# IMT-2000 에 장착된 USIM 서비스 지원을 위한 Securing Message 전송 기술에 관한 연구

설경수 , 이주화, 정민수
경남대학교 컴퓨터공학과

# Research about Securing Message transmission technology for USIM service support installed in IMT-2000

Kyungsoo Seol, Juhwa Lee, Minsu Jung
Dept. of Computer Engineering, Kyungnam Univ.
E-mail : soo7991@yahoo.co.kr

요 약

오늘날 USIM 서비스는 그 중요성과 사용자 요구에 의해 시장규모가 나날이 증가되어 가고 있는 추세이다. 본 논문에서는 USIM 서비스의 핵심 기술이라 할 수 있는 보안메카니즘 중 3GPP TS 23.048 과 자바카드 규격에 따라 IMT-2000 에 장착된 USIM 서비스를 지원하기 위한 Securing Message 전송 기술에 관하여 연구하였다.

## 1. 서론

IMT2000(WCDMA)은 제3세대 이동통신서비스로 전 세계적 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 IMT2000에서 제공하는 다양한 서비스를 제공 받기위해서는 사용자와 사용자 정보를 안전하게 보호할수 있는 보안 메커니즘이 필요하다. 이에 따라 ETSI(European Telecommunications Standards Institute)나 3GPP/3GPP2(3rd Generation Partnership Project) 같은 표준화 기구들은 UICC/USIM(Universal IC Card/Universal Subscriber Identify Module)을 IMT-2000의 UIM (User Identification Module) 표준규격으로 정하였다.

전 세계적으로 볼 때 SIM/USIM 카드 응용 프로그램 개발을 지원하는 개발 도구로 젬플러스 사와 ORGA 사 제품들이 있으나 이 제품들은 자국의 보안 정책상 암호화 모듈을 국외로 유출하는 것을 금하고 있어서 자국내를 제외한 국가에 대해서는 암호화 모듈과 사용자 인증 기술을 지원 및 제공하고 있지 않은 실정으로 무선통신망에서 모바일 서비스(무선상거래, 모바일 인터넷, 위치서비스, 전자지불시스템 및 전자화폐 등)를 이용할 경우 개인, 기업 및 금융 정보 등이 유출되는 보안사고가 발생하고 있고 증가되는 실정이다.

본 논문에서는 이러한 USIM 서비스의 보안사고를 미연에 방지하여 사용자와 사용자 정보를 안전하게 전송하기 위해 무선환경에서 서비스 제공 서버와 USIM간의 통신방식으로 SMS(Short Message Service)

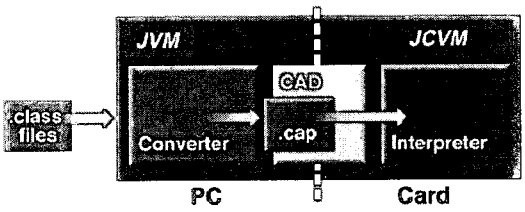
방식을 채택하였다. 안전한 데이터 전송을 위하여 SMS 패킷의 데이터 부분은 국제 암호 표준인 3DES 알고리즘을 사용하였고 3GPP TS 23.048 규격에 따라 서버와 USIM 간 안전한 SMS 통신을 위한 패킷을 설계 및 구현하였다.

## 2. 관련연구

### 2.1 자바가상기계(JCVM : Java Card Virtual Machine)

자바 카드 바이트코드를 수행하는 엔진인 JCVM은 JVM에 비해 스마트 카드에 적합하도록 최적화되어 Applet간의 방화벽 및 최적화된 명령어 등 Subset의 개념이라기 보다는 지원 내용은 작지만 별도의 새로운 수행환경을 구성한다.

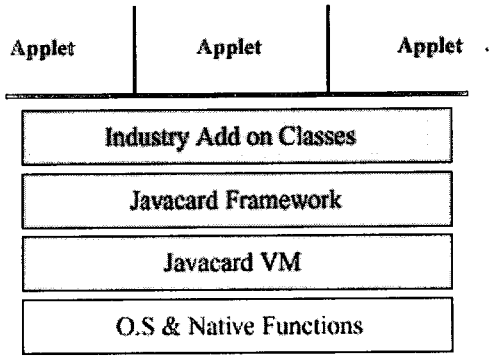
JCVM과 기존의 JVM의 차이점은 JCVM이 그림1과 같이 Off-Card VM과 On-Card VM으로 나뉘는 분할 가상기계로 이루어지며, 좁은 의미로는 수행 엔진인 인터프리터를 지칭하며 넓은 의미로는 프레임워크가 중심이 되는 시스템 클래스 API와 인터프리터, 메모리 관리 루틴, 예외처리루틴 그리고 운영체제와의 인터페이스 등을 포함하는 자바카드실행환경을 의미한다[1][2][4][5].




(그림1) 자바카드가상기계의 구성

### 2.2 자바카드 실행환경(JCRE:Java Card Runtime Environment)

자바카드실행환경은 스마트 카드 내에서 동작하는 컴포넌트들로 구성되는데 JCVM 역시 컴포넌트들의 하나다. JCRE는 카드 리소스 관리, 네트워크 통신, 애플릿 실행, On-Card 시스템 및 애플릿 보안에 대한 책임을 가진다.



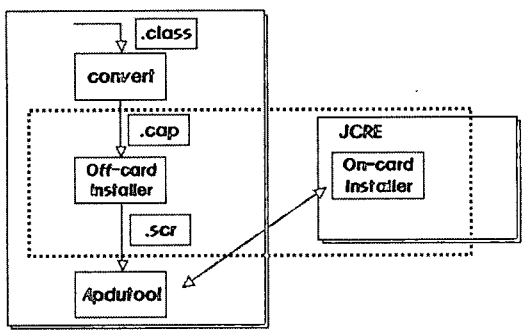

(그림2) On-Card 시스템 구성

### 2.3 자바카드 개발도구(JCDK : Java Card Development Kit)

자바카드개발도구는 Sun Microsystems 사에서 제공하는 것으로 ISO-7816의 표준화 규정에 따라 자바 카드 기술을 일반 워크스테이션에서 테스트할 수 있게 개발된 도구이며, 현재(2002.11) 2.2 버전까지 출시되었다[2][5][15].

### 2.4 자바카드 인스톨러(Java Card Installer)

자바 카드 인스톨러는 그림3과 같이 Off-Card 부분과 On-Card 부분으로 나누는데 그림으로 살펴보면 다음과 같다.



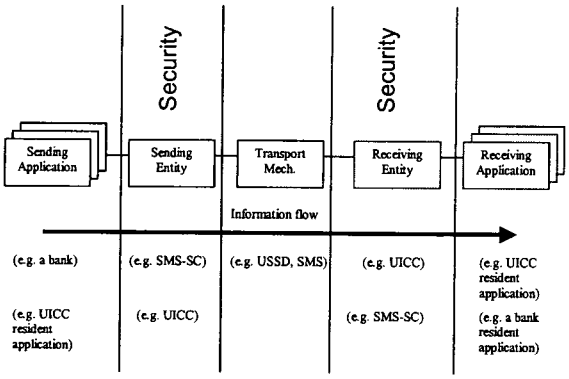

(그림3) 자바카드 인스톨 절차

Off_Card와 On-Card 두 부분 모두 하나의 실행파일

인 CAP 파일의 인스톨 과정을 돕는 역할을 한다. 각각 컴포넌트별로 나누어서 로딩단계를 거치게 되면, Off-Card 부분에서는 APDU 포맷으로 변형하여 카드와 CAD(Card Acceptance Device)간의 전송을 가능하게 한다.

2.5 3GPP TS 23.048

USIM과 서비스센터간에 안전하게 정보를 교환하기 위해 필요한 기술이 3GPP(3rd Generation Partnership Project) TS 23.048 Security Mechanism for (U)SIM Application Tool Kit의 Security API 이다. 그림4는 3GPP TS 23.048에 명시되어 있는 SMS(Short Message Service) 패킷 전송 방식을 이용하여 무선통신망에서 안전하게 정보를 송수신하는 방법이다.

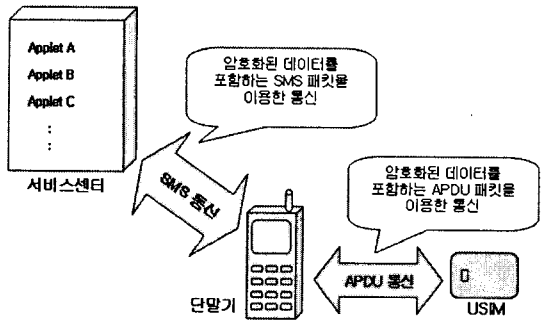



(그림4) 모바일에서 안전한 정보교환 방법

## 3. Securing Message 설계 및 구현

3.1 개요

본 논문에서 Securing Message 전송기술에 관한 설계는 크게 두가지 세션으로 나뉘어진다. 첫번째 세션은 서비스센터와 USIM 이 장착되어 있는 IMT-2000 단말기간의 통신이고, 두번째 세션은 IMT-2000 단말기와 그 단말기에 장착되어 있는 USIM 카드간의 통신이다.

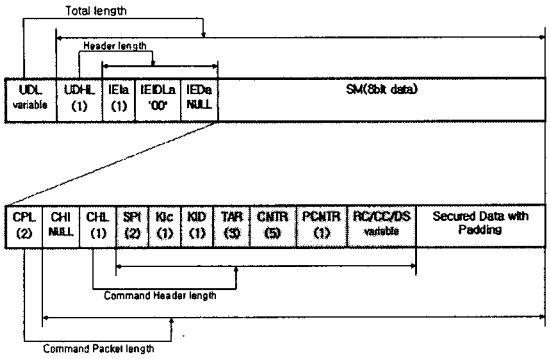



(그림5) 서비스센터, 단말기 및 USIM 의 통신

최초 사용자가 IMT-2000 단말기를 통해 서비스를 요구하면, USIM 과 서비스센터(서버)간에 세션이 맺어지고 동일한 암복호화 키를 생성한다. 그 다음 단계부터 서비스센터에서는 서비스에 필요한 데이터를 3DES 알고리즘으로 암호화한 후 무선통신이 가능한 SMS 패킷형식으로 포맷팅하여 IMT-2000 단말기로 전송하게 된다. 이때 단말기는 단지 전송받은 SMS 패킷이 일반 메시지가 아닌 USIM 까지 전달되어져야 하는 데이터라는 것을 확인한 후 그대로 USIM 까지 APDU 통신을 통해 Bypass 모드로 넘겨주는 기능만을 수행한다. USIM 은 단말기를 통해 서비스센터로부터 전송받은 SMS 패킷을 분석해서 데이터부분만을 추출해내고, 다시 암호화된 데이터를 동일한 암복호화 키를 이용하여 복호화하고 데이터의 무결성을 검증한다. 이로써 서버의 원본과 동일한 데이터를 얻은 후 USIM 의 인스톨러(Installer) 를 통해 카드에 설치하게 된다.

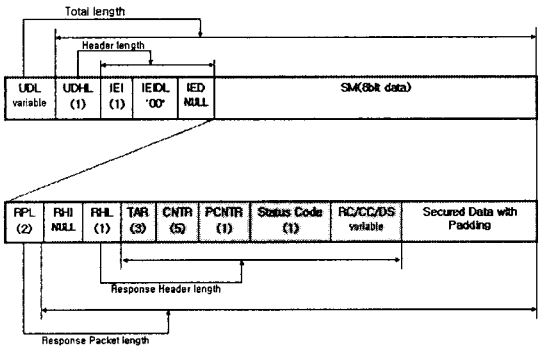
3.2 Securing Message 전송 설계

SMS 패킷은 Command, Response 의 두가지 타입으로 정의된다. 3GPP TS 23.048 규격에서 정의하는 Command 패킷의 구조를 기반으로 불필요한 태그를 제거하여 다음과 같은 구조로 설계하였다.




(그림6) SMS Command 패킷의 구조

SMS 패킷은 총 140옥텟(바이트와 동일)으로 구성되어 있다. 위 그림에서 상위패킷은 3GPP TS 23.048 스팩을, 하위 세부패킷 내용은 3GPP TS 23.040 (Technical realization of the Short Message Service)스팩을 기반으로 설계하였다. 상위 사용자 헤더부분에 해당하는 각 태그는 모두 1바이트로 설계하였으며, 하위 일반적인 보안 패킷 부분 중 커맨드 헤더 식별자인 CHI(Command Header Identifier)는 상위헤더부분에 식별자가 이미 존재하므로 NULL로 두어 사용하지 않는다. 그리고 헤더 바로 뒤로 나오는 암호화된 데이터(Secured Data with Padding)가 길면 CNTR(Counter) 태그를 카운터하여 SMS 패킷의 최대크기인 140바이트 만큼 분할하여 순차적으로 전송하도록 설계하였다.




(그림7) SMS Response 패킷의 구조

그림7은 SMS Response 패킷의 구조이다. 커맨드 패킷에 매칭되는 몇몇 태그를 제외하고는 동일한 구조이며, 단지 커맨드패킷을 받아 어떠한 동작을 했는지에 대한 응답패킷 상태를 보여주는 Status Code 만 추가되어있다.

SMS 패킷중커맨드 패킷과 응답패킷에 포함된 보안 관련 기능은 아래표와 같다.

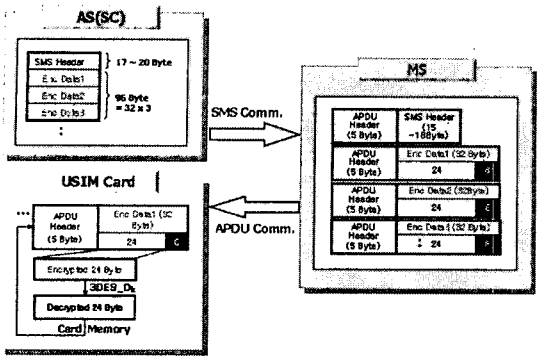
[표1] SMS 보안관련 태그필드

| 태그필드 | 내 용 | 비고 |
|---|---|---|
| SPI | - Cryptographic Checksum<br>- Chipering<br>- PoR response shall be ciphered | Command |
| KIc | - Algorithm Identifier<br>- DES-ECB, DES-CBC, 3DES-CBC(2/3key) | Command |
| KID | - Key Identifier<br>- DES-CBC, 3DES-CBC(2/3key) | 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 |

### 3.3 Securing Message 전송 구현

서비스센터-USIM간 전송은 중간자 역할을 하는 IMT-2000 단말기는 단순히 서비스센터의 SMS 패킷을 받아 그대로 USIM 까지 전달만 해주는 Bypass 기능만을 수행하는 것이 가장 이상적이다. 하지만 현재 IMT-2000-USIM 간 APDU 통신에서는 헤더(Header)를 포함해 최고 37바이트까지만 한번에 전송할 수 있다. 이러한 APDU 통신의 제약사항을 감안하여 Securing Message 전송을 서비스센터-IMT-2000 단말기간 전송과 IMT-2000-USIM간 전송으로 나누어서 구현을 하였다.

다음은 서비스센터-IMT-2000 단말기간 전송 및 단말기-USIM 간 통신을 도식화한 그림이다.

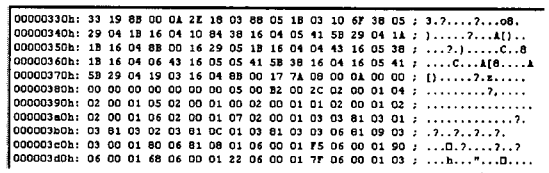



(그림8) 서비스센터-단말기-USIM 간 통신

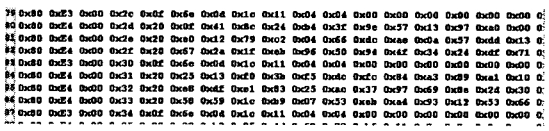
위 그림에서와 같이 서비스센터에서는 데이터를 암호화할 때 APDU 통신으로 전송할수 있는 크기인 32 바이트로 분할해서 암호화 한 후에 단말기에서 APDU 헤더로 5바이트가 붙여 총 37바이트가 된다. 또한, 암호화된 SMS 패킷을 수신한 IMT-2000단말기에서는 APDU 전송이 가능한 크기만큼 분할된 데이터를 APDU 형식으로 차례대로 파일에 저장하게 된다. 모든 데이터를 수신하면, 단말기에서 APDU 전송을 통해 USIM 으로 데이터를 전송하게 되고, USIM 에서는 SMS 헤더를 해석하고, 필요한 데이터를 추출, 복호화해서 Installer 에게 넘겨주게된다.


(그림9) 서버-단말기간 메시지 전송 실행

그림9는 서비스센터와 IMT-2000 단말기간 통신모듈을 구현하여 실행시킨 화면이다.



(그림10-1) 서버에 저장되어 있는 원본 Applet 파일



(그림10-2) 단말기에 저장되어 있는 APDU형식의 Applet 파일(암호화된 파일)

서비스센터에서는 그림10-1과 같은 Applet 헥사코드의 Applet 파일을 분할하고 암호화해서 단말기로 전송하게되고, IMT-2000 단말기에서는 그림10-2와 같이 APDU 형식으로 임의의 파일에 암호화된 Applet을 저장하게 된다. 이렇게 저장된 APDU 형식의 암호화된 Applet 파일은 APDU 통신을 통해 USIM 으로 전송되고, USIM 에서는 각 라인별로 복호화를 한후 USIM Installer 를 통해 USIM 의 메모리에 저장하게 된다.

## 4. 결론

본 논문에서는 차세대 IMT-2000 사업의 USIM 서비스 보안사고를 미연에 방지하여 사용자 정보를 안전하게 전송하고, USIM 의 다양한 서비스를 안전하게 제공받기 위한 Securing Message 전송에 관한 기술을 연구하였다. 이를 바탕으로 무선통신 환경에서 좀 더 안전한 메시지 전송이 가능할 것으로 전망된다. 또한 향후 IMT-2000 단말기나 USIM의 하드웨어 제약성이 극복될 것이 예상되기 때문에 앞서 언급한 서비스센터와 USIM 간의 이상적인 통신방식도 구현 가능할 것으로 전망된다.

본 기술을 상용화할 경우 국내의 스마트 카드 및 USIM 카드 응용 프로그램 개발 환경에 대한 개발 및 상용화 기술을 확보할 수 있다. 이는 스마트 카드 및

개발 지원 도구 분야의 핵심 기술들을 외국에서 도입해온 국내의 실정을 감안하면 이 분야의 기술 개발을 가속화 할 수 있을 것으로 판단된다. 무선통신망에서 Securing Message 전송 기술은 무선보안, 무선상거래, 모바일 인터넷, 전자지불 시스템 및 전자화폐, 위치서비스 및 교통카드시스템 등에 활용될 수 있다. 향후 모바일이나 USIM의 하드웨어 제약성이 극복될 것이 예상되기 때문에 공개키 암호 알고리즘(ECC) 과 3DES 알고리즘을 대체할 AES 알고리즘 그리고 무선공개키기반구조(WPKI; Wireless Public-Key Infrastructure)을 이용한 Securing Message 전송에 대한 연구가 필요하다.

## [참고문헌]


[1] 한국전자통신연구소, 경남대학교, "최종결과보고서"(Java Card Virtual Machine 성능개선에 관한 연구), 2001.

[2] 한국전자통신연구소, 디지탈홈네트, "최종결과보고서"(USIM Simulator개발), 2002.

[3] http://www.etimesi.com/ 전자신문 USIM 개발 및 기술동향 관련기사

[4] W.Rankl, W.Effing, "Smart Card Handbook, 2nd Edition ", John Wiley & Sons, 2001.

[5] Uwe Hansmann and Thomas Schäk, etc"Smart Card Application Development Using Java, Springer, 2002.

[6] De Gaudenzi, R. , "ESA Satellite Wideband CDMA Radio Transmission Technology for the IMT-2000/UMTS Satellite Component: Features & Performance", GLOBECOM -NEW YORK-, Vol.5 No.- ,1999

[7] Chaudhury, P., "The 3GPP Proposal for IMT-2000", IEEE communications magazine, Vol.37 No.12, 1999.

[8] Walker, M. "On the Security of 3GPP Networks", LECTURE NOTES IN COMPUTER SCIENCE Vol.- No.1807, 2000.

[9] Marinis, K. "On the Hardware Implementation of the 3GPP Confidentiality and Integrity Algorithms", LECTURE NOTES IN COMPUTER SCIENCE, Vol.- No.2200, 2001.

[10] "GSM Protocol Analyzer CRTU-G Changing of the guard: after more than 10 years, a new GSM reference system", NEWS- ROHDE AND SCHWARZ, Vol.- No.171, 2001.

[11] "3rd generation mobile systems UMTS/IMT 2000", ANNALES DES TELECOMMUNICATIONS, Vol.56 No.5-6 , 2001.

[12] Sun Microsystem. Java Card 2.1.1 Virtual Machine Specification, 2000.

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

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

[15] Sun Microsystems. JavaCard 2.2 Development Kit User's guide specification, 2002.

[16] Sun Microsystems. JavaCard 2.2 Application Programming notes, 2002.

[17] Gong L. Inside Java 2 platform security: architecture, API design, and implementation. The Java Series. Addison-Wesley, 1999.