휴대인터넷에서의 UICC 기반 EAP-AKA 인증처리 기술에 관한 연구

손영설,박준호,서명희,옥창석
KT 컨버전스본부
sonys@kt.co.kr, mobile@kt.co.kr, mhseo@kt.co.kr, csok77@kt.co.kr

A study on the UICC-based EAP-AKA authentication in WiBro

Sohn Young-Seol, Park Joon-Ho, Seo Myeong-Hee, OK Chang-Seok
KT Convergence BU

요 약

본 논문은 휴대인터넷에서 스마트카드 기반의 EAP-AKA 인증프로토콜을 이용하여 안전한 네트워크 접속 및 가입자 인증을 제공하기 위한 기술로써, 스마트카드의 가입자 인증 모듈과 인증센터(AuC)와의 peer-to-peer 간의 상호인증 및 EAP 인증 패킷 처리를 위한 프로토콜을 소개한다. 다양한 EAP 인증방식을 비교분석하고 휴대인터넷에서 요구되는 보안적 특성을 만족하기 위하여 EAP-AKA 가입자 인증 모듈을 어떻게 스마트카드에 구현하며, 이에 따라 고려하여야 사항들을 무엇인지 기술한다. 본 논문에서 소개하는 UICC 기반의 EAP-AKA 인증 방식의 적용은 최근 문제가 되고 있는 이동통신 단말의 불법 복제 문제를 휴대인터넷 분야에서 해결하는 강력한 보안대책의 일환으로, 서비스 이용 고객으로 하여금 자신의 개인정보를 안전하게 보호할 수 있는 수단으로 평가된다. 또한, 고객이 한 장의 UICC 를 이용하여 다양한 형태의 여러 휴대인터넷 단말에서 카드를 삽입하여 휴대인터넷을 자유롭게 사용할 수 있는 가입자 이동성을 제공한다.

I. 서론

휴대인터넷(WiBro) 서비스는 휴대형 단말을 사용하여 정지 및 이동 중 언제, 어디서나 고속의 전송속도(1 ~ 2Mbps)로 인터넷에 접속하여 다양한 정보 및 컨텐츠의 사용이 가능한 서비스로 정의할 수 있다[1].

PDA, 노트북, 스마트 폰, 등의 다양한 휴대인터넷 단말을 사용하여 인터넷 서비스를 제공하는 휴대인터넷 환경에서는 가입자에게 네트워크 접속 및 서비스 이용에 있어서 높은 보안 신뢰성을 제공해주어야 한다. 특히, 휴대인터넷 단말은 특화된 단말운영체제와 입력장치를 가진 폰(phone)형태의 기존 이동통신 단말과 달리 PDA, 노트북 등의 보다 범용의 운영체제 채택과 외부 환경에 노출되어있는 단말을 사용함에 따라 악의적인 단말 복제, 서비스 공격 등의 매우 취약한 보안 환경에 노출됨으로써 휴대인터넷 서비스 이용 및 네트워크 접속을 위하여 강력한 보안대응책이 요구된다.

이에 2005 년도에 정보통신부 및 정부기관 산하의 국내 표준기관인 TTA 휴대인터넷 프로젝트 그룹(PG302)에서 국내 휴대인터넷 접속 및 가입자 인증을 위하여 가입자 인증 모듈(SIM: Subscriber Identity Module)카드를 도입하기로 결정하고, 이에 대한 표준화 작업을 완료하였다. 국내 휴대인터넷에서 사용하는 가입자 인증 프로토콜은 IEEE 802.16e 에서 정의하는 PKMv2 의 EAP(Extensible Authentication Protocol) 인증 프로토콜과, 3 세대 이동통신 네트워크 시스템(UMTS: Universal Mobile Telecommunications System) 및 CDMA 2000 에서 사용하는 AKA 인증 메커니즘을 채택한 EAP-AKA 인증 방식을 사용하였다. EAP 인증프로토콜에 이동통신 네트워크에서 사용하는 인증방식을 적용한 사례는 2000 년대 초반 유럽 지역에서 몇몇 단말 제조사 및 스마트카드 제조사들에 의해 있었다. 당시 유럽에서 광범위하게 사용 중인 2 세대 이동통신 네트워크인 GSM/GPRS 과 무선 랜(WLAN, IEEE 802.11)과의 상호운용성(Interworking)을 고려한 EAP-SIM 인증 방식의 PCMCIA 카드를 출시하여 무선 인터넷을 사용할 수 있는 환경을 제공하였다.

본고에서는 국내 휴대인터넷에서 채택한 스마트카드 기반 EAP-AKA 인증 프로토콜을 구현하기 위하여 휴대인터넷의 서비스 및 보안적 특성을 고려하고, 다양한 EAP 인증방식을 비교 분석한 후, EAP-AKA 인증방식이 가지는 특징을 살펴보도록 한다. 또한, EAP-AKA 인증방식을 스마트카드 기반으로 구현함에 따라 얻을 수 있는 효율성 및 보안 특성을 기술하고, 이러한 인증 방식을 구현하기 위한 기술 사항을 검토하도록 한다.

II. 본론

가. 휴대인터넷의 보안 특성

휴대인터넷 시스템은 EAP 패킷 처리 및 AuC 와의 상호인증을 수행하는 가입자 인증 카드(SIM Card), 가입자가 휴대인터넷 서비스를 제공받기 위하여 사용하는 휴대인터넷 단말(User Equipment), 유선 네트워크의 종단에서 무선 인터페이스를 통하여 휴대인터넷 단말과 송수신하는 AP(Access Point)역할을