情報保護學會論文誌
第17卷 第2號, 2007. 4

무선 네트워크 연동을 위한 USIM 보안 모듈 설계 및 구현

김 춘 수†
국가보안기술연구소*

Design and Implementation of USIM Secuirty Module for the Wireless Network Interworking

Choonsoo Kim†
National Security Research Institute*

요 약

정보 보안을 위한 3GPP 표준을 따르는 USIM 기술은 3GPP 모바일 네트워크에서 보안 기능을 제공한다. USIM의 보안 기능은 사용자 계정 기밀성, 상호 인증, 사용자와 네트워크간에 키 교환 및 사용자 정보 보안 및 데이터 무결성 들이다. 본 논문에서는 일반적인 네트워크에 접근 방법, 3GPP 및 WLAN(Wireless LAN) 통신에서 인증 프로토콜, 및 RADIUS 기반에 AAA 서버 시스템에 보안 기능을 제공하는 USIM 보안 모듈을 설계 및 구현한다.

ABSTRACT

USIM(UMTS Subscriber Identity Module) technology that accept 3GPP(3rd Generation Partnership Project) standards for information security supports security function in 3GPP. Supported security functions of USIM are confidentiality of user identity, mutual authentication and key agreement between end user and network, confidentiality of user data and data integrity. It is very important technology in wireless network. It makes secure environment that user and service provider can use securely mobile service in network. In this paper, design and implementation USIM security module that supports common network access method and authentication protocol in 3GPP and WLAN(Wireless LAN) and AAA (3A-Authentication Authorization Accounting) server system based RADIUS.

Keywords : *USIM, WLAN, RADIUS, 3GPP*

Ⅰ. 서 론

IMT-2000(WCDMA) 사업자들은 2003년 하반기부터 3세대 이동 통신 서비스를 제공할 계획을 세웠으며, 초기부터 USIM(Universal Subscriber Identity Module) 칩의 사용이 필수적으로 요구되어 왔고 향후 IMT-2000 서비스가 전 세계적으로 확대 되면 USIM 칩의 수요가 폭발적으로 증가할 것으로 파악되고 있다. IMT-2000 환경에서의 USIM 칩셋 기술은 사용자 ID 기밀성, 사용자 및 망간 상호 인증과 키 일치성, 사용자 데이터의 기밀성 및 무결성 등의 정보보호에 대한 표준화를 수용하고, PKI (Public Key Infrastructure) 기능 통합형 USIM/UIM(User Identity Module) 카드를 외장형 혹

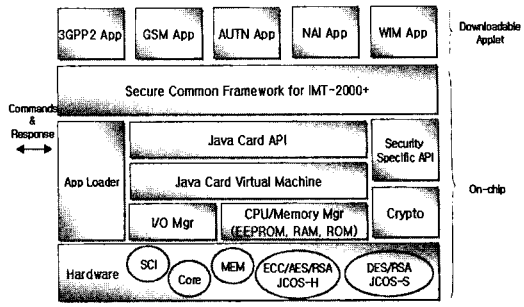
접수일: 2006년 10월 12일; 채택일: 2006년 12월 31일
† 주저자, jbr@etri.re.kr

은 내장형으로 개발하여 IMT-2000 망의 정보보호 기능을 조기에 구축할 수 있도록 하며, 무선 인터넷의 발전과 이동 통신의 발전 추세에 부합하는 매우 중요한 기술이다. IMT-2000 망에서는 정보보호 서비스를 물리적으로 정보보호 서비스의 안전성을 보장하는 USIM을 제공하도록 국제 표준화가 진행되었다. 따라서 3세대 이동통신 표준을 준수하는 USIM 칩을 통한 경쟁력 강화가 필요하며, 확보된 USIM 기술을 사용하여 사업자 및 이용자에게 안전한 무선 전자 상거래 서비스 제공 가능하다. 최근 무선통신시스템의 관심의 증대로 인하여 다양한 부가서비스를 제공하는 무선인터넷의 사용량이 급속히 증가되고 있는 상황에서 사용자에 대한 정보 및 서비스의 보안성에 대한 욕구 또한 증대되고 있어 USIM은 무선 네트워크의 보안 및 그 응용 보안의 핵심 요소로 자리 잡고 있다. 또한 IMT-2000을 통한 무선 데이터 통신 뿐만 아니라 PDA나 Mobile System과 같은 다양한 기기를 통한 802.1x 기반의 무선 네트워크 (Wireless LAN)에 대한 관심이 집중되고 있는 상태에서 사용자에게 언제 어디서나 다양한 네트워크 서비스를 제공하기 위하여 WLAN과 3G 환경 통합의 필요성이 대두 되고 있는 상태이며, 이러한 서비스 기술이 점점 발전하고 있는 추세이다.

이러한 사례를 통해서 사용자에게 다양한 네트워크 접속 서비스 제공에 따라 USIM 기술을 적용함으로써 얻어질 수 있는 이점은 무선 네트워크의 보안 서비스 고도화로 안전한 상호인증과 글로벌 로밍 서비스에 따른 편리함과 가입자 정보의 보호 및 안전한 전자상거래 서비스 제공이 가능하게 될 것이다. 그리고 다양한 네트워크 기기에 독립적으로 운용될 수 있는 USIM 기술을 적용함으로써 사용자에게 단일화 된 보안 모듈을 이용하여 서비스를 제공 받게 됨으로써 신뢰성의 향상과 호환성 증대에 따른 체계적인 정보보호 메커니즘 수용이 용이해 질 것이다.

본 논문에서는 보안 요구사항을 통해서 3G 환경 및 WLAN 환경에서의 공통적인 무선 네트워크 접속에 따른 표준화된 프로토콜 설계 및 구현을 통해서 가입자 인증 기능을 구현하고 가입자의 정보를 관리 및 보호하며 네트워크상의 데이터 보호를 위한 암호화 알고리즘 등을 적용한 USIM 보안 모듈을 설계및 구현한다.

Ⅱ. 관련연구



〔그림 1〕 Java 카드 운영체제 구조

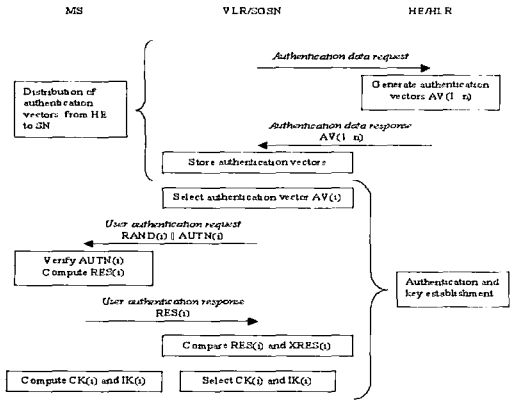
2.1 USIM

ITU-T에서 IMT-2000 서비스를 위한 단말 표준으로 제정된 USIM 플랫폼 규격은 3GPP/ETSI R5, Java Card 2.2.1[1], ISO규격, GP 2.1 규격을 준용한다. 이와 더불어, ECC, RSA, AES 등의 고급 암호 알고리즘 등 사용시 예상되는 요구 보안 기능들을 모두 탑재하였다. USIM 하드웨어 위에 올라가는 JCOS Platform은 하드웨어 제어와 카드 운영체제로서의 기능을 맡고 동시에 JCVM, JCAPI, UICC, GP 2.1, USAT 지원 부분들이 올라가게 된다. 또한 파일시스템(File System)을 구현하고 있어 이를 사용하는 이동통신사의 요구를 만족시키고 있고, 현재 망간의 상이성으로 인한 서비스의 차이들을 USIM 칩셋 상에서 해결할 수 있는 2G/3G 호환 기술을 탑재하고 있다.

JCOS의 구조는 〔그림 1〕 에서 보듯이 COS(Card Operating System), JCVM(Java Card Virtual Machine), JCAPI(Java Card Application Programming Interface)를 기본으로 포함하는 USIM 응용을 위한 각종 API들을 포함한다.

2.2 3GPP 상호인증 메커니즘

3GPP(3rd Generation Partnership Project) 방식의 IMT-2000 시스템은 고속의 멀티미디어 서비스 제공 및 글로벌 로밍을 특징으로 하고 이러한 이동통신 환경의 변화는 정보보호에 대한 새로운 대책을 요구함에 따라 정보보호 기술도 다양하게 발전하고 있다. 이에 3GPP는 기존의 GSM방식보다 더 강력하고 안전한 정보보호 메커니즘을 개발하였고 가입자와 네트워크간의 상호인증, 무선구간에서의 데이터 보호를 위해 암호화와 무결



〔그림 2〕 AKA 상호 인증 흐름

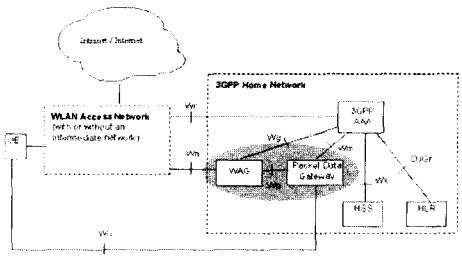
성 제공이 그것이다. 상호인증과 키 일치 메커니즘인 AKA(Authentication and Key Agreement)를 위해서 3GPP는 Milenage를 사용할 것을 권고하고 있으며, 이러한 알고리즘의 안전성에 관해서는 이미 여러 관점에서 검증이 되었다. 3GPP 환경에서 가입자에 대한 인증 수행을 위해서 사용자의 기본 정보가 저장되어 있는 HLR(HSS) 시스템과 사용자의 인증을 수행하는 VLR 시스템과 사용자의 단말기인 MS 로 이루어지며, 3개 모듈의 상호 연동을 통해서 인증과정이 수행되게 된다.

〔그림 2〕는 3GPP 환경에서 MS, VLR/SGSN, HE/HLR 간의 AKA 상호 인증의 흐름(TS 33.102)을 보이고 있다.

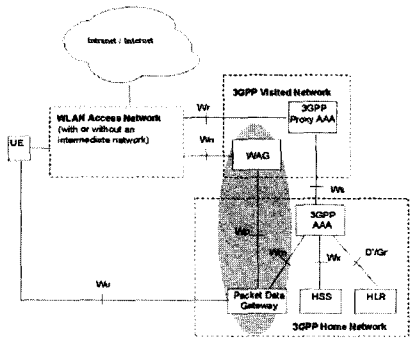
Ⅲ. 3GPP-WLAN 연동

3.1 개요

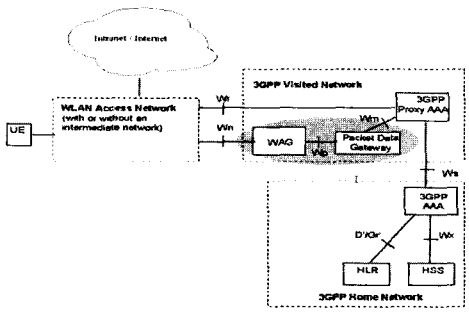
PPP(Point-to-Point) 형태의 인증 방식에 기반한 EAP(Extensible Authentication Protocol)는 IEEE 802.1x에서 규정하고 있는 다양한 인증방법을 구현할 때 사용되는 프로토콜이다. 여기에는 EAP-MD5, EAP-TLS, EPA-PEAP 등 다양한 인증 방식이 존재하는데, 3GPP-WLAN I연동을 위해서는 3GPP와 마찬가지로 AKA 방식을 이용하여 인증 및 세션키 분배를 수행하기 위해 EAP-AKA[2] 표준을 마련하고 있으며, USIM 모듈을 통하여 인증을 수행하고 있다. 이는 3GPP 서비스와 기능을 WLAN 접속 환경으로 확장함으로써 무선 네트워크 접속의 확장성을 높여준다. 이에 대한 표준으로 Spec.은 TS 22.234[3], TS 23.234/934[4].[5], TS



〔그림 3〕 Non Roaming 참조 모델



〔그림 4〕 Roaming 참조모델 - 홈 네트워크



〔그림 5〕 Roaming 참조모델-방문 네트워크

24.234[6], TS 33.234[7]에 명시되어 있다.

3GPP TS 23.234, TR 23.934 문서에서는 3가지 3GPP-WLAN 연동 참조 모델을 제시하고 있으며, 다음의 각 그림은 각각의 참조모델을 보이고 있다. (〔그림 3〕, 〔그림 4〕, 〔그림 5〕 참조)

〔그림 3〕의 Non-Roaming 참조 모델의 경우 가입자에 대한 인증 및 접근제어를 홈 네트워크가 책임지는 형태이며, 〔그림 4〕의 Roaming 참조 모델은 가입자가 방문 네트워크에 접속시 패킷을 홈 네트워크로 라우팅하여 Non-Roaming 참조 모델과 비슷하게 홈 네트워크

가 책임지는 형태이나, [그림 5]의 경우는 방문 네트워크에 존재하는 3GPP Proxy AAA를 통해서 홈 네트워크로 Gatewaying 되는 서비스를 제공하며, 방문지의 PDG가 개입을 하는 형태이다.

3.2 3GPP-WLAN 연동 보안 메커니즘

3.2.1. USIM 기반의 WLAN 엑세스 인증

3GPP-WLAN 연동 시스템은 WLAN UE와 3GPP AAA 서버 사이의 상호인증을 요구한다. 인증을 위한 long-term secret은 USIM 내부에 저장되어 사용되며, 이를 통해 EAP 기반의 AKA 인증 흐름을 사용하게 된다.

EAP-AKA에는 기본적으로 가입자에 대한 초기 네트워크 접근에 대한 인증을 위해 Full Authentication 이 존재하며, 장소와 위치에 따라 네트워크에 대한 핸드오버가 발생되는 경우 Fast Re-Authentication 기능을 제공하여 가입자는 지속적인 네트워크 사용이 가능하게 된다.

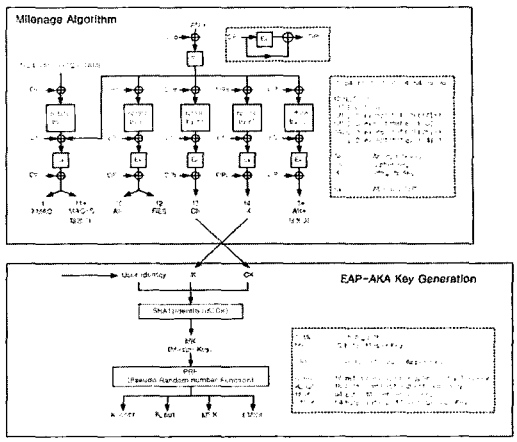
TS 33.234 는 USIM을 이용한 EAP-AKA에 대한 인증 흐름에 대해서 정의 하고 있으며, EAP-AKA에 대한 표준화 작업은 진행중에 있는 상태라 아직은 Draft 형태로 존재하고 있다.

3.2.2 3GPP-WLAN 연동 보안 요구사항

802.1x 기반의 WLAN의 경우 WLAN-AP와 UE 간에 전송되는 데이터에 대한 보안이 상당히 취약한 상태이다. 물론 이를 해결하기 위해 다양한 보안 기능을 제공하지만, 상당한 불편이 따르고 있어 이에 대한 적절한 보안성을 향상시키기 위해 3GPP AAA와 UE 간에 전송되는 데이터는 기존의 Milenage 알고리즘에 추가적인 연산 작업을 통해서 다양한 키쌍을 생성하고, 이를 통해서 데이터를 암,복호화 처리함으로써 WLAN에서의 보안성을 향상시키고 있다.

[그림 6]은 Milenage 알고리즘을 통해서 데이터 암, 복호화를 위한 키쌍을 생성하는 과정을 보이고 있다.

[그림 6]에서 볼 수 있듯이 EAP-AKA(Full Authentication) 인증 처리 과정에서 Milenage 알고리즘을 통해서 생성된 각각의 키 값을 기준으로 Master Key를 생성하고 이것을 통해서 fips186-2 표준에 명시된 PRF(Pseudo Random Number Funation) 를 이용하여 4개의 키를 생성하게 된다.



[그림 6] PRF를 통한 키 생성 메커니즘

각각의 키의 용도는 다음과 같다.

- 16 바이트 K_encr (메시지 암/복호화 키)
- 16 바이트 K_aut (메시지 인증 코드 생성/검증 키)
- 64 바이트 MSK (마스터 세션 키)
- 64 바이트 EMSK(확장된 마스터 세션 키)

상기의 키 값중 K_encr 의 경우 UE와 3GPP AAA 시스템간에 데이터를 암 · 복호화 처리하는 경우에 사용되며, K_aut 는 MAC 생성 및 검증에 사용되어진다. 추가적인 키로 MSK와 EMSK가 생성되는데, 이중에서 MSK는 WLAN의 AP와 UE간의 취약한 보안성을 강화하기 위해 WEP 키로서 사용되게 된다.

Ⅳ. USIM 보안 모듈 설계 및 구현

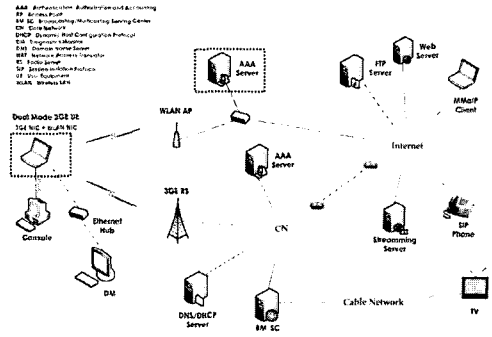
본 절에서는 USIM 보안 모듈 구현 목적 및 범위를 기준으로 설계 및 구현 한다.

4.1 개요

4.1.1 구현 목적

USIM 보안 모듈을 구현하는 기본적인 목적은 다음과 같다.

- USIM에 대한 구조 이해 및 내부 메커니즘 구현
- 3GPP 환경에서의 가입자 인증을 위한 보안 메커니즘 구현
- WLAN 환경에서의 가입자 인증을 위한 보안 메



〔그림 7〕 3GPP-WLAN 연동 환경

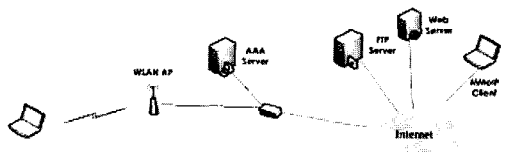
커니즘 구현

4.1.2 구현 범위 및 환경

3GPP-WLAN 연동을 위한 USIM 모듈을 개발하기 위해서는 기본적으로 3GPP 망 접속을 위한 3G Module을 필요로 하고, USIM Card와 Card Reader 가 연동이 되어 운용되어야 하며, 3G 망의 인증 시스템 및 HLR/VLR 시스템 등이 구축되어야 정상적인 3G 연동 시스템을 구성할 수 있다. 그러나 실제 이러한 환경을 구축하고 관련 모듈을 개발하는 것에는 상당한 어려움이 따른다. 따라서 본 논문은 실제 운용환경과 100% 일치할 수는 없지만, 기본적인 요구사항을 적용한 USIM Emulator 시스템 개발을 통해서 3GPP-WLAN 연동에서 필요로 하는 기본적인 요소를 적용하고 시험하도록 한다.

이러한 상황에 따라 USIM 보안 모듈 개발에 따른 Emulator 에 적용되는 기술은 다음과 같다.

- USIM 의 기본적인 Framework 개발
  - 하부 통신 모듈 :
    APDU(Application Protocol Data Unit) 지원
  - File System 모듈 :
    USIM의 파일시스템 구조 지원
  - Crypto API 모듈 :
    AES 및 SHA-1 알고리즘 지원
- 3GPP 환경에서의 가입자 인증을 위한 보안 메커니즘 구현
  - AKA 모듈 : Milenage 알고리즘 지원
- WLAN 환경에서의 가입자 인증을 위한 보안 메커니즘 구현
  - EAP 모듈 : AKA 모듈과 연동된 EAP 지원모듈



〔그림 8〕 3GPP-WLAN 테스트 시험 연동 환경

- 내부적으로 필요한 Crypto 알고리즘 지원
  - Block Cipher : AES 128bit
  - Hash : SHA-1
  - Random Generator : PRF

실제로 USIM 보안 모듈을 적용한 테스트 환경은 〔그림 7〕과 같은 구성을 가지나 본 논문을 통해 개발되는 USIM 보안 모듈의 경우 여러 가지 환경이나 여건이 어려운 관계로 다음과 같은 테스트 시험 환경에서 구현했다 (〔그림 8〕 참조).

위의 그림에서 볼 수 있듯이 가입자 시스템이 UE에는 802.1x 기반의 WLAN Card가 연결되어 있고, WLAN AP를 통해서 AAA Server와 EAP-AKA 기반의 인증을 수행하도록 환경을 구성 한다.

4.1.3 운용환경 및 개발 언어

본 논문을 통해서 개발하고자 하는 USIM 보안 모듈은 총 3가지 부분의 모듈로 나뉘며, 각각의 모듈에 대한 운용 환경 및 개발 언어는 다음과 같다.

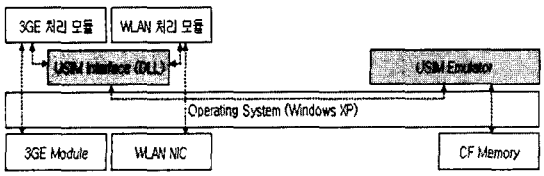
- EAP-AKA 지원을 위한 AAA 시스템
  - 개발 타겟 시스템 : x86 기반의 Linux (Kernel v2.6.x/한컴 리눅스)
  - 기본 베이스 프로그램 : FreeRADIUS v1.0.4
  - 개발 언어 : C (Compiler : GCC v3.4.1)
- USIM 보안 모듈 (Emulator)
  - 개발 타겟 시스템 : x86 기반의 MS Windows XP 이상
  - 개발 언어 : C++ (Compiler : Visual Studio v2003)
- USIM 연동 API
  - 개발 타겟 시스템 : x86 기반의 MS Windows XP 이상
  - 개발 언어 : C++ (Compiler : Visual Studio

v2003)

4.2 시스템 설계 및 구현

4.2.1 시스템 구조

전체 시스템 구성에서 UE(User Equipment) 단의 모듈의 구조는 다음과 같다.



〔그림 9〕 UE의 USIM 에뮬레이터 구조

〔그림 9〕에서 파란 색으로 칠해진 부분이 본 논문에서 개발한 범위이며 USIM Interface 모듈은 DLL 형태로 제공되며, 3GE 처리 모듈 및 WLAN 처리모듈이 필요시 마다 런타임 함수 호출을 통해서 USIM Emulator와 통신을 하며 필요한 명령 요청 및 응답을 처리하게 된다.

4.2.2 시스템 상세 구조

〔그림 9〕에서 보인 USIM Interface와 USIM Emulator 모듈에 대한 상세한 구조를 크게 두가지로 나타낸다.

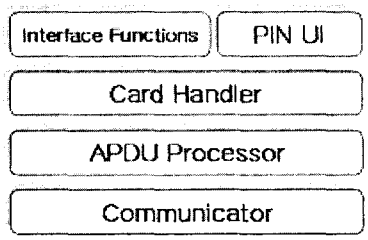
① USIM Interface 모듈

USIM Interface 모듈은 상위 어플리케이션인 3GE 처리 모듈 및 WLAN 처리 모듈이 런타임시에 호출하여 사용하는 DLL 모듈로 해당 응용 프로그램과 USIM Emulator간 연결을 위한 Interface역할을 수행하며, 해당 응용 프로그램과 USIM Emulator간 데이터 전송을 처리한다.

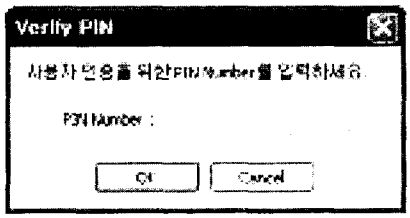
다음은 USIM Interface 모듈의 상세 구조를 보여준다(〔그림 10〕 참조).

세부 사항 중 PIN UI는 상위 응용 프로그램에서 USIM Interface Module에서 제공하는 함수를 호출하는 과정에서 USIM 모듈에 대한 접근 발생시 사용자 인증을 위하여 PIN 번호를 받게 된다.

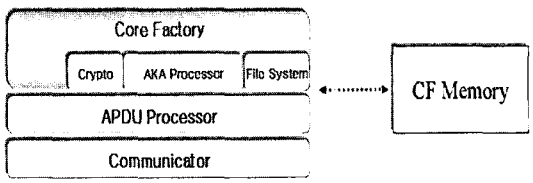
이 경우 사용자가 PIN 번호를 입력할 수 있도록 PIN



〔그림 10〕 USIM Interface 모듈 구조



〔그림 11〕 PIN 입력 User Interface 화면



〔그림 12〕 USIM Emulator 모듈 구조

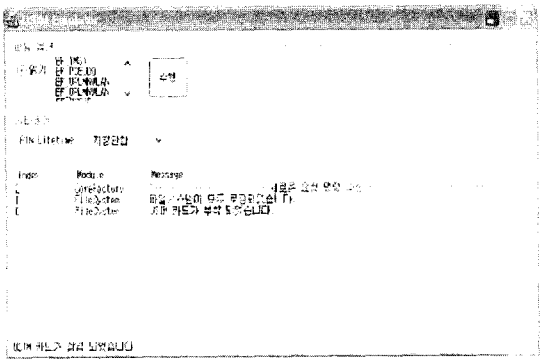
번호 입력을 위한 User Interface를 제공하는 모듈이다(〔그림 11〕 참조).

② USIM Emulator 모듈

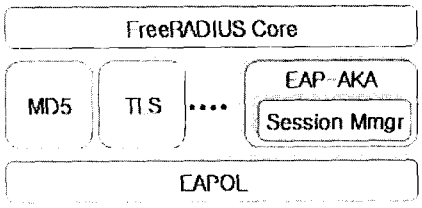
USIM Emulator 모듈은 실제 USIM 모듈을 담고 있는 Hardware를 에뮬레이션 하는 모듈이다. 본 모듈은 실제 USIM 카드 안의 정보를 관리하고 TE와의 통신을 통해서 데이터를 주고받는 부분을 에뮬레이션하며, USIM 카드는 CF 메모리 카드로 대체하고, USIM Card 내부의 Core 부분은 S/W적으로 에뮬레이션하며 3GPP TS 21.111에 준하는 기능을 제공한다.

다음의 USIM Emulator 모듈의 상세 구조를 보인다(〔그림 12〕 참조).

세부 사항 중 Core Factory는 실제 USIM 모델에서 COS 역할을 수행하는 모듈로 USIM Interface와 통신을 통해서 요청되는 정보를 하위 모듈인 Crypto, AKA Processor, File System과 유기적인 업무 분담을 통해서 적절하게 처리하여 결과를 전달하는 역할을 수행하며,



〔그림 13〕 USIM Emulator User Interface화면



〔그림 14〕 EAP-AKA 지원 인증시스템 구조

USIM Interface와의 세션관리 역할을 수행한다.

또한 USIM Emulator의 User Interface 역할을 수행하며, 각종 Event에 대한 정보를 로그로 남기고, 필요에 따라서 읽어야 하는 파일을 화면으로 보임으로써 직관적으로 USIM Emulator의 동작 상태를 확인할 수 있도록 하였다(〔그림 13〕 참조).

4.2.3 인증(AAA) 시스템

인증 시스템은 가입자에 대한 인증과 무선 네트워크 접속에 대한 과금 기능을 제공하기 위한 시스템으로 3G 혹은 WLAN 환경에서 필수적인 요소이다.

마찬가지로 인증시스템 역시 3G 및 WLAN을 통합한 형태의 인증을 제공하기 위하여 EAP-AKA 인증 기능을 제공하여야 한다.

인증시스템은 RADIUS 기반의 EAP-AKA를 지원하도록 하기위해 Open Source인 FreeRADIUS를 이용하여 EAP-AKA 기능을 추가 개발하였으며 이를 통해서 EAP-AKA 인증 서비스를 지원하도록 구현 하였다.

다음의 그림은 본 논문을 위해 개발된 부분을 보이고 있다(〔그림 14〕 참조).

① EAP-AKA 모듈

FreeRADIUS를 기반으로 한 AKA 서비스 지원을 위해 AKA 처리 모듈을 새로이 개발하였으며, AKA 방식의 인증 서비스를 제공하기 위하여 FreeRADIUS가 기존에 제공하는 Milenage 알고리즘과 PRF 알고리즘을 재사용하였다. (현재 FreeRADIUS는 EAP-SIM 인증 기능을 제공하고 있어 Milenage 알고리즘 및 PRF 처리 모듈은 기본적으로 포함되어 있다.)

또한 사용자 인증 과정에서 필요한 데이터 암/복호화를 위하여 따로 AES 알고리즘과 SHA-1 해쉬 알고리즘을 추가하여 모듈을 작성하였다.

② Session Manager 모듈

본 모듈은 FreeRADIUS에서는 제공하지 않는 세션 관리기능을 제공하기 위해 만들어진 기능으로, EAP-AKA에서는 가입자가 초기에 인증을 수행하기 위한 Full Authentication 기능과 초기 인증을 마친 가입자가 로밍 혹은 여러 가지 상황에 의해서 재인증을 하는 경우 빠른 인증 처리를 위해 Fast Re-Authentication 기능을 제공한다.

그러나 FreeRADIUS는 Fast Re - Authentication을 지원하기에는 시스템 구조가 맞지 않기 때문에 이러한 세션 관리 기능을 두어 사용자가 Full Authentication 처리 후 나중에 Fast Re-Authentication을 처리할 수 있도록 기능을 추가 함으로써 표준을 준용하도록 추가 개발하였다.

4.3 USIM 모듈 운용 및 테스트

본 절에서는 실제 WLAN 상에서 EAP-AKA 지원을 위한 RADIUS 시스템을 구축하고, 단말에 USIM Emulator를 적용하여 WLAN 기반의 EAP-AKA인증을 처리하는 과정을 보임으로써 테스트 서비스가 성공적임을 보인다.

4.3.1 EAP-AKA Full Authentication 처리과정

UE가 WLAN에 연결을 하고 초기 접속을 수행할 때 AP(Access Point)는 UE가 네트워크 접속에 따른 인증을 수행토록 하기 위해 가장먼저 UE의 단말 가입자 정보를 얻기위해 EAP-Request/Identity를 요청하게 된다.

이때 AP가 UE측에게 처음으로 EAP-Request/Identity를 전송하였을 경우 처리 과정은 실제 Windows의 RAS(Remote Access Serial) 측에서 처리하게 되며 기

본적으로 필요한 가입자의 계정 정보를 요청하여 리턴하게 된다. 다음의 화면은 간략히 표현한 USIM 측의 처리 내용을 보인다.

```
[INTERFACE] RasEapGetIdentity()
[USIM] Client Connected..
[USIM] [SESSION] USIM Interface Module
  Connected.
[USIM] Data Info : [==>> APDU Request
  Data]
                    :
[USIM] [FileSystem] Check PIN
[INTERFACE] GetPinNumber() Called..
[USIM] Data Info : [<<== APDU Response
  Data]

[USIM] 69 82                              i.
                    :
[USIM] Data Info : [==>> APDU Request
  Data]
[USIM] 00 b0 00 00 08                     .....
[USIM] [APDU] CLA=[00], INS=[b0], P1=[00],
  P2=[00], Lc=[00], Le=[08]
[USIM] Data Info : [[FileSystem] Read Binary
  Success]
[USIM] 07 61 6b 61 75 73 65 72      .akauser
[INTERFACE] Connection Info
  [Perm:akauser], [Pesudo:akauser],
[SSID:NGMT1]
[INTERFACE] RasEapGetIdentity()
[USIM] 07 61 6b 61 75 73 65 72 91 08
                              .akauser..
```

상기의 내용에서 볼 수 있듯이 초기에 EAP-Request/Identity 요청이 수신되면 Windows에서는 RAS Module의 RasEapGetIdentity() 함수를 호출하게 되고, USIM Module을 통해서 최종적으로 AAA측에 전송할 가입자의 기본 계정 정보를 리턴하게되어 'akauser' 라는 계정 정보를 AAA 측에 전송하게 된다.

이때 윈도우는 EAP-Response/Identity 패킷을 만들어 AP측에 전송하게 되고, AP는 이를 AAA 측에 전달함으로써 인증 처리를 시작한다.

```
Ready to process requests.
rad_recv: Access-Request packet from host
 129.254.219.73:1645, id=26, length=130
        User-Name = "akauser"
        Framed-MTU = 1400
        Called-Station-Id = "0013.c39c.1080"
        Calling-Station-Id = "0012.f023.096e"
        Service-Type = Login-User
        Message-Authenticator =
  0xe118aa32eb1abeb797e2eaf84d1bc010
        EAP-Message =
 0x0202000c01616b6175736572
        NAS-Port-Type = Wireless-802.11
        NAS-Port = 505
        NAS-IP-Address = 129.254.219.73
        NAS-Identifier = "NGMT1"

                    :
auth: type "EAP"
  Processing the authenticate section
  of radiusd.conf
                    :
Sending Access-Challenge of id
    26 to 129.254.219.73:1645
EAP-Message
    = 0x0143000c170500000d010000
Message-Authenticator
    = 0x00000000000000000000000000000000
State = 0x68d60022b39106082361cf38726610c1
Finished request 0
    Going to the next request
```

다음은 AAA에서 EAP-Response/Identity 를 수신한 경우의 로그 내용을 보인다.

위의 내용에서 볼 수 있듯이 'akauser' 계정을 가진 단말에서 전송된 EAP-Response /Identity 패킷을 이용해서 내부의 사용자 DB를 검색하고, 가입자 정보가 존재하면 해당 가입자에 대한 상세 계정정보를 요청하기

위해 EAP-Request /AKA-Identity를 생성하여 단말 쪽으로 전송하는 것을 보이고 있다.

V. 결론

본 논문을 통해서 3G 환경 및 WLAN 환경에서 USIM을 통한 인증 보안 모듈을 개발 하였다. 실제 제작된 보안 모듈이 실제 3G 환경과 WLAN 환경에 적용하기에는 어려운 Emulator 수준에서의 개발이지만, USIM의 내부적으로 동작되는 모듈을 구현 해 봄으로써 실제 USIM을 개발하는데 필요한 관련 표준 문서와 내부적인 서비스 프로세스에 대한 개념을 분석하였으며, 이를 통해서 향후 USIM 관련 기술 개발에 도움이 될것으로 사료된다. 현재 이동통신과 관련된 분야에서 국내의 경우 USIM에 대한 개발 및 연구는 활발하게 이루어지고 있지만, 실제 필드에서 적용한 예는 극히 드물게 존재하는 상태이며, 이제 이동통신 시장에서 기지개를 펴고 있는 상황이라 판단된다. USIM을 이용한 다양한 BM(Business Model)이 존재할 것임을 믿어 의심치 않는다. 또한 3G 환경과 WLAN 환경의 통합 시장 역시 국내의 대기업에서 과감한 투자에 의해서 적극적인 시장 개척을 하고 있으나 아직은 USIM 과 연동된 서비스를 제공하고 있지 않은 상태이다. 향후 Wibro 기술의 성공적인 기술 개발 및 서비스 성공을 통해서 3대 무선 네트워크에 대한 통합 인증에 대한 요구사항도 급격히 증대될 것이며 이러한 환경에서 특히나 보안의 중요성은 강조될 것으로 생각한다.

참고문헌

[1] Chen, Zhiqun, Java Card Technology for Smart Cards, Addison-wesley, 2000.

[2] draft-arkko-pppext-eap-aka-15, June2005: "Extensible Authentication Protocol for UMTS Authentication and Key Agreement (EAP-AKA)."

[3] 3GPP TS 22.234 : "Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)"

[4] 3GPP TS 23.234 "3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3GPP system to Wireless Local Area Network(WLAN) Interworking ; System Description"

[5] 3GPP TR 23.934 "3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3GPP system to Wireless Local Area Network(WLAN) Interworking; Functional and architectural definition."

[6] 3GPP TS 24.234 : "3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3 (Release 6)"

[7] 3GPP TS 33.234 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects ; 3G Security Wireless Local Area Network (WLAN)nterworking security(Release 6)."

[8] TTA, "2.3GHz 휴대 인터넷 표준-물리계층," TTAS, KO-06.0064, June 2004.

[9] TTA, "2.3GHz 휴대 인터넷 표준-물리계층," TTAS, KO-06.0065, June 2004.

〈著者紹介〉

김 춘 수 (Choonsoo Kim)
1987년: 숭실대학교 전기공학과(학사)
1989년: 숭실대학교 전기공학과 대학원(석사)
1996년: 숭실대학교 전기공학과 대학원(박사)
2006년 현재: 국가보안기술연구소 팀장
<관심분야> 정보통신 정보보호