스마트 카드 시스템의 보안기능 분석 및 설계에 관한 고찰

신 진원° , 권 태경, 송 주석

연세대학교 컴퓨터과학과

A Survey on Analysis and Design of Smart Card System Security

JinWon SHIN° , TaeKyoung KWON, JooSeok SONG

Dept. of Computer Science, Yonsei University

요 약

최근 스마트 카드는 다양한 분야에서 시스템의 보안성을 향상시키기 위하여 사용되고 있다. 그러나 스마트 카드가 사용되어진 시스템들이 모두 뛰어난 보안성을 제공하는 것은 아니다. 아직까지 카드 운영체제의 보안기능이 관련 국제 표준을 따르고 있지 않을 뿐만 아니라, 또한 시스템의 보안설계가 잘못되어 취약점이 나타나는 경우도 있다.

본 논문에서는 스마트 카드 시스템에서 요구되는 보안 기능 및 관련 국제 표준안에 대하여 살펴보고, 이들을 기반으로 하여 안전한 시스템의 설계 방법을 제시한다.

1. 서론

최근 컴퓨터와 정보통신의 발달로 인한 정보화 사회에서는 정보가 핵심적인 역할을 담당하며, 시스템의 안전한 운영과 보호가 중요한 문제로 대두되었다. 이에 대한 대응책으로 스마트 카드를 이용하여 사용자의 신분확인 및 인증으로 중요한 정보를 보호하는 시스템들이 등장하게 되었다. 금융분야에서는 기존의 마그네틱 카드보다 높은 보안성 및 다양한 서비스를 제공하기 위하여 사용되며, 정보통신 분야에서는 위성 방송과 개인이동통신(PCS:Personal Communication Service)의 가입자 관리에 사용되고 있다 [1][2].

그러나 스마트 카드를 도입한 시스템들이 모두 뛰어난 보안성을 제공하는 것은 아니다. 스마트 카드는 단지 보안성을 향상시키는 하나의 장치일 뿐이며, 보다 안전한 운영과 보호를 위하여 시스템의 도입부터 체계적인 보안설계와 대책이 마련되어져야 한다. 시스템의 보안설계는 다음의 세 가지 기본 보안기능을 만족하여야 한다.[3]

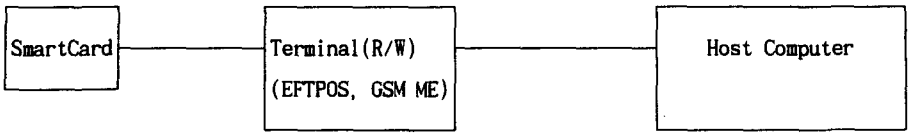
1) 비밀성(Confidentiality) : 중요 정보가 비인가자에게 노출되는 것을 방지

2) 무결성(Integrity) : 중요 정보가 비인가자에 의하여 불법 변조되는 것을 방지

3) 가용성(Availability) : 인가자의 시스템 사용을 항상 허용

위의 세 가지 기본 기능을 만족하기 위하여 각각의 보안기능들은 스마트 카드, 스마트 카드와

단말, 단말과 호스트간의 관계에서 하드웨어 및 소프트웨어로 구현되어져야 한다. 각각의 시스템에 따라 구성도의 차이는 있을 수 있지만 전형적인 구성도[그림 1. 참조]은 다음과 같다.



[그림 1. 일반적인 스마트 카드 시스템의 구성도]

본 논문에서는 세 가지 기본 보안기능을 만족하기 위한 스마트 카드 시스템의 요구 보안기능에 대하여 살펴보고, 이들을 기반으로 하여 안전한 시스템의 설계 방법을 제시한다.

2. 스마트 카드의 보안성

스마트 카드의 보안성은 크게 물리적 보안과 논리적 보안의 두 가지 측면으로 구분되어진다. 물리적 보안은 하드웨어의 불법 복제 및 변조를 의미하며 논리적 보안은 카드 내의 운영체제 소프트웨어의 안전성을 의미한다.

1) 물리적 보안

스마트 카드의 불법 복제하거나 변조는 내부의 마이크로 프로세서 분석을 통하여 이루어질 수 있다. 하지만, 한 장의 카드 보안기능을 분석하여 얻는 이익보다 많은 노력이 들어가도록 한다면 안전할 것이다. 이를 위하여 스마트 카드 보안성을 하드웨어에 의존하는 것이 아니라 논리적으로 각각의 카드가 서로 다르게, 카드마다 고유한 인증키와 암호화키를 사용한다면 카드의 물리적 보안 침해는 줄어들 것이다.

2) 논리적 보안

스마트 카드 내부 소프트웨어는 기본적인 운영체제와 응용 프로그램으로 구분된다. 운영체제는 카드 내의 화일, 디렉토리 등의 자료구조를 할당, 기록, 삭제, 읽기, 수정하는 정보 저장/관리 기능, 이들 정보를 비인가자로부터 보호하기 위한 접근제어 및 암호화 기능, 카드 내의 정보에 수행가능한 명령어들로 구성된다. 응용 프로그램은 카드의 정보를 외부 유출없이 운용체제 제어하에서 수행되어지는 명령어들의 집합이다.

가. 자료구조 관리 기능

카드의 이용이 한 가지 용도에서 탈피하여 점차 다목적 용도로 발전하면서 더욱 큰 메모리 용량을 요구하고, 이를 효율적으로 관리할 수 있는 자료구조 관리 기능이 더욱 중요시되고 있다. 이를 위하여 ISO 7816 4부에서는 메모리의 기본구조 및 TLV(Tag Length Value)를 이용한 효율적인 자료관리 방법을 정의하고 있다.[4] 하지만 아직도 많은 운영체제에서 화일을 논리적 참조 방법인 TLV 개념을 도입하지 않고 있어 카드의 효율적인 자료관리가 어렵다. 이에 따른 물리적

참조 방법의 이용으로 단말에서 참조하고자 하는 화일의 물리적 주소를 알고 있어야 하며, 이는 정보의 외부유출이 가능하도록 한다. 보다 안전하고 효율적인 시스템의 도입을 위해서는 스마트 카드 선택시 운영체제의 국제표준안 준수 여부를 확인하여야 한다.

나. 접근제어 및 암호화 기능

시스템에서는 PIN(Personal Identification Number) 또는 지문과 같은 신체적 특징을 이용한 사용자 인증을 통하여 정당한 사용자들만이 카드에 저장되어진 정보에 접근할 것을 요구한다. PIN은 오직 카드의 소지자만이 알고 있다고 전제하고, 사용자가 핀패드를 통하여 PIN을 입력하면 단말은 PIN을 스마트 카드로 전송한다. 카드는 메모리에 저장되어져 있는 비밀번호와 PIN을 비교하여, 사용자의 정당성을 여부를 확인하고 난 후에 특정한 정보에 대하여 접근을 허가하거나 또는 일치되었음을 단말에 알려준다.

PIN의 노출은 시스템 침해요소 중의 하나이다. 이와 같은 침해를 방지하기 위하여 단말은 PIN을 전송하기 전에 카드와의 세션키를 사용하여 암호화한다. 암호화되어진 PIN은 세션키를 가진 카드에서만 복호화 되어짐으로 통신과정에서의 노출은 방지할 수 있다. PIN의 암호화 이외에도 단말과 카드간의 자료 전송시 동일한 방법으로 암호화하여 정보의 노출을 방지할 수 있다.

다. 명령어

ISO 7816 4부에서는 16개의 기본 명령어를 정의하고, 정보보호에 관련된 명령어는 다음과 같다.

명령어	기 능
VERIFY	PIN을 이용한 사용자 인증을 지하는 명령어
INTERNAL AUTHENTICATE	단말에서 보내어진 Challenge값과 카드에 저장되어진 암호화키를 이용하여 인증 값을 계산을 지시하는 명령어
EXTERNAL AUTHENTICATE	단말에서 보내어진 인증 값을 카드에 저장되어진 암호화키와 생성한 Challenge값을 이용하여 단말의 인증여부를 지시하는 명령어
GET CHALLENGE	EXTERNAL AUTHENTICATE에 사용되는 Challenge값의 생성을 카드에 지시하는 명령어

[표 1 정보보호에 관련된 명령어]

그러나 정보보호를 위하여 필요한 암호화와 인증에 사용되는 알고리즘에 관하여는 표준안에 정의되어 있지 않으므로 시스템의 설계자가 선정하여야 한다. 다음 장에서는 스마트 카드의 인증에 사용 가능한 인증 프로토콜에 대하여 살펴본다.

3. 스마트 카드의 인증 프로토콜

스마트 카드에서 사용되어지는 인증은 크게 사용자 인증과 실체 인증의 두 가지로 구분된다.

사용자 인증은 앞에서 설명되어진 것과 같이 스마트 카드의 소지자가 정당한 사용자라는 것을 PIN(Personal Identification Number) 또는 지문과 같은 신체적 특징을 통하여 확인하여 불법사용을 방지하기 위한 것이다.

실체 인증은 스마트 카드와 단말간의 상호 정당성을 증명하여 위조카드 또는 단말의 사용을 통

한 정보의 불법유출 및 변조를 방지한다. 실체 인증에는 인증에 사용되어지는 알고리즘에 따라 "대칭형 암호화 알고리즘을 이용한 인증", "공개키 암호화 알고리즘을 이용한 인증" 그리고 "영지식 알고리즘을 이용한 인증"의 세 가지 방법이 있다.[5] [6] 이들 방법은 각각의 시스템 운영 환경에 따라 적절한 방법이 선택되어져야 한다.

3.1 대칭형 암호화 알고리즘을 이용한 인증

ISO/IEC 9798-2에서는 대칭형 암호화 알고리즘을 이용하는 여섯 가지 인증기법을 정의한다.[6] 이들은 일방향 인증과 상호인증으로 구분되며, 다시 신뢰성 있는 제3자의 필요 유무로 구분된다. 대칭형 암호화 알고리즘을 이용하여 외부에 카드의 인증키를 노출하지 않고 인증 하는 효율적인 방법이다. 그러나 양쪽에서 동일한 인증키를 가지고 있어야 하며, 이를 위하여 안전한 키 분배와 관리가 요구되어진다.

그러나 대량의 카드가 호스트의 데이타 베이스에 접속없이 OFF-LINE으로 상호인증 되어야 하는 시스템의 경우에는 단말이 모든 카드의 인증키를 관리하는 것은 불가능하다. 실제 스마트 카드 시스템에 사용하기 위하여 보다 효율적인 키 분배와 관리가 가능한 인증기법이 요구된다.

인증키 다양화 기법은 카드마다 다른 인증키를 단말에서 생성하는 방법으로 대칭형 암호화 알고리즘을 이용한 스마트 카드의 인증에 가장 적합한 방법이다.

카드의 최초 발급 시에 시스템의 마스터키 (KEY_{Master})와 유일한 값을 가지는 카드의 신분확인 데이타 (I_{Card})를 암호화하여 카드마다 서로 다른 인증키 (KEY_{Card})를 생성하여 저장한다.

인증키 생성을 위하여 대부분의 스마트 카드에서 지원되어지는 DES와 같은 대칭형 암호화 알고리즘을 사용한다. 대칭형 암호화 알고리즘 대신에 일방향 해쉬(One-Way Hash)함수의 이용도 가능하다. 스마트 카드의 인증은 다음과 같은 절차로 이루어진다 [그림 2. 참조].

이와는 반대로 유일한 값을 가지는 단말의 신분확인 데이타($I_{Terminal}$)을 카드로 보내어 카드가 단말을 인증하도록 하여 상호인증을 수행한다. 이 방법은 오직 정당한 카드와 단말 사이만 정보를 주고받을 수 있도록 하여 시스템의 보안성을 향상시킬 수 있다.

인증키 다양화 기법을 통하여 모든 스마트 카드가 유일한 인증키를 가지게 됨으로 인증키 유출에 따른 전체 시스템의 피해는 최소화할 수 있다. 하지만 모든 카드의 인증키를 생성하기 위하여 단말과 스마트 카드에 저장되어져야 하는 시스템의 마스터키 (KEY_{Master})의 노출 시에는 전체 시스템의 보안성에 큰 문제가 발생한다. 이에 대응하기 위하여 여러 개의 시스템 마스터키를 사용하여 키의 유효시간을 고려하며, 변경하여 사용하는 방법이 있다. 키의 유효시간은 키를 추론해 내는 것이 계산상 불가능하도록 선택하며, 알려진 평문에 의한 공격과 선택된 평문의 공격을 막을 수 있도록 선택되어져야 한다.

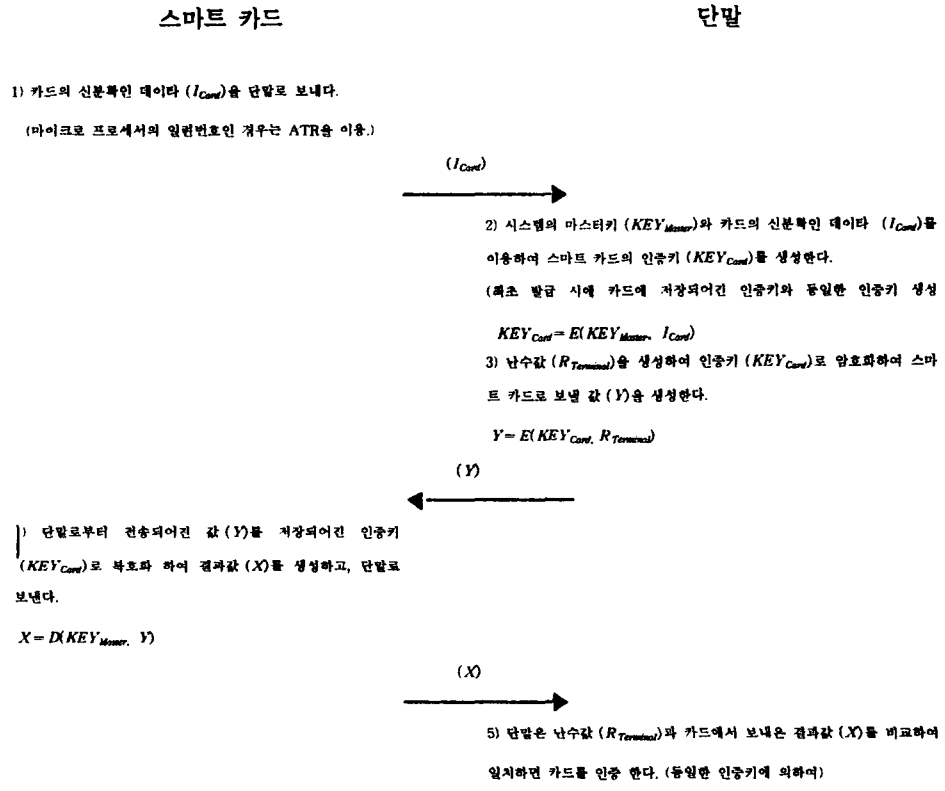
또한, 단말에서는 마스터키의 노출을 방지하고 보호하기 위한 SAM(Security Application Modules)을 가지고 있어야 한다. 스마트 카드의 형태 또는 IC 칩 형태로 되어진 것이 있으며, 어떠한 형태든지 물리적이나 논리적으로 안전하여야 한다. SAM은 ISO 10202 4부에서 최소한의 요구조건을 정의하며, 다음과 같은 보안관련 기능들을 수행하여야 한다.[8]

1) 카드와 상호인증 기능 : Off-Line으로 운영시 카드와 단말간의 상호인증 하는 기능
2) 호스트와 상호인증 기능 : On-Line으로 호스트와 데이타 전송하기 전에 단말과 호스트 간의 상호인증 하는 기능
3) 데이타 암호화 기능 : 암호화 알고리즘을 이용하여 카드 또는 호스트와의 데이타

전송시 정보보호를 위한 암호화하는 기능

4) 키 관리 기능 : 인증키 생성을 위한 마스터키와 데이타 암호화를 위한 암호화키를 저장하고 관리하는 기능

5) 응용프로그램 수행 기능 : 응용 시스템에서 스마트 카드에 기록되어진 값을 변경하는 프로그램 또는 데이타를 저장하고 관리하는 기능



[그림 2. 대칭형 암호화 알고리즘을 이용한 인증 프로토콜]

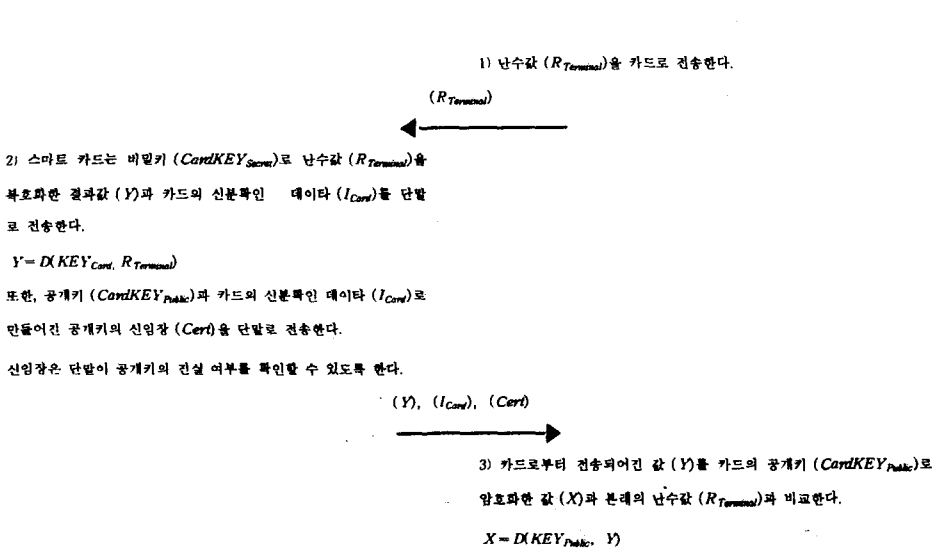
3.2 공개키 암호화 알고리즘을 이용한 인증

ISO/IEC 9798-3에서는 공개키 암호화 알고리즘을 사용하는 인증기법을 정의한다.[9] 이들은 비밀키로 인증값을 생성하여 자신을 증명하고, 공개키를 통하여 검증하는 방법이다. 공개키 암호화 알고리즘을 이용한 인증에서는 대칭형 암호화 알고리즘을 이용한 인증에서의 문제점이었던 비밀키의 분배 및 관리의 문제는 해결되었으나 공개키의 리스트를 관리하여야 하는 문제점이 대두되었다. 이를 해결하기 위하여 인증서를 이용하여 공개키를 얻는 방법이 사용된다.

인증서 ($Cert$)는 카드가 최초에 발급되어질 때 시스템의 마스터 비밀키 ($MasterKEY_{Secret}$)를 사용하여 만들어진다. 단말에는 스마트 카드에 의하여 제공되어지는 인증서 ($Cert$)를 확인하기 위한 시스템의 마스터 공개키 ($MasterKEY_{Public}$)가 저장되어져야 한다. 스마트 카드가 공개키 ($CardKEY_{Public}$)에 대한 인증서 ($Cert$)를 제공하였을 때 단말은 시스템의 마스터 공개키와 카드

의 신분확인 데이타 (I_{Card})로 카드의 공개키를 복호화 한다.

RSA(Rivest-Shamir-Adelman) 스마트 카드 시스템에서 가장 많이 사용되는 공개키 암호화 알고리즘으로 스마트 카드의 비밀키를 사용하여 인증값을 생성하고, 단말의 공개키를 사용하여 검증한다. 스마트 카드의 인증은 다음과 같은 절차로 이루어진다 [그림 3. 참조].



[그림 3. 공개키 알고리즘을 이용한 인증 프로토콜]

이와는 반대로 카드가 난수값(R_{Card})을 단말로 보내어 카드가 단말을 인증 하도록 하여 상호인증을 수행한다. 이 방법도 오직 정당한 카드와 단말 사이만 정보를 주고받을 수 있도록 하여 시스템의 보안성을 향상시킬 수 있다.

그러나 RSA 알고리즘을 스마트 카드에 구현하기 위하여는 인증값을 계산하기 위한 지수승 계산, 모듈러 계산 등을 위한 보조 프로세서, 계산 중간값을 기록하기 위한 많은 양의 메모리(RAM), 알고리즘을 수행을 위하여 필요한 추가적인 명령어들을 저장할 큰 프로그램 메모리(ROM) 등이 필요하다..

NIST(National Institute of Standards and Testing)에서 개발한 DSS(Digital Signature Standard)는 미국 정부의 전자문서 서명을 위하여 개발되었고, 정부의 다른 응용분야에서도 인증을 위하여 사용되어질 수 있다. 이 알고리즘은 소인수분해의 어려움에 안전성을 두고 있는 RSA와는 달리 이산대수를 계산하는데 어려움이 있음에 기반하고 있다. 특히, DSS는 인증을 위한 중간값을 사전에 계산할 수 있다는 장점을 가지고 있어 인증을 위한 소요시간 단축이 가능하여 스마트 카드의 인증에 사용되기에 적합하다.[10]

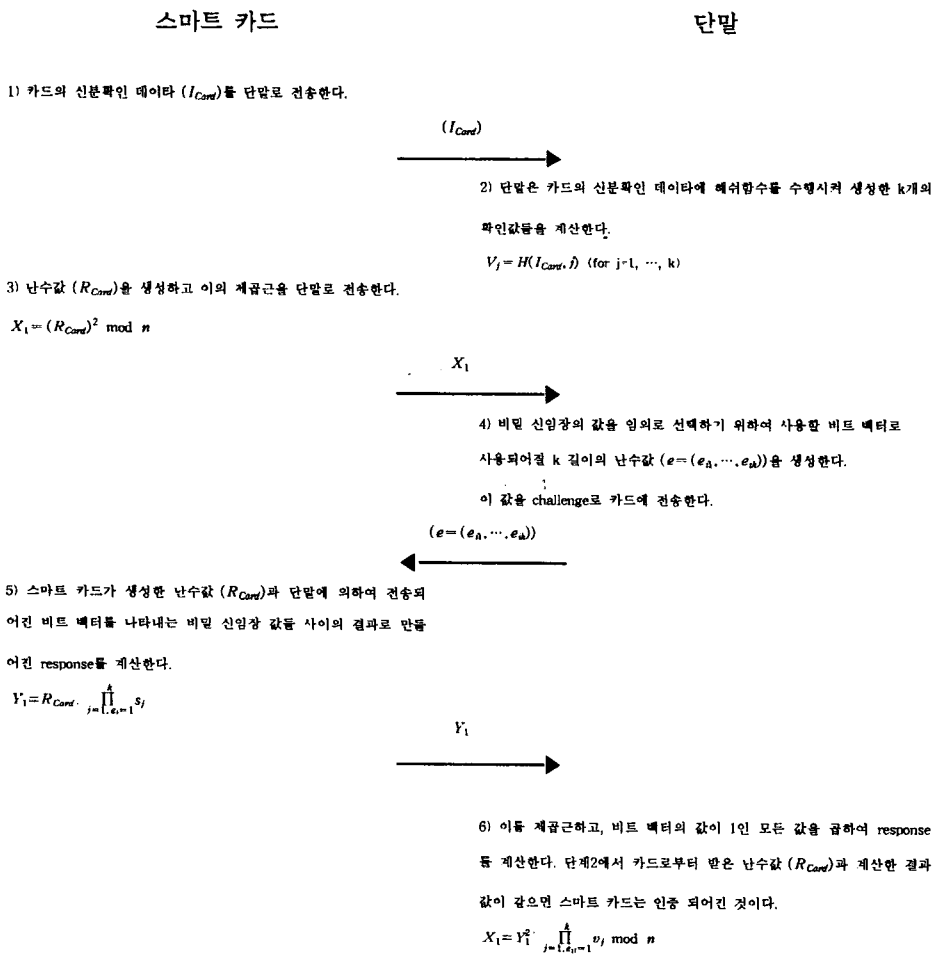
3.3 영지식 알고리즘을 이용한 인증

영지식 알고리즘을 이용한 인증기법은 앞에 설명한 두 가지 인증기법과는 다르게 키의 분배와

관리 없이도 인증이 가능한 효율적인 방법이다.

영지식 알고리즘을 이용한 인증은 Challenge/Response 프로토콜이며, 인증을 위하여 암호화 알고리즘을 사용하지 않는다. 확인자는 증명자를 인증하기 위하여 인증에 사용되는 어떠한 비밀키도 가지고 있지 않으며, 증명자가 비밀 신임장(Accreditation)을 가지고 있다는 것을 추론하여 인증을 수행한다. 이를 위하여 확인자가 한번 이상의 Challenges를 보내고, 증명자는 같은 횟수만큼의 Response를 보냄으로써 수행된다. 확인자와 증명자간의 Challenge와 Response의 횟수에 상관없이 증명자는 비밀 신임장에 대한 아무런 정보도 노출하지 않는다.

최초의 실질적인 영지식 알고리즘은 A. Fiat와 A. Shamir에 의하여 제안되었다.[11] 이 알고리즘을 스마트 카드에 적용하기 위하여 카드의 초기 발급에서 다음과 같은 작업이 선행되어야 한다. 카드의 발급자는 두 개의 큰 소수(p, q)의 곱(n = p*q)으로부터 시스템의 공개 상수값 (n)을 계산한다. 카드의 신분확인 데이타로부터 해쉬함수를 이용하여 비밀 신임장(Accreditation) 값의 집합을 계산하여 각각의 카드에 저장한다. 비밀 신임장 값들과 시스템의 공개 상수값 (n)들은 다음 순서와 같은 카드의 인증절차에서 사용되어진다 [그림 4. 참조].



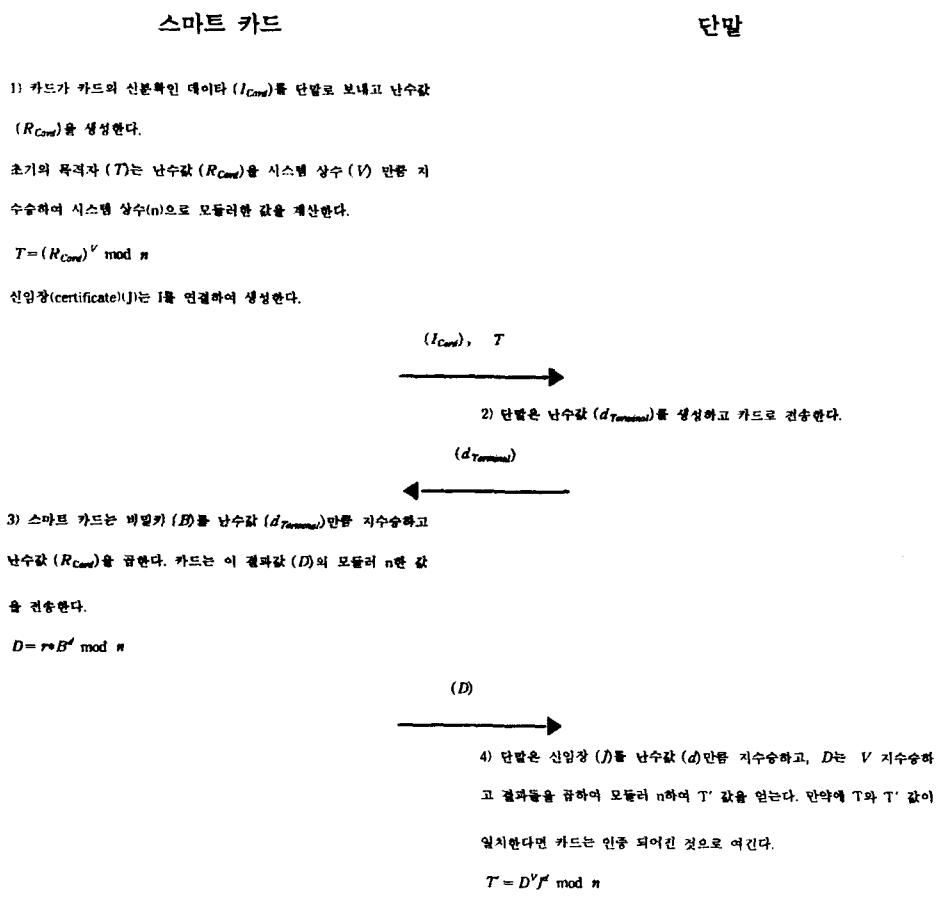
[Fiat-Shamir의 영지식 알고리즘을 이용한 인증 프로토콜]

이 방법의 보안성은 Challenge/Response 쌍의 수의 곱과 비밀 신임장 값들의 수에 따라 지수승하게 증가된다. 하지만 카드와 단말간의 전송량과 신임장 값들의 수 증가는 많은 시간과 메모리를 요구한다. 그래서 전송량과 신임장 값들을 최소화하는 방법이 제안되어졌다.

Guillou-Quisquater는 계산량은 양은 증가하였지만 Fiat-Shamir 방법보다 적은 전송량과 신임장 값들로 같은 정도의 보안성을 제공하는 방법을 제안하였다.[12]

이 방법에서는 카드의 발급을 위하여 두 개의 큰 소수(p, q)를 선택하여, (각각 256 bit이상) 이 두 소수의 곱(n = p * q)을 구한다. 두 소수는 비밀키로 간직하고, 오로지 카드 발급자만이 알고 있어야 한다. n은 공개 상수값으로 단말에 저장되어 있어야 한다. 단말의 인증을 위하여 n과 함께 V가 시스템 상수로 단말에 저장되어 있어야 한다. V의 크기는 30bit 정도이고, 크기에 따라 계산량과 시스템의 안전성이 증가된다. 각각의 카드는 카드의 신분확인 데이타 (I_{Card})와 비밀값 B가 카드에 저장되어져 있어야 한다. B값은 다음과 같은 공식에 의하여 생성된다. J는 카드의 신분확인 데이타의 연결하여 생성된다. $(J * B^v \pmod n) = 1, (n = p*q)$

Guillou-Quisquater 인증을 다음과 같은 순서로 이루어진다 [그림 4. 참조].



[Guillou-Quisquater 알고리즘을 이용한 인증 프로토콜]

4. 스마트 카드 보안관련 국제 표준안

스마트 카드 보안 표준안들은 ISO(International Standard Organization)에 의하여 카드 생산 업체 간의 호환성을 위한 표준안과 금융 분야를 위한 표준안의 두 개 부문으로 구분되어 ISO/IEC JTC1/SC17/WG4와 ISO/TC68/SC6/WG7에서 각각 진행중이다. SC17/WG7에서 정의한 ISO 7816-4에서는 앞에서 설명한 Verify, External Authentication, Internal Authentication과 같은 보안을 위한 명령어들과 안전한 메시지 전송하는 방법을 포함한다. 하지만, 이들은 모두 최소한의 조건만을 갖추고 있으며, 전자 현금과 같은 금융분야에서는 추가적인 보안기능이 요구되어진다. SC6/WG7에서 정의한 ISO 10202는 스마트 카드를 사용하는 금융거래를 위한 보안구조에 관한 표준안이다. ISO 10202는 스마트 카드 자체와 이를 이용한 시스템에서 지켜야할 최소한의 보안 요구조건에 관하여 정의하고 있다. 하지만 보안을 위한 명령어들, 보안의 구현 방법 또는 스마트 카드를 위한 보안 설계 등에 대하여 정의하는 것은 아니다. 또한, 이 표준안은 일반적인 응용을 위하여 정의하는 것은 아니라 단지 스마트 카드를 이용하여 금융거래 시스템을 구현할 경우 고려하여야 하는 것의 목록이다. 그러나 다른 응용 시스템에서의 보안설계시 다음사항을 고려하여야 한다.

- 카드의 최초 발급 시부터 폐기까지의 보호과정
- 카드와 단말간의 정보전송의 안전성
- SAM(Security Application Modules)
- 인증 및 암호화를 위하여 사용하는 알고리즘
- 사용자 인증 메커니즘
- 인증키 및 암호화키 관리
- 보안 서비스 및 정책

이와 같은 사항을 구현하기 위하여 각종 분야별로 별도의 표준안들이 재정되고 있다. 특히, 최근에는 금융 분야에서 Europay/MasterCard/VISA가 함께 직불과 신용카드를 위한 표준화 작업이 진행 중이다. GSM에서는 사용자 인증 및 실체 인증의 표준안을 GSM 11.11에 정의한다.

5. 결론

지금까지 우리는 스마트 카드의 보안성과 인증 프로토콜에 관하여 알아보았다. 보다 안전한 시스템의 구현을 위하여는 스마트 카드의 운영체제의 기능들이 국제표준을 준수하여 보다 안전하고 효율적인 자료관리가 이루어져야 한다. 또한, 스마트 카드의 응용 시스템에서 최초의 보안은 사용자 인증을 통하여 소지자의 정당성 여부를 판별하여 불법사용을 방지하고, 이에 따라 사용권한을 제한하고, 실체 인증을 통하여 스마트 카드와 단말간의 상호 정당성을 증명하여 위조카드 또는 단말의 사용을 통한 정보의 불법유출 및 변조를 방지하기 위한 인증 프로토콜을 시스템의 운영환경에 따른 적절한 선택을 하여야 한다. 대칭형 암호화 알고리즘과 공개키 암호화 알고리즘을 이용한 인증 프로토콜에서는 안전한 키 분배 및 관리가 요구되어졌다. 이들 키의 노출은 시스템의 보안성에 치명적인 영향을 미치며, 이를 방지하기 위한 노력이 이루어져야 한다. 이를 위하여 보다 안전한 키 관리가 가능한 SAM의 설계 및 구현이 이루어져야 한다.

[참고문헌]

[1] Patrice Peyret, Gilles Lisimaque, T. Y. Chua, "Smart cards provide very high security and flexibility in subscribers management," IEEE Trans. on Consumer Electronics, Vol. 36, No. 3, AUGUST 1990, pp. 744-752.

[2] Siegmund M. Redl, Matthias K. Weber, Malcolm W. Oliphant, "An Introduction To GSM," Artech House Publishers, 1995, pp. 35-49.

[3] Edward Amoroso, W.E Kleppinger, David Majette, "An Engineering Approach to Secure System Analysis, Design, and Integration," AT&T Technical Journal Vol. 73, No. 5, 1994, pp. 40-51.

[4] 이 필중, "ISO/IEC JTC1/SC27의 국제표준소개(5) : ISO/IEC IS9798-1 정보기술-보안기술-실체인증 기법, 제1부 : 일반모델", 통신정보보호학회지, 제4권, 제3호, 1994, pp. 83-90.

[5] Hans-Peter Konigs, "Cryptographic Identification Methods for Smart Cards in the Process of Standardization," IEEE Communications Magazine, June 1991, pp. 42-48.

[6] 이 필중, "ISO/IEC JTC1/SC27의 국제표준소개(6) : ISO/IEC IS9798-2 정보기술-보안기술-실체인증 기법, 제2부 : 대칭형 암호기술을 이용한 인증", 통신정보보호학회지, 제4권, 제4호, 1994, pp. 95-112.

[7] Gilles Garon, "Overview of smart card security and standards," CardTech/SecureTech Conference Proceedings, 1995, pp. 507-522.

[8] 이 필중, "ISO/IEC JTC1/SC27의 국제표준소개(7) : ISO/IEC IS9798-3 정보기술-보안기술-실체인증 기법, 제3부 : 공개키 알고리즘을 이용한 인증", 통신정보보호학회지, 제5권, 제1호, 1995, pp. 85-100.

[9] Digital Signature Standard(DSS), Federal Information Processing Standards Publication 186, May 1994.

[10] A. Fiat and A. Shamir, "How to Proof Yourself:Practical Solution to Identification and Signature Problem," Crypto '86, Lecture Notes in Computer Science, Vol. 263, pp. 186-194, Springer Verlag.

[11] L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors and Minimizing Both Transmission and Memory," Eurocrypt '88, Lecture notes in Computer Science, Vol. 330, pp. 123-128, Springer Verlag.