스마트카드를 이용한 무선 인터넷 보안 기술 현황 및 전망

한국전자통신연구원 김신효 · 정병호

1. 서 론

지금은 검색엔진에서 간단한 명령어만으로 원하는 내용의 정보를 어디서나 찾아내어 활용할 수 있는 인터넷의 세대가 주도하는 네트워크의 시대이다. 시간 및 공간에 제약받지 않고 언제 어디서나 원하는 정보의 검색과 전자 상거래 커뮤니케이션에 활용이 가능하도록 하는 인터넷이 우리 생활과 밀접하게 관련되어질수록 무선화는 당연한 방향일 것이다. 또한 우리나라 IT 산업과 통신 인프라를 세계 일류로 끌어올린 이동통신 서비스 사업자들도 무선시장의 높은 성장성과 향후 수요 창출 면에서의 무선 인터넷 서비스를 주력으로 꼽는데는 주저하지 않는다. 특히 월드컵을 전후로 새로운 이동통신 콘텐츠가 대거 등장해 하반기 이후 대대적인 무선 인터넷 성장이 일어날 것으로 전망한 바 있다[1].

초기 인터넷 성장에 전자상거래와 같은 E-비즈니스가 기여했던 것과 마찬가지로, 무선 인터넷에서도 단말기를 이용한 뱅킹, 증권거래, 전자지불 등 다양한 형태의 모바일 커머스(Mobile commerce)가 주도적인 역할을 할 것으로 기대되고 있다. 이러한 모바일 커머스의 걸림돌은 유선에 비해 훨씬 간단한 방법으로 데이터의 유추와 분석이 가능하여 기존 인터넷과 동일한 방법으로 무선 상의 보안 서비스를 제공하는 것이 어렵다는 점이다. 단말에서 보안 서비스 제공을 위해 유럽 중심의 3세대 이동통신 표준화 기구인 3GPP(Third Generation Partnership Project)에서는 MExE(Mobile Execution Environments)를 발표하였으나[2][3][4], 여기에 사용되는 각종 암호 기술들이 단말기에서 완벽하게 수행되기 위해 필요한 CPU 및 메모리, 입/출력장치 등의 성능이 뒤떨어지기 때문에 효율적인 보안 서비스의 제공이 어렵다.

이러한 단말 환경의 열악한 환경을 극복하기 위해서는 자체 연산 능력과 메모리를 보유하고 있는 스마트카드와의 연동을 통해 암호 연산을 분산시키는 등의 암호 서비스 최적화가 필요하다. 더불어 스마트카드는 비밀키 등과 같은 개인 비밀 정보의 저장 장소로써는 최상의 조건을 가지고 있으며, 복잡한 암호 연산을 하나의 칩으로 구현된 암호 연산 가속기의 장착으로 강력한 암호 연산 능력의 제공이 가능하고 이동성도 뛰어나다[5].

무선 단말기 업체 중심의 WAP 포럼에서는 무선 인증 모듈(WIM: WAP Identity Module)를 무선전송계층 보안(WTLS: Wireless Transport Layer Security)과 전자서명 등 응용계층 보안에 활용하고 있으며[6], 3세대 이동 단말기기에 삽입되어 네트워크 인증과 부가 기능을 제공하는 사용자 인증 모듈(USIM: Universal Subscriber Identity Module)로 스마트 카드를 사용하고 있다[2]. USIM 카드는 차세대 이동통신 환경에서 한 장의 카드로 세계 어느 곳에서든 자신의 휴대폰 번호로 전화가 가능하도록 하는 로밍에서의 핵심 기술일 뿐만 아니라, 개인정보인 보안 관련 정보를 저장할 수 있는 수단으로 사용된다. 이동통신 환경에서 정보보호 서비스를 제공하는데 있어서도 중요한 역할을 수행하는 USIM 카드를 기반으로, 2002년 유럽에서는 CDMA및 GSM 망간의 글로벌 로밍 서비스를 제공할 예정이다[1].

본 고에서는 무선 인터넷 기술 및 보안 기술에 대한 기술과 보안 서비스의 활성화를 위해 반드시 필요한 스마트 카드 기술 관련 표준화 동향과 무선 인터넷에서 스마트 카드가 어떻게 활용되고 있으며, 어떻게 진화할 것인지에 대하여 논하고자 한다.

2. 스마트카드 기술 동향

국제적으로 스마트 카드의 테스트 방법, 물리적 특성, 전송 프로토콜 및 송수신 메시지 구조 등에 대한 표준 논의는 표준화 기구인 ISO/IEC JTC1/SC17의 WG4와 WG8에서 수행하고 있으며, 이 표준은 대부분의 카드 제조회사 및 응용 개발자 및 서비스 사업자들이 준수하고 있다.

스마트카드의 물리적 특성을 정의한 ISO/IEC 7816-1과 접점의 크기 및 위치를 정의하고 있는 ISO/IEC 7816-2는 가장 기본적인 물리적인 특성이 기술되어 있어 현존하는 대부분의 카드는 이 규격을 완전히 만족한다. ISO/IEC 7816-3은 전기적 신호와 전송 프로토콜, 그리고 스마트카드와 단말기 사이에서 교환되는 정보구조를 규정하고 있으며[7], ISO/IEC 7816-4는 기본적인 산업간 명령어(Inter-industry Commands)를 APDU(Application Protocol Data Unit) 형태로 정의하고[8], ISO/IEC 7816-8에서는 보안기능과 관련된 산업간 명령어를 정의하고 있다[9]. 다양한 응용의 등록 절차 및 ID 부여를 위한 규격, 스마트카드와 리더 사이의 데이터 원소(Data Elements)에 관한 규격, SCQL(Structured Card Query Language) 데이터베이스 개념과 관련된 산업간 명령어에 대한 규격들도 ISO/IEC 7816 나머지 부분에서 정의하고 있다.

스마트카드에 전원이 공급되면 자신이 서비스를 제공할 준비가 되었음을 알리는 ATR(Answer to Reset)로 응답한다. 여기에는 스마트카드와 무선단말기가 사용할 전송 프로토콜과 카드가 지니는 수행능력에 대한 정보가 담겨있으며 이를 근거로 단말은 최종적인 전송프로토콜을 결정하게 된다. 또한 ATR 송수신 이후에는 PPS(Protocol and Parameter Selection) 절차를 통하여 스마트카드에서 응답한 전송 프로토콜이 아닌 새로운 전송 프로토콜을 이용할 수도 있다[7].

현재 스마트 카드의 데이터 전송에 일반적으로 가장 널리 사용되는 프로토콜은 T=0 프로토콜과 T=1 프로토콜이다. 접촉형 스마트카드 응용 규격에서 일반적으로 필수적인 구현요소로 규정하고 있는 T=0 프로토콜은 'Half-duplex transmission of asynchronous characters'로써 단순한 바이트 단위 전송 기술을 사용하여 카드 내에서 필요로 하는 메모리의 크기가 작다는 장점이 있어, 현재의 대부분의 접촉형 스마트 카드와 카드 단말에서 대부분 지원하고 있다. 'Half-duplex asynchronous transmission of blocks'로 정의된 T=1 프로토콜은 명령 APDU (Application Protocol Data Unit)를 I-block(Information-block)의 정보영역(Information field)에 실어 전송하는 블록 단위 전송을 수행한다. 이러한 블록 단위의 데이터 전송은 보안성이 요구되는 메시지 전송이나 복잡한 인터페이스 처리가 가능하지만 카드내의 상당한 크기의 메모리와 처리 능력을 필요로 하여 현재까지 사용되는 예는 없으며, 추후 카드의 성능향상과 다양한 응용에서의 카드 역할이 증대될 경우에 유용하게 사용되어질 것이다.

무선단말기와 스마트카드 사이의 일반적인 동작인 명령-응답 형태를 위한 송수신 데이터 단위는 APDU이며, 이는 단말기에 의한 명령에 대한 카드의 응답으로 구분된다. 이러한 APDU의 구성은 그림 1에 도시하였다.

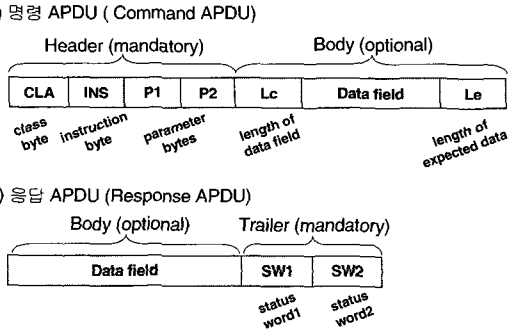

그림 1 명령 및 응답 APDU 형식

명령 APDU는 반드시 전송되어야 하는 헤더부와 송신 또는 수신할 데이터의 유무에 따라 데이터의 필드들이 채워지는 바디로 나뉘어지며, 명령어 종류를 나타내는 CLA, INS 한 바이트씩과 명령어의 파라미터를 나타내는 P1/P2는 헤더에 속하며, 바디는 카드로 송신할 데이터의 길이를 나타내는 Lc와 이후에 이 길이만큼의 데이터가 따르며 마지막에는 단말이 수신하여야 하는 데이터의 길이를 나타내는 Le로 구성된다. 명령 APDU는 카드 명령에 따라 전체 길이가 다르며 항상 5바이트로 쪼개어 전송하도록 되어 있는 T=0 전송 프로토콜이 사용되는 경우 총 4가지 방식으로 전송이 가능하다. 응답 APDU는 데이터 필드와 명령어 처리 수행 결과를 알려주는 2바이트의 상태 워드로 구성되며, 데이터는 명령 APDU의 종류에 따라 그 전송 유무가 결정된다.

대부분의 스마트카드와 단말 사이의 명령어 전송과 응답은 ISO/IEC 7816-3에서 정의하고 있는 전송 프로토콜을 통해 이루어지고, 이 때 전송되고 응답되는 명령어는 ISO/IEC 7816-4와 ISO/IEC 7816-8에서 정의하고 있는 위에서 설명한 APDU 형식을 준수한다.

3. 무선 인터넷 기술 동향

무선 인터넷은 대역폭이 좁고 신호의 단절/연결이 자주 발생하고 무선 전송에 의한 지연 시간과 데이터의 오류 발생율이 높은 무선 망의 열악한 환경과 작은 디스플레이 화면과 메모리 및 처리 능력의 제한 등에 의한 단말기의 성능 부족으로 인하여 유선 인터넷과 다른 방향으로 서비스가 진화되었다. 1997년에 단말기 제조회사를 중심으로 하는 WAP 포럼을 결성하여 무선 인터넷 서비스 단말기를 표준화하고 무선 환경에 적합한 프로토콜을 개발하기 위한 노력을 기울여 WAP 1.0 규격을 발표하였다. 이 규격은 무선 환경을 고려하여 유선 인터넷에서의 표준 프로토콜인 TCP/IP가 아닌 WDP(Wireless Datagram Protocol) / WTP(Wireless Transaction Protocol)을 제안하였으나 유선망과의 연동에 어려움으로 인하여 많은 인터넷 옹호론자들의 비판의 대상이 되었다. 그리하여 2001년에는 TCP/IP를 무선망에서 수용하도록 하는 WAP2.0을 발표한 바 있다[10]. WAP2.0 규격에서는 기존의 WAP1.x규격을 위한 역행 호환성(backward compatibility)을 제공함은 물론 무선환경에 적합한 보안 서비스를 위한 TLS(Transport Layer Security)와 단말간 호환성을 제공하기 위한 보안 토큰(cryptographic token) 규격을 만족한다.

스마트카드와 같은 보안 토큰이 저장하고 관리하여야 하는 정보가 파일 구조로 정형화된 형태라면 여러 단말과 응용에서 동일한 보안 토큰이 사용될 수 있어 단말기 개발자와 서비스 사업자 및 사용자 모두에게 일관성을 제공할 수 있으며, 공개키 암호 방식의 경우에는 RSA Laboratories가 개발하여 표준화한 PKCS (Public-Key Cryptography Standards) #15 규격이 이러한 내용에 대한 정의를 포함하고 있다[11].

PKCS #15에 기반으로 하는 정보형식은 파일 구조는 그림 2에 도시한 바와 같이 하나의 MF(Master File)과 여러 개의 DF(Dedicated File)과 EF(Elementary File)로 구성되어 있다. 하나의 토큰에는 하나의 MF와 각 EF 또는 DF가 저장된 위치를 알려주는 하나의 EF(DIR)을 가지며 여러 응용에 따라 다른 DF를 정의하여 사용이 가능하다. 특히 PKCS#15용 DF의 경우에는 카드에 저장된 다른 오브젝트들의 위치를 알려주는 EF(ODF)와 비밀키 및 공개키 또는 인증서와 관련된 EF(SKDF), EF(PrkDF), EF(PuKDF), EF(CDF)들이 DF(PKCS#15) 하위에 있으며, 개인 PIN(Personal Identification Number) 등의 인증 정보에 대한 EF(AODF), EF(ODF)와 토큰 정보 및 사용되지 않는 필드들에 대한 정보를 가진 EF(Token Info)와 EF(Unused Space)들도 있으며 가장 하위에는 실질적인 내용이 저장되어 있다. EF 내부는 DER (Distinguished Encoding Rules) 방식으로 인코딩된 형태로 저장되며[11][12], 여기에 저장되어 있는 각 파일은 독자적인 접근 권한을 가진다. 접근 권한은 파일의 종류에 따라 항상 가능, 항상 불가능, 사용자 인증이후 가능, 시스템에 의해 카드 발급자에게만 가능 등으로 구분된다.

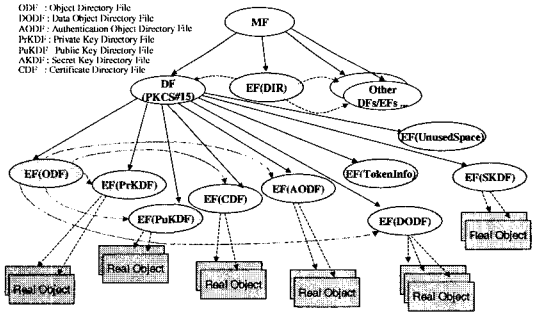

그림 2 PKCS#15내의 파일 구조

외부 단말기에 의한 파일의 접근은 원하는 정보에 대한 EF들을 읽어서 디코딩을 수행하고 접근 권한을 획득한 이후 실질적인 데이터의 조회가 가능하며, 데이터의 수정은 파일에 대한 접근 권한을 만족시키고 데이터에 대한 인코딩을 수행한 이후에나 시도가 가능하다. 즉, 카드에 저장된 모든 데이터는 정형화된 형식으로 단말기에 의해 읽고 쓰여지므로 인코딩/디코딩 동작은 단말에서만 수행하고 카드는 이러한 데이터를 안전하게 관리하는 역할을 수행하게 된다.

PKCS #15를 비롯한 PKCS 규격은 공개키를 사용하는 보안토큰의 정보 저장과 액세스에 대한 일관된

규칙을 적용함으로써 국제적인 호환성을 제공함은 물론, 하나의 스마트카드에 여러 응용을 탑재할 수 있는 다중 응용 카드 구현에 대한 지원과 기능 확장성을 제공할 수 있으므로 추후 무선 인터넷 단말에서는 반드시 만족하여야 할 것이다.

4. 스마트카드 기반 무선 인터넷 보안 기술 동향

무선 인터넷은 모든 데이터가 무선 접속으로 전달되므로 유선 인터넷에 비해 훨씬 간단한 방법으로 데이터의 변조와 감청이 가능하므로, 정보보호 서비스 제공은 무선 인터넷 서비스 활성화에 매우 중요하다. 정보보호 서비스란 무선 인터넷 데이터의 기밀성(Confidentiality), 무결성(Integrity), 사용자 인증(Authentication) 및 부인방지(Non-Repudiation) 기능을 의미하며, 이를 보장하기 위한 정보보호 기술로써 무선 공개키 기반구조(WPKI, Wireless Public Key Infrastructure)의 활용 및 단말기 보안과 스마트카드 기술의 사용과 전송 계층 보안 또는 응용 계층 보안 등이 있으며, 그 중에서도 스마트카드는 모든 다른 정보보호 서비스를 제공하는 주체로서 가장 중요한 요소이다.

현재로서는 무선 인터넷 보안을 제공할 수 있는 스마트 카드는 유럽에서의 3세대 이동통신에서의 대칭키 기반의 USIM과 인증서를 기반으로 하는 WAP 포럼에서의 WIM으로 대별된다. 이에 대한 기술동향은 다음과 같다.

4.1 WIM(WAP Identity Module)

무선 인터넷 접속 프로토콜의 사실상 국제 표준이라 할 수 있는 WAP 프로토콜에서 사용하는 무선 인증 모듈인 WIM은 스마트카드 규격인 ISO/IEC 7816과 PKCS#15를 만족함은 물론, 전송계층 보안을 위한 WTLS 핸드쉐이킹과 응용계층에서의 전자서명을 지원하는 역할을 수행하며, 사용자 비밀키와 인증서 및 개인 비밀번호 등과 같은 중요정보를 저장하고 랜덤수의 생성 및 마스터 시크릿(master secret)을 계산하는 동작을 포함하는 ECC(Elliptic Curve Cryptography) 또는 RSA 방식의 공개키 암호연산을 수행한다[13].

무선인증 모듈용 스마트 카드는 ISO/IEC 7816의 물리적 전송 규격과 전송 프로토콜을 처리하는 카드 명령어 처리 모듈과 데이터 접근과 장치 관리 및 파일 관리 및 검증 및 암호 연산을 담당하는 카드 관리 모듈, 그리고 저장 공간으로써의 파일을 필요로 한다. 또한 단말기는 스마트 카드 전송 규격을 만족하도록 전송 프로토콜의 변환과 WIM 서비스 프리미티브를 제공할 수 있는 카드 인터페이스, 카드로부터 가져온 PKCS#15 데이터 형식을 해독하고 단말에서 필요로하는 데이터 형태로 재가공할 수 있는 파일 관리자, WTLS 핸드쉐이킹과 전자 서명과 데이터 복호 및 암호 서비스를 담당하는 카드 서비스 모듈로 구성될 수 있다. 이러한 WIM을 이용한 정보보호 서비스 제공방식은 그림 3에 도시하였다.

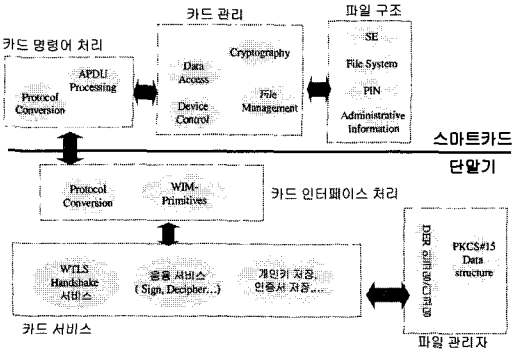

그림 3 WIM을 이용한 정보보호 서비스 제공 방식

WAP 포럼에 의한 WIM 규격은 무선 인터넷상의 전송계층과 응용계층을 위한 암호 서비스의 제공이 주기능이었지만, 현재 IETF에서는 TLS에서 WIM을 활용하기 위해 논의가 진행중이다[14].

4.2 USIM(Universal Subscriber Identity Module)

음성 데이터의 암복호에 필요한 키 생성과 인증을 수행하는 USIM은 인증과 키 일치(AKA : Authentication and Key Agreement) 과정을 수행하고, 이 과정에서 생성된 암호키를 이용하여 단말기가 사용자 데이터에 대한 암호 및 인증 서비스를 제공한다[15].

먼저 단말(MS : Mobile Station)은 인증을 위해 자신의 TMSI(Temporary Mobile Subscriber Identity) 또는 IMSI(International Mobile Subscriber Identity)를 VLR(Visitor Location Register)에게 전송하여 자신을 알리면 VLR은 인증 데이터 요구 메

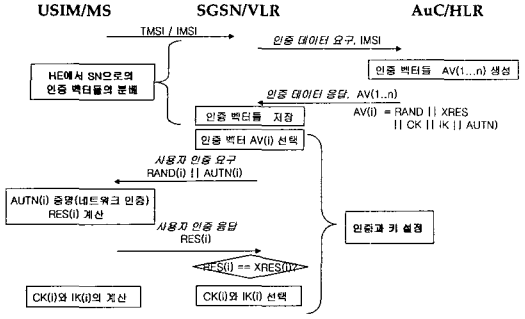

그림 4 USIM에서의 인증 및 키 일치 과정(AKA)

시지와 단말에서 수신한 IMSI/TMSI를 인증 센터(AuC : Authentication Center)에게 전송한다. 인증 센터는 수신한 IMSI에 대한 인증벡터 AV를 생성하여 인증 데이터 요구에 대한 응답으로 VLR에게 전송한다. VLR은 저장된 인증 벡터 중 하나를 선정하고 랜덤수를 생성하여 인증 벡터 내의 인증 토큰(AUTH)을 추출하여 단말에서 사용자 인증 요구를 시도한다. 단말은 USIM의 네트워크 인증 알고리즘을 이용하여 이 데이터에 대한 인증을 마치고 사용자 인증을 위한 사용자 인증 응답을 VLR에게 전송하는 한편 암호화 세션 키 CK와 IK를 생성한다. VLR은 수신한 RES와 자신이 저장하고 있는 XRES를 비교하여 단말과 사용자를 인증한 후 사용자 데이터 암호화에 이용될 세션키를 생성하여 인증과 키 일치 과정은 완료된다. 이 과정을 도시하면 그림 4와 같다. 이러한 키 공유와 인증이 완료되면, 단말과 RNC (Radio Network Control)에 장착되어 있는 사용자 데이터 암호화를 위한 동기식 스트림 암호 알고리즘과 트래픽 무결성 검증을 위한 알고리즘으로 무선 구간의 기밀성과 무결성을 제공하게 된다. 사용자 데이터의 암호 및 무결성 제공은 단말기가 담당하며, 카드는 인증 과정을 포함하는 키 생성 과정을 전담하게 된다.

USIM은 인증 및 키 일치를 위한 난수 발생 알고리즘(f0), 네트워크 인증을 위해 XMAC을 생성하는 함수(f1), 재동기화 인증함수(f1*), RES(user RES ponse) 생성을 위한 사용자 인증 함수(f2), 암호화키 CK(Cipher Key)를 생성하는 함수(f3), 무결성 검증용 키 IK(Integrity Key)를 생성하는 함수(f4)를 반드시 제공하여야 하며, 익명키 AK(Anonymity Key) 생성 함수(f5) 및 재동기화를 위한 익명 키 유도함수(f5*)와 2세대 SIM과의 호환성 제공을 위한 함수(c2, c3)를 옵션으로 필요로 한다. 2세대와 3세대 이동통신에서의 암호 및 인증 방식에 대하여 요약하면 표 1과 같다

4.3 무선 인터넷용 스마트 카드의 진화 방향

표 1 유럽식 2세대 및 3세대 이동통신 암호 및 인증 방식에 대한 비교

	종 류	2세대(SIM)	3세대(USIM)
스마트카드	인증 알고리즘	A3	f1, f1*(네트워크인증) f2(사용자 인증)
	키 생성 알고리즘	A8	f3(기밀성) f4(무결성) f5, f5*(익명성)
	랜덤수 발생 알고리즘	-	f0
	호환성 제공 알고리즘	-	c2 : XRES를 SRES로 변환 c3 : CK, IK를 Kc로 변환
	랜덤수 크기	RAND (128비트)	RAND (128비트)
	사용자 응답 크기	SRES (32비트)	XRES (32-128비트)
	암호화 세션키 크기	Kc (64비트)	CK (128비트) IK (128비트)
단말기	알고리즘 커널	-	KASUMI
	암호 알고리즘(기밀성)	A5	f8
	인증 알고리즘(무결성)	-	f9

WIM은 인증서 기반의 응용 계층 또는 전송 계층에서의 무선 데이터에 대한 보안 서비스를 제공하는 방식인 반면에, USIM은 스트림 암호 기법을 이용한 음성 데이터의 암호화에 사용될 키를 생성하고 사용자 및 네트워크에 대한 인증 기능을 수행한다. 즉, 하나는 네트워크 및 사용자 인증과 키 생성 기능을 단말기에 제공하고, 다른 하나는 무선 데이터에 대한 전자 서명 및 암/복호 서비스를 단말기에 제공하므로 동일한 단말기로 두 카드를 사용하기 위해서는 다음 몇가지 방법으로 운용이 가능할 것이다.

- 단말에 카드 장착용 슬롯을 2개 두고 USIM/WIM을 사용하는 경우

단말 제조업체가 두가지 디바이스에 대한 제어 부담이 가중될 뿐만 아니라 단말기의 소형화/경량화 경향에 뒤떨어진다.

- 단말 내장형

단말 내장형이란 단말 내부에 USIM/WIM 기능을 수행하는 모듈을 장착하여 카드와의 인터페이스 없이 서비스가 가능한 단말을 의미한다. 서비스 사업자에게는 비용면에서 장점이 있지만 보안기능 강화를 위한 불법변조 방지장치(Tamper-resistant device)로 스마트 카드를 사용할 수 없으며 다른 방식에 비해 유연성과 이동성이 떨어진다.

- 단말 내장형과 슬롯을 두는 경우

단말 내부에 USIM 역할을 하는 암호 키 생성 및 인증 알고리즘을 장착하고 인증서 발급 등의 과정을 필요로 하는 WIM은 카드 형태로 서비스를 제공하는 방식이다.

- 하나의 슬롯을 두고 통합된 USIM/WIM 카드를 사용하는 경우

하나의 카드로 독립적인 서비스의 제공이 가능하도록 하는 방식으로 멀티 애플리케이션용 카드를 의미하며, 이 경우엔 스마트 카드의 연산능력 및 메모리가 매우 커야 한다.

유럽의 스마트 카드 제조사의 하나인 슈럼버져(Schlumberger)는 자바 기반의 SIM과 WIM 기능을 결합한 뱅킹 등에 활용할 수 있는 스마트카드를 개발하여 SWIM(Subscriber WAP Identity Module) 이라는 이름으로 출시한 바 있다[16].

5. 결 론

본 고에서는 스마트 카드의 표준으로 자리잡고 있는 ISO/IEC 7816 중에서 APDU의 형식과 전송 프로토콜에 대한 내용과, 무선 인터넷 단말에 대한 호환성 제공이 가능하도록 하는 PKCS#15의 파일 구조와 무선 인터넷 응용 서비스 표준과 관련된 WAP 포럼의 동향에 대하여 살펴 보았다. 그리고 스마트 카드 기반 무선 인터넷의 대표적인 주자인 WIM과 USIM에 대한 구조 및 이러한 무선 인터넷 스마트 카드의 진화 방향에 대하여 논하였다.

지금까지 국내에서 스마트카드의 활용은 교통카드 위주로 전개되었으며 실질적인 카드 칩셋은 외국에 의존하고 있는 실정이며, 금융 분야에서도 2000년도에 접어들어 K-Cash, V-cash, A-Cash등 스마트카드 기반 전자화폐 및 신용/직불 스마트카드 서비스 개발이 진행되고 있지만, 이동 통신 분야에서는 스마트카드를 응용하는 것은 매우 부족한 실정이다. 하지만 이동 통신 시장에서는 포화 상태에 다다른 음성 통화 이외에 새로운 수요 창출을 바라는 사업자의 요구와 양질의 무선 인터넷 컨텐츠의 제공과 사용자 인증 및 컨텐츠 보호에 대한 사용자의 서비스 욕구가 높아진다면 스마트 카드를 이용하는 무선 인터넷은 유선에서의 그것과 비교할 수 없을 정도로 큰 폭발력을 가지며, 향후 무선 인터넷에서 정보보호 서비스를 비롯한 각종 서비스를 제공하는데 있어서 WIM과 USIM의 통합에 의한 멀티 애플리케이션 카드로의 진화도 가능할 것이다. 또한 이동 단말을 이용한 응용 서비스, 즉, 전자 상거래, 뱅킹, 홈 트레이딩 등을 가능하게 할 수 있는 보안 구조와 기반을 마련하는 것은 매우 중요하며, 자바카드와 같은 개방형 플랫폼을 지원하는 스마트카드 기술에 대한 보다 적극적인 연구가 이루어져야 할 것이다.

참고문헌

[1] 전자 신문, http://www.etnews.co.kr
[2] Third Generation Partnership Project, http://www.3gpp.org/
[3] 3GPP TS 22.057: "MExE Service description, Stage 1", V4.0.0, Oct. 2000
[4] 3GPP TS 23.057: "MExE Functional description, Stage 2", V4.0.0, Dec. 2000
[5] "무선 인터넷정보보호용 스마트카드 기술동향", ETRI 주간기술동향, 2000.8.30
[6] WAP 포럼, http://www.wapforum.org/

[7] ISO/IEC 7816-3, "Information Technology - Identification cards - Integrated Circuit(s) cards with contacts - Part 4: Interindustry commands for interchange, International Organization for Standardization," Dec. 1995.
[8] ISO/IEC 7816-4, "Information Technology - Identification cards - Integrated Circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols, International Organization for Standardization," Sep. 1995.
[9] ISO/IEC 7816-8, "Identification cards - Integrated Circuit(s) cards with contacts - Part 8: Security related interindustry commands, International Organization for Standardization," Oct. 1999.
[10] "Wireless Application Protocol Architecture", Version 12-July 2001, WAP 포럼, July 2001
[11] "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard", RSA Laboratories, Jun. 2000.
[12] ISO/IEC 8825-1, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)," Dec. 1998.
[13] "Wireless Application Protocol Identity Module Specification, Part: Security, Version 12-July-2001," WAP 포럼, July 2001.
[14] The Internet Engineering Task Force, http://www.ietf.org/html.charters/tls-charter.html
[15] 3GPP TS 33.102: "3G Security: Security Architecture", V3.10.0, Dec. 2001.
[16] Schlumberger Homepage, http://www.slb.com/smartcards/

김 신 효

1990 2 전남대학교 전산통계학과 졸업 (학사)
1989 2 충남대학교 컴퓨터과학과 졸업 (석사)
1990~현재 한국전자통신연구원 무선 인터넷보안연구팀 선임연구원
관심분야:무선 인터넷보안, 제한수신시스템, 정보보호
E-mail:shykim@etri.re.kr

정 병 호

1988 전남대학교 컴퓨터과학과(이학사)
2001~현재 충남대학교 컴퓨터과학과 (박사과정)
1988~2001 국방과학연구소, 선임연구원
2001~현재 한국전자통신연구원 무선 인터넷 보안연구팀장
관심분야:무선 인터넷 보안, 이동통신, 네트워크 보안
E-mail:cbh@etri.re.kr