主題

# 이동 통신에서의 보안 표준화 연구 현황

한국전자통신연구원 문종철, 김신효, 김유혁, 김재명

차 례



## I. 서 론

1990년대에 나타난 통신 분야의 커다란 흐름은 두 가지로 압축할 수 있다. 하나는 이동전화, 무선 LAN 그리고 위성 통신의 대중화이고 다른 하나는 인터넷을 중심으로 한 데이터 통신 및 멀티미디어 통신이라고 할 수 있다. 90년대에 주류를 이룬 이동 통신은 2000년 초반에는 글로벌 오퍼레이션, 서비스 능력의 향상 그리고 시스템 성능의 개선이라는 세가지 특징을 가지는 IMT-2000 3세대 이동 통신 시스템이[1][2] 등장하여 초미의 관심을 갖게 될 것으로 예상된다. IMT-2000 시스템은 현재 그리고 미래의 개별적인 통신망과 시스템을 통합하여 서로 다른 무선환경(협대역 CDMA, 광대역 CDMA, 위성등)에서도 단일 단말기 및 사용자 카드를 이용하여 고속, 고품질의 다양한 서비스를 제공하는 것을 목적으로 하고 있다.

현재 국내에서는 불법 사용에 의한 손실 규모가 정확하게 파악되고 있지는 않으나, 최근 불법 복제 단말기 유통이 사회적인 문제로 대두되고 있으며, 이에 대한 대책의 필요성이 인식되고 있으며, 이를 해결하기 위한 이동 통신에서의 보안 기술들이 대두되고 있다. 또한 다수의 이동통신 망 들이 존재함에 따라 네트워크 상호간의 연동 및 가입자 이동에 따른 가입자 식별을 뒷받침할 가입자 및 개인의 정보 관리 안전성과 복잡성 문제들이 대두되고 있는 실정이다.

이동 통신에서의 불법 사용에 대한 대책과 안전한 이동 통신 서비스 실현을 위하여 선진 각국은 이동 통신 업무의 표준화에 인증기능을 추가하고 있다. 미국의 TIA/EIA에서 권고하고 있는 인증 및 암호화 기능이나, 유럽에서 추진하고 있는 GSM(Global System for Mobile communication) 등과 같은 표준에서는 이미 인증을 포함한 시큐리티 서비스를 포함하고 있다.

국내에서는 한국전자통신연구원을 중심으로 미국

의 Qualcomm사와 공동으로 CDMA 방식을 이용한 이동통신 시스템 CMS(CDMA Mobile System)를 개발하였다. CDMA 이동 통신 시스템에서는 시스템의 가입자 수용 능력을 획기적으로 증가 시킬 수 있을 뿐 아니라 가입자 인증 기능을 포함하고 있어 불법 사용을 방지할 수 있다. 또한 미국의 TIA/EIA 표준 TR45.0을 근거로 만들어진 한국통신기술협회(TTA: Telecommunications Technology Association) 국내 표준[3]에서는 시도-응답(Challenge-response) 방식에 근거한 인증 기능의 제공을 권고하고 있다. 미국에서는 시도-응답 방식에 의한 인증기능을 제공하기 위하여 CAVE(Cellular Authentication and Voice Privacy)라고 하는 인증 알고리즘을 개발하여 사용하고 있다. GSM에서는 A3라고 불리는 인증 알고리즘을 사용하고 있으며, 암호 알고리즘 A5 스트림 암호(54비트)는 3GPP에서 개발하고 있는 무선 접속방식UTRAN(UMTS Terrestrial mobile Radio Access Network)에 부적합하여, 메시지에 대한 가변 길이의 비트 스트림을 출력하는 새로운 암호 알고리즘이 개발이 필요하다고 인식이 되어, 3GPP PCG TSG 분과의 SA(Security Aspects)에서는 알고리즘에 관한 설계 기준을 제시하고, 설계 규격을 검토하며, 알고리즘 선정 및 평가 작업을 수행하고 있는 중이다. 그러나 선진 각국들은 인증 알고리즘과 같은 암호 기술에 대해서는 공개하지 않고 수출 또한 제한하고 있다. 그리하여 국내에서도 이와 같은 공동 작업에 참여하여 공동 지적재산권을 확보하여야 한다.

본 고에서는 현재의 이동 통신망 시스템 개요 및 보안 표준화 동향을 알아보고 차세대 이동 통신 표준화에서 논의되는 보안 기술들과 이동 통신 망 보안의 핵심 요소들 중에 하나인 가입자 스마트 카드의 현황에 대하여 설명하고자 한다.

# II. 이동통신 망 개요 및 보안

## 1. CDMA 시스템

본 절에서는 CDMA 표준으로 사용되고 있는 IS-95A의 시스템 및 인증 과정을 살펴본다[4]. IS-95A 이동 통신 시스템은 그림 1과 같이 이동국(MS, Mobile Station), 기지국(BS, Base Station), 이동 통신망을 위한 교환센터(MSC, Mobile Switching Center), 가입자 홈 위치 등록 레지스터(HLR, Home Location Register), 방문자를 위한 위치 등록 레지스터(VLR, Visitor Location Register), 그리고 인증 센터(AC, Authentication Center)로 이루어져 있다.

이동국은 이동 통신 서비스를 제공 받는 단말기이며 기지국은 이동국과의 무선접속 그리고 무선교환센터와 단말기 연결 기능을 제공한다. 무선교환센터는 유선 통신망과 연동하며 이동 전화 가입자의 회선교환, 호처리, 핸드오프 등의 역할을 담당한다. 홈 위치 등록 레지스터와 방문자를 위한 위치 등록 레지스터는 일종의 데이터 베이스로서 이동 단말기의 현재 위치 정보, 상태 그리고 서비스 관련 정보 등을 관리한다. 인증 센터는 단말기의 마스터 키 관리, COUNT 관리, 인증 절차 수행 등과 같은 기능을 수행한다.

IS-95A를 따르는 CDMA 시스템에서의 인증 절차는 인증 센터와 이동국간에 시도-응답(challenge-response)형태의 단방향 그리고 대칭키 암호 알고리즘을 기반으로 수행된다. 인증을 위한 입력 키 값으로는 A_key(Authentication Key)로부터 유도된 두 개의 키 SSD_A, SSD_B 중 SSD_A가 사용된다. SSD_B는 음성 비화(voice privacy) 및 데이터 암호화를 위해 사용된

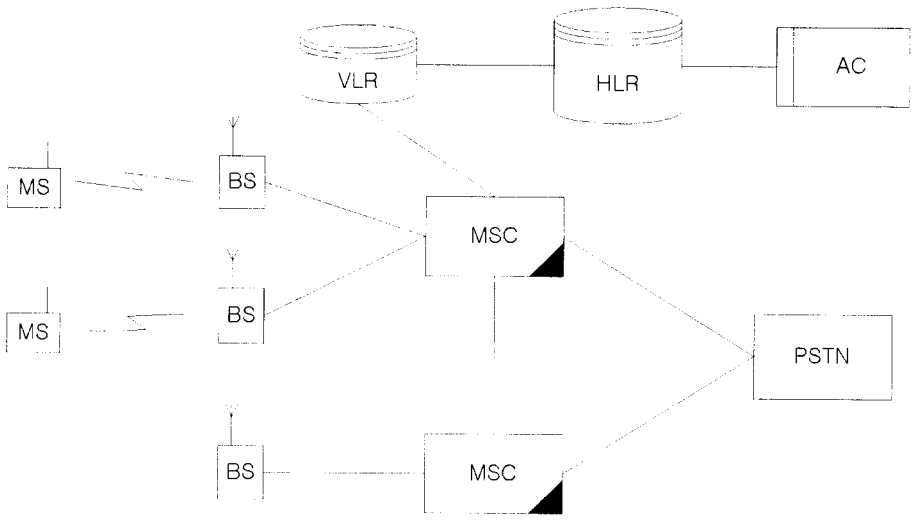



그림 1. IS-95 A 시스템의 구성

다. 그림 2는 인증 서명 값인 AUTH_SIGNATURE를 계산하는 과정을 나타낸다.

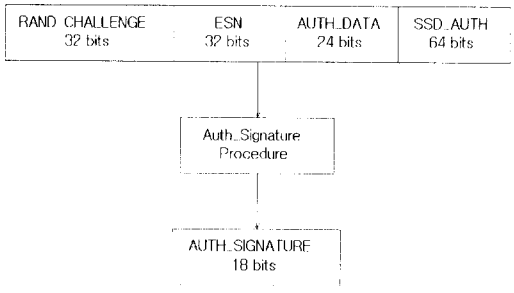



그림 2. 인증 서명의 생성 과정

IS-95A 시스템에서 인증에 사용되는 알고리즘은 CAVE(Cellular Authentication and Voice Encryption) 알고리즘으로 148비트의 입력에 대해 18비트의 인증 서명 값을 생성한다. 이동국에 대한 인증은 등록(registration), 발호(origination), 착호(termination), 공유비밀데이터 갱신(SSD update), 유일 시도 응답(unique challenge-response)의 경우에 이루어 지며 모든 경우에 대해 32비트의 RAND값은 기지국에서 이동국으로 보내지는 액세스 파라미터 메시지를 통해 전달된다. 만약 이동국의 등록, 발호, 착호 과정의 인증이 실패하게 되면 기지국은 유일 시도 응답을 위한 인증 절차를 시작하며 이 과정에서 이동국이 인증되지 않으면 기지국은 이동국에게 SSD 갱신 메시지를 RANDSSD 값과 함께 보내고 갱신된 SSD를 이용해 다시 이동국의 인증을 시도하게 된다.

## 2. GSM 시스템

GSM은 ETSI(European Telecommunication Standard Institute)에 의해 제안된 TDMA 이동 통신 방식이다[5]. 보호 서비스와 관

련된 기본적인 GSM 시스템의 구조는 그림 3과 같다.

GSM 시스템에서는 IS-95A 시스템과 달리 SIM(Subscriber Identity Module) 카드를 사용하는데 이것은 GSM 시스템의 개별 가입자 인증키 Ki와 인증 알고리즘인 A3 그리고 암호화 키 생성 알고리즘인 A8를 포함하고 있다. 그리고 이동국에서는 암호화 알고리즘인 A5를 수행한다. BSS/MSC(Base Station Subsystem / Mobile Switching Center)는 이동국과의 무선 인터페이스를 제공하며 A5 알고리즘을 수행한다. VLR은 하나 혹은 여러 개의 MSC와 연결되어 그 지역을 방문한 가입자의 정보를 저장할 뿐 아니라 TMSI(Temporary Mobile Subscriber Identity)를 생성, 저장하고 인증의 성공 여부를 판단한다. HLR은 이동국의 IMSI(International Mobile Subscriber Identity)와 연관된 인증을 위한 triplet인 Kc(ciphering key), RAND 그리고 인증 서명 값인 SRES 리스트를 저장한다. AuC에서는 Ki가 저장되어 있으며 triplet을 생성하기 위한 A3, A8 알고리즘을 수행한다. 그림 4는 인증 서명 값인 SRES 생성 과정을 보여준다.

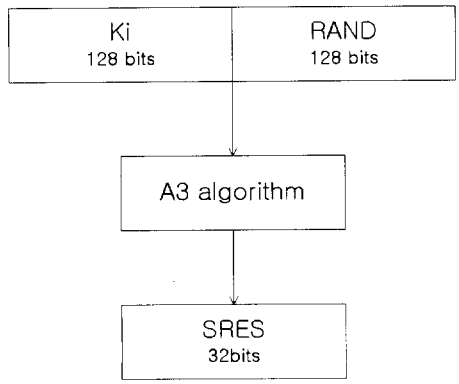
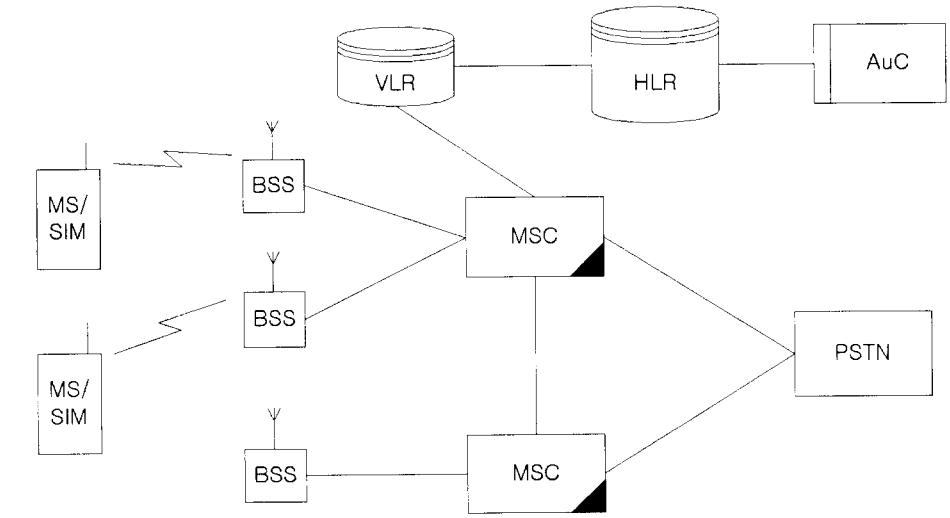



**그림 4. SRES의 생성 과정**

GSM 시스템에서의 인증은 이동국 위치등록




MS : Mobile Station
BSS : Base Station Subsystem

MSC : Mobile Switching Center
VLR : Visitor Location Register
HLR : Home Location Register
AuC : Authentication Center
PSTN : Public-Switched Telephone Network

**그림 3. GSM 시스템의 구성**

(location registration), 위치갱신(location updating) 및 호 설정 절차(call set-up)시 VLR에서 수행된다. GSM의 인증 과정의 흐름은 그림 5와 같다.

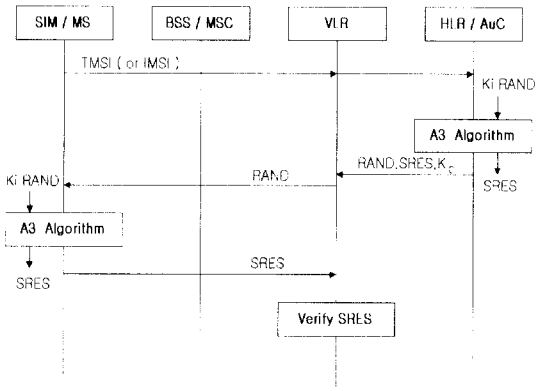



그림 5. GSM에서의 인증 과정

먼저 이동국이 인증을 위해 자신의 TMSI또는 IMSI를 VLR에게 전송하여 자신을 알리면 VLR은 그 정보를 인증 센터에게 전송한다. 인증 센터는 수신한 IMSI에 대해 n 개의 triplet을 생성하여 HLR에 저장하고 다시 VLR에게 전송한다. VLR은 저장된 triplet중 하나를 사용하여 이동국에게 시도(challenge)하고 이동국은 A3/A8 알고리즘을 사용하여 SRES와 Kc를 생성한 후 SRES를 VLR에게 보낸다. VLR은 수신한 SRES와 저장된 SRES를 비교하여 이동국을 인증한 후 이동국에게 새로운 TMSI를 할당한다.

## 3. 미국식 IMT-2000 망 구성

IMT-2000 시스템은 현재 또는 미래의 개별적인 통신망과 시스템을 통합하여 서로 다른 무선접속 환경에서도 단일 단말기 및 사용자카드에 의해서 고속, 고품질의 다양한 서비스를 제공할 수 있는 시스템이다. 미국 방식인 동기식 IMT-2000 시스템의 망 구성도는 그림 6과 같다.

## 4. 유럽식 UMTS 망 구성

유럽의 비동기 방식 UMTS 망 구성도는 그림 7과 같다.

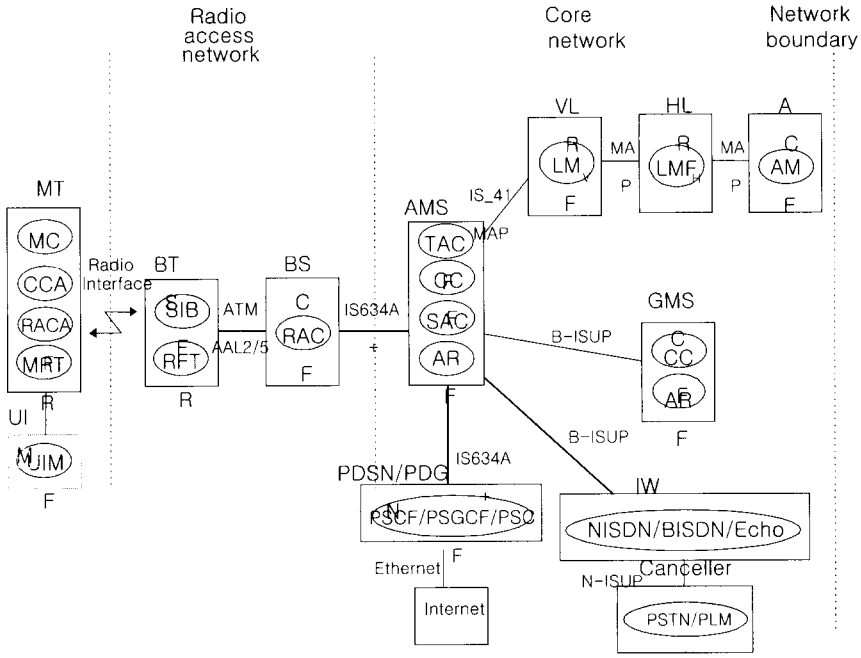
## 5. 이동 통신망에서의 보안

### 5.1 CDMA 망에서의 보안

CDMA망은 기지국이 이동국을 인증하는 단방향 인증으로 비밀키 암호법을 사용하고 있으며, 마스터 키인 A_Key로부터 유도된2차 비밀키(SSD_A, SSD_B)를 사용한다. 그 중 SSD_A는 인증시 사용되는 유일한 비밀값으로 기지국은 이 값과 랜덤수를 이용해 시도-응답형 인증을 행한다. 또한 인증시 COUNT를 사용하여 인증의 안전성을 높이지만 이전 COUNT 값을 알기 위한 부가적 시간이 요구된다.

CDMA 시스템에서 데이터 암호화 및 음성 비화(Voice Privacy)가 이루어지는 구간은 단말에서 기지국까지의 무선 구간에 한정되고 end-to-end 통신을 위한 상호인증 및 암호화가 제공되지 않아 유선구간에서 음성 및 데이터 노출의 위험성이 존재한다. 또한 시스템이 인증 센터에 의한 단말기의 인증에만 의존하고 단말기에 의한 인증 센터의 인증 기능은 제공되지 않음으로 인한 인증 센터의 위장 가능성을 내재하고 있다. 그리고, 사용자의 영구 ID가 평문으로 전송되어 사용자의 익명성과 비추적성이 제공되지 않는다.

한편, 인증 서명 값 생성 알고리즘인 CAVE 알고리즘의 입력 파라미터인 MIN과 ESN이 평문으로 전송되어 제 3자에 의해 검출될 수 있을 뿐 아니라 CAVE 자체도 암호학적으로 안전하지 못한 것으로 알려져 있다. 또한 CDMA 시스템은 단말 장치에 인증 및 암호 알고리즘과 함께 가입자 정보 등이 단말 내부에 저장됨으로써 사용자의 이동성 보장이 어렵다는 단점도 있다.




MT - Mobile Terminal
BTS - Base Station Transceiver System
AMSC - Anchor Mobile Switching Center
AC - Authentication Center
IWF - Inter Working Function
PDGN - Packet Data Gateway Node
UIM - User Identification Module
BSC -Base Station Controller
VLR/HLR -Visitor/Home Location Register
GMSC - Gateway MSC
PDSN - Packet Data Serving Node

그림 6. IMT-2000 시스템 구성도

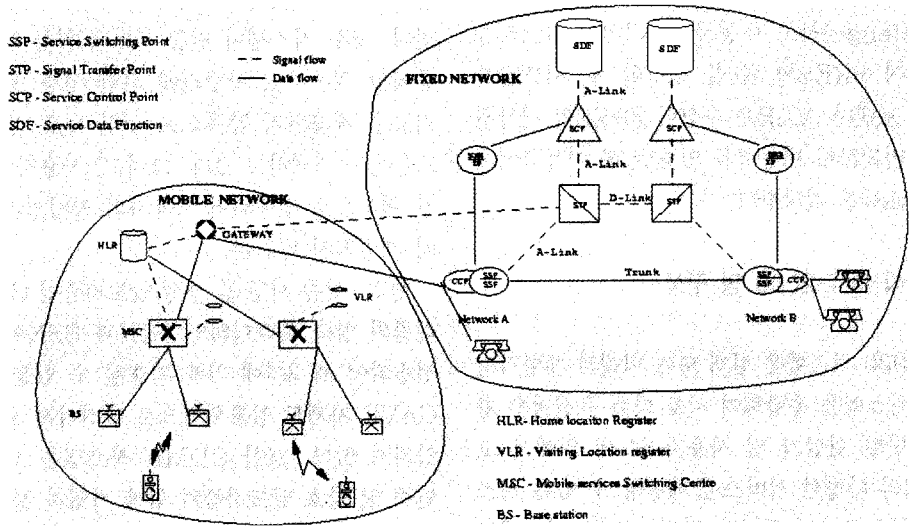



그림 7. 비동기식 UMTS 망 구성도

### 5.2 GSM망에서의 보안

GSM 시스템은 CDMA 시스템과 같이 비밀키 암호 방식을 사용하는 단방향 인증을 채택하고 있으며 인증 센터에서 미리 생성한 랜덤 값과 인증 서명 값을 이용한 challenge-response형 인증을 행한다. 이동국은 임시 이동국 식별자(TMSI) 사용하여 해당 기지국에 인증을 시도하며 SIM 카드에 내장된 마스터 키(Ki)를 인증 서명 생성 값의 입력으로 사용한다.

음성 비화(Voice Privacy)는 단말에서 BS까지의 무선 구간에 한정되어 있으며, 단말기의 인증만을 제공하는 단방향 인증 방식을 취함으로 인해 CDMA 시스템과 마찬가지의 취약점을 내포하고 있다. 이동국은 영구 ID 대신 임시 ID인 TMSI를 사용하지만 최초의 이동국 인증 및 TMSI를 사용한 이동국 인증 실패시 영구 ID를 평문 형태로 사용하므로 결과적으로 익명성과 비추적성은 제공되지 않는다. 한편 인증 센터에서 생성한 인증 서명 값과 암호화 키 그리고 이동국에 시도(challenge)하기 위한 랜덤 값이 평문 형태로 이전 VLR과 현재 VLR, 인증 센터 및 HLR, VLR 사이를 이동하기 때문에 유선구간에서 중요한 인증 데이터의 누출 가능성이 존재한다.

한편, 이동국에서 스마트 카드 형태의 SIM을 사용하므로 사용자의 이동성이 보장되며, 인증 서명값 생성 알고리즘과 암호화키 생성 알고리즘이 마스터 키 그리고 중요한 가입자 정보와 함께 카드 내부에 존재함으로써 보다 안전한 형태의 저장 방식을 제공한다.

### 5.3 IMT-2000에서의 보안

IMT-2000에서의 보안 방식에 대해 구체적으로 알려진 것은 없다. 다만 이들 방식이 CDMA와 GSM에서 진화한 방식이며 IMT-2000시장에 뛰어든 여러 개발 업체에서 다양한 인증/암호 방식에 대한 제안이 이루어지고 있으므로 여기에 나타난 문제점을 충분히 보완한 형태의 안전성을 제공하리라는 것은 분명하다[6].

## III. 이동 통신 관련 표준화 동향

### 1. 3GPP(3rd Generation Partnership Project)에서의 보안 표준화 동향

#### 1.1 3GPP 구조

비동기식으로 알려진 유럽식 IMT-2000 표준화 기구는 조직의 파트너로 ETSI, CWTS, 한국의 TTA, 일본의 ARIB, TTC가 참여하고 있다. 또한 Market Representation Partner로 GSA (Global Mobile Supplier Association), GSM Association, UMTS Forum, UWCC (Universal Wireless Communications Consortium)이 참가하고 있고 참관인 자격으로 TIA, TSACC가 참가하고 있다. 3GPP(Third Generation Partnership Project)로 알려지기도 한 표준화 기구의 구조는 그림 8과 같다[1].

- TSG CN : 3GPP Technical Specification Group Core Network (3GPP_TSG_CN)
  - CN1 : Working Group CN1 : MM/CC/SM(Iu) (3GPP_TSG_CN_WG1)
  - CN2 : Working Group CN2 : CAMEL/MAP (3GPP_TSG_CN_WG2)
  - CN3 : Working Group CN1 : interworking with external networks (3GPP_TSG_CN_WG3)
- TSG RAN : 3GPP Technical Specification Group Radio Access Network (3GPP_TSG_RAN)

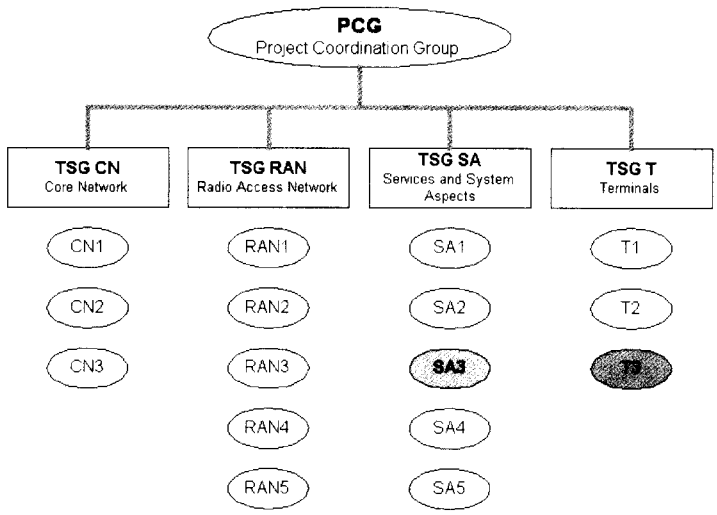



그림 8. 3GPP 구조

- RAN1 : Working Group RAN1 : radio layer 1 specification (3GPP_TSG_RAN_WG1)
- RAN2 : Working Group RAN2 : Radio layer 2 specification and radio layer 3 RR specification (3GPP_TSG_RAN_WG2)
- RAN3 : Working Group RAN3 : Iub specification, Iur specification, Iu specification and UTRAN O&M requirements (3GPP_TSG_RAN_WG3)
- RAN4 : Working Group RAN3 : Radio performance and protocol aspects from a system point of view - RF parameters and BS conformance (3GPP_TSG_RAN_WG4)
- AHG1 : Ad-hoc group on ITU (internal) co-ordination (3GPP_TSG_RAN_AHG1)

● TSG SA : 3GPP Technical Specification Group Services & System Aspects (3GPP_TSG_SA)

- SA1 : Working Group SA1 : Services (including value added services) (3GPP_TSG_SA_WG1)
- SA2 : Working Group SA2 : Architecture (3GPP_TSG_SA_WG2)
- SA3 : Working Group SA3 : Security (3GPP_TSG_SA_WG3)
- SA4 : Working Group SA4 : Codec (3GPP_TSG_SA_WG4)
- SA5 : Working Group SA5 : Telecom Management (3GPP_TSG_SA_WG5)

● TSG T : 3GPP Technical Specification Group Terminals (3GPP_TSG_T)

- T1 : Working Group T1 : Mobile Terminal Conformance Testing (3GPP_TSG_T_WG1)
- T2 : Working Group T2 : Mobile Terminal Services & Capabilities (3GPP_TSG_T_WG2)
- T3 : Working Group T3 : Universal Subscriber Identity Module (USIM)

(3GPP_TSG_T_WG3)

3GPP와 TTA의 PG01과의 대응관계는 그림 9와 같다[3].

### 1.2 보안 관련 표준화 Working Group

Security와 관련된 표준은 Services and System Aspects Technical Specification 그룹(3GPP_TSG_SA)의 3번째 Working Group(3GPP_TSG_SA_WG3)에서 논의하고 있으며, 구성은 ETSI, T1P1, ARIB, TTA와 TTC로 이루어져 있다. 이들의 중요 논의 대상은 보안의 대상, 구조 및 요구 사항들의 도출이며 상세한 논의 대상은 아래와 같다.

- 사용자, 사업자 그리고 제조업체의 필요성, 시장의 활성화를 고려한 UMTS(Universal Mobile Telecommunication System) 보안 대상 및 우선 순위 결정
- UMTS에 대한 위협 요소 분석 (Threat Analysis)
- UMTS에 대한 보안 요구사항 정의 : 서비스, 사용자 서비스 접근, 과금, 운용 및 유지 보수 등에 관한 보안 요구사항 정의
- UMTS의 물리적 요소들에 대한 보안 요구사항 정의 : radio access network, core network, core network과 non-UMTS network간의 인터페이스, 단말, user identity module, UMTS network들 간의 인터페이스에 관한 보안 요구 사항들의 정의
- 보안 요구사항들을 만족하고 UMTS 시스템 구조에 부합하는 보안 구조의 정의
- 보안구조의 모든 구성 요소들에 대한 표준 제공
- 보안 구성 요소들의 운용과 관리에 대한 표준 제공
- 보안 구성 요소들이 필요로 하는 암호 알고리즘

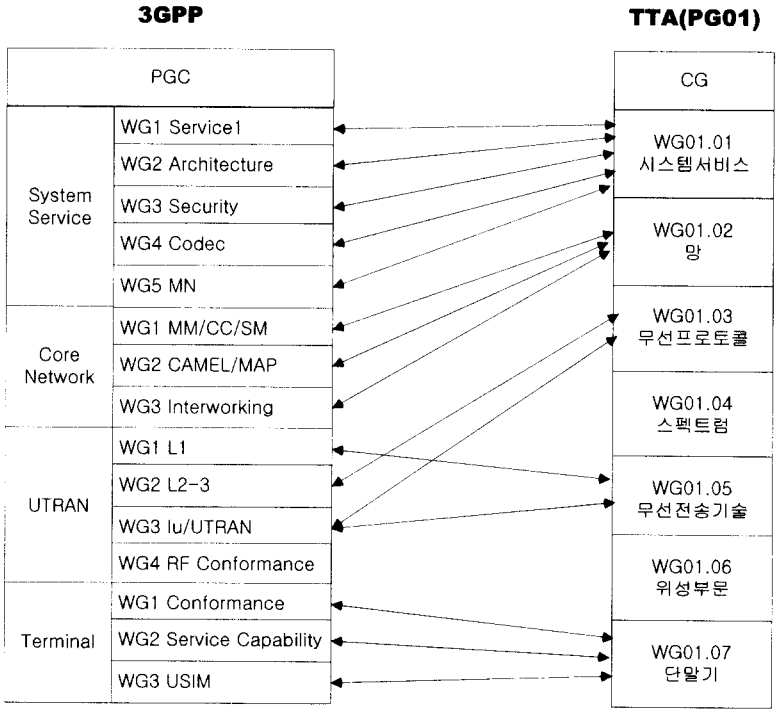



그림 9. 3GPP와 TTA PG01과의 대응 관계

에 대한 요구 사항 제공

### 1.3 Subscriber Identity Module(SIM) 관련 표준화 Working Group

UMTS 네트워크의 중요 보안 구성 요소들 중에서 하나인 USIM(Universal Subscriber Identity Module)에 대한 표준은 단말에 대한 표준을 다루는 TSG-T의 Working Group3에서 논의하고 있으며, ETSI IC Cards 관련된 ETSI SMG working group 9 그리고 PDC와 관련된 ARIB 27 working group과 제휴하여 논의하고 있다. 중요 논의 내용은 UMTS 보안 요구 사항들을 만족하는 USIM 기능의 설계 그리고 SIM를 기초한 GSM 서비스의 UMTS로의 적용 등이며, 상세한 논의 대상들은 아래와 같다.

- MTS 보안 요구 사항들을 만족하는 USIM 기능의 설계
- 서비스 창출을 위한 가능성 제공 (예, SIM Application Toolkit 그리고 APIs 등의 향상을 통한 새로운 서비스의 창출)
- 응용 서비스들에 대한 다운로드 메커니즘의 정의
- 단일 또는 다중 카드 리더를 내장한 단말에서 다중 응용 서비스를 제공하기 위한 USIM 기능들의 정의
- GSM SIM기능의 차세대 이동통신으로 진화 정의
- 현재 GSM SIM 카드의 물리적 기계적 인터페이스 향상 정의(예, 전기적 파라미터, 트랜스포드 프로토콜, 호 기록 저장 등)
- GSM 망에서 UMTS 망으로의 변형된 로밍 방법의 제공과 2세대 이동통신 망에서 UMTS 망으로의 변형된 로밍 방법의 연구
- UMTS 이동통신 망에서 2세대 망으로의 변형된 로밍 방법의 연구

### 1.4 Security 관련 표준화 동향

TSG SA WG3의 5번째 회의가 8월에 Sophia Antipolis와 Bonn에서 개최 되었다. 이 회의에서 논의된 주요 내용은 UMTS에서 Mobile IP 운용에 대한 인증 문제, 단말기 인증을 위한 COUNT 사용 방법에서 GSM과 UMTS 연동 문제, 재난에 대비한 다중 인증 알고리즘 또는 다중 키 사용에 관한 논의 등이 이루어졌다. 또한 중요한 논의 대상으로 UMTS와 GSM간의 핸드오프와 로밍 시에 보안 문제가 Bonn회의에서 논의되었다. 현재 TSG SA WG3에서 다루어지는 논제의 경향은 MAP(Mobile Application Protocol)과 관련된 Mobile IP 운용시의 보안과 GSM의 UMTS로의 발전에 따른 로밍 및 핸드오프 시에 발생할 수 있는 단말기 인증에 필요한 키 관리 문제 등 보안에 대한 논의가 활발히 이루어지고 있다.

## 2. 3GPP2(3rd Generation Partnership Project 2)에서의 보안 표준화 동향

### 2.1 3GPP2 구조

제3세대 ANSI-41 네트워크 및 이를 기초로 한 cdma2000 무선접속 기술 및 단말기 등 세부 규격 작성을 위해 TIA, ARIB, TTC, TTA가 결성하였으며 그림 10과 같이 Steering Committee를 중심으로 6개의 Technical Specification Group(TSG)가 있으며, 이들 TSG에는 표준화 작업을 위한 Working을 두고 있다[2].

3GPP2에서 보안에 관련된 논의는 TSG-C cdma2000그룹에서 프라이버시, 인증 그리고 암호와 관하여 이루어지고 있으며, TSG-P Wireless Packet Data Networking에서 Secure Private Network Access, Wireless IP 서비스 및 네트워크 구조 정의에서 보안 관련 프로토콜들이 논의되고 있다.

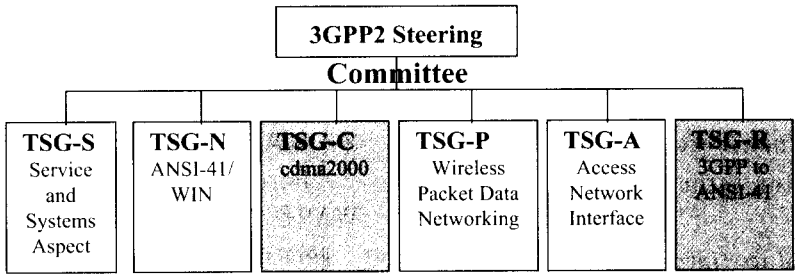



그림 10. 3GPP2 구조

3GPP2와 TTA의 PG01과의 대응관계는 그림 11과 같다 [3].

### 2.2 보안 관련 표준화 그룹

보안과 관련된 프라이버시, 인증 그리고 암호의 논의는 TSG-C cdma2000에서 이루어지고 있으며, 이 그룹의 역할은 cdma2000 infrastructure에 관한 요구사항, 기능 그리고 인터페이스의 표준을 정의한다. 다루어지고 있는 상세한 분야들은 아래와 같다.

- Radio Layer 1 표준
- Radio Layer 2 표준
- Radio Layer 3 표준
- MS/BS Radio 성능 표준
- Radio Link Protocol
- enhanced privacy, authentication and encryption
- Digital Speech Codecs

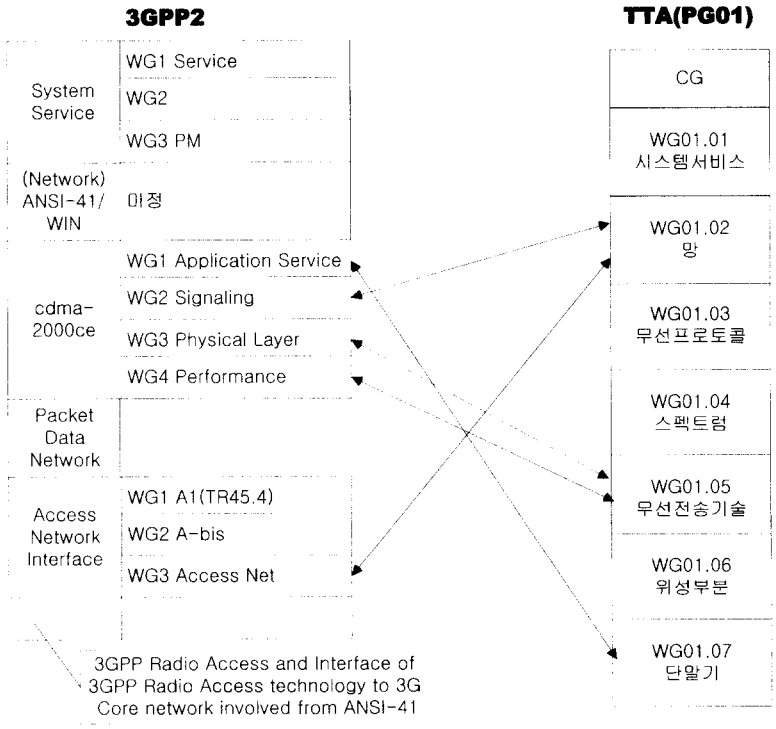



그림 11. 3GPP2와 TTA PG01과의 대응 관계

- Video Codec adoption
- Data and Other Ancillary Services support
- Conformance Test Plans
- MS-Adapter Interface

### 2.3 Wireless IP 그리고 데이터 서비스 관련 표준화 그룹

Wireless IP 그리고 데이터 서비스 관련된 표준화는 TSG-P Wireless Packet Data Networking 그룹에서 다루어지고 있다. 이 그룹에서는 인터넷 접속을 포함한 무선 패킷 데이터 서비스를 지원하기 위한 패킷 데이터 기술을 정의하며 상세한 논의 분야는 아래와 같다.

- Wireless IP Services (including IP Mobility Management)
- Wireless IP network architecture design
- Voice over IP
- Secure Private Network Access
- Internet Access
- Packet Data Accounting
- Multimedia Support
- QoS Support

### 2.4 Security 관련 표준화 동향

1999년 9월에 개최된 3GPP2 Workshop on 3G Harmonization에서 3GPP와 3GPP2에 대한 단일 표준으로 G3G에 관한 논의가 있었으며, 보안과 관련된 논의 결과는 MAP(Mobile Application Protocol)에 관한 것은 기본적으로 GSM/UMTS의 보안 요구사항의 무결성, 사용자 인증 등을 수용하는 것으로 방향을 잡았으며, 앞으로의 연구 과제로 cdma2000에서 적용한 암호 알고리즘의 적합성과 GSM-MAP 키 관리 스킴의 적용 문제로 남겨 놓았다.

## 3. 이동 통신 환경하에서 응용 서비스를 위한 표준화 동향

### 3.1 WAP (Wireless Application Protocol) Forum

WAP은 이동통신 환경에서 디지털 단말, 페이저, 개인휴대 전화 등을 이용하여 인터넷 서비스와 향상된 Telephony 서비스를 제공하기 위한 표준을 만들자는 목적에서 시작되었으며 하부의 이동 통신환경과는 독립적인 서비스를 지향하고 있다. 1997년 9월 WAP에 대한 구조를 발표하고 포럼 내에서는 하부의 네트워크 구조와는 독립적인 프로토콜을 만들어 GSM, CDMA, IMT-2000 뿐만 아니라 여러 다른 무선 기반과 동작하도록 하고 있다[7]. 현재 Ericcson을 포함한 여러 기업에서 WAP을 표준으로 채택하고 있으며, 그 이유는 기존의 XML이나 IP와 같은 인터넷 표준을 기반으로 하고 있어서 업계에서 수용이 용이하다는 이유가 있다.

현재 WAP Forum에서 승인한 표준은 Wireless Application Protocol Architecture Specification, WMLScript Language Specification등을 포함한 20개의 표준이 있다. 보안에 관한 표준은 승인된 문서들 중에서 Wireless Transport Layer Security Specification에서 응용을 위한 보안 알고리즘, 프로토콜이 정의되어 있다. WAP에 대한 인프라구조는 그림 12에 도시하였다.

현재 참여하고 있는 업체는 루슨트, AT&T, Ericsson, Motorola, Sonera 등이 참여하고 있으며 한국에서는 LG IC, 삼성이 참여하여 활동하고 있다.

### 3.2 Radicchio

Radicchio는 안전한 무선 전자 상거래와 무선

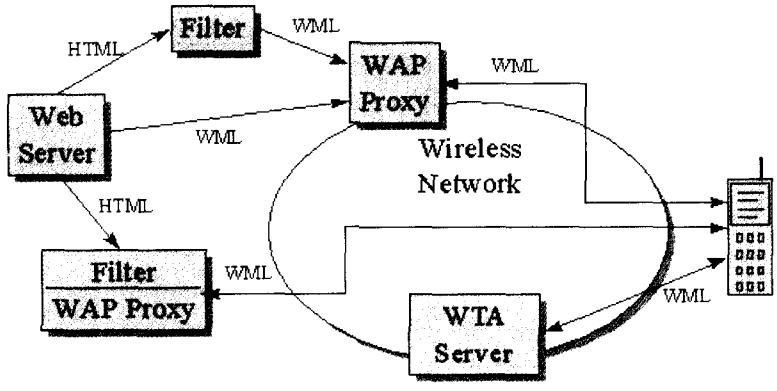



그림 12. WAP Infrastructure

단말 및 네트워크 상에서 PKI(Public Key Infrastructure)의 발전을 도모하기 위하여 결성된 조직이다. 1999년 PKI기반의 안전한 전자 상거래 시장 선점을 위하여 프랑스의 Gemplus, 미국의 EDS, 핀란드의 Sonera 스마트 트러스트를 중심으로 결성되었으며, 아래와 같은 PKI기반의 무선 전자 상거래 시장의 활성화를 위한 개발 및 전략으로 활동을 시작했으며 아직 조직은 구성되지 않았고 참여를 희망하는 업체들을 기다리고 있다[8].

- 안전한 무선 전자 상거래와 PKI에 대한 업계 및 가입자 인식의 확산
- 안전한 무선 상거래의 트랜잭션 처리를 위한 PKI 개발
- 무선 전자 상거래 시장의 개발과 활성화 유도
- 디지털 서명 인증 발급과 등록 과정들에 대한 정의
- PKI 기반의 무선 전자 상거래 솔루션 제공을 위한 포룸의 제공

# IV. GSM의 SIM 카드 현황

## 1. SIM카드 활용 현황

스마트 카드가 초기 서비스를 진행하던 1996년에는 표 1에서 보는 것과 같이 단순 메모리 형태의 전화 카드가 발급된 스마트 카드의 대부분을 차지하였으며 GSM의SIM(Subscriber Identity Module) 카드는 매우 적은 양이었다.

(자료출처 : 1996년, Frost & Sullivan)

| 이용 분야 | 스마트카드 발급량 |
|---|---|
| 전화 | 5억 7500만장 |
| 금융 | 3600만장 |
| Data & ID Card | 3000만장 |
| GSM | 1700만장 |
| Pay-TV | 1500만장 |
| 기타 | 380만장 |
| 총 계 | 6억7600만장 |

표 1. 1996년 분야별 발급된 스마트 카드 양

스마트 카드에 대한 카드 제조 업체인 Gemplus에서의 예측은 표2.에 도시하였다. 이는 제조 업체에 의한 조사로서 객관성이 결여되어 전체 스마트 카드 양에 대해서는 정확한 예측이라고는 보기 어렵다. 하지만 GSM SIM 카드는 1997년부터 전화 카드에 이은 두번째로 큰 스마트 카드 시장이며 2003년까지는 그 수준을 유지할 것이라는 예측은 참고할만하다.

(자료 출처 : Gemplus market study)

| 이용 분야 | 1997 Million units | 2003 Million units | Average Yearly Growth |
|---|---|---|---|
| Phonecards | 684 | 3270 | 30% |
| GSM | 69 | 760 | 49% |
| Banking | 49 | 690 | 55% |
| Loyalty | 22 | 320 | 56% |
| Healthcare | 16 | 210 | 54% |
| Pay-TV | 12 | 150 | 52% |
| Ticketing | 8 | 240 | 77% |
| Gaming | 2 | 70 | 78% |
| Access Control | 10 | 260 | 72% |
| Identity | 2 | 50 | 71% |
| Information Technology | 1 | 120 | 142% |
| Other | 24 | 170 | 38% |
| Total | 900 | 6310 | 38% |

**표 2. 스마트 카드 수요 예측**

표 3에 의하면 세계적인 스마트 카드 시장은 유럽과 아시아가 가장 크며 이들 두 지역은GSM서비스 지역이므로, GSM에서의 스마트 카드 활용 빈도가 높음을 알 수 있다.

(자료 출처 : Frost & Sullivan)

| Region | Market Share (%) |
|---|---|
| Latin America | 7.0 |
| North America | 6.1 |
| Asia Pacific | 17.9 |
| Europe | 67.1 |

**표 3. 스마트 카드 시장 : 1998년 총수입을 기준으로 한 지역별 시장 분포**

아시아 지역에서 SIM 카드의 활용은 CDMA 및 GSM에 종속적이며, 이들의 통합이 이루어진다면 2002년에는 그 규모가 200백만장에 이를 것이라고 Frost & Sullivan Telecommunication Research에서 예측하였다[9].

아일랜드에 위치한 GSM Association에 의하면 GSM 가입자는 130여개국의 1억 4천만명 정도이며(이러한 숫자는 작년에 7천만명이었던 것에 비하면 비약적인 발전에 이르렀음을 알 수 있음), 이 단말 중에서 1억 천5백만명이 칩을 기반으로 하는 SIM 카드를 소지하고 있을 것으로 예측하고 있다. 전체 GSM 시장은 2000년에는 2억 5천만명에 이를 것으로 예측하고 있다[10] .

현재 가장 큰 GSM 시장인 중국은 올해 2월달에 CHINA TELECOM이 Gemplus 와SIM 카드를 1억장 납품을 계약하였다고 발표한 바 있다[11]

pre-paid SIM 카드에 대한 서비스를 세계 여러 나라(영국, 이태리, 스웨덴, 독일, 네덜란드, 호주, 스페인, 인도네시아, 미국, 싱가폴, 홍콩,.....) 에서 서비스하고 있다[12].

## 2. 단말 내장형과 SIM 카드 사용의 장단점 및 특징

단말 내장형이란 GSM단말 내부에 SIM 역할을

하는 S/W 모듈을 장착하여 별도의 SIM카드와의 인터페이스 없이 서비스가 가능하도록 하는 단말을 의미한다. 이는 SIM 카드의 장착보다는 빠른 응답 시간을 제공할 수 있지만 유연성(flexibility)과 이동성이 SIM 카드의 사용시에 비해 떨어진다. 반면에 SIM 카드는 현재까지의 스마트 카드의 처리 능력의 제한으로 응답시간은 길어지지만 높은 유연성과 이동성 및 안전성(Security)을 보장할 수 있다.

## 3. 활성화를 위해 필요한 조건

SIM 카드 활성화에 어려움을 주는 이유 중의 하나는 기존의 카드 크기가 GSM 단말에 장착되기에는 너무 부담스러운 크다는 사실이다. 단말의 크기는 소형화 되었지만 카드의 크기는 기존의 신용 카드 크기를 고수함으로 인해 사용자의 불편함을 초래하였다. 이의 해결을 위해 새로운 mini-SIM 카드가 등장하였고 이에 대한 표준화 수정을 위하여 ISO-7816 스마트 카드 인터페이스 규격이 재검토되고 있다. (4절 SIM카드 관련 표준화 참조)

또 이러한 크기가 작은 mini-SIM card는 보관에 어려움이 있으므로 덴마크에서는 그림 13과 같은 어댑터도 출현하였다[13].


그림 13. mini-SIM 카드 어댑터

SIM 카드의 활용을 증대 시키기 위해서는 GSM에서의 단순한 활용 뿐만 아니라 다른 응용 서비스와의 결합을 통한 multi-application SIM카드의 개발 및 서비스의 개발이 필요하다. 이러한 시도는 카드 제조업체와 GSM 서비스 업체 및 기타 업체에서 활발한 논의가 진행 중이다.

## 4. SIM 카드 관련 표준화

GSM SIM card 와 관련된 표준은 다음과 같다.

[1] GSM 11.11 (ETS 300 608), Digital cellular telecommunications system (Phase 2): Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface. GSM 11.11 (ETS 300 977), Digital cellular telecommunications system (Phase 2+): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface.

[2] GSM 11.12 (ETS 300 641), Digital cellular telecommunications system (Phase 2): Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface.

[3] GSM 11.14, Digital cellular telecommunications system (Phase 2+): Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface.

[4] GSM 11.17, SIM test specification

[5] GSM 02.48, Security Requirements for the SIM toolkit

[6] ISO/IEC 7816, Information

technology - Identification cards - Integrated circuit(s) cards with contacts.

Part 1 : 1987, Physical characteristics. (Under review)

Part 2 : 1988, Dimensions and location of the contacts. (Under review)

Part 3 : 1989, Electronic signals and transmission protocols. (Under review)

Part 4 : 1995, Interindustry commands for interchange

Part 5 : 1994, Numbering system and registration procedure for application identifiers.

Part 6 : 1994, Interindustry data elements.

Part 7(Draft) : Interindustry commands for Structured Card Query Language (SCQL).

Part8(Draft) : Security related interindustry commands.

Part 9(Draft) :Enhanced interindustry commands.

Part 11(Draft) : Security architecture.

스마트 카드 규격(ISO/IEC 7816)에는 포함되지 않는 3V에서 구동되는 저전력 소모 SIM카드에 대한 토의가 GSM 11.12에서 논의되고 있으며, mini-SIM카드 규격을 위하여 카드의 물리적 인터페이스에 대한 기술(ISO/IEC 7816 part 1,2,3)이 재검토되고 있다. 검토되는 규격의 내용은 원래 카드 dimension에 비해 GSM단말에 장착하기 편리하도록 축소된 크기의 물리적 인터페이스를 제안하고 있다. 이에 대한 도면은 그림 14에 도시한 바와 같다.

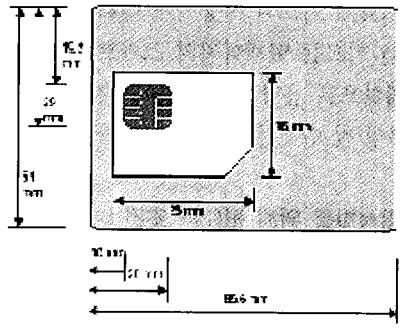


그림 14. ISO/IEC 7816에 따른 스마트 카드 Dimension

## V. 결 론

본 고에서는 CDMA, GSM, 미국식 IMT-2000, 유럽식 IMT-2000 시스템의 구성과 단말의 인증을 위한 알고리즘 및 프로토콜, 이동 통신 시스템 표준과 관련된 표준화 단체인 3GPP와 3GPP2, 그리고 응용 서비스 표준과 관련된 단체인 WAP, Radicchio에 대한 구조와 동향에 대하여 살펴 보았다. 그리고 GSM망의 보안 핵심 요소들 중에 하나인 가입자 SIM 카드에 대한 현황 및 활성화를 위한 조건을 논하였다.

3세대 이동 통신 서비스의 개시를 앞두고, 이동 통신은 유럽과 미국 시스템으로 양분되고는 있으나 IMT-2000 글로벌 정신에 부합되기 위해서는 단일화된 표준의 시스템으로 귀결될 것으로 예상된다. 이를 위해서는 어떤 국가, 어떤 대륙에서도 가입자에 대한 인증과 보안은 필수적인 요소이며, 이를 해결하는 표준화 단체의 활동에 적극 동참하는 것이 필요하고, 또한 현재 상이한 구조를 가지고 있는 두

시스템의 통합을 위한 인증과 보안 기술 개발과 기능 구현 기술의 노하우를 획득하는 것이 필요하다.

지금까지는 이동 통신에서 양질의 통화 서비스를 제공하여야 한다는 사업자 측의 사업 전략에 밀려서 가입자의 인증 등의 보안 서비스가 도외시 되어온 것이 사실이다. 하지만 이동 통신 시장의 활성화와 더불어 단말기 오용 등의 이동 통신 역기능 방지를 요구하는 사용자들의 요구가 거세지면서 이에 대한 대처 기술 개발과 보안 표준의 적용이 필요한 시점이 되었다.

그리고 현재의 이동 통신 가입자 증가 추세가 인터넷 가입자 증가 추세를 앞지르는 상황에서 이동 단말을 이용한 응용 서비스, 즉, 전자 상거래, 인터넷 뱅킹, 홈 트레이딩 등을 가능하게 할 수 있는 보안 구조와 기반을 마련하는 것은 매우 중요하며, 이는 빠른 시일 내에 진행되어야 할 시급한 연구 과제이다.

## ※참 고 문 헌


1. http://www.3gpp.org/
2. http://www.3gpp2.org/
3. http://www.tta.or.kr/
4. TIA/EIA IS-95A, Mobile-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System, Intrim Standard 95, July 1993.
5. ETSI, European Digital Cellular Telecommunication System(Phase 2) - Security Related Network Functions, July 1993.
6. http://www.esat.kuleuven.ac.be/cosic/aspect/
7. http://www.wapforum.org/
8. http://www.radicchio.org/
9. http://www.frost.com/
10. http://www.faulknergray.com/
11. http://pluton.gemplus.fr/
12. http://home.swipnet.se/OsbyMikro/presime.htm
13. http://www.scandy.com/hitec/simcard.html

## 문 종 철

1997년 2월 경북대학교 전자공학과 졸업(학사)
1999년 2월 경북대학교 전자공학과 졸업(석사)
1999년 2월~현재 한국전자통신연구원 정보보호시스템연구부 연구원
※관심분야:이동통신 정보보호, IC카드 시스템 정보보호

## 김 신 효

1990년 2월 전남대학교 전산통계학과 졸업(학사)
1999년 현재 충남대학교 컴퓨터과학과 석사과정 수료
1990년 2월~현재 한국전자통신연구원 정보보호시스템연구부 선임연구원
※관심분야:제한수신시스템, 정보보호, 이동통신 전자상거래

## 김 유 혁

1988년 2월 서울대학교 수학과 졸업(학사)
1991년 2월 서울대학교 대학원 계산통계학과 졸업(석사)
1991년 2월~현재 한국전자통신연구원 정보보호기술연구본부 유료서비스기술연구팀장
※관심분야:디지털 유료방송시스템, 이동통신 전자상거래, 통신망 및 프로토콜

## 김 재 명

1974년 2월 한양대학교 공과대학 전자공학과 졸업(학사)
1974년2월~1977년12월 한국과학기술연구원(KIST) 연구원
1977년12월~1979년6월 한국통신기술연구소(KTRI) 전임연구원
1981년 8월 미국 남가주대학교(University of Southern California) 졸업(석사)
1987년 8월 연세대학교 전자공학과 졸업(박사)
1982년 9월~현재 한국전자통신연구원 책임연구원
1999년 현재 한국전자통신연구원 정보보호기술연구본부장