 처리(Batch Processing)
- 정산 처리(Clearing Processing)

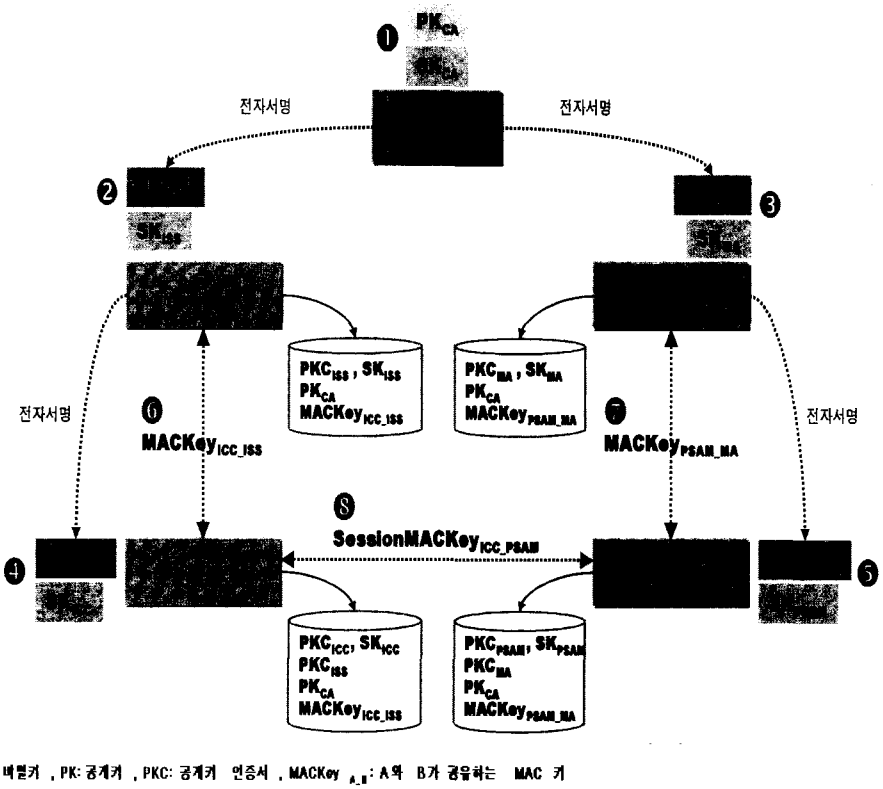


〈그림 5〉 배치 처리



〈그림 6〉 정산 처리

7. 전자화폐 인증시스템 구성도



〈그림 7〉 전자화폐 인증시스템 구성도

Ⅲ. 결 론

최근 국내에서는 인터넷 PC 판매 등 PC의 보급 확대에 따라 인터넷, 전자상거래 이용 인구가 확대되고 있으며 전자거래 기본법 및 전자서명법의 시행으로 전자상거래를 위한 제도적 정비가 이루어지고 있어 보다 안전하고 편리한 사이버 지불 결제수단을 위한 경쟁이 더욱 치열해지고 있다. 이미 선진 외국의 경우에는 MONDEX, VISACASH, PROTON 등의 다양한 전자화폐 상품이 개발되어 사용되고 있고 국내에서도 다양한 전자화폐가 개발 및 사용되고 있다. 여기에 국제간 통용이 가능한 개방형 전자화폐 시스템 개발은 매우 필요하다. 특히 거래 문서의 위·변조, 개인 정보 누출, 신용카드 번호의 누출 또는 해킹의 위험성으로 인한 사용자들의 거부감을 해소하고 안전한 거래를 위하여 완벽한 보안 체계를 확보하여야한다. 결제시스템은 경제 주체간의 금전적 교환이 신뢰할 수 있는 제3자를 통해 이루어지기 시작하면서부터 발전되어 왔으며 금융거래를 위해서는 무엇보다도 안전성 및 무위험성을 보장할 수 있는 결제 시스템이 구축되어야 한다. 전자화폐를 이용한 금융의 전자화 추세는 다양한 부가 서비스를 파생시키고 있으며 기존의 금융권 고유의 사업에서 머무르지 않고, 부가가치 통신회사는 물론 컴퓨터관련 회사들까지도 결제시스템을 개발하고 있다.

IC카드는 자체의 연산능력을 가진 IC칩에 암호화 기술이 결합되어 강력한 보안솔루션을 제공한다. 이런 이유로 IC카드는 자기띠 카드가 가지고 있는 취약한 보안성과 정보축적 한계를 한꺼

번에 극복할 수 있는 가장 현실적이고, 이상적인 대안으로 현재 전세계적으로 각광을 받고 있다. 또한 IC카드 운용 서버 시스템에서도 카드와 단말의 인증을 구현하고, 거래 전문도 암호화 및 복호화 과정을 통해 송수신 되므로 카드 보안뿐 만 아니라 IC카드 시스템 전체의 강력한 보안기능을 지닌다.

상기 언급한 바와 같이 시장 및 환경의 변화가 이미 일어나고 있다. 이러한 시점에 국내 독자 기술로 세계시장의 흐름과 호환될 수 있는 시스템인 IC카드방식의 개방형 전자화폐 시스템(Teeni)은 거래의 안전성, 부정사용으로부터의 안전성, 범용 기능의 카드 편리성 등을 제공한다. 또한 본 시스템은 급속도로 변화하고 있는 IC카드 및 주변 기술의 발달과 더불어 전자화폐, 신용/직불카드, 교통카드 등 다양한 대금 결제 수단을 동일한 카드에 적용하여 카드 사용자에게 그 선택의 폭을 다양하게 제공하고 국내외에서 사용이 가능한 전자화폐 및 시스템을 개발하여 국내 표준을 제시했다. 이는 국내 시장과 산업을 보호하고 이후 환경 변화와 기술 발전에 능동적으로 대처할 수 있는 기술 독립을 의미하고, 현재 그 가치가 날로 부각되는 개인 정보, 소비 정보, 국가 기반 경제 활동 정보 등에 대한 국외 유출 방지에도 크게 기여할 것이다.

참 고 문 헌

〔1〕 EMV(Europay, Master, Visa) Specification Version 4.0, 2000

〔2〕 VOP(Visa Open Platform) 〈http://www.visa.com〉

〔3〕 JavaCard API 〈http://www.sun.com〉

〔4〕 Cross-Industry Working Team, Electronic Cash, Tokens and Payments in the National Information Infrastructure

〔5〕 [5] CEPS(Common Electronic Purse Specification) Version 2.2 Functional Specification, Business Specification, Technical Specification

저 자 소 개

吳 慶 錫

1982년 2월 서울대학교 물리학과 졸업, 2000년 8월 연세대학교 경영대학원 졸업, 1982년 1월~2002년 6월 : (주)효성 근무, 2002년 7월~2002년 10월 : 노틸러스 효성(주), 〈주관심 분야 : 스마트카드 Application, 금융자동화 기기 등〉

許 信

1973년 서울대학교 전자공학(학사), 1979년 미국 Southern California Univ. 컴퓨터공학(석사), 1986년 미국 South Florida Univ. 컴퓨터 공학(박사), 1988년 The Catholic Univ. of America 조교수, 1998~2001년 2월 : 한양대학교 정보통신원 부원장, 1999~현재 : 한국 IC카드 연구조합 전자화폐과제 총괄 책임자, 1999~현재 : 한국 정보과학회 이사, 2001~현재 : 한국 정보처리학회 이사, 2001~현재 : 한국 PKI 포럼 기술개발 분과위원, 〈주관심 분야 : Distributed Computing Systems, Fault-Tolerant Systems, Electronic Cash, GIS(Geographic Information System)〉

都 敬 九

1980년 한양대학교 산업공학(학사), 1987년 미국 Iowa State University 전산학(석사), 1992년 미국 Kansas State University 전산학(박사), 1993년 4월~1995년 9월 : 일본 University of Aizu 교수, 1995년 9월~현재 : 한양대학교 부교수, 〈주관심 분야 : 프로그래밍언어, 프로그램 분석 및 검증, 스마트카드〉

柳 在 哲

1985년 2월 한양대학교 산업공학과 졸업(학사), 1988년 5월 Iowa State Univ. 전산학과 졸업(석사), 1990년 12월 Northwestern Univ. 전산학과 졸업(박사), 1991년 2월~현재 : 충남대 정보통신공학부 교수, 〈주관심 분야 : 인터넷 보안, 전자지불 시스템〉

金 雲

1992년 2월 한양대학교 무기재료공학과 졸업(학사), 2002년 2월 동국대학교 대학원 수료(석사 수료), 1993~1995 : (주)삼성전자 스마트카드 사업팀, 1995~1998 : 한국 IC카드 연구조합, 1998~2001 : 젬플러스 코리아 한국 지사장, 2001~현재 : (주)스마트카드 연구소 대표이사

金 炯 周

1978~1982 : 서울대학교 전산기공학(학사), 1982~1985 : 미국 텍사스 대학교 전산학(석사), 1985~1988 : 미국 텍사스 대학교 전산학(박사), 1982~1988 : 미국 텍사스 대학교 조교, 1986. 4~1986. 12 : 미국 MCC 연구원, 1988. 4~1988. 8 : 미국 텍사스 대학교 POST-DOC, 1988. 8~1990. 12 : 미국 조지아 공과대학 조교수, 1991. 1~1997. 12 : 서울대학교 중앙교육연구전산원 부장, 부원장, 1999~2000. 2 : 서울대학교 컴퓨터공학과 학과장, 2000. 3~2001. 2 : 서울대학교 컴퓨터공학부, 교무담당 부학부장, 1995. 7~현재 : 서울대학교 인지과학 협동과정 겸임교수, 2002. 1~현재 : 서울대학교 중앙교육연구전산원 원장, 1991~현재 : 서울대학교 컴퓨터공학부 조교수, 부교수, 교수, 〈주관심 분야 : 객체지향시스템(Object-oriented System), 데이터베이스(Database), 전자상거래(Electronic-Commerce)〉