2.3GHz 휴대인터넷(와이브로™) 상호 인증 메커니즘 (TTAS.KO-06.0110)

한 진 희 한국전자통신연구원 선임연구원

1. 서론

휴대인터넷 (와이브로™) 서비스는 전송속도, 이동성, 셀 반경 등을 고려해볼 때 이동전화와 무선LAN (Local Area Network)의 중간영역에 위치하며, 도심지 내에서 1Mbps 이상의 무선인터넷 서비스를 이동 중에도 끊김없이 사용할 수 있는 대표적인 차세대 이동통신 기술로 정의된다.

휴대인터넷 (와이브로™) 서비스를 사용자에게 안전하게 제공하기 위해 고려되어야 할 보안사항 중 IEEE 802.16e-2005, TTAS.KO-06.0082/R1 표준에서 명시하고 있는 인증방법을 살펴보면 X.509 인증서 기반 RSA 인증방식과 EAP (Extensible Authentication Protocol) 기반 인증방식의 2가지 방법이 명시되어 있다. 하지만, PSS (Portable Subscriber Station : 휴대인터넷 단말)에서 모든 인증절차를 처리하도록 정의하고 있기 때문에 외부 침입자로부터 사용자의 개인 정보 및 중요한 키 값을 안전하게 보호해 줄 수 있는 PSS용 물리적 보안장치 또는 보안 플랫폼이 제공되지 않을 경우 보안상이 취약한 부분을 많이 내포하게 된다.

2.3GHz 휴대인터넷 상호 인증 메커니즘 (TTAS.KO-06.0110)은 PSS에서 발생가능한 보안 취약성을 최소화하고 휴대인터넷 서비스 사용자에게 안정성 및 신뢰성을 제공하기 위해 PSS를 개인 정보 및 중요한 키 값을 저장하는 PISIM(Portable Internet Subscriber Identity Module : 휴대인터넷(와이브로™) 가입자 인증 모듈)과 PISIM 탈부착이 가능한 PE (Portable Equipment: 단말)로 구성하고 RFC 3748과 4187 문서에 기반하여 EAP-AKA 인증 프로토콜을 PISIM상에서 수행하는 휴대인터넷 (와이브로™) 상호 인증 절차를 규정하고, 이 과정에서 요구되는 PE와 PISIM 사이의 인터페이스 정의를 위해 필요한 세부 항목을 정의한다.

2. 휴대인터넷 (와이브로™) 상호 인증절차

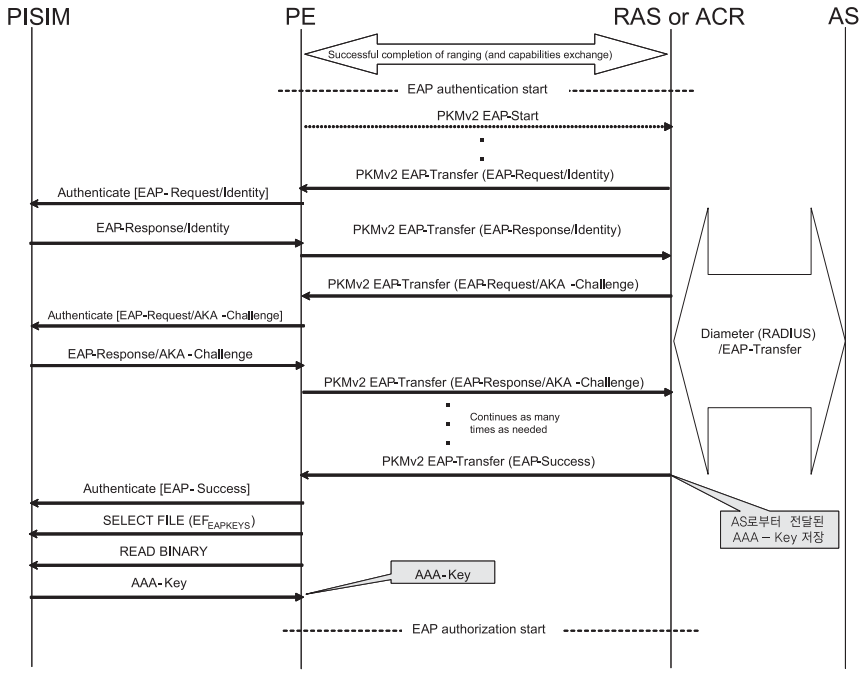
휴대인터넷(와이브로™) 상호 인증절차는 EAP-AKA (Authentication and Key Agreement)를 휴대인터넷(와이브로™)에 적용하되 기본적으로는 휴대인터넷(와이브로™)의 PKMv2 (Privacy Key Management version 2) 프로토콜을 따르며 인증절차는 휴대인터넷(와이브로™) 표준인 "TTAS.KO-06.0082/R1"에 기술된 'PKMv2 EAP 인증' 단계에 EAP-AKA 인증 프로토콜을 적용하여 재구성한다. [그림 1]은 PISIM을 이용한 휴대인터넷(와이브로™) 상호 인증과정 흐름을 보여준다. EAP-AKA 인증 프로토콜을 이용한 인증 과정은 MSK(Master Session Key)를 생성하는 과정까지이며, 이후 파생되는 세션 키 생성과정은

"TTAS.KO-06.0082/R1"의 키 유도절차를 따르며, EAP-AKA 메시지는 PKMv2 프로토콜에 정의된 PKMv2 EAP-Transfer 메시지에 포함되어 전송된다.

[그림 1]의 PE는 휴대인터넷(와이브로™) 접속 기능을 제공하고, PISIM은 EAP 종단점으로써 사용자 비밀정보 및 키 값 저장, 인증 알고리즘 처리기능 등을 제공한다.

3. PE-PISIM 인터페이스

PE와 PISIM 인터페이스상의 전송속도, 전압, 파일 제어 파라미터 등과 같은 물리적, 논리적 특성은 3GPP TS 31.101 표준을 따르며, PE가 PISIM에게 EAP-AKA 메시지를 전달하기 위해 사용하는 AUTENTICATE 명령어와 인증 관련 데이터 저장 및 관리를 위해 요구되는 파일들은 ETSI TS 102.310 표준에 정의된 내용을 준수한다. 또한, PISIM 제어 명령어 및 파일 제어 명령어는 3GPP TS 31.101과 ETSI TS 102.221를 준수한다.



[그림 1] PISIM을 이용한 휴대인터넷(와이브로™) 상호 인증과정

TTAS.KO-06.0110 표준에서 정의하고 있는 PE는 PISIM 탈/부착이 가능한 단말 또는 PISIM 기능을 hard-wired logic 형태로 제공하는 machine-to-machine 형태의 단말로 국한한다.

PISIM은 PE로부터 EAP-Success 메시지를 수신한 후 EAP-AKA 인증절차가 성공적으로 수행되었음을 확인하고, PE는 이후 PKMv2 키 유도방법을 이용하여 휴대인터넷(와이브로™) 세션 키 값들을 생성하기 위해 필요한 AAA-Key (MSK)를 $EF_{EAPKEYS}$ 파일로부터 읽어온다.

3.1 인증 애플리케이션 선택

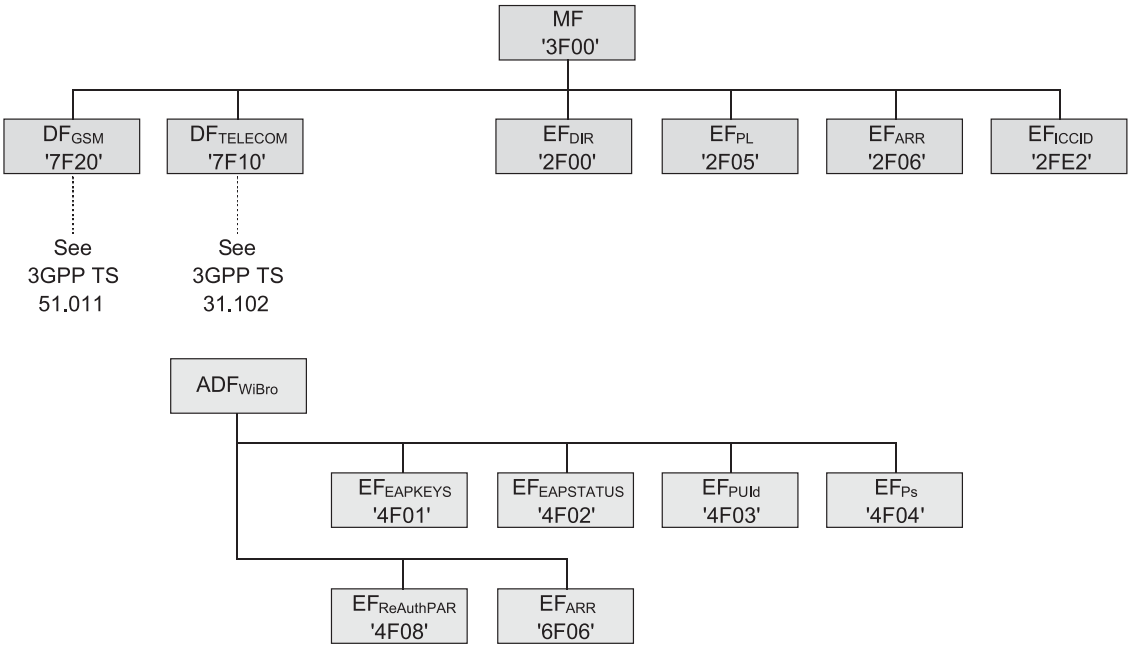
PISIM이 활성화된 이후에, PE는 EF_{DIR} 파일에 저장되어있는 휴대인터넷(와이브로™) 인증 애플리케이션 AID (Application Identifier)를 찾아 선택하게 되는데, 휴대인터넷 애플리케이션 AID는 다음과 같은 특성을 갖는다.

- 휴대인터넷(와이브로™) 애플리케이션 AID는 ISO/IEC 7816-4를 준수하며, 국제 호환성을 고려한다.
- 휴대인터넷(와이브로™) 애플리케이션 AID의 RID (Registered application provider Iden- tifier)는 ISO/IEC 7816-4 및 ISO/IEC 7816-5에 따라 ISO/IEC에 의해 할당된 값을 사용 한다.
- 휴대인터넷(와이브로™) 애플리케이션 AID의 PIX (Proprietary application Identifier exten- sion) 정의 및 형식은 ETSI TS 101.220 표준 내용을 참고 한다.

3.2 파일

표준에서 정의하여 사용하는 ADF_{WiBro}는 휴대인터넷(와이브로™) 인증을 수행하는 인증 애플리케이션의 최상위 파일이며, 휴대인터넷(와이브로™)과 관련된 인증 및 네트워크 정보를 저장하는 파일들은 [그림 2]와 같이 모두 ADF_{WiBro}의 아래에 위치한다. 표준에서 정의한 파일 외에 구현되어야 하는 필수(mandatory) 파일의 형식 및 내용은 3GPP TS 31.102와 ETSI TS 102.221를 준수한다.

휴대인터넷 사업자로 선정된 KT와 SKT는 2006년 상반기에 휴대인터넷(와이브로™) 서비스 상용화를 계획하고 있으며, 사용자 정보의 안정성 및 보안성을 고려하여 TTAS.KO-06.0110 표준에 언급된 상호 인증 방식을 휴대인터넷 인증 절차로 채택하여 운영할 것으로 전망된다. TTA PG302는 현재 AID 및 추가 필요사항들을 반영하여 금년도 상반기 중으로 TTAS.KO-06.0110 표준을 개정할 계획이다. TTA



[그림 2] PISIM 파일 구조