韓國 OA學會 論文誌
第4卷 第4號, 1999.12.

99-4-4-1-2

# 스마트 카드에 적합한 인증 프로토콜에 관한 연구

이 지 영*

# A Study on the Authentication Protocols Fitted for Smart Cards

Jie-Young Lee*

## 요 약

공개키 암호화 알고리즘을 사용하는 인증기법은 비밀키로 인증값을 생성하여 자신을 증명하고, 공개키를 통하여 검증하는 방법이다. 본 연구에서는 대칭형 암호화 알고리즘을 이용한 인증에서의 문제점이었던 비밀키의 분배 및 관리의 문제점은 해결하고 공개키 리스트에 대한 관리 문제를 인증센타를 통하여 인증서를 발급받는 형태의 방법을 제공하여 공개키 관리를 효율적으로 할 수 있는 알고리즘을 제시한다.

## Abstract

The authentication technique, which uses public key cryptographic algorithms, proves itself by generating authentication value through secret keys and gives verification by means of public keys.

This paper is believed to 1) solve the problem of distribution and management of secret keys, which still remain the problem of authentication used in symmetric cryptographic algorithm.

2) provide the method to receive a certificate of handling the problems of public key lists through the authentication authority, and finally 3) suggest an algorithm which will enable us to run the public keys more effectively.

* 세명대학교 컴퓨터과학과 교수
** 본 논문은 1997년도 세명대학교 교내연구비로 연구되었음.
논문접수:1999.7.30. 심사완료:1999.11.18.

## Ⅰ. 서 론

스마트 카드에서 사용되어지는 인증에는 크게 사용자 인증과 실체 인증의 두 가지로 구분된다. 사용자 인증은 스마트 카드의 소지자가 정당한 사용자라는 것을 PIN (Personal Identification Number)또는 지문과 같은 신체적 특징을 통하여 확인하여 불법으로 사용하는 것을 방지하기 위한 것이다.

실체 인증은 스마트 카드와 단말기간의 상호정당성을 증명하여 위조카드 또는 단말기의 사용을 통한 불법유출 및 변조를 방지한다. 기존의 실체 인증에 사용되어지는 알고리즘에는 연산부하가 적은 DES를 이용한 대칭형 암호화 알고리즘을 이용한 인증이 대부분이다.

그러나 이러한 대칭키 암호화 알고리즘은 비밀키의 분배 및 관리에 대한 문제를 내포하기 때문에 본 연구에서는 공개키 암호방식을 사용하여 빠른 속도와 적은 키 용량을 필요로 하는 스마트 카드를 이용한 인증 프로토콜을 제시한다.

## Ⅱ. 스마트 카드의 구조 및 특성

스마트 dimensions, 기계적 특성 및 전기적 인터페이스는 ISO규격 7816에서 규정하고 있으며 IC에는 5MHZ로 동작하는 마이크로프로세서가 내장되어 있으며 사용자 메모리는 8K이다. 일반적으로 CPU는 8bit이며 비동기식 입출력 방식을 사용하고 있으며 EEPROM에는 가입자의 자격, 고유번호, 난수발생기의 초기치를 암호화 했던 암호화된 형태의 키와 같은 서비스키들이 저장되며 RAM에는 복호화 알고리즘 등이 동작하면서 사용되는 데이터들이 일시적으로 저장되며 Masked ROM에는 카드의 운영프로그램과 복호화 알고리즘이 저장되어 있다.

이들 메모리와 마이크로 프로세서는 단일 칩상에 설계되어 메모리와 프로세서 사이의 데이터 흐름을 외부에 노출시키지 않도록 되어 있으며 만일 그러한 시도가 있으면 EEPROM의 내용이 자동삭제 되도록 안전성 목적을 위해서 특별히 설계 되어있다.

그림 1은 스마트 카드의 칩 구조 블록 다이아 그램을 나타낸다.[1]

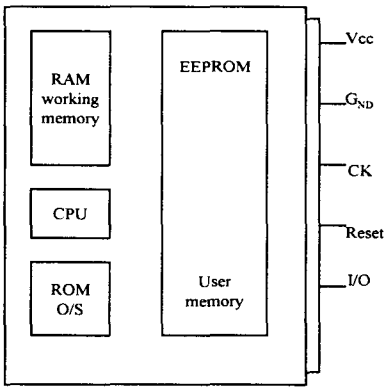


그림 1. 스마트 카드 칩 구조 블록 다이아그램
Fig. 1 Chip structure block-diagram of smart card

스마트 카드 마이크로프로세서 상에서의 메모리 할당은 세가지 영역으로 분할되는데 첫 번째 ROM 영역은 스마트카드 운영체제(SCOS)를 포함하며 크기는 6~8KB이다.

두 번째 EEPROM 영역에는 응용데이타가 쓰여지며 6~8KB의 크기를 가지며 비밀영역에는 키 등의 주요데이타가 저장될 수 있으며 세 번째 RAM 영역은 일반적으로 160바이트의 크기이며 운영체제가 명령을 수행하는데 있어 일시적인 저장장소로 사용되며 전원 차단시 데이터가 삭제된다.

스마트 카드의 운영체제(SCOS)는 여러 명령어를 다루며 전체시스템의 안전을 유지한다. 스마트 카드에서 소프트웨어의 역할은 매우 중요하며 이의 기능에 따라서 카드의 능력이 좌우된다.

그림 2는 스마트 카드의 응용환경을 보여주고 있다.[2]

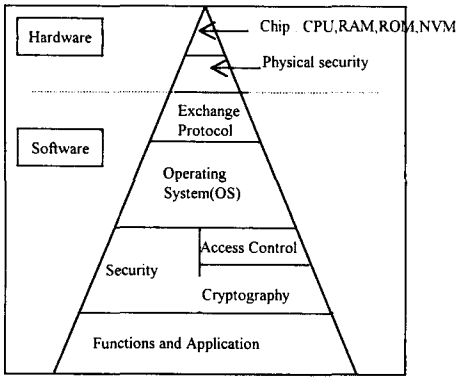


그림 2. 스마트 카드의 응용환경
Fig. 2 Application environment of Smart Card

스마트 카드의 특성은 여러 가지이며 상호 독립적인 면들로 이루어져있다.[3]

### 1. 위조불가(Anti fraud capability)

신용한도나 잔액이 카드에 저장되어 있어서 초과지불을 요할 경우 즉시 적발 가능하다. 안전성을 요구하는데 이터에의 접근이 필요할 때 또는 다량의 현금인출을 요구할 때 신분의 재확인을 요구할 수 있다.

### 2. 계속적인 응용과 거래확인 및 인증(continuous application and transaction validation)

어떤 시스템이나 응용에 스마트 카드가 접속되었을 경우마다 패스워드(사용자)나 비밀키(시스템)를 요구 할 수 있다.

### 3. 유용성(Flexibility)

카드와 시스템의 상호작용은 각각에 저장되어 있는 소프트웨어에 의해 정확히 제어된다. 스마트 카드에 바탕을 두는 시스템의 장점은 카드 소프트웨어와 반응형태는 카드의 NVM 부분의 재프로그래밍에 의해 간단히 바뀔 수 있다. 즉 부족한 점은 수정될 수도 있고 새로운 기능이 첨가 될 수 있음을 의미한다. 또한 여러 가지 응용이 하나의 카드에서 독립적으로 존재하며 수행 가능하다.

### 4. 다목적(Multipurpose)

단지 응용의 수는 메모리의 크기에만 제약을 받으며 다른 응용프로그램들은 지능적으로 처리한다.

### 5. 오프라인 능력(Offline capability)

카드는 스스로 시스템이나 사용자를 인증할 수 있다. 어떤 기준이 되는 정보가 저장되어 있어서 수상한 거래에 대하여 외부 인증을 요구할 수 있다. 이 능력이 비용을 줄이며 거래속도를 높인다.

### 6. 적극적 사용자 인증(Positive user authentication)

신체특징정보(biometric data)를 이용한 사용자 인증 없이도 사용자는 자신의 PIN을 정할 수 있다.

### 7. 사용중재구성(reconfiguration in use)

어떤 응용이 갱신되었을 경우 그 후 중앙컴퓨터에의 접속시 프로그램되어 사용자에게 투명(transparent)하며, 쉽고 저렴하고 빠르다.

### 8. 안전성(security)

암호 알고리즘을 이용한 데이터 인증 및 실체 인증과 칩의 안전성 면에서 보면 링크가 가능하고 불법 추출 회수 발견 회로등이 장착되어 있다.

### 9. 속도(speed)

전화선을 통한 중앙컴퓨터의 접속은 비용과 속도가 낭비적이지만 지역 거래(local transaction)과정은 저렴하고 빠르다.

### 10. 사용자 친밀성(user friendly)

개인 정보나 PIN의 갱신 및 잔액조회나 신용조회가 사용자에 의해 가능하다.

## Ⅲ. 스마트 카드의 안정성

스마트 카드의 마이크로프로세서 운영체제(SCOS)는 데이터에 접근하는데 대한 제어를 담당하는 기능을 제공하여 칩안의 안전한 영역에 모든 패스워드를 관리하고 있

어 칩 제조자나 카드의 발행인조차도 접근이 불가능하도록 되어 있다. 일반적으로 스마트 카드는 하드웨어 상의 안전성과 소프트웨어상의 안전성 측면으로 나누어 볼 수 있다.

하드웨어 측면에서 보면 소비전력을 들 수가 있다. 명령어들은 그 코드가 실행되는 도중에 전력소모를 측정함으로써 추적될 수 있다. 스마트 카드 프로세서는 거짓 연산을 수행하거나 엉뚱한 전력소모를 발생시켜서 외부의 공격을 방어할 수 있다.[1] 또한 칩의 보호장치가 제거되면 칩이 동작하지 않는다.

전압 측면에서 보면 프로세서는 기준 전력을 두어 실제 전력과 비교하여 실제 전력이 높거나 낮으면 카드는 동작을 멈추게 된다. 그리고 카드는 아주 강한 빛에 의해 특정된 메모리가 삭제될 수 있다. 카드메모리는 비밀정보를 없앨 수 있는 이러한 공격을 막기 위해 스크램블 되어진다.

소프트웨어 측면에서 보면 스마트 카드는 카드내의 몇몇 패스워드에 의해 보호되며 하나 또는 그 이상의 알고리즘이 카드의 비밀 저장영역에 저장되고 이 암호 알고리즘의 암호화키는 제조자나 특정 발행인에 의해 저장된다.

접근제어(Access control)는 비밀영역에 패스워드가 저장되면 나중에 접근시 제출된 패스워드가 정당한 것인가를 SCOS가 비교한다.

제조자는 personalization 에 대한 개인 정보를 저장하며 불법사용자에 의해 제조된 카드로부터의 비밀을 보장한다. 발행자 키는 패스워드 일 수도 있고 제조자에 의해서 건네진 특별한 키일 수도 있다.

또한 각 파일마다 패스워드가 존재할 수 있어 여러 종류의 패스워드를 논리적으로 조합할 수 있어 특정영역을 보호하는데 조합된 패스워드를 사용할 수 있다.

## Ⅳ. 인증 방식

사용자 인증은 사용자가 입력한 PIN에 의해 수행하는 접근제어 프로토콜이며 개체 인증은 검증자와 증명자간의 프로토콜이다. 스마트 카드는 증명자이고 터미널은 검증자가 되며 상호인증을 수행하기도 한다. 또한 개체 인증시에 사용되는 방식으로는 관용키 방식과 공개키 방식으로 나누어지며 결국 증명자가 정당한 비밀키를 가지고 있다는 점을 검증자에게 증명하는 것이다.

관용암호 방식을 이용한 인증은 검증자와 증명자 사이의 인증을 위해 비밀키 암호알고리즘을 사용하는 방식으로 인증시 사용되는 암호알고리즘의 비밀키 관리문제가 발생한다. 이 문제 해결을 위해 스마트 카드 식별자를 단말기로 전송하고 단말기는 식별자를 자신의 마스터 키로 암호화하여 이들 스마트 카드와 공통 비밀키로 사용한다. 마스터 키는 발행인이 설정해준 모든 단말기에 공통인 키이다.

그림 3과 같이 단말기는 난수를 발생하여 스마트 카드에 전송하고 스마트 카드는 자신의 비밀키로 이를 암호화해서 단말기로 재 전송한다.[4]

그러면 단말기는 카드의 ID와 마스터키로 스마트 카드와 비밀키를 생성하여 복호화를 수행한다음 이미 발생된 난수와의 비교를 통해 검증한다.

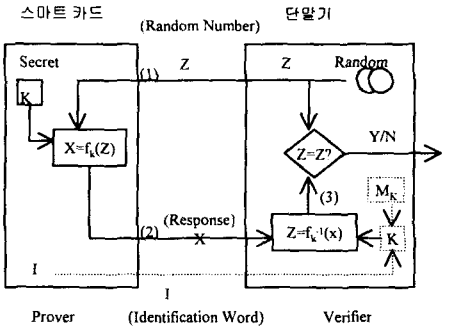


그림 3. 관용키 방식을 사용한 개체인증[4]
Fig. 3 Entity anthentication using conventional key system

본 논문에서는 공개키 암호방식을 이용한 인증 프로토콜에 관하여 고찰한다.

이 방식은 비대칭 암호방식으로 단말기가 유지해야할 비밀 정보가 필요 없는 장점을 갖는다.[5]

스마트 카드 인증에서 공개키 암호화 알고리즘을 사용하는 인증기법은 비밀키로 인증값을 생성하여 자신을 증명하고, 공개키를 통하여 검증하는 방법이다.

### 1. 요구기능

본 시스템의 스마트 카드 인증은 다음과 같은 보안 관련 기능들을 제공한다.

① 카드와 상호 인증 기능 : Off-Line 으로 운영시 카드와 단말간의 상호인증 기능
② 호스트와 상호 인증 기능 : On-Line 으로 호스트와 데이터 전송하기 전에 단말과 호스트간의 상호 인증 기능
③ 데이터 암호화 기능 : 암호화 알고리즘을 이용하여 카드 또는 호스트와의 데이터 전송시 정보보호를 위한 암호화 기능
④ 키 관리 기능 : 인증키 생성을 위한 마스터키와 데이터 암호화를 위한 암호화키를 저장하고 관리하는 기능
⑤ 응용프로그램 수행 기능 : 응용 시스템에서 스마트 카드에 기록되어진 값을 변경하는 프로그램 또는 데이터를 저장하고 관리하는 기능

### 2. 인증 과정

그림 4는 본 논문에서 제안한 스마트 카드와 단말기 간의 상호 인증 과정을 나타낸 것이다.

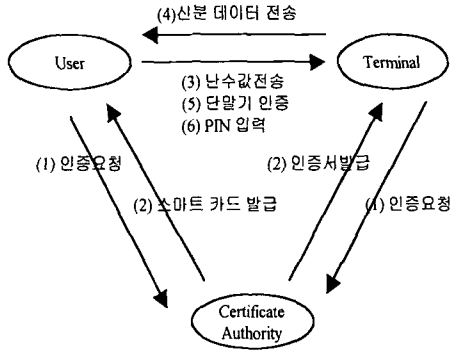


그림 4. 단말기 인증 과정
Fig. 4 Process of terminal authentication

① 사용자와 단말기는 인증센터에 인증을 요청한다.
② 인증센터는 사용자와 단말기가 적법한지를 확인한 후 사용자에게는 인증서가 담긴 스마트 카드를, 단말기에는 인증서를 발급한다.
③ 스마트 카드는 단말기의 인증을 위하여 임의의 난수값(Ruser)를 단말기에 보낸다.
④ 단말기는 자신의 비밀키(TKsecret)로 난수값(Ruser)를 복호화한 결과값(Yresult)와 단말기의 신분확인 데이터(TID)로 만들어진 공개키의 신임장(Cert)을 스마트 카드로 전송한다. 이때, 신임장은 스마트카드가 공개키의 진실 여부를 확인할 수 있도록 한다.
⑤ 단말기로부터 전송되어진 값(Yresult)을 단말기의 공개키(TKpublic)로 암호화한 값(Xresult)과 본래의 난수값(Ruser)를 비교한다.
⑥ 공개키의 인증을 위하여 전송되어진(TID)를 공개키(TKpublic)로 암호화한 값과 전송된 신임장(Cert)를 비교하여 공개키를 인증한다.

본 시스템의 인증프로토콜에서는 대칭형 암호화 알고리즘을 이용한 인증에서의 문제점이었던 비밀키의 분배 및 관리의 문제점을 해결하고 공개키 리스트에 대한 관리 문제를 인증센터를 통하여 인증서를 발급받는 형태의 방법을 제공함으로써 공개키 관리를 효율적으로 할 수 있다.

## V. 결 론

실체 인증에 사용되어지는 알고리즘에는 연산 부하가 적은 DES를 이용한 대칭형 암호화 알고리즘을 이용한 인증이 주류를 이루고 있었지만 이 대칭키 알고리즘은 비밀키의 분배 및 관리에 대한 문제를 내포하고 있어서 속도가 늦고 키 용량이 컸으나 본 논문에서는 적은 키 용량과 빠른 속도를 요하는 스마트 카드 인증을 위한 새로운 알고리즘을 사용한 인증프로토콜을 제시하였다.

향후 스마트 카드의 발달과 더불어 더 적은 키 용량과 더빠른 속도의 인증을 위한 새로운 알고리즘의 개발이 필요할 것이다.

## 참고문헌

[1] Josě Luis Zoreda and Josě Maneul Otŏn, "Smart cards", Artech House, Inc., 1994.
[2] Simmons, G.J.(Ed.),"Contemporary Cryptology: The science of information integrity", IEEE PRESS, chap.12, 1992.
[3] Mike Peterson, "SMART CARDS: how to deal yourself a winning hand", Motorola Semiconductor Engineering Bulletin, EB405, 1991.
[4] Hans-Peter Kŏnigs, "Cryptographic Identification Methods for Smart Cards in the Process of Standardization", IEEE Communications Magazine, PP.42-48, June 1991.
[5] 원동호, "정보와 부호이론", Ohm사, 1993.
[6] Jack M. Kaplan, "Smart Cards", Thomson Computer Press, 1996.
[7] Bruce Schneier, "Applied Cryptography", John wiley & sons, Inc., 1994.

## 저자소개

이 지 영
한국OA학회 논문지
제4권 제2호(99-4-2-1-4)참조
연구분야 : 정보이론, 암호이론, 고속연산 알고리즘, 운영체제