# 서명을 이용한 스마트카드 사용자 인증

송영상*, 신인철**, 이완석***, 손법수***
*단국대학교 전자컴퓨터 공학과
**단국대학교 전기전자컴퓨터 학부
***(주)패스싸인
E-mail : yssong@dankook.ac.kr

# User Authentication in Smart card Using Signature

Young-Sang Song*, In-Chul Shin**, Wan-Suck Lee***, Byub-Soo Son***
*Dept. of Electronic and Computer Engineering, Dankook University
**School of Electrical and Electronic and Computer Engineering, Dankook University
***Corporation Passsign

요 약

최근 개인의 정보보호에 관한 관심이 높아져 가고 있으며 자신의 정보보호를 위해 스마트카드가 사용되어지고 있는 추세이다. 기존의 스마트카드는 카드 주체를 확인하는 과정으로 PIN(Personal Identity Number) 제출을 요구한다. 본 논문에서 이러한 사용자의 확인 과정에 사용되는 PIN 대신 생체인식 중 서명을 스마트카드에 저장하였으며 이를 이용하여 사용자 인증을 위한 시스템에 대해 연구하였다. 본 논문은 스마트카드의 패스워드의 분실이나 강제에 의한 도용을 방지하고, 사용자에 좀더 익숙하고 안전한 서비스를 보장 받게 될 것이다.

## 1. 서론

최근 인터넷 및 정보 통신의 발달로 인해 개인 정보 보호에 관심이 높아져 가고 있는 추세이며, 자신의 정보를 보호하기 위한 많은 제품 및 연구가 되어지고 있다. 스마트카드는 일반 플라스틱 카드에 마이크로프로세서와 메모리 시스템을 내장하고 있는 칩을 가지고 있다. 그러므로 자체적인 계산 능력과 데이터 저장 능력을 가지며 이로 인해 뛰어난 보안성과 응용 능력을 이용하여 개인 신분 증명, 접근제어 등 금융 분야 및 여러 응용 분야에서 활발히 사용되고 있다.

다양한 분야의 정보보호 시스템의 효율적인 지원을 위해 스마트카드 내부의 메모리에는 운영체제가 내장 되어 있다. 카드운영체제(COS : Card Operating System)는 파일 관리, 데이터 통신, 보안 시스템을 내장하여 암호 알고리즘 수행, 데이터 무결성, 사용자 인증, 단말기와 카드간의 상호 인증을 위한 보안 모듈을 가지고 있다. 그러나 스마트카드의 사용자 확인을 위한 사용자의 패스워드의 분실 및 강제에 의한 패스워드 도용을 방지 하기는 힘들다.

본 논문에서는 기존의 스마트카드의 사용자 확인을 위한 패스워드 대신 자신만이 지닐 수 있는 데이터 즉 생체 인식 중 서명을 이용하여 스마트카드 사용자 인증 시스템을 연구 개발 하였다. 서명 시스템은 전자펜 또는 Stylus을 이용하여 입력된 개인의 특성을 검증하는 것으로써 서명의 모양, 속도, 필압, 획 순서 등의 특징 정보를 통합하고 비교 분석하여 본인 여부를 확인하기 위해 등록과정과 인증 과정으로 구성된다. 발급 과정에서는 사용자의 특징 데이터를 통합하여 스마트카드 메모리에 저장하였으며, 인증 과정에서는 카드에 저장 되어있는 사용자 특징 데이터를 받아 사용자 인증을 하게 된다. 이때 터미널과 카드간의 프로토콜은 ISO 7816에 따르며, 3DES를 이용하여 암호 하여 데이터를 송수신하게 된다.

본 논문에서 제안하는 서명을 이용한 스마트카드 사용자 인증 시스템은 사용자가 패스워드의 분실 및 불법 도용에도 안전하며, 편리하게 사용할 수 있을

것이다.

## 2. 서명 인증 시스템

서명 인증 시스템은 전자펜 또는 stylus펜(PDA용)을 이용하여 입력된 개인의 특성을 검증하는 것으로써 서명의 특징 즉 모양, 속도, 필압, 획 순서 등의 정보를 통합하여 비교 분석하여 본인 여부를 확인하게 된다. 이를 위해 크게 등록 과정과 인증 과정으로 구성된다.

등록 과정은 3번의 서명을 입력하여 추출된 개인의 고유한 특징 파라미터를 통합한 데이터를 등록하게 된다. 사용자가 본인 확인을 받고자 할 때는 자신의 서명을 입력하여 입력된 데이터와 등록된 서명 데이터를 비교하여 본인 여부를 확인하는 인증 과정을 거치게 된다. 다음은 서명의 등록 및 인증처리 단계를 보여주고 있다.

### 2.1 전처리(Preprocessing)

진 서명(Genuine Signauture)과 가 서명(Forgery)을 효과적으로 구별할 수 있는 특성벡터를 추출하기 위하여 특성벡터 추출전의 모든 과정을 말하는 것으로 정규화(normalize), 분할, 잡음(noise) 제거, 기울임 보정 등이 있다.

### 2.2 특징 추출(Feature Extraction)

어떤 서명을 특성화하기 위하여 선택된 특징을 추출하는 과정으로, 진 서명으로부터 고유한 특징을 추출하여 거짓 서명을 구별할 수 있는 특징 파라미터들을 추출한다.

### 2.3 참조서명 구축

한 사람의 참조 서명 DB를 구축하기 위해서는 여러 개의 서명 샘플로부터 추출한 특징 정보를 가지고 등록할 데이터를 만들게 된다.

### 2.4 비교(Comparison)

어떤 사람이 본인 확인을 요청하면서 서명을 수행하게 되면, 그 사람의 특징들이 요구된 참조 서명 데이터 즉 특징들과 비교하게 된다. 일반적으로 두개의 특성들 사이의 유사도(Similarity)를 비교하기 위해 거리측정법(Distance Measure), Neural Network, DP matching 등의 방법이 사용되고 있다.

### 2.5 진위판별(Decision Making)

만약에 위에서 구한 거리가 정해진 임계 값보다 작으면 서명 인증 시스템은 사용자를 인증하고, 그렇치 않으면 사용자 인증이 거부된다.

다음 그림 1.은 서명 인증 시스템의 구조도이다.

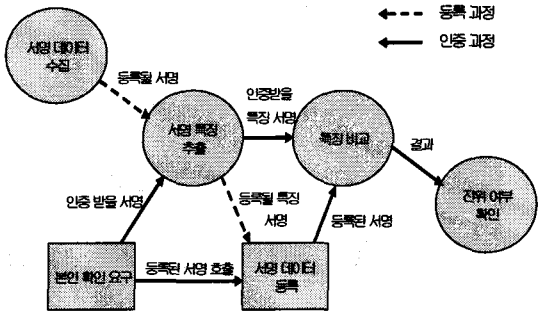


그림 1. 서명 인증 시스템

## 3. 스마트카드의 파일 구조

스마트카드의 파일 시스템은 기본적으로 부르는 명칭만 틀릴 뿐 DOS의 계층적인 파일 시스템과 아주 유사하다. 파일 구조는 가장 상위 루트에 속하는 MF(Master File : 3F00)있다. 그 밑에 보조 디렉토리 역할을 하는 DF(Dedicate File)는 한 개 이상의 기본파일 EF(Elementary File)들을 포함 하고 있다. MF 밑에 EF파일의 계층을 전역계층(Global level)이라하고, MF 밑에 DF와 그 밑의 EF파일의 계층을 전역 계층(Local Level)이라한다. 그림 4.은 스마트카드의 파일 구조를 보여주고 있다.

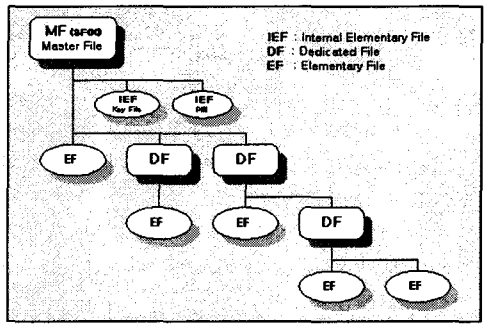


그림 4. 스마트카드의 파일 구조

## 4. 스마트카드 보안 메커니즘

스마트카드의 보안 메커니즘은 파일 권한을 제한하는 Access Control, 카드의 주체를 확인하는 패스워드(PIN), 단말기와 카드 간의 송수신되는 데이터 암호/복호화를 위해 Session Key생성, 단말기가 단

말기의 랜덤 넘버를 카드에 보내 카드를 인증하는 절차로 내부인증, 카드의 랜덤 넘버를 받아 단말기에서 처리된 응답값으로 카드가 단말기를 인증하는 외부 인증, 데이터 암/복호화, MAC(Message Authentication Code)로 이루어져 있다.

4.1 AC(Access Control)

파일에 대한 파일 권한을 제한하게 된다. Access Control은 다음과 같이 파일 헤더에 AC1, AC2의 접근 권한이 존재한다. 접근권한마다 그 권한에 적용되는 명령이 구분되어 있다. 그림 2.는 Access Control의 파일이 정의 되어 있다.

| 1st Byte | | | | | | | |
|---|---|---|---|---|---|---|---|
| b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 |
| Lock | PIN | Mode | SFI | | | | |

그림 2. Access Control 정의

- Lock : set 또는 1이면 카드 자체 access를 금지 한다.
- PIN : 0 - 파일 보호 및 제한하지 않음
  1 - key 또는 secret code에 의해 파일 보호
- Mode : 0 - Global Level, 1 - Local Level

4.2 패스워드(PIN)에 의한 사용자 인증

스마트카드를 발급할 때 사용자 패스워드를 메모리에 저장하게 된다. 카드를 사용할 때 사용자는 패스워드를 제출하게 된다. 패스워드가 암호화 하여 전송되면 카드는 패스워드를 복호화 하여 카드 메모리에 저장되어 있는 패스워드랑 비교하게 되며 일치하면 카드는 단말기에 사용자 인증 응답을 전달해 주게 된다. 이러한 과정을 통해 사용자는 자신의 카드에 사용 권한을 얻게 된다.

## 5. 서명을 이용한 스마트카드 사용자 인증

서명을 이용한 스마트카드 사용자 인증은 크게 두 부분으로 나뉘게 된다. 우선 사용자 등록을 하는 과정과 등록된 사용자의 확인을 하는 사용자 인증과정이다. 데이터의 기밀성을 유지하기 위해 블록암호 알고리즘 3DES를 사용한다.

5.1 사용자 등록 과정

서명 프로그램을 사용하여 사용자는 자신의 ID로 3번의 서명을 실행 자신의 특징 데이터를 추출하게 된다. 추출된 데이터는 4KByte의 크기이고, 스마트카드에 저장하게 된다. S3C89K8의 스마트카드용 Target Boards를 사용하였으며, EEPROM은 8K의 크기를 가지고 있다. 본 논문에서의 파일 구조는 가장 기본 틀을 갖는 파일 구조로 COS를 설계하였으며, 서명데이터를 저장하기 위한 EF파일을 지정된 Local Level에 두었다. 그림 5.는 사용자의 등록 과정과 추출된 특징 데이터를 보여 주고 있다.

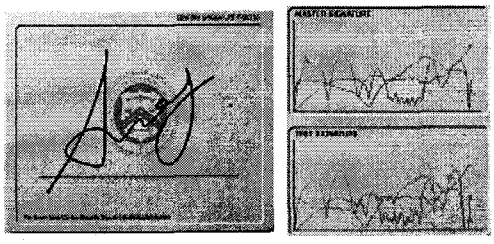

그림 5. 사용자 등록 및 특징 추출데이터

위와 같은 과정을 통해 추출된 데이터는 3DES로 암호화 되어 전송되며 카드 내에서 복호화 하여 카드에 저장 되게 된다. 그림 6.은 암호화된 서명데이터를 카드에 전송하여 기록하는 과정으로 C++ Builder5.0 로 프로그래밍 하였다.

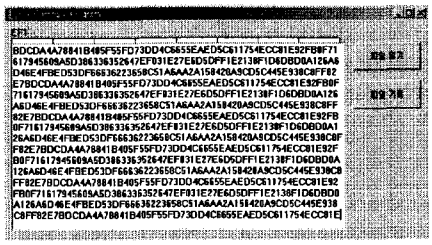

그림 6. 카드에 서명 데이터를 쓰는 과정

5.2 사용자 인증 과정

등록 과정을 통해 스마트카드를 지닌 사용자가 자신의 카드의 주체 확인을 하는 절차로 카드에 대한 권한을 얻기 위해 서명을 하게 된다. 이때 카드는 데이터 보안을 위해 단말기와 세션키 생성하여 서로 공유하는 과정을 거치게 된다. 사용자가 제출한 서명 데이터와 카드에 저장되어 있는 데이터를 암호화 하여 단말기에 전송 하게 된다. 단말기는 암호화 된 데이터를 복호화 하여 비교하게 된다. 미리 정해 놓은 임계 값 보다 작으면 사용자 인증이 이루어지고, 높으면 재 서명 요구 및 사용자 인증을 거부하게 된다. 그림 7. 사용자가 서명을 하고 카드에서 전송된 서명

데이터와 비교하여 임계값에 의해 사용자 인증이 이루어진 화면을 보여 주고 있다.

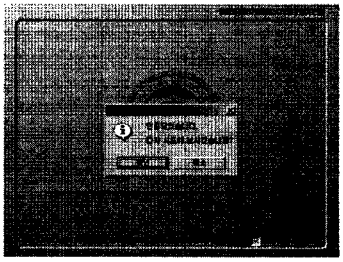

그림 7. 사용자 인증

## 6. 결론

최근 사용자의 주체 확인과 개인 정보보호를 위해 위해 생체인식 및 보안성이 우수한 스마트카드에 관심이 높아져 가고 있다. 스마트카드는 마이크로프로세서가 내장된 카드로 기존의 마그네틱카드보다 많은 데이터를 저장할 수 있고, 자체적인 계산능력까지 갖추고 있는 소형컴퓨터라 할 수 있다. 운영체제가 탑재되기 때문에 카드 메모리의 사용과 관리에 대한 새로운 가능성을 제시하고 있다. 스마트카드 안에 저장된 데이터에 대한 읽기 및 쓰기 작업, 그리고 스마트카드와 외부와의 통신은 스마트카드의 물리적인 보안과 정교한 암호 기법을 통해서 엄격히 통제 보호된다. 그러나 기존의 카드는 패스워드로 주체 확인을 함으로써, 카드의 도난과 패스워드 분실 및 강제에 의한 패스워드 도용이라는 문제점이 있다.

본 논문에서는 변하지 않는 사용자의 생체인식을 이용함으로써 반영구적으로 사용가능하며, 사용자가 좀더 편리하고 안전한 시스템을 이용할 수 있게 될 것이다.

스마트카드의 표준인 ISO7816의 Part3, 4를 참조하여 기본 명령어 및 프로토콜을 구성하였으며, OPENice i500 Emulator와 Target Board로는 스마트카드 칩 S3C89K8을 사용하였다. 메모리 용량에 상당한 제약이 있는 한계로 인하여 서명 데이터 처리를 위한 비교 알고리즘을 직접 구현하기는 어려운 실정이다. 최근 스마트카드의 하드웨어 사양이 좀더 좋아져 가는 추세이므로 비교 알고리즘의 내장 및 공개키 암호 알고리즘을 이용한 시스템구성은 계속 연구되어 질 것이다.

## 참고 문헌


[1] Russ Housley, Tim Polk, "Planning for PKI", WILEY

[2] 이만영 외5명 공저, "전자 상거래 보안 기술", 생능출판사, 1999

[3] NASH, DUANE, JOSEPH, BRINK, "PKI Implementing and Managing E-Security", Mc Graw Hill

[4] 이민섭, "현대 암호학", 교우사

[5] W.Rankl, "Smart Card Handbook" 2ed, John Wiley & Sons, 1999.

[6] Cheol-han Park, Dae-wha Seo, "A Design of Expandable IC Card Operating System", 통신 정보보호학회 논문지 제9권, 제2호, 1999.

[7] Smart Cards and Security Overview, http://www.smartcardbasics.com /

[8] 이장원, 홍기융, 조현숙, "스마트카드를 이용한 네트워크 가입자 신분 확인", 한국정보처리학회 논문지 제3권 제5호, pp.1170-1178, 1996.

[9] GEMPLUS, GPK4000 Reference Manual, GEMPLUS CEDEX, 1997.

[10] GEMPLUS, GPK4 Reference Manual, GEMPLUS, 1999.

[11] CHAN, Siu-cheung Charles, "An Overview of Smart Card Security"

[12] 이경호, 차영태, 심주걸, 원동호, "직접적인증을 제공하는 안전하고 효율적인 키동의 프로토콜", 한국정보처리학회 논문지, 제6권 제12호, pp.3613-3621, 1999.

[13] 김진형, "온라인 서명 검증의 현황 및 방법론 소개", KAIST, 2001

[14] 원지연 외4, "iC 카드를 이용한 생체인식 기술 개발 동향", 한국전자통신연구원.

[15] "암호와 보안 프로토콜", SoftForum, http://www.softforum.com