스마트카드를 이용한 원카드 시스템의 설계 및 보안

이대식* · 윤동식* · 안희학**

요 약

급속한 컴퓨터와 유·무선 인터넷의 발달로 인해 네트워크를 통한 정보의 교류가 활발해지고 있다. 또한 전자상거래와 관련된 산업의 규모가 커지면서 편리한 사용자 인증 시스템의 필요성이 요구되어 보안과 편리성을 갖춘 새로운 인증방식에 대한 연구가 체계적으로 진행되고 있다. 새로운 인증방식의 하나인 스마트카드는 높은 보안성과 기능성 및 편리성으로 인해 기존의 인증방식의 문제점을 극복하여 다목적 기능을 갖춘 하나의 카드로 대치될 것으로 전망된다. 본 논문에서는 스마트카드의 보안과 모든 분야에서 사용 가능한 하나의 원카드 시스템 구현에 대하여 제시하고자 한다.

A Design and Security of One Card System using Smart Card

Dae Sik Lee* · Dong Sic Yun* · Heui-Hak Ahn**

ABSTRACT

According to rapid development of computer and wired-wireless internet, information exchange of networking is growing. Also according as size of industry related e-commerce is bigger, it is Required the necessity of convenient user authentication system. So, the study of new authentication method to have a security and convenience is progressing systematically. Smart card of new authentication method overcome problem of established scheme. So it prospect that will be replaced One Card to have a high security and multi-function. In this papar, we suggest about the implementation of One Card System that the security of smart card and usable in all fields.

Key words : Smart Card, One Card System

* 안동과학대학 사이버테러대응학과
** 관동대학교

1. 서 론

스마트카드의 출현은 높은 보안성과 기능성 및 편리성으로 인해 기존의 카드(마그네틱, 바코드, RF)들이 지니고 있는 높은 위·변조 가능성으로 인한 낮은 보안성, 저기능성 등의 문제점을 극복하는 장점을 가지고 있다[1]. 우리는 그 스마트카드에 대하여 각종 개인정보를 카드 하나에 담아 사용할 수 있고 각종 신분증 등 카드 한 장으로 모든 서비스가 가능한 원카드 시스템(one card system)의 구현과 동시에 개인정보 보안의 신뢰성을 목표로 스마트카드의 다목적 활용 측면에서 그 통합 방안을 모색하고자 한다[2, 3].

우선 스마트카드란 무엇이며 어떠한 것인가에 대한 개념 분석을 시도한다. 그리고 현재 생활에 이용되고 있는 스마트카드의 시장 전망 및 산업동향을 알아본다. 다음은 스마트카드의 이점을 이용 원카드 시스템의 구축에 대한 전반적인 이해 및 설계 및 보안 체제에 대하여 방향을 제시하고자 한다.

2. 스마트카드

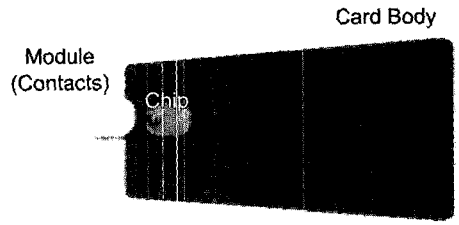
2.1 스마트카드의 정의

IC카드 또는 CHIP카드로 불리는 스마트카드는 마이크로프로세서와 메모리를 내장하고 있어서 카드 내에서 정보의 저장과 처리가 가능한 플라스틱 카드를 말한다. 일반적 Magnetic 카드에 비해 현저히 많은 정보 저장이 가능하다[4, 5].

스마트카드는 "하나의 칩에 모든 정보"라는 특징처럼 연산기능을 갖춘 IC칩을 내장하여 카드를 통한 기본적인 일반은행업무 이외에 신용카드, 교통카드, 신분증 등에 다양하게 적용할 수 있다. 스마트카드는 플라스틱카드에 CPU와 메모리를 내장하여 기존 마그네틱 카드보다 저장용량이 크고, 보안성이 뛰어나기 때문에 다양한 목적으로 사용할 수 있다. 이러한 스마트카드는 기존 마그네틱 카드를 대체하면서 기존 신용카드 이외에 통신, 의료, 교통, 신분증 등에 다양하게 활용되고 있다[6].

2.2 스마트카드의 종류

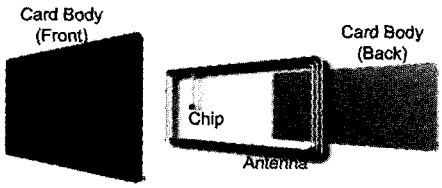
스마트카드는 인터페이스 방식에 따라 접촉식 카드와 비접촉식 카드로 분류할 수 있으며, 이들을 결합시킨 콤비카드 및 하이브리드 카드가 있다[7, 8]. 접촉식 카드란 인터페이스 장치(Interface Device(이하 IFD))에 삽입되었을 때 카드의 접점이 IFD의 접점에 접촉됨으로써 카드가 활성화되는 형태의 카드를 말하고 고도의 보안을 요하는 시스템에 적합하다. 이 카드는 전자화폐와 같은 금융 어플리케이션이나 네트워크 접속 등에 사용된다.



(그림 1) 접촉식 카드의 구조

비접촉식 카드란 카드 판독기와 물리적으로 접촉하지 않는 것으로, 카드를 판독기 내에 삽입하는 대신 일정 거리 떨어져서 작동하기 때문에, 접촉식 카드에서 발생하는 금박 접촉점에 대한 손상 문제를 방지할 수 있다. 이 카드의 장점으로 첫째, 카드 판독기/기록기에 카드 구동 장치가 필요 없고, 정확한 카드 위치 맞춤이 필요 없어 설계·제작이 용이하다. 이 때문에 견고하고 저렴하게 단말기를 제작할 수 있어 유지보수 비용이 절감된다. 둘째, 화학적 손상, 습도와 마찰 등에 강하여 접촉식 IC 카드에 비해 장기적 사용으로 경비가 절감된다. 셋째, 접점단자를 노출시키고 있기 때문에 부정침입으로부터의 보안 보호가 용이하다. 넷째, 표면에 접속단자가

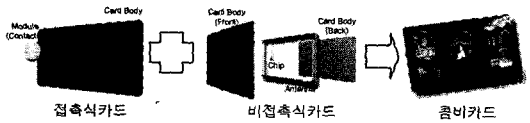
없어 카드 전면을 디자인에 활용이 가능하다. 이것은 여러 기업 혹은 여러 어플리케이션의 다기능 카드 작성에 유용하다. 마지막으로 진동, 먼지 등이 많은 나쁜 환경에서의 운용에도 강하다. 조작이 용이하여 다양한 환경에서 사용가능하며, 적용업무의 선택폭이 넓다는 것이다.



(그림 2) 비접촉식 카드의 구조

하이브리드 카드란 접촉식 카드와 비접촉식 카드의 형태를 모두 지원하는 형태로 두 가지 형태의 기능에 대한 장점을 갖춘 것이라고 할 수 있다. 접촉식 카드는 마이크로프로세서 칩 모듈에 의해 사용되며, 비접촉식 카드는 메모리 칩 모듈에 의해 사용되는데, 메모리 공유는 불가능하다.

콤비카드란 하나의 카드 내에서 접촉/비접촉식 카드가 공유할 수 있는 부분들을 상호 공유하는 화학적 결합형태의 카드로, 내부 자원공유를 통한 이질적 어플리케이션(예 : 칩 운영체제, 동일키나 패스워드)의 통합효과를 가져온다.



(그림 3) 콤비카드의 구조

2.3 스마트카드의 특징

스마트카드 출현의 가장 큰 원인 중 하나는 카드가 가지는 보안성과 활용성을 들 수 있다. 또한 외부 프로그램의 접근에 대해 완벽한 보안체제를 제공하기 때문에 보안성이 높고, IC CHIP을 이용한 새로운 서비스 추가가 용이하다. 기억용량이 매우 크기 때문에 저장 및 사용이 간편해지는 동시에 다목적 활용이 가능하다는 것도 스마트카드의 특성중 하나이다. 보안 특성은 보안 매커니즘, 파일접근제어로 구분할 수 있고, 보안 매커니즘에는 기밀성, 인증, 부인봉쇄가 있다.

2.4 스마트카드의 응용분야

세계 각국에서 스마트카드의 사용은 대세로 인정되고 있으며, 그 활용분야는 통신, 금융, 결제, 의료, 교통, 에너지, 유통, 오락 및 휴양시설 등 산업 전반에 걸쳐 응용되고 있다.

2.5 국/내외 활용사례

2.5.1 외국 사례

외국의 활용사례를 보면, 1991년 덴마크에서 카드 소유자들이 소액결제에 널리 보급된 Danmont 카드를 가지고 다니는 전자지갑의 Open 시스템으로 단몬트는 시스템 오버레이터라는 개념을 도입한 카드를 사용하였다. 1994년 영국에서는 금융과 통신 기능을 통합시킨 새로운 전자화폐 시스템 즉 선불형 전자지갑인 몬덱스를 사용하였다. 몬덱스는 은행계정을 통하지 않고 개인간의 자유로운 전자화폐 가치의 이전을 할 수 있어 은행 간의 차액결제 및 정산이 없고 즉시결제가 가능한 것이 다른 전자지갑과 구별되었다. 미국의 경우에는 애틀란타 올림픽기간 동안 "비자 캐시 카드"를 시범 운용했다. 1985년 일본은 최초로 IC카드시스템 도입을 추진하여 빌딩, 학교 등과 연계하여 자행의 ATM이용, 각종 편이 시설 이용대금결제, 자판기 음식점 이용, 급여 이체 등의 금융서비스 제공은 물론 출퇴근 관리, 출입구 통제, 경비지출 등 입주업체 관리서비스를 제공해 오고 있다.

2.5.2 국내 사례

스마트카드의 시작은 교통요금 카드였다. 예를 들면, 하나로 교통카드는 카드 하나로 지하

철, 시내버스, 개인택시 요금을 결제할 수 있게 한 통합 교통 요금 징수 시스템이다. 또 다른 예로 신한은행의 '스마트 원카드'는 종이통장을 대체할 전자통장 기능과 현금카드 10개, 공인인증서, 전자화폐, 직불카드, 교통카드 등을 한 장의 카드에 구현한 다기능 카드이다. 이 카드는 기존의 자기 띠 형태의 카드와는 달리 카드에 IC칩이 내장되어 있어 복제가 불가능하다.
신한은행은 '스마트 원카드'를 통해서 종이 통장 거래를 없애고, 금년 말 도입 예정인 공과금 전용 수납기를 통하여 거래내역을 출력할 수 있는 전자통장 서비스를 실시할 예정이다. 전자통장이 활성화 되면 고객은 기존 종이통장을 사용함에 따른 보관 및 통장정리 등의 불편함을 없앨 수 있으며 창구에서 거래할 경우에도 청구서 작성없이 창구에 설치된 PINPAD에 스마트원 카드를 삽입하여 고객이 직접거래를 할 수 있다.

〈표 1〉 스마트카드의 응용분야

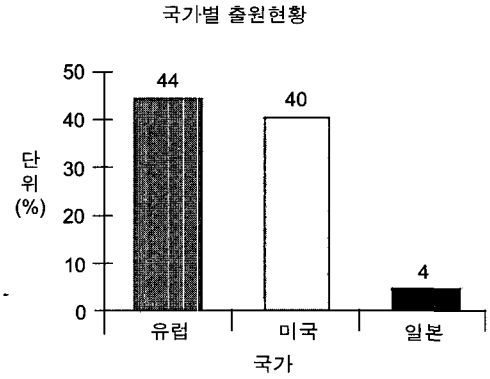
영 역	응 용 분 야
금융(은행)	신용, 직불카드, 자금이체
전자지갑	소액거래 (호텔, 자판기)
전자화폐	전자상거래 소액 처리
교통	통행료, 버스, 열차 등
의료	병력사항 기록, 서비스 개선
전화	IC카드를 이용한 지불시스템
자동차	자동차 구매자에게 제공
로얄티카드	소매상, 항공사 등
도시카드	특정지역(도시별)에서 사용
주차	주차요금 지불시
Pay TV	스크램블 제거
신분증	학생증, 회원카드, 주민등록증
컴퓨터 보안	컴퓨터 네트워크 연결
레져	스포츠클럽, 스키장 이용
전기 · 수도 · 가스	납부시 선불카드 활용
홈뱅킹/쇼핑	전화나 단말기 이용구매
데이터저장	거래정보, 플로피디스크 대체
전자여권	출입국시 여권대신 사용

2.5.3 향후 발전가능성 응용분야

향후 발전 가능성의 응용 분야로는 전자 지갑(Electronic Wallet), TV Top Terminals, 복수 보너스 카드, 지능형 장치제어(Smart Device Control) 등이 있다. 전자 지갑은 다양한 종류의 재무, 신용 및 부채 상태, 기타 거래 계정에 대한 저장기능을 담당하는 카드이며, TV Top Terminals은 TV 의 확장기능 사용을 제어하는데 사용하는 카드로 쓰인다. 다른 카드의 종류로는 복수 보너스 카드가 있다. 이 카드는 단일 보너스 카드와 유사하나 한 회사에 국한되지 않고 여러 회사를 연결하여 사용실적에 따라 보너스를 지급받을 수 있다. 지능형 장치제어(Smart Device Control) 카드는 다양한 형태의 지능형 장치를 제어하는데 사용되는 카드이다.

2.6 스마트카드 시장전망 및 산업동향

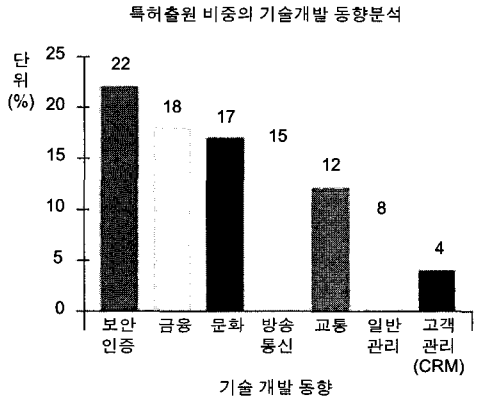
현재 스마트카드의 세계시장규모는 1999년에 15억매가 출하된 후 2004년에 40억매 돌파가 예상되어 5년간 약 270% 증가할 것으로 전망된다.
특허청의 자료에 따르면 1987년부터 2002년까지 지속적으로 스마트카드 기술에 관한 특허출원이 증가하고 있으며 국내에 출원된 총 1130건 중 외국인 출원은 285건, 내국인 출원은 845건으로



(그림 4) 국가별 출원현황

2000년부터 내국인 출원이 대폭 증가한 것으로 나타났다. 외국인 출원을 국가별로 보면, 유럽(프랑스, 독일, 영국 순) 44%, 미국 40%, 일본 4% 순으로 나타났는데, 이러한 사실은 스마트카드 기술이 1968년부터 유럽에서 시작되어 유럽을 중심으로 발전되었기 때문으로 분석된다.

관련 기술개발동향을 특허출원 비중으로 분석하여 보면, 보안·인증분야가 22%, 전자화폐 등의 금융·전자상거래 분야가 18%, 예약서비스 등의 문화·의료·공공서비스 분야가 17%, 방송·통신 분야가 15%, 교통·자동차 분야가 12%, 일반관리 분야가 8%, 포인트·마일리지 서비스 등의 고객관리(CRM) 분야가 4% 순으로 나타났다. 또한 국내기업은 응용기술 분야에서, 외국기업은 회로·알고리즘 기술 분야 및 장치·제조 기술 분야에서 상대적으로 특허출원건수가 앞선 것으로 나타났다.

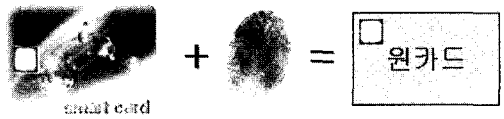


(그림 5) 특허출원 비중 기술 개발 동향

앞으로 스마트카드는 마이크로프로세서 속도의 증가, 메모리 용량의 증가, 소프트웨어 기술의 발달에 힘입어 사회전반에 걸쳐 그 응용분야가 확대될 것으로 보인다. 따라서, 국내기업은 반도체, 통신의 앞선 기술력과 뛰어난 IT인력을 이용하여 스마트카드 관련기술 분야 중 상대적으로 취약한 회로, 알고리즘 기술 및 장치·제조 기술 분야의 원천 기술에 대한 연구 및 투자가 더욱 요구되고 있다.

3. 원카드 시스템의 설계 및 보안체제

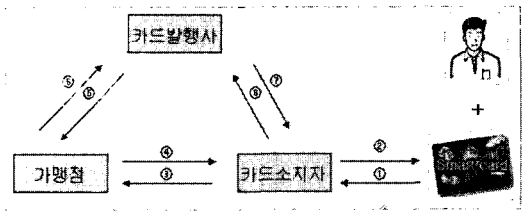
스마트카드의 활용은 점점 그 기능이 통합화되어가면서 보안은 스마트카드에 있어서 가장 중요한 부분을 차지하게 되었다. 스마트카드의 보안성은 단일 칩으로 설계되어 내부 시그널을 감지하기 매우 어렵고, 제작 단계에서 물리적/논리적으로 잠금을 해서 잠금을 풀어 내부구조에 대해 재구성이 불가능하다는 보안상의 장점이 있다. 하지만 만약 카드를 분실하였을 경우, 혹은 악의를 가진 사용자가 남의 카드를 이용하고자 할 경우, 어떻게 이러한 사용을 막을 수 있는가 하는 점이다. 카드에 저장된 정보는 그 사람의 모든 신상정보가 담겨져 있기 때문에 정당하지 않은 이용자의 악용은 개인적으로나 사회적으로 큰 문제가 아닐 수 없다. 이러한 해결책의 하나로 우리는 여기서 기존의 스마트카드에 생체인증방식중 하나인 지문인식을 결합시켜 새로운 보안체제인 스마트카드를 설계, 기존 스마트카드의 보안성을 한 단계 업그레이드 시킨 원카드 시스템을 제시한다. 이 카드는 의료, 금융, 교통, 전화 등의 정보를 담아 하나의 카드로서 사용하게 한다[9, 10]. 다음 (그림 6)은 원카드의 구조에 대하여 설명한다.



(그림 6) 원카드의 구조

다음은 원카드를 이용하여 신용카드로 사용시의 보안성 및 편리성을 예시로 나타낸 것이다. 먼저 카드 발급시의 개인의 각종 신상 명세와 함께 지문 데이터를 카드에 저장한다. 그 후 카드를 사

용 가능하게 하는데 이는 8단계의 과정으로 스마트카드의 인증 단계부터 후에 카드대금 지불까지의 방법이며 다음 (그림 7)과 함께 설명한다.



(그림 7) 스마트카드 사용자 결제시스템 구조도

① 카드에 있는 지문인식기에 지문을 인식시킨다.
② 카드에 있는 개인정보의 지문과 사용자의 지문이 일치하는지 검사(일치하면 카드 결제 승인이 이루어짐)
③ 카드소지자의 카드 제시 및 매출표 서명 단계
④ 상품 및 용역거래 단계
⑤ 대출 대금 청구 단계
⑥ 대출대금 비급 단계
⑦ 사용대금 청구 단계
⑧ 카드대금 지불 단계

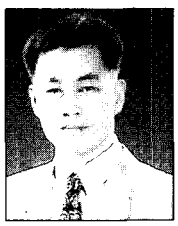
이는 현재 사용되는 신용카드 거래구조에 스마트카드의 기술을 도입함으로써 금융결제 및 각종 서비스의 보안 및 편리성을 한 단계 강화시키는 효과를 얻게 된다.

4. 결 론

지금까지 스마트카드에 대한 분석과 스마트카드의 시장전망 및 산업동향, 보안성 및 효율성에 대하여 살펴보았다. 급속한 정보화로 인하여 개인의 정보보안과 편리성의 문제점에 대하여 현재 여러 방면에서 체제적으로 연구가 진행중이며, 스마트카드에 대한 원카드 시스템의 움직임도 이미 시작되고 있다. 국내에서도 이와 같은 스마트카드의 기술이 개발되었다. 본 논문에서는 현재 생활에 이용되고 있는 스마트카드의 시장 전망 및 산업동향을 살펴 이점을 이용한 원카드 시스템의 구축에 대한 전반적인 이해와 설계 및 보안체제에 대하여 연구 방향을 제시하였다.

참 고 문 헌

[1] J. Adams, "Survey : Biometrics and smart card", Aug 2000.
[2] Naomaru Itoi, Tomoko Fukuzawa, Peter Honeyman, "Secure Internet Smartcards", 2000.
[3] 이성인, "Smart Card형 전자화폐의 보안 기술과 대응방향", 2003.
[4] http://www.kisti.re.kr.
[5] http://www.tta.or.kr.
[6] 이대갑, "지문과 스마트카드를 이용한 출입관리 시스템", 2003.
[7] http://www.itfind.or.kr.
[8] http://www.infotrust.co.kr.
[9] 문대성, 길연희, 안도성, 반성범, 정용화, 정교일, "지문 인증을 이용한 보안 토큰 시스템 구현", 2003년 8월.
[10] 이만식, "지문인식시스템에 관한 연구", 2004.



이 대 식
1995년 관동대학교 전자계산공학과(공학사)
1999년 관동대학교 전자계산공학과(공학석사)
2004년 관동대학교 전자계산공학과(공학박사)
2003년~현재 안동과학대학 사이버테러대응학과 교수

윤 동 식

1992년 관동대학교
전자계산학과(공학사)
1994년 관동대학교
컴퓨터공학과(공학석사)
2000년 관동대학교
컴퓨터공학부(공학박사)
1999년~현재 안동과학대학 사이버테러대응학과 교수

안 희 학

1981년 숭실대학교
전자계산학과(공학사)
1983년 숭실대학교
전자계산학과(공학석사)
1994년 숭실대학교
전자계산학과(공학박사)
1984년~현재 관동대학교 컴퓨터학부 교수