논문 2006-43IE-1-7

# 자바카드를 이용한 파일 접근제어 시스템의 설계 및 구현

## ( Design and Implementation of File Access Control System using Java Card )

구 은 희*, 우 찬 일**

( Eun Hee Koo and Chan Il Woo )

## 요 약

최근 정보를 안전하게 관리하기 위한 방법으로 휴대가 용이하며 물리적, 전기적 그리고 소프트웨어적인 공격으로부터 안전한 스마트카드 시스템이 주목받고 있다. 자바카드는 스마트카드 플랫폼에 자바 기술을 접목시킨 것으로 객체지향 기법을 적용한 보안상 매우 우수한 장점을 지니고 있으며 특성이 다른 하드웨어에서 동일한 동작을 수행할 수 있는 개방형 운영체제를 가짐으로써 다양한 응용 프로그램을 수용할 수 있는 유연성을 가지고 있다. 본 논문에서는 지금까지 각각의 스마트카드 하드웨어에 맞추어져 수행되던 불편함을 자바의 플랫폼 독립적인 실행 특성을 도입함으로써, 통일된 개발 환경을 구축하고 있는 자바카드 기술을 이용하여 하나의 카드로 소유자 이외에도 다수의 관리자가 각기 다른 접근권한으로 접근통제가 가능한 회원카드를 설계하였다. 제안한 방법에서 사용자 인증은 일반적으로 사용되고 있는 PIN과 함께 서명데이터를 이용하여 PIN이 가지고 있는 본래의 보안취약점을 개선하여 보다 안전한 사용자 인증을 수행한다. 본 논문에서 제안한 방법은 사용자 인증, 파일 보안 등급의 차등적인 접근권한을 설계하고 구현함으로써 보다 안전하고 편리한 사용방법을 제공한다.

## Abstract

Recently, smart card system which is known as easy to portable and also safe from physical, electrical, and software attack is observed to manage information that becomes the target of security in safety. And java card graft upon java technology to smart card platform is having very good advantage with object-oriented techniques and also, java card have the open type OS that can show the same action in different hardware characteristic which allows various application programs. In this paper, we introduced independent execution characteristic of java platform because being set to each smart card was uncomfortable till now and we designed access control member card that allows several administrators in different access privilege by single card using java card. Several administrators can approach to various information of file type that is included on issued card to user by using different PIN. In the proposed method, confirmation of personal information, administration contents update, demand by contents, is possible by single card. At this moment, wish to do safer user certification that improve security limitation which is from PIN, used for user certification, and signature data. In the proposed method, as design and implementation of utilization technology of java card, biometrics, user certification which uses multi PIN, provide that more safety and conveniently.

**Keywords** : Smart Card, Java Card, Authentication.

## I. 서 론

정보통신의 발달로 실생활의 많은 부분들이 가상공간에서 이루어지면서 사용자들의 정보보호에 대한 인식이 점차 확산되고 있으며 사용자 인증 및 보안 유지에 대한 요구가 증가함에 따라 정보보호를 위해 다양한 기능을 수행할 수 있는 대체수단이 필요하게 되었다. 따라서 최근에는 정보들을 안전하게 관리하기 위한 방법으로 휴대가 가능하며 물리적, 전기적 그리고 소프트웨어적인 공격으로부터 안전하다고 알려진 스마트카드 시스템이 주목을 받고 있다[1,2].

스마트카드를 사용하는 가장 큰 목적은 카드 내에 저

* 학생회원, 단국대학교 대학원 전자컴퓨터공학과
(Dept. of Electronics&Computer Engineering Graduate School, Dankook University)
** 종신회원, 서일대학 정보통신전공
(Dept. of Information and Communication Engineering, Seoil College)
접수일자: 2005년1월13일, 수정완료일: 2006년3월15일

장된 사용자 데이터를 안전하게 보호하는 것으로, 현재까지 스마트카드는 컴퓨터 시스템에 대한 정보보호 기술만을 제공해 왔으나 자바 언어를 스마트카드에 적용한 자바카드는 스마트카드의 정보보호 특성을 그대로 보존할 뿐만 아니라 카드를 하나의 새로운 응용 플랫폼으로 활용할 수 있도록 하였다. 자바카드는 개별 스마트카드 하드웨어에 구애받지 않는 통일된 개발환경을 구축하고, 다수의 애플릿이 하나의 카드 내에서 보안상의 충돌 없이 공존할 수 있어 카드 애플리케이션 개발에 있어서 가장 효과적인 방법으로 자리 잡게 되었다. 기존의 스마트카드는 기본적으로 하나의 사용자만이 사용가능하나 자바카드는 카드의 메모리 증가로 여러 개의 PIN과 다양한 애플릿을 사용하여 다수의 사용자가 하나의 카드를 이용하는 경우가 발생하여 사용자 인증 및 각 사용자의 접근을 제한하는 통제시스템이 중요하게 대두되고 있다[3-5]. 사용자 인증을 위해서 패스워드 또는 PIN(Personal Identification Number)을 이용한 방법이 가장 일반적으로 사용되고 있다. 그러나 고의 및 강제에 의한 유출 및 망각 등에 대한 문제점으로 이를 해결하기 위하여 사용자의 지문, 얼굴모양, 음성, 온라인 서명 등의 생체인식 기술을 이용한 사용자 인증 방법이 제안되었다[6,7].

본 논문에서는 정보의 안전성을 더욱 강화하기 위해 자바카드를 이용하여 하나의 카드에 여러 사용자를 인증하기 위하여 PIN의 단점을 보완한 생체인식의 방법 중 개인의 서명을 검증하는 서명데이터(signature)를 이용한다. 서명은 오래된 습관적인 행위로서 본인의 의지가 아니면 유출되거나 수행되기 어려운 개개인의 고유한 행위적인 특징으로 절도나 누출에 의해 전달될 수 없으며, 변경이나 분실이 어려운 장점이 있다. 따라서 이러한 서명데이터를 PIN과 사용하여 신뢰성이 높은 사용자인증 보안시스템을 구현하였으며 여러 사용자가 하나의 카드에 접근 하여 사용하기 때문에 이러한 시스템의 접근 시 사용자의 권한등급에 따라 카드자원의 접근을 제어하는 시스템을 설계 및 구현한다.

## Ⅱ. 관련기술

### 1. 스마트카드

스마트카드는 카드 내에 CPU를 내장한 것으로 스마트카드 내의 메모리는 재 프로그래밍이 가능하고 하나의 카드에서 여러 개의 애플리케이션 들이 사용될 수 있다. 카드는 저장매체로서의 기능뿐만 아니라 키 페어

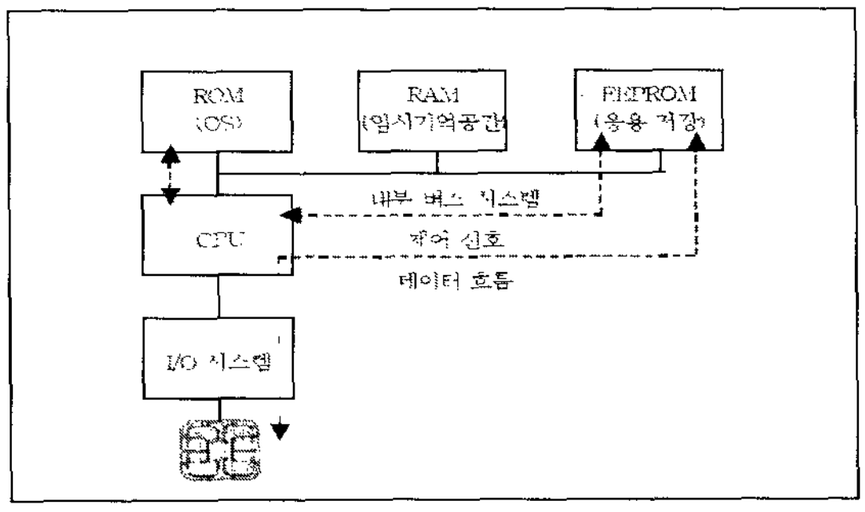


그림 1. 스마트카드 구조
Fig. 1. Architecture of smart card.

의 개발, 디지털 서명의 인증 그리고 데이터 보호역할을 하는 역할도 수행 할 수 있다. 스마트카드 COS(Card Operating System)는 마이크로프로세서에 내장되어 있는 시스템 프로그램으로서 응용 프로그램의 H/W 접근을 가능하게 할뿐만 아니라 스마트카드의 기본적인 기능을 결정한다[1,2]. COS의 주된 기능은 카드와 단말기 사이의 데이터 송수신, 명령어 수행 및 제어, 데이터 관리 그리고 암호 알고리즘 등을 수행 한다. COS는 각각의 응용 분야 개별적으로 개발되어져 있어 활용분야에 맞추어 작성된 스마트카드 애플리케이션이 필요하게 된다. 그러나 카드가 발급된 이후에는 스마트카드 애플리케이션을 업그레이드 하거나 추가하기가 쉽지 않다[8,9].

### 2. 자바카드

자바카드는 일반적인 스마트카드의 단점을 보안하기 위한 카드로 운영체제인 COS위에 JCVM(Java Card Virtual Machine)이 내장된 구조로 플랫폼 독립적이고 다중 애플리케이션을 수행할 수 있는 장점을 가지고 있다[4-7]. 자바카드는 그림 2에서 보는 것처럼, 자바카드 API(Application Programming Interface)와 JCVM으로 이루어진 자바카드 수행환경(JCRE:Java Card Runtime Environment), COS, Applet 등으로 구성된다[4][5][8].

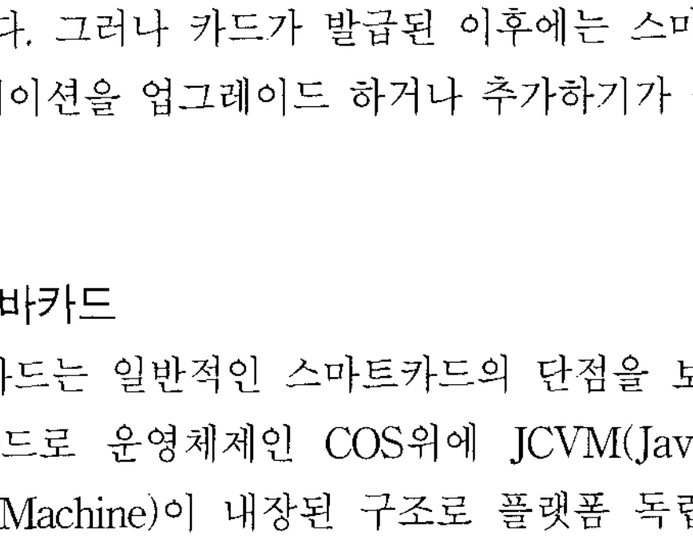


그림 2. 자바카드 구조
Fig. 2. Architecture of Java card.

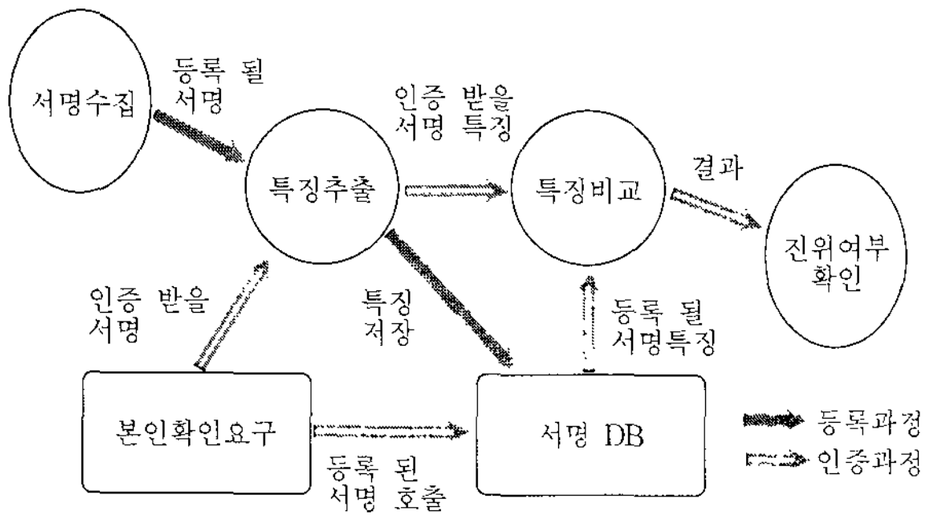


그림 3. 서명 인증 시스템
Fig. 3. Signature authentication system.

### 3. 서명인식

서명 인식 시스템은 전자펜 또는 Stylus펜을 이용하여 입력된 개인의 특성을 검증하는 것으로 서명의 특징(모양, 속도, 필압, 획 순서 등) 정보를 비교 분석하여 본인 여부를 확인하기 위해 등록 과정과 인증 과정으로 구성된다. 카드 사용 시 사용자의 서명데이터가 입력되면 전처리, 특징 추출, 참조서명 DB구축, 비교, 진위판별의 과정으로 사용자 인증과정을 거치게 된다. 그림 3은 서명 인증 시스템의 구조도를 나타낸다[6,7].

### 4. 사용자 인증

사용자 인증 메커니즘은 다음의 세 가지 개념에 기초를 두고 있다.

① 인증 요구자는 암호, 또는 PIN 등 자신이 알고 있는 정보를 제시하고자 한다.
② 인증 요구자는 인증서나 스마트카드 등에 저장된 개인키(private key)를 보여줄 수도 있다.
③ 변하지 않으면서 확인이 가능한 음성, 지문 등을 이용하여 정당한 사용자인지를 구별할 수 있다.

이 중 두 가지 이상의 방법을 이용하여 인증을 수행함으로써 보안성을 한층 강화시킬 수 있다[7][9].

### 5. 접근권한

시스템 자원에 대한 접근통제와 각 자원에 대해 기밀성, 무결성, 가용성 등의 보안 서비스를 하는 것을 접근통제 시스템이라 하며, 접근통제 시스템은 사용자에 대한 접근제한 조건을 두어 관리한다[10,11].

## Ⅲ. 제안 방법 및 설계

### 1. 제안 방법

본 논문에서 제안하는 방법의 전체적인 시스템은 자바카드를 기반으로 하여 휘트니스 스포츠 센터를 대상으로 하며 카드 사용자는 카드를 발급받은 사용자, 스포츠센터 관리자, 각 운동별 트레이너로 제한한다.

#### (1) 시스템 구성

본 논문에서는 자바카드를 이용하여 서명데이터와 PIN으로 사용자 인증을 수행한 후 다중 사용자의 접근을 제한하는 시스템을 설계하였다. 그림 4는 본 논문에서 제안한 휘트니스 센터의 사용절차를 나타낸다.

카드 사용자는 관리자에게 카드발급을 요청하고 클럽은 카드 사용자의 신원을 인증한 후 사용자의 데이터와 함께 카드를 발급한다. 그리고 운동 종목별 트레이너에게 사용자의 운동내용을 지시하고 사용자는 운동량을 요청한다. 트레이너는 사용자의 카드에서 사용자 정보를 읽은 후 운동을 처방하여 카드에 넣을 수 있게 관리자에게 권한을 요청한다. 관리자는 트레이너의 처방을 확인 후 운동에 관한 내용을 수시로 체크 및 관리할 수 있는 권한을 설정한다. 트레이너는 권한을 부여 받은 후 사용자의 카드에 운동량을 처방하여 사용할 수 있도록 한다. 사용자는 이러한 처방내용과 함께 발급된 카드를 클럽에서 사용한다. 표 1은 카드 사용자와 사용 방법을 나타내고 있다.

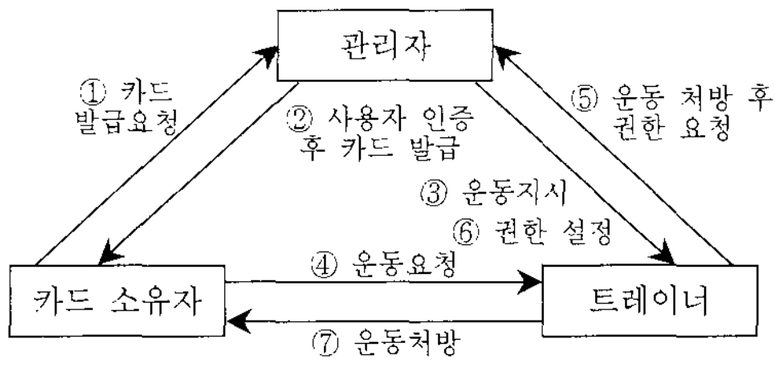


그림 4. 카드 발급 및 사용절차
Fig. 4. Card issuing and use procedure.

표 1. 카드 사용자 및 사용 방법
Table 1. Card user and use method.

| 사용자 | 사용 방법 |
|---|---|
| 일반 회원 (카드 소지자) | 출 입 문 : 센터회원임을 확인<br>라 커 : 물품보관 및 도난방지<br>운동 기구 : 처방별 운동량 셋팅<br>회 비 : 클럽의 회비내역<br>본인 정보 : 본인정보 열람 및 운동처방 열람<br>부대 시설 : 사워 및 센터의 시설이용 |
| 관 리 자 | 사용자인증 : 등록 시 회원을 인증<br>사용자관리 : 카드 사용자의 지속적인 관리<br>회 비 : 등록과 함께 회비 산출하여 데이터 관리 |
| 트 레 이 너 | 운동 처방 : 회원의 정보를 통한 운동처방<br>사용자관리 : 회원의 지속적인 관리 |
| 총 무 과 | 회 비 : 등록과 함께 달별, 혹은 연별로 회비 정산 |
| 센 터 | 사용자인증 : 등록 |

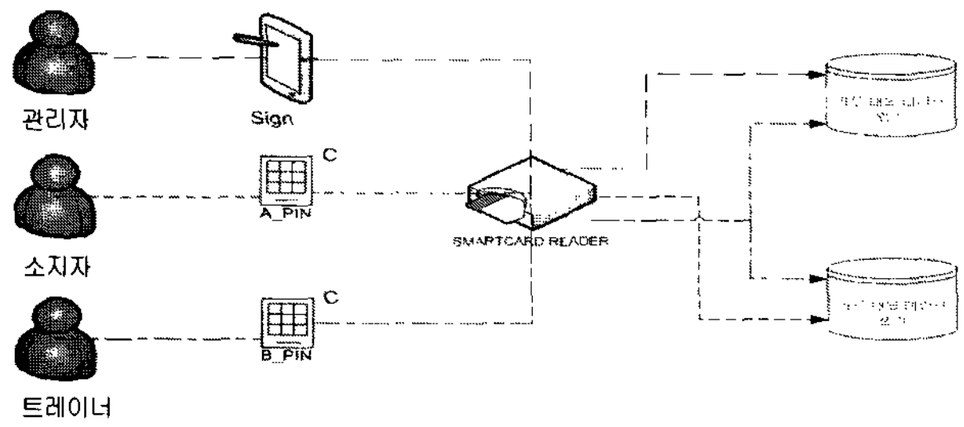


그림 5. 사용자 인증
Fig. 5. User Authentication.

(2) 서명을 이용한 사용자 인증

본 논문에서는 PIN을 이용한 사용자 인증 방법을 서명을 이용하여 PIN과 함께 동시에 사용하였다. 서명은 개인 고유의 특성이기 때문에 복제가 어렵고 공유가 거의 불가능하기 때문에 본인 이외의 다른 사람이 도용하는 것을 막을 수 있다. PIN 인증은 카드 내에서 수행되며, 사용자 서명의 인증은 그 알고리즘의 복잡성과 프로그램의 크기 문제로 외부에서 수행되고 이를 위한 프로그램은 상용제품을 사용하여 처리된 서명데이터를 PIN과 함께 사용자 인증을 위해 사용하였다. 그림 5는 사용자 인증과정을 나타내고 있다.

(3) 파일 접근제어

다수의 사용자가 하나의 시스템에 접근하는 시스템에서는 사용자들의 요구사항에 대한 효율적인 관리가 필요하다. 사용자의 정보관리와 정보에 대한 접근을 위하여 PIN과 서명을 이용한 사용자 인증이 이루어진 후에는 시스템 자원과 정보에 접근하기 위하여 사용자의 ACL(Access Control List)등급에 따라 접근 권한을 부여하며 표 2에 접근권한 유형을 나타내었다.

표 2. 제안 시스템의 접근 권한
Table 2. Access authority of proposed system.

| | 관리자(A) | | | | 트레이너(T) | | | | 카드소지자(U) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 사용자 인증 Type | 개인식별데이터 (signature) | | | | 개인식별번호 (PIN) | | | | 개인식별번호 (PIN) | | | |
| 권한유형 | a | r | w | d | a | r | w | d | a | r | w | d |
| 개인정보 | o | o | o | o | o | o | x | x | o | o | o | x |
| 운동정보 | o | o | x | x | o | o | o | o | o | o | x | x |
| 회비정보 | o | o | o | o | x | x | x | x | o | o | x | x |
| A : 관리자, T : 트레이너, U : 카드소지자 | | | | | | | | | | | | |
| a: Access, r: Read, w: Write, d: Delete | | | | | | | | | | | | |

(4) APDU(Application Protocol Data Unit)

단말기와 카드 사이에 전송되는 명령어 메시지나 응답 메시지를 포함하는 기본 단위로써 데이터를 포함한다. 본 논문에서 사용된 명령어는 ISO-7816 명령어 표준을 따르고 있다. 하지만 본 논문에서는 PIN과 서명 데이터를 이용하고, 카드 사용자에 따른 접근권한을 두어 애플릿(applet)을 설계하므로 ISO-7816 표준에 없는 새로운 명령어를 표 3과 같이 설계하였다.

표 3. APDU(Application Protocol Data Unit)
Table 3. APDU(Application Protocol Data Unit).

| 코드 | 값(HEX) | 비고 |
|---|---|---|
| CLA | 90 | 사용자 영역 |
| INS | 20 | PIN을 이용한 사용자1, 2 확인 |
| | 60 | 사용자 File 값 읽기 |
| | 62 | 사용자 File 값 업데이트 |
| | 70 | 운동정보 File 값 읽기 |
| | 72 | 운동정보 File 값 업데이트 |
| | 80 | 회비정보 File 값 읽기 |
| | 82 | 회비정보 File 값 업데이트 |
| | A0 | 사용자 인증된 값 구분, 확인 |
| | B0 | 서명 File 값 읽기 |
| | D0 | 서명 File 값 업데이트 |
| | F0 | 서명 값 비교, 확인 |
| Applet-specific status words | 6300 | 인증실패 |
| | 6301 | PIN 값 확인 실패 |
| | 9400 | 서명 값 확인 실패 |
| 표 APDU 설계 | | |

## Ⅳ. 시스템 구현

### 1. 개발환경

표 4. 시스템 구현 환경
Table 4. System embodiment environment.

| 종류 | 세부사항 |
|---|---|
| 운영체제 | Window 2000 Server |
| 개발도구 | J2se verson 1.2.2<br>Java(TM) Communications API specification2.0<br>Java_card_kit_2_2_1<br>서명등록 및 인증 프로그램<br>SMARTCAFE. PROFESSIONAL Toolkit V2.0 |
| 개발언어 | Applet : Java, Application : Visual Basic |
| 카드 | Jcop 2.0, Smartcafelife(G&D) |
| 단말기 | SCRx31 CCID, PCT2000(G&D) |
| 타블렛 | 디지타이져(WACOM) |

### 2. Applet 구현결과

카드와 단말기 사이의 접속은 항상 인증 단계를 요구하고 TCP/IP 프로토콜을 이용하여 제안된 서명 및 다중 PIN을 이용한 접근권한 시스템과 통신 한다. 사용자는 관리자, 일반사용자, 트레이너로 식별데이터를 이용하여 접근하는 파일 시스템을 애플릿으로 구현하였다. 기존의 PIN 사용자 인증은 자바카드에서 지원하는 API에 구현되어 있으나 본 논문에서는 서명데이터를 이용하기 때문에 서명데이터를 저장하고 비교할 공간을 필

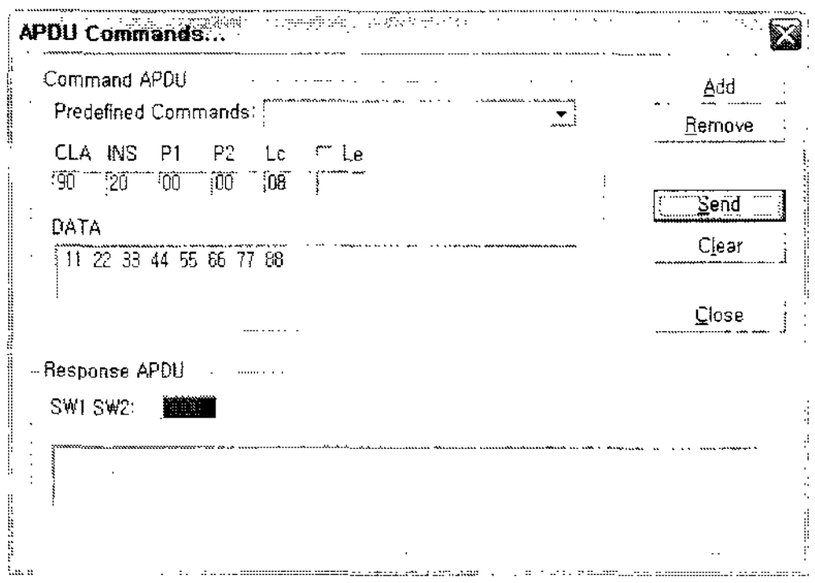


그림 6. PIN의 사용자 인증
Fig. 6. User Authentication of the PIN.

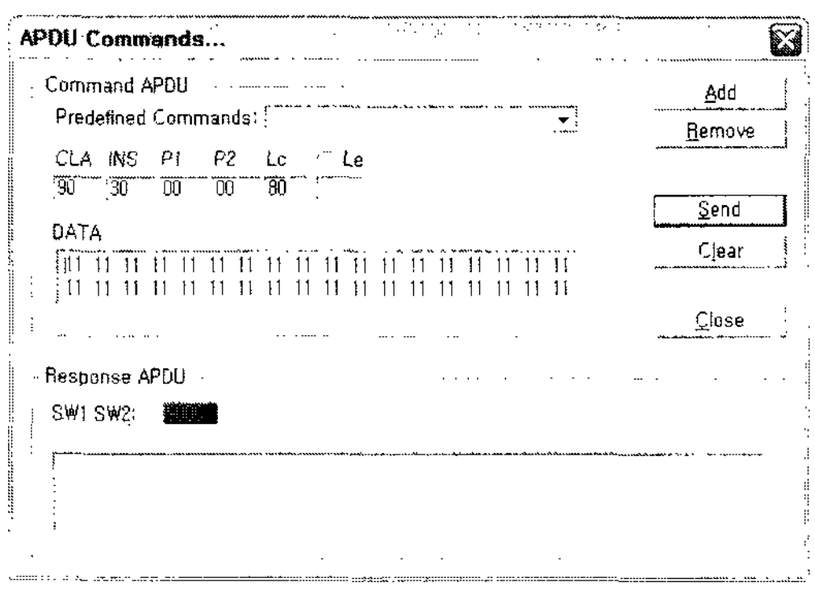


그림 7. Sign의 사용자 인증
Fig. 7. User authentication of the sign.

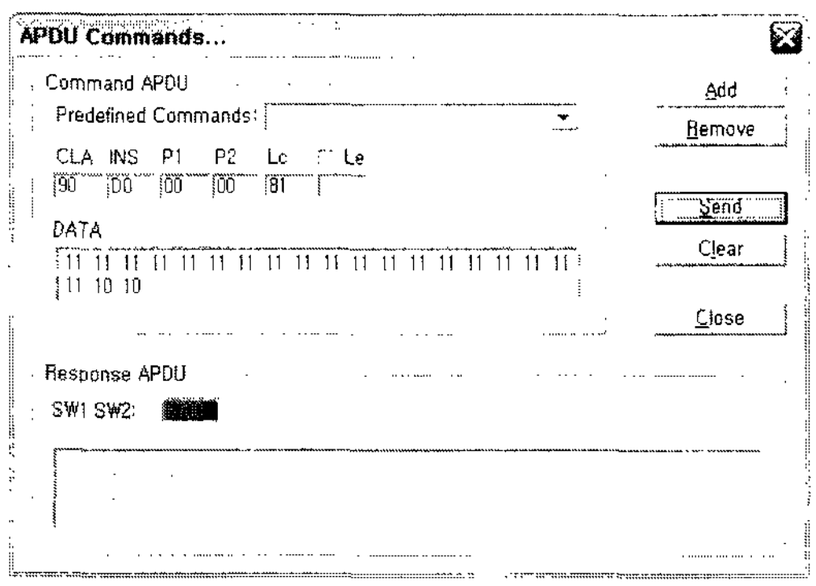


그림 8. 인증 후 파일 read
Fig. 8. Authentication after file read.

요로 하여 카드 내의 사용자 서명데이터 비교를 위해 서명데이터의 공간을 각각 4Kbyte로 나누었으며 PIN 저장을 위해 서로 다른 PIN 데이터 공간 8byte를 설계하였고 추가될 임의의 데이터를 위해 2Kbyte의 데이터 공간을 설계하였으며 서명 데이터는 128byte씩 읽어서 비교한다. 애플릿에서 사용되는 APDU는 PIN과 서명데이터가 서로 다른 데이터 공간을 사용하기 때문에 구분하여 지정하였으며 이러한 데이터 공간과 앞에서 설명한 개념을 이용하여 서명데이터 및 다중 PIN을 이용한 사용자 인증 부분을 구현하였다.

그림 6과 7은 PIN과 서명의 사용자 인증이 이루어지

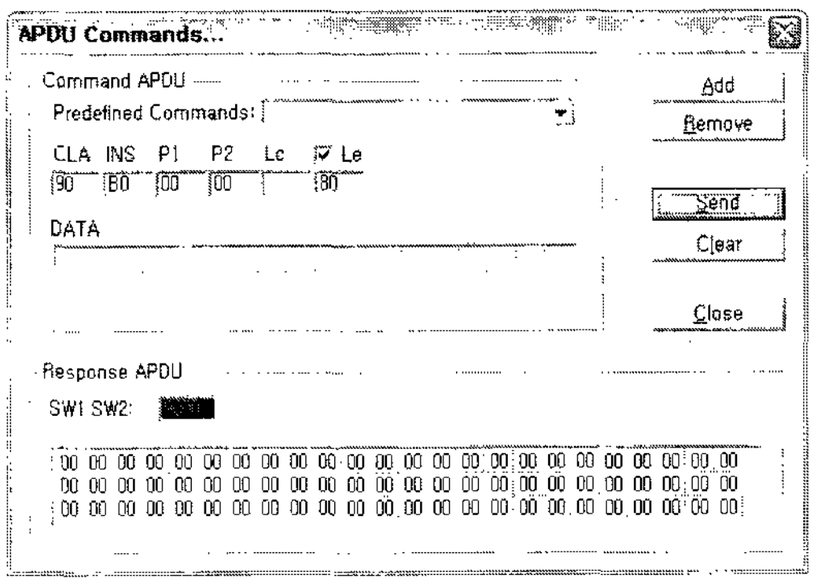


그림 9. 인증 후 Write 할 수 없음
Fig. 9. Authentication after file can not Write.

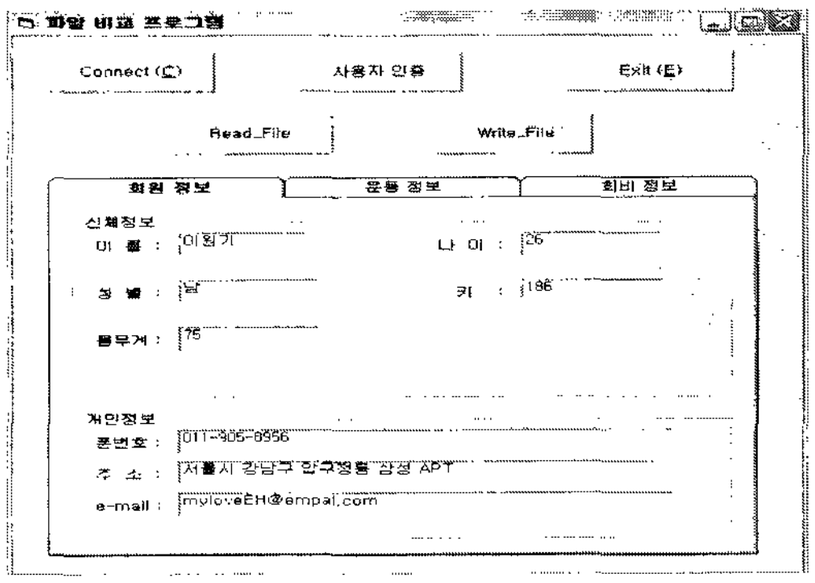


그림 10. 실행 결과
Fig. 10. Execution result.

는 결과를 나타낸다.

그림 9는 인증이 이루어진 사용자에게 접근 권한이 이루어져 파일을 Read할 수는 있고, Write할 수는 없는 화면이다. 이렇듯 사용자가 완벽하게 인증된 후에 파일에 대한 권한을 얻을 수 있다. 이러한 애플릿을 구현한 후 사용자가 보다 쉽고 다양하게 사용하기 위하여 응용 프로그램을 구현하였으며 프로그램을 실행하면 카드 Connect를 지시하는 창이 나온다. 그림 10은 구현된 애플릿을 실행한 화면을 보여준다.

## V. 결 론

본 논문에서 제안한 시스템은 스마트카드의 차세대 IC카드로 주목받는 자바카드를 이용하여 구축하였다. 자바카드 기술은 자바 언어를 이용하여 스마트카드를 사용이 편리한 개방형 애플리케이션 개발 구조를 제공한다. 따라서 하드웨어에 독립적으로 효율적인 애플리케이션 프로그램을 개발할 수 있다. 본 논문에서 제안한 방법은 자바카드를 사용하여 기존의 PIN과 생체인식정보의 하나인 서명데이터를 이용하여 사용자 인증을 수행 하였다. PIN 비교, 다중 PIN 비교 그리고 서명을

비교하기 위하여 각각의 메모리를 할당하여 이를 비교하여 인증하였으며 이러한 인증 및 카드내의 데이터의 READ, WRITE, UPDATE, DELETE의 과정을 사용자가 보다 쉽고 다양하게 하기 위하여 응용 프로그램을 구현하여 사용하였다. 이러한 인증 후에는 ACL의 등급에 따라 각 사용자의 권한을 제어하여 사용자가 마음대로 파일을 취할 수 있는 약점을 보안하였다. 이러한 연구의 결과로 PIN이 가지는 보안상의 취약점을 해결하였고, 사용자의 접근권한을 적용함으로써 개인정보의 안전성과 신뢰성을 보장하는 것을 확인하였으며 사용자의 편의를 위한 응용 프로그램은 여러 애플리케이션을 실제로 활용할 수 있는 기반을 제공하였다.

향후 사용자 인증을 위한 PIN을 서명데이터만이 아닌 다양한 생체정보를 적용하여 사용자 인증을 가능하게 함으로써 다양한 생체인식 기술을 추가할 수 있는 유연한 구조의 설계가 수행되어야 할 것이고, 접근권한을 보다 다양하게 하여 여러 시스템으로의 확장이 가능한 방법에 대한 연구가 수행되어야 할 것이며 이를 위해 스마트카드에 저장될 다양한 애플리케이션의 국제적인 규격과 개발이 뒷받침되어야 할 것이다.

## 참 고 문 헌


[1] Jose Luis Zoreda Jose Manuel Oton, "Smart cards," Artech House, 1994.

[2] Wolfgang Effing and Wolfgang Rankl, "Smart Card Handbood," Jahn Wiley & Sons, 2000.

[3] Patrice Peyret, "Java Card Technology for Smart Cards Architecture and Programmer's Guide," April, 2000.

[4] E. Vetillard, "Tools for Integrating the Java CardTM API into Jini™ Connection Technology," javaoneconf., 2000.

[5] Zhiqun Chen, "Java Card Technology for Smart Cards," Addison-Wesley, pp.42-77, 2000.

[6] C. P. Schnorr, "Efficient Signature Generation by Smart Cards", Advances in Cryptology Crypto'89, Lecture Notes in Computer Science, G. Brassard (ed.), Berlin Springer-Verlag, Vol.435, pp.239-252, 1990.

[7] J. Bigun, "Multi-modal Person Authentication," Face recognition, Sringer-Verlag, pp.26-50, 1997.

[8] 윤치영, 염희균, 전성익, 황선명, "자바카드 애플릿의 검증 방법에 관한 연구", 정보처리학회 춘계학술대회, Vol.9, No.1, pp.489-492, 2002.

[9] 임영이, 이윤철, 강회일, 이동일, "스마트카드 시스템의 보안 기술", 전자통신동향분석, 제14권 5호, pp.42-54, 1999.

[10] 강세나, 이기한, "IC 카드에 의한 원외 전자처방전 보안을 위한 시스템 구축", 정보처리학회 논문지, Vol.C, No.3, pp.281-286, 2003.

[11] 백장미, 강병모, 홍인식, "Java Card를 이용한 마일리지 통합관리 시스템 구현", 정보과학회 학회지, Vol.28, No.2, pp.214-216, 2002.


## 저 자 소 개


구 은 희(학생회원)

2002년 단국대학교 전자컴퓨터 공학부 학사 졸업.

2004년 단국대학교 전자컴퓨터 공학과 석사 졸업.

2006년~현재 단국대학교 전자컴퓨터공학과 박사과정.

<주관심분야 : 정보보호, 네트워크보안, 자바카드, 스마트카드 보안>

우 찬 일(종신회원)

1993년 단국대학교 전자공학과 학사 졸업.

1995년 단국대학교 전자공학과 석사 졸업.

2003년 단국대학교 전자공학과 박사 졸업.

2004년~현재 서일대학 정보통신전공 교수.

<주관심분야 : 디지털 워터마킹, 정보보호 시스템, 스마트카드 보안, 데이터베이스 보안>