자바카드 기반 무선단말기용 사용자 인증 프로토콜의 설계 및 구현

이 주 화[†] · 설 경 수[††] · 정 민 수[†††]

요 약

자바카드는 스마트카드 플랫폼에 자바의 기술을 접목시킨 것으로 스마트카드와 같은 작은 메모리를 가진 임베디드 장치를 위한 프로그래밍에 필요한 패키지와 클래스를 정의하고 있다. 또한, 자바카드는 국제 표준인 ISO-7816과 산업 명세 표준인 EMV와 호환된다. 그러나, 현재 국내외적으로 USIM이 장착된 IMT-2000에 자바카드를 이용한 사용자 인증 프로토콜을 지원하고 있지 않다. 본 논문은 표준화된 3GPP 규격(SMS), 자바카드 기술규격(APDU) 그리고 암호화 기술 등을 사용하여 자바카드 기반 무선단말기에 적용 가능한 사용자 인증 프로토콜을 설계 및 구현하였다. 표준화된 기술을 이용한 자바카드 사용자 인증 기능 지원으로 자바카드 응용 프로그램 개발 지원 도구의 보안 기능, 무선상거래, 무선보안, 전자지불시스템, 모바일 인터넷, 위치서비스 그리고 유비쿼터스 컴퓨팅 환경 등에 적용 가능하다.

Design and Implementation of User Authentication Protocol for Wireless Devices based on Java Card

Ju-Hwa Lee[†] · Kyoung-Su Seol[††] · Min-Soo Jung[†††]

ABSTRACT

Java card is one of promising smart card platform with java technology. Java card defines necessary packages and classes for Embeded device that have small memory such as smart card. Java card is compatible with EMV that is industry specification standard and ISO-7816 that is international standard. However, Java card is not offers user authentication protocol. In this paper, We design and implement an user authentication protocol applicable wireless devices based on Java Card using standard 3GPP Specification (SMS), Java Card Specification (APDU), Cryptography and so on. Our Java Card user authentication techniques can possibly be applied to the area of M-Commerce, Wireless Security, E-Payment System, Mobile Internet, Global Position Service, Ubiquitous Computing and so on.

키워드 : 인증(Authentication), 일회용패스워드(OTP), 자바카드(Java Card)

1. 서 론

IMT2000(WCDMA)은 제 3세대 이동통신서비스로 전세계적 표준화 및 동일 주파수를 활용하여 세계적인 로밍이 되고고품질의 음성, 인터넷, 영상 등 멀티미디어 통신이 가능하여 무선 인터넷 같은 다양한 데이터 통신과 무선상거래가 가능하다. 이와 같이 IMT-2000에서 제공하는 다양한 부가 서비스를 제공받기 위해서는 가입자 인증과 결재 방식이 필요하다. 이에 따라 ETSI(European Telecommunications Standards Institute)나 3GPP(3rd Generation Partnership Project) 같은 표준화 기구들은 UICC/USIM(Universal IC Card/Universal Subscriber Identify Module)을 IMT-2000의 UIM(User Identification Module) 표준 규격으로 정하였다[1-2].

현재 이동통신서비스 개발을 위해 상용화된 개발 도구로는 유럽의 GSM(Global System for Mobile Communications) 방식의 SIM(Subscriber Identify Module) 카드 응용 프로그램 개발을 지원하는 젬플러스사의 GemXpresso RAD Ⅲ Kit 등이 있으나 IMT-2000을 기반으로 하는 USIM 카드 응용 프로그램 개발 지원 도구는 상용화된 제품이 없다. 또한, 전 세계적으로 볼 때 SIM/USIM 카드 응용 프로그램 개발을 지원하는 개발 도구로 젬플러스사와 ORGA사 제품들이 있으나 이 제품들은 자국의 보안 정책상 암호화 모듈을 국외로 유출하는 것을 금하고 있어서 자국내를 제외한 국가에 대해서는 암호화 모듈과 사용자 인증 기술을 지원

† 정 회 원 : 경남대학교 대학원 컴퓨터공학과
†† 준 회 원 : 경남대학교 대학원 컴퓨터공학과
††† 종신회원 : 경남대학교 정보통신공학부 교수
논문접수 : 2003년 5월 26일, 심사완료 : 2003년 9월 30일

및 제공하고 있지 않은 실정으로 무선통신망에서 모바일 서비스(무선상거래, 모바일 인터넷, 위치서비스, 전자지불시스템 및 전자화폐 등)를 이용할 경우 개인, 기업 및 금융정보 등이 유출되는 보안사고가 발생하고 있고 증가되는 실정이다. 그래서 유럽을 중심으로 USIM 카드 응용 프로그램 개발 지원도구의 개발이 추진되고 있으며 곧 상용화가 가능할 것으로 전망하고 있다. 국내에서는 한국전자통신연구원(ETRI), KT 아이컴 등에서 USIM 카드 개발을 추진하고 있다. 그러나 현재 국내에서 USIM 카드 응용 프로그램 개발을 위한 개발 지원 도구를 상용화 제품으로 생산하는 업체는 없으므로 국내의 USIM 카드 개발 및 상용화와 함께 개발 지원 도구의 개발이 병행되는 추세이다.

본 연구진은 현재 국내외적으로 USIM이 장착된 제 3세대 이동통신 단말기인 IMT-2000(WCDMA)에서 정보보안 기술을 지원하고 있지 않기 때문에 표준화된 3GPP 규격, 자바카드 기술과 규격 그리고 암호화 기술 등을 사용하여 USIM 카드에 사용자 인증 기술의 적용 가능성을 고려한 자바카드 기반(인증서버/단말기/자바카드) 사용자 인증 프로토콜을 설계 및 개발하고자 한다.

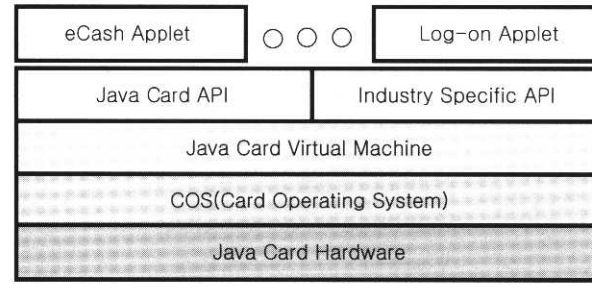
본 논문의 구성은 다음과 같다. 2장에서는 자바카드 요소기술에 대해 소개하고, 3장에서는 무선 이동통신망에서 요구되는 보안사항에 대해 기술한다. 4장에서는 자바카드 기반 무선단말기용 사용자 인증 시스템의 개요와 사용자 인증 프로토콜 설계 내용을 기술하고, 이 설계 기술을 이용하여 5장에서는 사용자 인증시스템 구현 테스트와 제안된 인증 프로토콜의 안전성을 분석한다. 6장에서는 결론과 연구결과의 활용 방안 그리고 앞으로의 연구 방향에 대해 기술한다.

2. 자바카드 기술

스마트카드는 오늘날 가장 작은 컴퓨팅 플랫폼으로 인식되고 있다. 스마트카드의 메모리는 보통 1KB(Kilo Byte)의 RAM과 16KB의 EEPROM, 그리고 24KB의 ROM으로 구성(최근에는 Flash 메모리도 사용되는 추세)되어 있다. 이러한 환경에서의 자바카드 기술은 Java 언어로 작성된 프로그램이 스마트카드, USIM이 장착된 IMT-2000 혹은 그 밖에 제한적인 자원을 가진 장치에서의 동작을 가능하게 한다.

2.1 자바카드(Java Card)

자바카드란 스마트카드 기술을 기반으로 하여 자바의 기술을 접목시킨 것으로 (그림 1)과 같이 COS(Card Operating System) 위에 JCVM(Java Card Virtual Machine) 이 래핑(Wrapping)되어 있는 구조의 IC 카드를 말한다[3].



(그림 1) 자바카드 구조

자바카드 API는 자바카드상의 JCVM상에서 자바를 이용한 응용 소프트웨어 개발에 필요한 API들을 정의한 것이다. 이것은 스마트카드의 보안성을 연구하던 Schlumberger 사의 연구팀에 의해 1996년에 소개되었다. 이후 발표된 자바카드 API 1.0은 단지 명세서의 역할만을 했다. 그러나 1997년 Sun Microsystem 사에서 자바 API의 일부 제한된 기능을 수행하는 API 2.0을 발표하였다[4]. 그후 계속 발전하여 현재 2.1.2 버전까지 개발되어 있는 상태이다. 자바카드 API는 전자상거래, 네트워크 접근, 인증을 위한 차세대 네트워크 기술을 제시하였다[4]. Bull, Gemplus, Schulmberger 등 전 세계 스마트카드 제조회사의 90% 이상이 자바카드의 개발을 위해 라이센스를 이미 받은 상태이다[6].

자바카드 API는 스마트카드와 같은 작은 메모리를 가진 임베디드 장치를 위한 프로그래밍에 필요한 패키지와 클래스만을 정의하고 있다. 또한 국제 표준인 ISO-7816과 산업 명세 표준인 EMV(Europay/MasterCard/Visa)와 서로 호환된다.

자바카드는 스마트카드 기술에 자바의 기술을 접목 시켰기 때문에 다음과 같은 특징들을 제공한다[7].

- **플랫폼 독립성** : 자바카드의 JCAE(Java Card Application Environment)를 기반으로 동작하도록 작성된 애플릿은 서로 다른 업체에서 생산된 자바카드들에서 동작할 수 있다.
- **복수의 응용프로그램** : 하나 이상의 응용 프로그램이 하나의 카드 상에서 동작할 수 있다. 자바는 상속구조와 코드의 다운로드 가능성을 가지고 있기 때문에, 보다 쉽게 하나의 카드상에서 복수개의 응용프로그램을 안전하게 실행할 수 있다.
- **응용프로그램의 갱신** : 카드가 발급된 후에 응용프로그램을 설치할 수 있다. 사용자는 카드를 발급 받은 이후에 변경되는 응용프로그램들을 보다 쉽게 갱신 또는 추가할 수 있다. 다시 말해, 새로운 응용 프로그램들이 설치된 카드를 추가적으로 발급 받는 것이 아니라 이미 존재하는 카드의 응용 프로그램만을 변경하거나 추가함으로써 새로운 서비스를 이용할 수 있다.

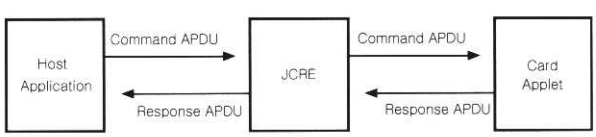
- **융통성** : 자바카드 기술의 객체지향 기술은 스마트카드 프로그래밍에 융통성을 제공한다.
- **호환성** : 자바카드는 국제 표준인 ISO-7816과 산업 표준인 EMV와 호환된다.

2.2 자바카드 애플릿

자바카드 애플릿은 자바카드 상에서 실행될 수 있는 자바 프로그램이다[4]. 자바카드 애플릿은 일반 자바 애플릿과 달리 브라우져 환경에서는 실행될 수 없다. 자바 응용프로그램과 달리 애플릿은 카드의 ROM에 설치될 필요가 없고, 단지 카드상에 다운로드함으로써 사용이 가능하게 된다. 자바카드 애플릿의 특징은 다음과 같다.

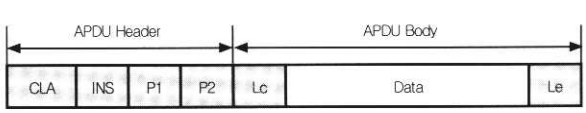
- JCRE(Java Card Runtime Environment)에서 수행된다.
- APDU(Application Program Data Unit) 교환을 통해 JCRE와 통신한다.
- AID(Application IDentifier)에 의해 식별된다.
- 자바카드상에 동적으로 다운로드 될 수 있다.

애플릿과 호스트간의 통신은 (그림 2)와 같이 명령 APDU와 응용 APDU로 구성되는 APDU 교환을 통해서 이루어진다. APDU 교환은 애플릿과 호스트간에 직접 이루어지는 것이 아니라 JCRE를 매개로 하여 이루어지고, JCRE는 애플릿과 호스트간에 교환되는 APDU의 관리와 감독 역할을 수행한다. 따라서 애플릿과 CAD(Card Access Device) 또는 호스트간의 직접적인 통신은 불가능하며, JCRE를 통한 통신만이 가능하다[4].

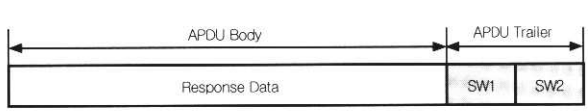


(그림 2) 애플릿 통신

APDU는 카드상의 통신에서 사용되는 전송 메시지의 형태로 ISO 7816에 구성되어 있다. 전송방식은 명령(Command)과 응답(Response)으로 이루어져 있다. (그림 2.1)과 (그림 2.2)은 APDU 구조를 살펴본 것이다[5].



(그림 2.1) 명령(Command) APDU 구조



(그림 2.2) 응답(Response) ADPU 구조

3. 무선 이동통신의 보안 요구사항

무선 이동통신에서 제공하는 다양한 부가 서비스를 제공받기 위해서는 가입자 인증과 결재방식이 필요하다. 이에 따라 유럽의 ETSI와 DECT(Digital European Cordless Telecommunications), 미국의 TIA/EIA(Telecommunications Industry Association/Electronic Industries Association) 그리고 한국의 TTA(Telecommunications Technology Association)에서 디지털 이동통신 무선 인터페이스 표준에 인증기능을 권고하고 있다.

3.1 가입자 인증(Subscriber Authentication)

무선 이동통신 시스템에서는 가입자와 이동통신 네트워크간의 유선접속방식이 존재하지 않기 때문에 무선접속 서비스의 불법적인 사용 즉, 단말기 가입자 번호를 전파 스캐너로 도청한 후 해당 가입자로 로그인하여 가입비와 사용료를 물지 않고 응용 서비스를 받게 되므로 사업자와 가입자 양쪽에 엄청난 피해가 발생한다. 따라서, 안전한 이동통신 서비스를 제공하기 위하여 각국의 이동통신 표준화 기구에서는 이동통신 표준화에 인증기능 추가를 권고하고 있다.

가입자 인증 및 세션 키 설정에 사용되는 암호방식은 크게 비밀키 암호기반 방식과 공개키 암호기반 방식으로 나눌 수 있다. 비록, 공개키 방식이 키 관리 측면에서 유리하지만 구현상에 있어서 많은 계산량 요구되기 때문에 무선 이동단말기에서는 하드웨어적인 제약성으로 인하여 원활한 지원을 못하는 실정으로 비밀키 암호기반 방식을 사용하고 있다[8].

3.2 일회용 패스워드(OTP ; One-Time Password)

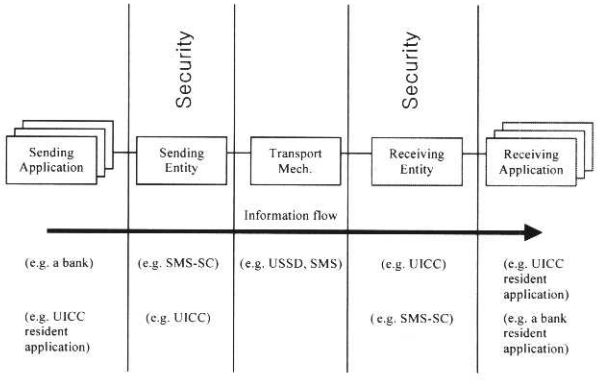
일반적인 ID와 패스워드를 입력하는 인증 방식은 Sniffer에 의한 패킷 가로채기 공격을 당할 수 있기 때문에 매번 로그인 할 때 마다 새로운 패스워드를 사용하는 일회용 패스워드 방식이 필요하다. 인증서버(혹은 시스템)가 로그인하려는 사용자에게 난수(Random Number)[or 시각표(Time-stamp), 순번(Sequence Number)]을 보내면, 사용자는 자신의 패스워드와 난수[or 시각표, 순번]를 일회용 패스워드 계산기에 입력하여 일회용 패스워드를 얻은 후 인증서버로 보낸다. 인증서버는 일회용 패스워드를 받아 자신이 계산한 값과 비교하여 시스템 및 응용서비스 접근 권한을 결정한다.

그러므로 일회용 패스워드는 무선통신의 공중망상에서 패스워드가 노출되더라도 패스워드의 유효기간을 1회로 한정했기 때문에 더 이상 오용할 수 없다는 장점을 갖고 있다. 일회용 패스워드 기술의 종류는 S/Key 일회용 패스워드 시스템, Time-Synchronous 방식 그리고 Challenge-Response 방식 등이 있다. 이 방식 중 Challenge-Response 방식은 여

러 번의 절차로 인해 다소 느리다는 단점이 있기는 하지만, Time-Synchronous 방식에 비해 복잡성이 덜하고 안전성이 높기 때문에 최근 이 방법을 적용한 인증 시스템이 국내외에서 많이 개발되고 있다[9].

3.3 3GPP TS 23.048 Security Mechanism(SMS)

자바카드와 인증서버(서비스센터)간에 안전하게 정보를 교환하기 위해 필요한 기술이 3GPP(3rd Generation Partnership Project) TS 23.048 Security Mechanism for (U)SIM Application Tool Kit의 Security API이다. (그림 3)는 3GPP TS 23.048에 명시되어 있는 SMS(Short Message Service) 패킷 전송 방식을 이용하여 무선통신망에서 안전하게 정보를 송수신하는 방법이다[1].



(그림 3) 무선통신망에서 안전한 정보교환 방법

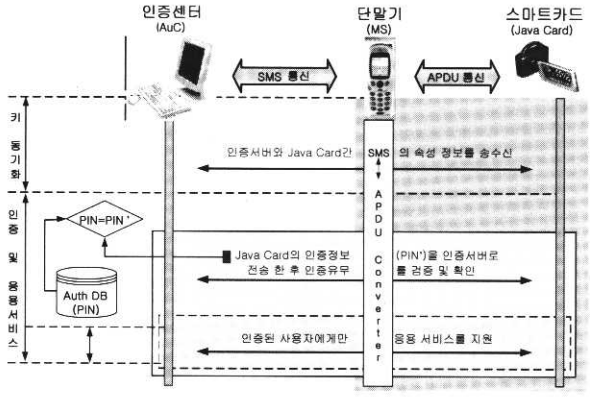
4. 자바카드 기반 무선단말기용 사용자 인증 프로토콜의 설계

본 연구진이 개발한 자바카드 기반 무선단말기용 사용자 인증 시스템은 정보보호 모델의 설계(세션 키 설정 및 가입자 인증)와 각 프로토콜별 사용되는 표준화된 암호 알고리즘, 메시지 인증코드, 해쉬함수 및 수행절차 그리고 무선통신에서 3GPP(유럽중심)/3GPP2(북미중심)의 안전한 단문서비스 방법을 사용하여 설계 및 구현하였다.

4.1 시스템 개요

자바카드에 필수적인 보안기능은 인증기술과 접근제어 이다. 이중 인증서버와 단말기 및 자바카드간의 사용자 인증 기술은 안전한 SMS 및 APDU 통신, 3DES-CBC 알고리즘과 메시지 인증코드 그리고 일회용 패스워드를 이용한 시도-응답 인증방식을 사용하고, 인증절차는 키 동기화 부분과 사용자 인증 부분으로 나누어져 있다.

(그림 4)와 같이 안전한 SMS 및 APDU 통신을 통하여 인증서버(서비스센터)와 단말기 그리고 자바카드 간에 속성정보(난수, 가입자 정보 등)를 전송하여 세션 키(Session Key)를 생성하고, 이 세션 키로 속성 정보(난수, 가입자 정보 등)를 암호화하여 상호전송 및 검증함으로써 인증서버와 단말기 기기간의 인증 및 키 동기화가 이루어진다. 그리고 키 동기화 한 후 인증서버는 일회용패스워드 방식을 이용하여 단말기에서 세션 키로 암호화한 스마트카드 PIN′ 정보를 전송받아 복호화 한 후, 인증 DB의 MD(PIN′s) 정보와 MD(PIN′) 정보를 비교하여 동일한 값이 존재하면 인증한다. 그리고 인증에 성공한 사용자에게만 응용 서비스(프로그램 다운로드)를 실행할 수 있는 권한을 부여한다(단말기의 역할은 인증서버와 자바카드 사이에서 SMS 패킷을 APDU 형태로 혹은 그 역으로 변환하고 정보를 전달하는 역할만 수행한다).



(그림 4) 자바카드 기반 무선단말기용 사용자 인증 시스템

4.2 사용자 인증 프로토콜

사용자 인증 프로토콜은 크게 3부분으로 나누어져 있다. 첫째는 서버에서 3GPP의 Secure SMS 패킷을 이용한 안전한 정보 전송 방식이고 둘째는 인증서버와 자바카드사이의 세션 키 설정(키 동기화) 프로토콜이며, 그리고 나머지 하나는 인증서버와 자바카드간의 사용자 인증 프로토콜이다.

본 논문에서 제안하는 세션 키 동기화 및 사용자 인증 절

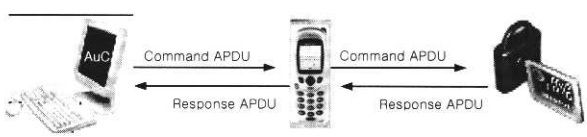
〈표 1〉 사용자 인증 프로토콜 표기

표 기	의 미
||	두개의 문자열을 연접한다는 의미
ki	인증서버와 자바카드 사이에 설정된 초기 암호 키
E	Encryption의 약자로 암호화 수행을 의미
D	Decryption의 약자로 복호화 수행을 의미
sk	인증서버와 자바카드 사이에 설정된 세션 키
mk	인증서버와 자바카드 사이에 설정된 MAC 키
Server_r	인증서버에서 생성한 난수
JC_r	자바카드에서 생성한 난수
IMSI	International Mobile Subscriber Identity의 약자
SOTPr	인증서버에서 OTP 검증용으로 생성한 난수
E_last8	암호화된 정보의 끝에서 8바이트 축출
MAC	3DES-CBC Mode를 사용한 메시지인증코드
PIN	Personal Identification Number(개인식별번호)
fail_count	사용자 인증 실패 횟수를 계산

차의 특징은 GSM 인증 방식과 비교해 볼 때 초기 암호키를 계속 사용하지 않고 세션 및 MAC 키를 서버와 자바카드의 고유 정보를 사용하여 생성함으로써 키 노출에 대한 대비와 기기간의 상호인증이 가능하고, 일회용패스워드 시도-응답 사용자 인증방식을 사용함으로써 위장공격을 막을 수 있어 사용자 인증 기능 및 신뢰성을 향상 시킬수 있습니다. <표 1>은 본 프로토콜에 사용되는 표기법을 나타낸다.

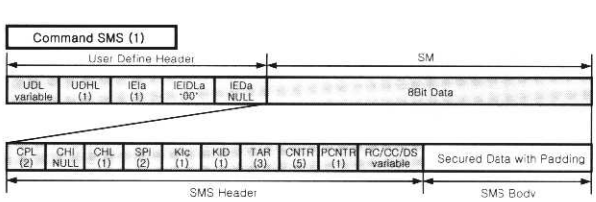
4.2.1 인증서버에서 자바카드로 Securing Message 전송방식

무선통신망(AuC에서 단말기)에서 안전하게 정보를 송수신 하기 위하여 3GPP TS 23.048 규격에 명시된 'Implementation for SMS(Secure SMS)'을 기반으로 설계하였으며, 단말기와 자바카드간은 APDU 통신을 기반으로 아래와 같이 설계하였다.

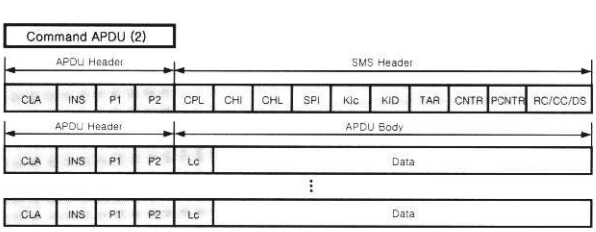


(그림 5) 서버/단말기/자바카드 사이의 Securing Message 전송방식

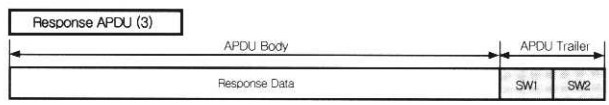
(그림 5)에서 보는 것과 같이 정보 전송절차는 인증센터(AuC ; Authentication Center)에서 단말기(MS ; Mobile Station)로 3GPP 23.048(Secure SMS 패킷)에 명시된 Command SMS을 구성하여 메시지를 전송하고, 단말기는 전송 받은 Command SMS을 자바카드로 ISO 7816에 명시된 Command APDU를 구성(변환)하여 전송한다. 자바카드는 전송받은 Command APDU에 대한 Response APDU를 단말기로 보내면, 단말기는 Response SMS을 구성(변환)하여 인증센터로 전송하여 키 동기화 및 인증을 수행한다.



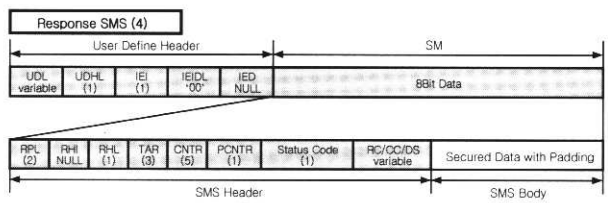
(그림 5.1) Command SMS 패킷 구조



(그림 5.2) Command APDU 구조



(그림 5.3) Response APDU 구조



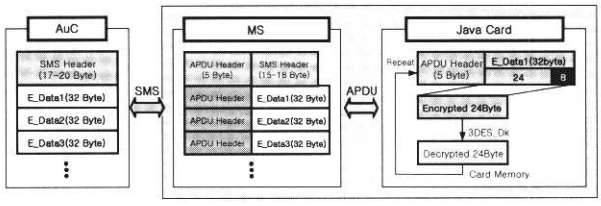
(그림 5.4) Response SMS 패킷 구조

(그림 5.1)과 (그림 5.4)는 3GPP 통신 보안 메커니즘으로 제공하고 있는 23.048 규격을 기반으로 설계된 안전한 SMS 패킷의 구조로 전송방식은 명령(Command)과 응답(Response) 방식으로 이루어져 있다. 또한 (그림 5.2)과 (그림 5.3)은 자바카드 상의 통신에 사용되는 전송 메시지의 형태로 ISO 7816에 규정된 APDU 통신으로 전송방식은 명령(Command)와 응답(Response)으로 이루어져 있다. <표 2>는 안전한 SMS 통신에 사용되는 보안관련 태그 필드들을 정리한 내용이다.

<표 2> SMS 보안관련 태그필드

태그 필드	내 용	비 고
SPI	• Cryptographic Checksum • Ciphering • PoR response shall be ciphered	Command
KIc	• Algorithm Identifier • DES-ECB, DES-CBC, 3DES-CBC(2/3 Key)	Command
KID	• Key Identifier • DES-CBC, 3DES-CBC(2/3 Key)	Command
PCNTR	• Padding Counter	Command Response
Secured Data with padding	• Encrypted information included data and padding	Command
Additional Response Data	• Request encrypt data with padding	Response

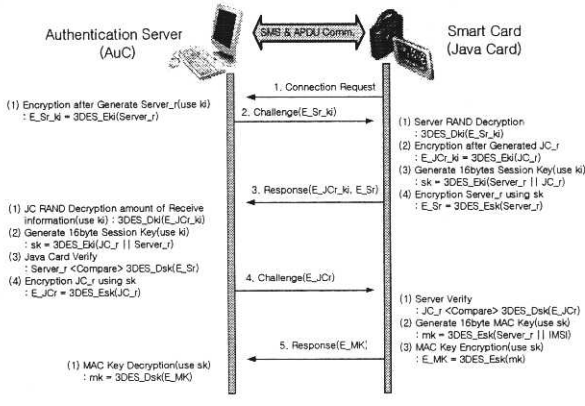
(그림 6)은 Securing Message 구조로 기기간 보안 메시지 구성과 전달 절차는 인증센터(AuC ; Authentication Center)에서 단말기(MS ; Mobile Station)로 3GPP 23.048(SMS 패킷)에 명시된 140바이트(헤더와 암호화된 32바이트 문자열 3개[96Byte]를 연접한 정보)를 구성하여 전송하고, 단말기는 전달 받은 정보를 APDU에서 읽을 수 있는 형태(헤더와 32바이트 문자열)로 변환시킨 후 APDU를 통하여 자바카드로 전달하면 자바카드는 전달 받은 정보를 복호화한다.



(그림 6) 서버/단말기/자바카드간의 Securing Message 구조

4.2.2 기기간 상호 인증 및 키 동기화 절차

무선통신망에서 안전하게 정보를 전송하기 위하여 먼저 기기간 상호인증 및 키 동기화 절차가 필요하다. 기기간 상호인증 및 키 동기화는 다음과 같은 절차로 수행된다.



(그림 7) 서버/단말기/자바카드간의 기기인증 및 세션 키 설정 프로토콜

단계 1 (AuC < Java Card) : 서버로 접속 요청을 한다.

단계 2 (AuC > Java Card) : 서버의 난수를 생성한 후 ki로 암호화하여 자바카드로 전송한다(**E_Sr_ki**).

단계 3 (AuC < Java Card) : E_JCr_ki와 E_Sr을 서버로 전송한다.

① 전송 받은 서버의 난수를 복호화한다.

② Java Card(JC)의 난수를 생성하고 ki로 암호화한다(**E_JCr_ki**).

③ Server_r과 JC_r을 연접한 후 ki로 암호화하여 16바이트의 세션 키를 생성한다.

④ sk로 Server_r을 암호화한다(**E_Sr**).

단계 4 (AuC > Java Card) : E_JCr을 자바카드로 전송한다.

① 전송 받은 E_JCr_ki를 ki로 복호화한다.

② JC_r과 Server_r을 연접한 후 ki로 암호화하여 16바이트의 세션 키를 생성하여 **세션 키를 동기화** 한다(***세션키 동기화 완료***).

③ 세션 키로 복호화[3DES_Dsk(E_Sr)] 한 값과 Server_r를 비교하여 **자바카드 기기를 검증[인증]** 한다.

④ sk로 JC_r를 암호화한다(**E_JCr**).

단계 5 (AuC < Java Card) : E_MK를 서버로 전송한다.

① 세션 키로 복호화[3DES_Dsk(E_JCr)] 한 값과 JC_r를 비교하여 **서버 기기를 검증[인증]**한다(***상호 인증 완료***).

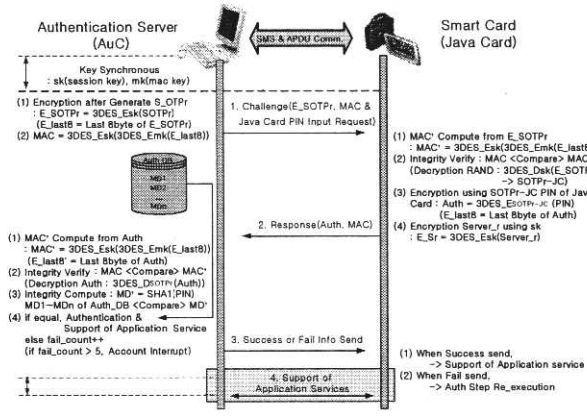
② Server_r과 IMSI(가입자 식별번호)을 연접한 후 sk로 암호화하여 16바이트의 MAC 키를 생성한다.

③ sk로 mk를 암호화한다(**E_MK**).

단계 6 (AuC) : 인증센터는 전송받은 E_MK를 sk로 복호화하여 **MAC 키를 동기화** 한다(***MAC 키 동기화 완료***).

4.2.3 사용자 인증 절차

무선통신망에서 안전하게 정보를 전송하기 위해서는 세션(sk) 키 동기화 이후 사용자 인증절차가 필요하다. 일회용 패스워드를 이용한 시도-응답 사용자 인증 절차는 다음과 같은 절차로 수행된다.



(그림 8) 서버/단말기/자바카드간의 사용자 인증 프로토콜

단계 1 (AuC > Java Card) : Java Card로 E_SOTPr과 MAC을 전송하고 자바카드의 PIN 정보 입력을 요구한다.

① OTP 검증에 사용한 서버 난수(SOTPr)를 생성한 후 sk로 암호화한다(**E_SOTPr**).

② E_SOTPr문자열의 끝에서 8바이트를 축출하여 mk로 암호화한 후 다시 sk로 암호화 한다(**MAC**).

단계 2 (AuC < Java Card) : Auth와 MAC을 서버로 전송한다.

① 전송 받은 E_SOTPr로부터 mk와 sk를 사용하여 MAC'을 계산한다.

② MAC와 MAC'을 비교하여 인증 데이터에 대

한 무결성을 검증한다(무결성 검증에 성공하면, sk로 E_SOTPr를 복호화한다.
-> SOTPr-JC).

③ 입력한 PIN을 SOTPr_JC로 암호화한다(Auth).

④ Auth 문자열의 끝에서 8바이트를 축출하여 mk로 암호화한 후 다시 sk로 암호화 한다(MAC).

단계 3 (AuC > Java Card) : 성공 혹은 실패 정보를 자바카드로 전송한다.

① 전송 받은 Auth로부터 mk와 sk를 사용하여 MAC'를 계산한다.

② MAC와 MAC'을 비교하여 무결성을 검증한다 (**무결성 검증에 성공하면 SOTPr로 Auth를 복호화[OTP를 검증]하고, 무결성 검증에 실패할 경우 해당 인증절차를 취소한다[*일회용 패스워드 검증 완료*]**).

③ 복호한 Auth 문자열에서 PIN을 축출한 후 SHA1 해쉬함수를 사용하여 MD'을 계산하여 MD1~MDn까지 비교한다.

④ 만약 동일한 값이 인증DB에 존재한다면 응용서비스를 지원하고, 존재하지 않으면 실패횟수(fail_count)를 카운트하여 5회 이상 연속 인증에 실패하였을 경우 해당 계정을 차단한다 (Success/Fail).

단계 4 (Java Card) : 자바카드에서는 Success가 전송되면 응용서비스를 지원하고, Fail이 전송되면 인증과정을 재 수행한다.

5. 구현 테스트와 안전성 분석

본 논문에서 제안한 사용자 인증 프로토콜의 설계를 토대로 구현 테스트와 안전성을 분석하였다. 자바카드 기반 무선단말기용 사용자 인증 시스템은 호스트 환경에서 크게 3부분으로 나누어 구현하였다. 즉, 하나는 사용자인증 정보를 등록하는 부분이고 다른 하나는 사용자 인증 서비스를 지원하는 인증서버 그리고 마지막으로 자바카드가 장착된 무선단말기의 역할을 하는 클라이언트 Emulator로 구성되어 있다. 안전성 분석은 제안한 방식이 제한된 자원을 가지고 있는 무선환경 조건에 적합하고 안전성을 보장하는지에 대하여 분석하였다.

5.1 개발 도구 및 환경

자바카드 기반 무선단말기용 사용자 인증 시스템의 구현 및 실행 환경은 다음과 같이 인증센터, 무선단말기 및 자바카드 각각의 역할에 맞는 자바언어로 구현하였다[14].

- **JDK1.3 이상** : http://java.sun.com/j2se 사이트에서 다운로드 가능하고, 자바 응용프로그램을 컴파일하여 클래스 파일(.class)을 생성하는 썬 사에서 제공하는 개발 도구이다.
- **Java Card 2.1.2 DK** : http://java.sun.com/javacard/dev_kit 사이트에서 다운로드 가능하고, 클래스 파일(.class)을 캡 파일(.cap) 파일로 변환해 주는 개발 도구이다.
- **Java Communications API 2.0 Package** : http://java.sun.com/products/javacomm 사이트에서 다운로드 가능하고, 자바카드와 카드리더 사이에 APDU 통신을 지원하는 패키지이다.
- **SunJCE v1.2.x 이상** : http://java.sun.com/products/jce 사이트에서 다운로드 가능하고, 호스트에서 암호화 API를 지원하는 패키지이다.

5.2 사용자 인증정보 등록(UAIR)

사용자 인증정보 등록(UAIR ; User Authentication Information Register) 프로그램은 (그림 9)에서 보는 것과 같이 사용자 ID와 6자 이상의 PIN(or Password)를 입력하도록 구현하였다.

(그림 9) 자바카드 사용자 인증정보 등록 화면

인증정보 입력시 동일한 ID로 등록된 사용자 있을 경우에는 등록 수행을 중단한 후 재입력을 요구하며, 등록된 ID가 존재하지 않을 경우 정상적으로 암호 모듈을 사용하여 인증정보를 인증 데이타베이스에 저장하여 관리자가 관리한다.

5.3 사용자 인증 및 응용서비스 지원 테스트

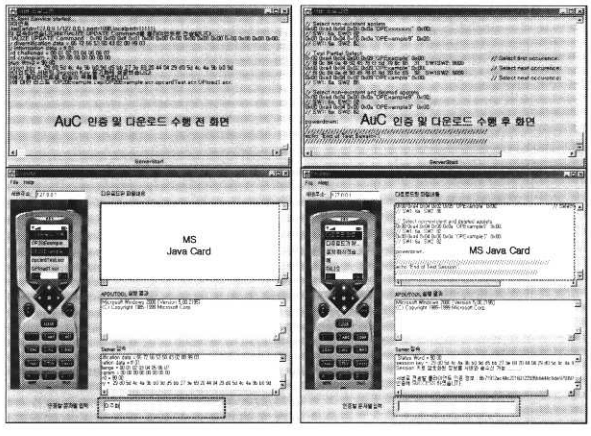
사용자 인증 프로토콜은 크게 인증서버와 자바카드를 포함하고 있는 클라이언트 Emulator 부분으로 나누어져 있다. 사용자 인증정보 등록을 통하여 생성한 인증정보는 인증서버에서 관리 운영하도록 구현하였다.

인증서버는 서버와 클라이언트 사이의 접속상태와 보안

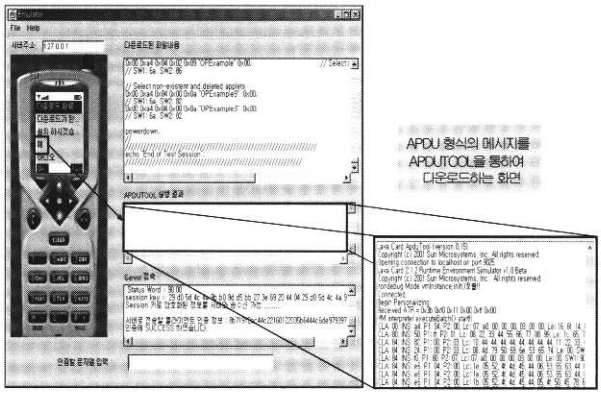
을 위한 세션 및 MAC 키 그리고 인증 및 클라이언트로의 응용서비스 지원 결과가 나타나며, UAIR에서 등록한 인증 DB와 응용 서비스 정보를 관리하는 역할을 한다.

클라이언트 Emulator는 인증서버로부터 전송 받은 정보를 자바카드까지 전송하면 자바카드는 해당정보를 수신 받아 처리하는 프로그램으로서 서버와 클라이언트 접속상태, 보안을 위한 세션 및 MAC 키 그리고 카드로 응용프로그램 전송 결과 등이 나타난다.

(그림 10)과 (그림 11)은 세션 키 설정 후 사용자 인증을 수행하기 전 화면과 자바카드로부터 PIN정보를 입력 받아 사용자 인증을 수행 한 후 클라이언트와 서버간에 송수신된 암호화 정보들과 응용 서비스(애플릿 다운로드)의 지원 결과를 보여주는 화면이다.



(그림 10) 서버/단말기/자바카드의 인증 수행 전후 화면



(그림 11) 무선단말기에서 자바카드로 CAP 파일 전송 화면

5.4 국내외 유사 기술과의 비교 분석

전 세계적으로 SIM 카드 응용프로그램 개발을 지원하는 개발 도구로 젬플러스사의 GemXplore Case 3.1 for Java Card와 ORGA사의 The Smart Card Integrator 등이 있으나 USIM 카드 응용프로그램 개발 지원 도구는 아직 상용화된 제품이 없는 상황이다. 특히 암호화 API나 인증기능을 제공 또는 지원하지 않는다. <표 3>은 이들 기술과 본 논문에서 구현한 기술을 비교 분석한 자료이다.

5.5 본 논문에서 제안하는 방식에 대한 보안의 안전성 및 성능 분석

본 논문은 무선환경에서 정보보호를 위하여 제안된 기술로 다음과 같이 무선환경에 적합한 처리 속도와 보안 강도를 고려하여 설계하였다.

- **기밀성(Confidentiality)** : 무선환경에서 시스템적인 제한요소와 무선환경의 특수성을 고려하여 보다 빠른 처리기능을 가진 암호 알고리즘이 요구됨으로 공개키 암호 방식보다는 처리 효율과 대량의 데이터 암복호화에 유리한 비밀키 암호 방식(Key Size 128bit 이상)을 사용하여 구현하였다.
- **무결성(Integrity)** : 무선환경에서 저장 및 전송데이터의 처리 효율성과 안전성을 고려하여 3DES-CBC 방식을 이용한 MAC 즉, 안전한 공유 무결성 키를 사용하여 무결성 값의 생성 및 점검을 수행함으로써 무결성 점검 기능을 향상시켰다.
- **개체 인증(Entity Authentication)** :
  - **기기간 상호인증** : 인증을 수행하는 두 개체에서 키 일치 및 사용자 인증을 수행하기 전에 먼저 인증을 수행할 정당한 기기인지 상호인증을 통하여 먼저 검증해야 한다. 이것을 수행함으로써 여기에서 새로 설정되는 안전한 세션 키와 무결성 키를 사용하여 네트워크 안전성을 보장한다.
  - **사용자 인증** : 시도-응답 일회용 패스워드(OTP)를 사용함으로써 위장공격에 대한 대비로 강력한 사용자 인증을 수행함으로써 한 시점에서 정당한 사용자에게만 응용서비스를 제공할 수 있다. 이것은 유용한 자원에 대한 제 3자의 임의 접근방지와 응용 서비스 지원에 대한 안전성을 보장한다.

〈표 3〉 자바카드 응용프로그램 개발 지원 기술 비교

구 분	GemXplore CASE3.1 for Java Card(GEMPLUS)	The Smart Card Integrator(ORGA)	본 기술
암호화 API	지원하지 않음	지원하지 않음	지원함
사용자 인증 기술	지원하지 않음	지원하지 않음	지원함
3GPP 23.048 (SMS)	지원하지 않음	지원하지 않음	지원함

- **키 일치(Key Agreement)** :
  - **세션키 일치** : 초기에 사용한 암호 키를 그대로 사용하는 것이 아니라 AuC와 자바카드 사이에 기기간 인증을 통하여 세션키를 동기화하여 사용함으로써 데이터 정보의 안전성을 향상시킬 수 있다.
  - **무결성 키 일치** : 일반적인 해쉬함수를 사용하지 않고 무선환경에 적합하면서 보안강도가 높은 3DES-CBC 방식과 안전한 공유 무결성 키를 이용하여 무결성을 점검함으로써 처리 속도와 보안 강도를 증대 시킬 수 있다.

<표 4>는 Pentium II 400에서 OpenSSL에서 지원하는 암호 알고리즘의 수행 속도를 비교 분석한 자료이다[11].

〈표 4〉 암호 알고리즘 수행 속도 비교

암호 알고리즘	OpenSSL	GoNative Provider
DES (KB/s)	6,792	5,165
3DES (KB/s)	2,392	2,142
RC4 (KB/s)	32,363	13,872
SHA-1 (KB/s)	22,838	10,014
DSA(sign/s)/(verify/s)	60/49	48/40

6. 결론 및 연구 결과의 활용방안

본 논문에서는 국내 최초로 USIM에 사용자 인증 기술 적용 가능성을 고려한 자바카드 기반 무선단말기용 사용자 인증 시스템을 설계 및 구현하였다. 인증서버와 단말기 그리고 자바카드간의 사용자 인증은 안전한 Securing Message(SMS/APDU), 3DES-CBC 알고리즘과 MAC, SHA1, Random Number 그리고 일회용 패스워드를 이용한 시도-응답 인증방식을 사용하고, 인증절차는 키 동기화 부분과 인증부분으로 나누어져 있다.

본 기술을 상용화할 경우 국내의 스마트카드(자바카드) 및 USIM 카드 응용 프로그램 개발 환경에 대한 개발 및 상용화 기술을 확보할 수 있다. 이는 스마트카드 및 개발 지원 도구 분야의 핵심 기술들을 외국에서 도입해온 국내의 실정을 감안하면 이 분야의 기술 개발을 가속화 할 수 있을 것으로 판단된다. 무선통신망에서 사용자 인증 기술은 무선 보안, 무선상거래, 모바일 인터넷, 전자지불 시스템 및 전자화폐, 위치서비스 및 교통카드시스템 등에 활용될 수 있습니다. 향후 모바일, 자바카드 및 USIM 카드의 하드웨어 제약성이 극복될 것이 예상되기 때문에 공개키 암호 알고리즘(ECC)을 이용한 시도-응답 인증 시스템과 3DES 알고리즘을 대체할 AES 알고리즘, 무선공개키 기반구조(WPKI ; Wireless Public Key Infrastructure) 그리고 유비쿼터스 컴퓨팅 환경에 대한 연구가 필요하다.

참 고 문 헌

[1] 한국전자통신연구소, (주)디지탈홈네트, "최종결과보고서(USIM Simulator 개발)", pp.1-122, 2002.

[2] 김충남, 이승준, 최호규, 신상욱외, "IMT-2000 이동통신 표준 개론", 한국정보통신기술협회(TTA), pp.3-80, 2002.

[3] 김연선, 이창욱, "자바카드 애플릿 설계 및 검증에 관한 연구", 한국통신정보보호학회 종합학술발표회논문지, Vol.10, No.1, p.805, 2000.

[4] Z. Chen, "Java Card Technology for Smart Cards," Addison-Wesley company, pp.42-72, 2000.

[5] 김성중, 이희규, 조한진, 이재광, "자바카드 기반 공개키 암호 API를 위한 임의의 정수 클래스 설계 및 구현", 정보처리학회 논문지C, Vol.9-C, No.2, pp163-172, 2002.

[6] http://java.sun.com/products/javacard/datasheet.html.

[7] http://java.sun.com/products/javacard/.

[8] 박창섭, "암호이론과 보안", 대영사, pp.359-383, 1999.

[9] http://www.kisa.or.kr/technology/sub4/password.html, "일회용패스워드 기술", 한국정보보호진흥원(KISA).

[10] 박중길, 장태주, 박봉주, 류재철, "시간을 이용한 효율적인 일회용 패스워드 알고리즘", 정보처리학회논문지C, Vol.8-C, No.4, pp.373-378, 2001.

[11] Rescorla, Eric., "SSL and TLS(Designing and Building Secure Systems)," Addison-Wesley company, pp.175-217, 2001.

[12] http://www.3gpp.org/spec/specs.htm, SMS Packet Specification.

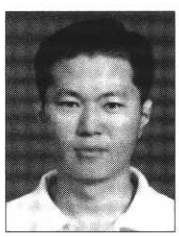
[13] http://www.tta.or.kr/fileDB/choan/TTAE.3G-23.048(R4-4.3.0).doc, Security Mechanisms for the (U)SIM application toolkit ; Stage 2 (Release 4)).

[14] http://java.sun.com/, Sun Microsystems, Java Home Page.

[15] http://www.3gpp.org, W-CDMA 유럽중심의 표준화 기구.

[16] http://www.3gpp2.org, CDMA-2000 북미중심의 표준화 기구.

[17] http://www.tta.or.kr, 한국정보통신기술협회.



이 주 화

e-mail : f13310@hotmail.com

1996년 경일대학교 컴퓨터공학과(공학사)

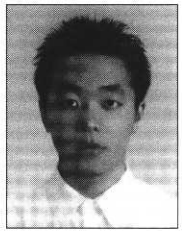
2000년 경남대학교 산업대학원 컴퓨터공학과(공학석사)

1996년~1999년 대한민국 해군 정보통신 장교 복무

2000년~2002년 (주)데이타게이트인터내셔널 부설 보안기술 연구소 주임연구원(IDS K4 인증 및 보안모듈 개발)

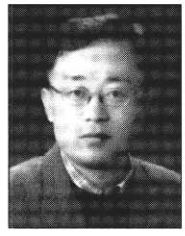
2003년~현재 경남대학교 컴퓨터공학과 박사과정

관심분야 : 정보보안, 자바카드 보안, 유무선 보안, 유비쿼터스 보안



설 경 수

e-mail : soo7991@yahoo.co.kr
2002년 경남대학교 컴퓨터공학과(공학사)
2002년~현재 경남대학교 컴퓨터공학과 석사과정
관심분야 : 스마트카드, 임베디드 시스템, 모바일 소프트웨어



정 민 수

e-mail : msjung@eros.kyungnam.ac.kr
1986년 서울대학교 컴퓨터공학과(공학사)
1988년 KAIST 전산학과(공학석사)
1994년 KAIST 전산학과(공학박사)
1988년~1990년 KAIST 전산학과 T.A 및 R.A
1990년~현재 경남대학교 정보통신공학부 교수
2000년~현재 (주)디지탈홈네트 기술이사
관심분야 : 자바카드, 임베디드 시스템, 유비쿼터스