스마트카드 기반 휴대단말 보안기술 동향

The Trend of Smart Card Based Mobile Equipment Security

김신효(S.H. Kim) 무선인터넷보안연구팀 선임연구원
정병호(B.H. Chung) 무선인터넷보안연구팀 선임연구원, 팀장

본 고에서는 현재 개인용 보안장치로 가장 널리 사용되고 있는 스마트카드를 이용한 휴대단말기의 보안 기술 동향에 대한 분석으로써, WAP 포럼에서의 WIM과 3GPP에서 논의되고 있는 USIM에 대한 기술과 향후 전망에 대해 기술하고자 한다.

I. 서 론

1997년 세계 최초로 CDMA를 이용한 상용 디지털 이동전화 서비스를 시작한 이래 최근 이동 전화 가입자가 3천만 명에 도달하였다. 이러한 이동 전화기는 초기 음성 통화만 가능하였으나, 시간과 장소에 구애 받지 않고 다양한 서비스를 제공받기 원하는 사용자의 요구를 반영하여 진화를 거듭하여 현재와 같은 무선 휴대단말기에 이르렀다. 무선 휴대단말기를 이용한 뱅킹, 증권거래, 전자지불 등 다양한 형태의 모바일 커머스(mobile commerce)가 향후 무선 서비스의 커다란 흐름이 되리라는 사실에 이의를 제기하는 사람은 없을 것이다. 하지만 무선 단말기의 성능은 데스크탑 PC의 그것과는 비교할 수 없을 정도로 열악하고 데이터는 전파를 이용한다는 특성으로 유선에 비해 훨씬 간단한 방법으로 데이터의 유추와 분석이 가능하며, 많은 정보를 저장하고 있는 단말기의 분실에 따른 개인 정보의 노출이라는 단점을 지니고 있다.

유럽 중심의 3세대 이동통신 표준화 기구인 3GPP(Third Generation Partnership Project)에서는 단말기에 정보의 다운로드가 자유로운 MExE (Mobile Execution Environments)를 발표하였으나[1]-[3], 단말기에 각종 암호 기술을 적용하기 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. 반도체 및 부품기술의 발전으로 스마트카드는 처리 능력 및 메모리의 증가와 함께 암호 기능의 역할 분담이 가능해졌다. 즉, 스마트카드는 복잡한 암호 연산을 하나의 칩 내에 구현한 암호 연산 가속기의 장착으로 보다 강력하고 빠른 암호 연산을 제공할 수 있다. 또한 비밀키 등과 같은 개인비밀정보를 안전하게 저장할 수 있을 뿐만 아니라, 크기는 신용카드와 동일한 크기로 휴대가 간편하여 이동성도 뛰어나다[4].

무선 단말기 업체 중심의 WAP 포럼에서는 무선 인증 모듈(WAP Identity Module: WIM)로 스마트카드를 이용하여 무선전송계층 보안(Wireless Transport Layer Security: WTLS)과 전자서명 등 응용계층 보안에 활용하고 있다[5]. 또한 3세대 이

동 단말기기에 삽입되어 네트워크 인증과 부가 기능을 제공하는 사용자 인증 모듈(Universal Subscriber Identity Module: USIM)로 스마트카드를 사용하고 있다[1]. USIM 카드는 차세대 이동통신 환경에서 한 장의 카드로 세계 어느 곳에서든 자신의 휴대폰 번호로 통화가 가능하도록 하는 로밍에서의 핵심 기술이며, 이동통신 환경에서 정보보호 서비스를 제공하는 데 있어서도 중요한 역할을 수행한다. 유럽의 소너라 프로젝트에서는 USIM 카드와 무선 공개키 기반 구조(Wireless Public Key Infrastructure: WPKI)를 이용하여 휴대단말 뱅킹 기능을 시연한 바 있다. 또한 2002년 올해 유럽에서는 USIM 카드를 기반으로 CDMA 및 GSM 망간의 글로벌 로밍 서비스 제공을 계획하고 있다[6].

본 고의 II장에서는 휴대단말 보안 서비스를 위해 휴대의 편리함과 비밀정보의 저장이 용이하여 가장 널리 사용될 스마트카드 기술 관련 동향을 기술한다. 그리고 III장에서는 스마트카드를 이용한 휴대단말 보안 분야에서 가장 앞서가는 표준 중의 하나인 WAP 포럼의 WIM과 3GPP에서의 USIM 기능과 동작원리와 이들의 통합 가능성을, 마지막 IV장에서는 결론을 맺고자 한다.

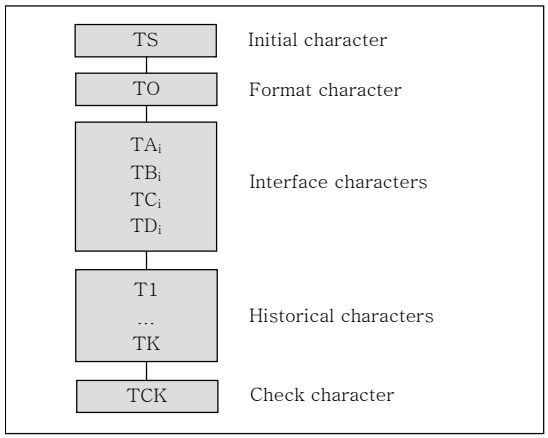
II. 스마트카드 기술 동향

스마트카드는 초기 메모리만 있던 단순한 형태에서 반도체 부품 기술의 발전으로 경량화된 마이크로컨트롤러와 메모리가 하나의 칩으로 고집적화 되면서 발전을 거듭하고 있다. 현재는 8비트 또는 16비트 마이크로 컨트롤러 및 암호 연산 가속기와 16K 또는 32K 메모리의 내장이 일반적이다. 카드 운용체제와 API를 이용하여 카드 응용 서비스 제공업자가 다양한 분야에서 적합한 형태로 프로그래밍이 가능하도록 플래시 메모리를 장착하여 “white card” 환경을 제공하기도 한다. 이러한 대표적인 예가 자바 카드이다[7].

ISO/IEC 7816은 접촉형 스마트카드 관련 규격으로써, 대부분의 스마트카드 응용에서는 이 표준을 준용한다. 특히 ISO/IEC 7816-1은 카드의 물리적 특성을, ISO/IEC 7816-2는 접점의 크기 및 위치를 정의한다. 또, ISO/IEC 7816-3은 전기적 신호, 전송 프로토콜과 스마트카드와 단말기 사이에서 교환되는 정보구조를 규정하고 있다[8]. ISO/IEC 7816-4는 기본적인 산업간 명령어(interindustry commands)를 APDU(Application Protocol Data Unit) 형태로 정의하고[9], ISO/IEC 7816-8에서는 보안기능과 관련된 산업간 명령어를 정의하고 있다[10]. 이 장에서는 ISO/IEC 7816-3, 4, 8을 중심으로 카드 표준에 대하여 논한다.

1. ISO/IEC 7816-3

스마트카드에 전원이 공급되면 단말에게 서비스를 제공할 준비가 되었음을 알리는 ATR(Answer to Reset)로 응답한다. 여기에는 카드가 지니는 수행능력에 대한 정보가 담겨 있으며 이를 근거로 단말은 최종적인 전송 프로토콜을 결정하게 된다. (그림 1)은 이 ATR에 대한 구조를 도시하였다. Initial Character인 TS는 카드와 통신하는 단말기가 어떤 형태로 이후 데이터를 수신해야 하는지를 표시하며, Format character인 T0는 그 다음 ATR 바이트들의 존재 유무를 표시한다. 이 두 바이트는 ATR에 반드시 포함되어야 하는 정보이며 다른 데이터들은 카드에 따라 생략 가능한 값들이다. Interface



(그림 1) ATR 구조

characters는 T=0 또는 T=1 프로토콜의 사용 가능 유무와 파라미터 협상 정보를 포함하고 있으며, Historical characters는 단말기가 카드 운용체제 버전과 같은 카드 특성을 파악하기 위해 사용된다. 마지막의 Check character는 ATR 내의 모든 바이트들의 체크섬으로 전송 에러에 대한 확인용으로 사용된다.

Interface characters의 TDi에 의해 결정되는 스마트카드 전송 프로토콜은 T=0 프로토콜과 T=1 프로토콜이 있다. T=0 프로토콜은 단순한 바이트 단위 전송 기술을 사용하여, 명령 APDU를 5바이트로 고정하여 카드에 전달하므로 카드 내에서 필요로 하는 메모리의 크기가 작다는 장점이 있다. 현재의 대부분의 접촉형 스마트카드와 단말에서 지원하고 있다. T=1 프로토콜은 APDU를 블록 단위로 전송한다. 이러한 블록 단위의 데이터 전송은 보안성이 요구되는 메시지 전송이나 복잡한 인터페이스 처리가 가능하지만, 카드 내의 상당한 크기의 메모리와 처리 능력을 필요로 하여 현재까지 카드에서 사용되는 예는 없다. 하지만 추후 카드의 성능 향상과 다양한 응용에서는 유용하게 사용되어질 수 있다.

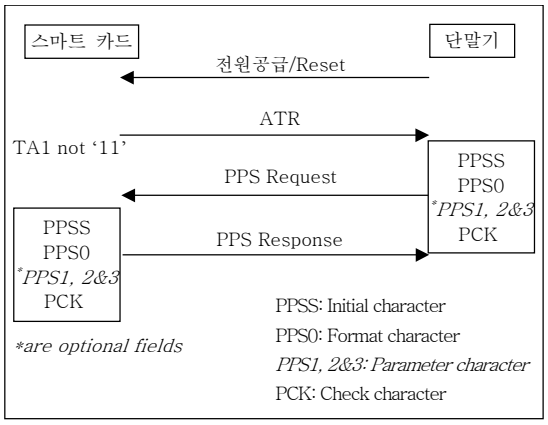
또한 ATR의 세번째 필드인 Interface characters의 TA1의 값이 '11'가 아닐 경우에는 PPS (Protocol and Parameter Selection) 절차를 통하여 스마트카드에서 응답한 전송 프로토콜이 아닌 다른 전송 프로토콜로 변환이 가능하다. PPS를 요청하고자 하는 단말은 PPSS 및 PPS0 2바이트와 파라미터 속성 값(PPS1, PPS2, PPS3)과 PCK를 카드로 전송하고, 이에 대한 카드로부터의 응답이 동일할 경우 PPS는 성공적으로 완료된다. 이에 대한 순서는 (그림 2)에 도시하였다.

이러한 ATR의 송수신과 PPS 과정을 마치면 카드와 단말은 명령과 응답을 통한 암호 정보 등의 송수신이 가능해진다.

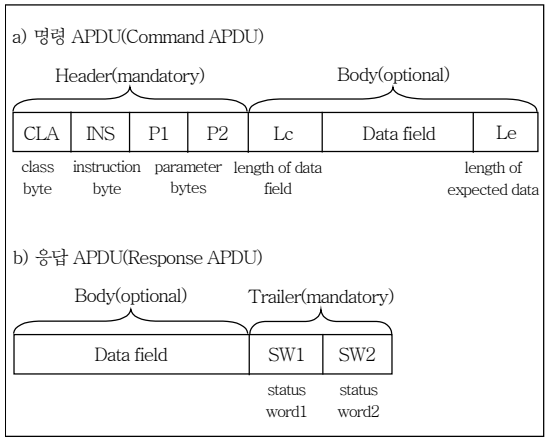
2. ISO/IEC 7816-4, 8

스마트카드와 단말 사이의 명령어 전송과 응답은 ISO/IEC 7816-4와 ISO/IEC 7816-8에서 정의하고 있는 APDU 형식을 준수한다. APDU는 다시 단말기에 의한 명령 APDU에 대한 카드의 응답 APDU으로 구분되며, 이러한 구성은 (그림 3)에 도시하였다.

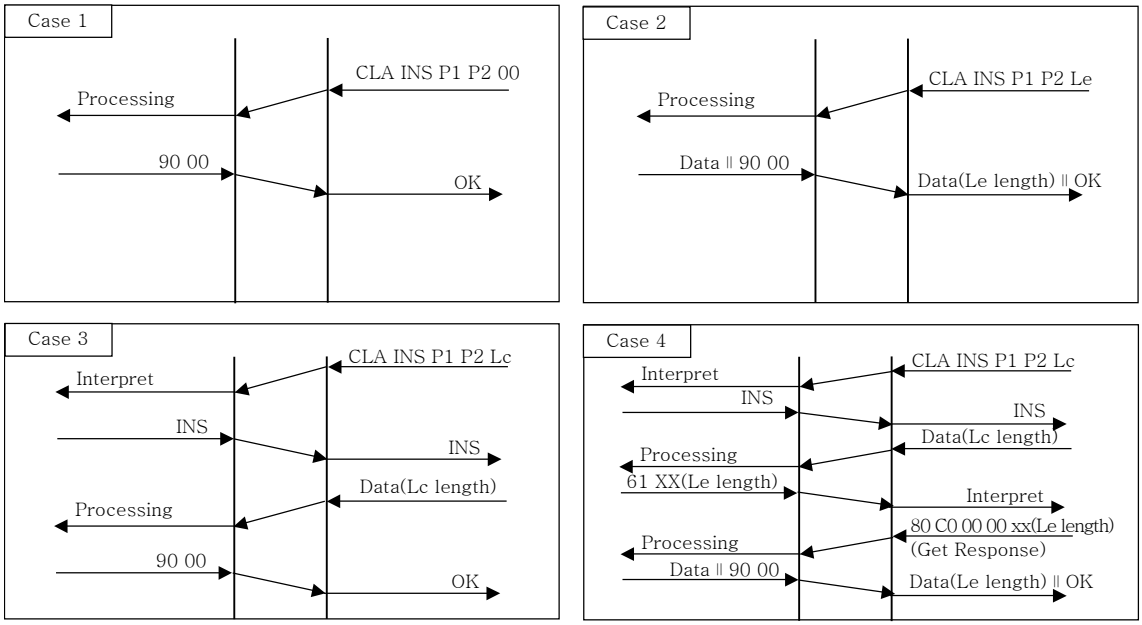
명령 APDU는 반드시 전송되어야 하는 헤더부와 송신 또는 수신할 데이터의 유무에 따라 데이터의 필드들이 채워지는 바디로 나뉘어진다. 이 바디는 명령의 종류에 따라 그 전체 데이터의 크기가 달라진다. 명령어 종류를 나타내는 CLA, INS 한 바이트씩과 명령어의 파라미터를 나타내는 P1/P2는 명령 APDU의 헤더에 속하며, 바디는 카드로 송신할 데이터의 길이를 나타내는 Lc와 이후에 이 길이만큼의 데이터가 따르며 마지막에는 단말이 수신하여야 하는 데이터의 길이를 나타내는 Le로 구성된다. 응답



(그림 2) PPS 과정



(그림 3) 명령 및 응답 APDU 형식



(그림 4) 명령/응답 전송의 4가지 경우

APDU는 명령 APDU의 종류에 따라 그 전송 유무가 결정되는 데이터 필드와 명령어 처리 수행 결과를 알려주는 2바이트의 상태 워드로 구성된다. 이때의 상태 워드는 반드시 전송되어야 한다. T=0 전송 프로토콜이 사용되는 경우의 명령 APDU는 항상 5바이트로 쪼개어 전송하고, (그림 4)에 도시한 바와 같이 총 4가지 케이스로 전송이 가능하다.

케이스 1은 가장 간단한 형태의 명령과 응답 절차로써 명령어 헤더와 바디 대신에 0×00값을 채운 5바이트를 전송하면, 상태워드만을 카드가 발생시킨다. 케이스 2는 명령어 헤더에 요구되는 응답 데이터의 길이 정보 Le가 포함되어 있으며, 스마트카드는 이에 해당하는 응답을 하는 경우이다. 케이스 3은 처음 단계에 전송하고자 하는 데이터의 길이 Lc를 카드에 알려주고 두번째 단계에서 그 데이터를 전송하는 경우이고, 케이스 4는 단말이 송수신하여야 하는 데이터가 모두 존재하는 경우로 3단계로 데이터를 송수신한다. 이 케이스에서는 카드에 전송할 데이터가 있음을 알리는 단계, 카드로 데이터를 전송하는 단계, 카드로부터 데이터를 수신하는 마지막 단계로 데이터를 송수신한다.

III. 스마트카드 기반 휴대단말 보안 기술 동향

휴대단말 보안을 위한 정보보호 서비스는 데이터의 기밀성(confidentiality), 무결성(integrity), 사용자 인증(authentication) 및 부인방지(nonrepudiation) 기능을 포함하는 포괄적인 서비스를 의미하며, 현재로서는 휴대단말 보안을 제공할 수 있는 스마트카드는 유럽에서의 3세대 이동통신에서의 대칭키 기반의 USIM과 인증서를 기반으로 하는 WAP 포럼에서의 WIM으로 대별된다. 이에 대한 기술동향은 다음과 같다.

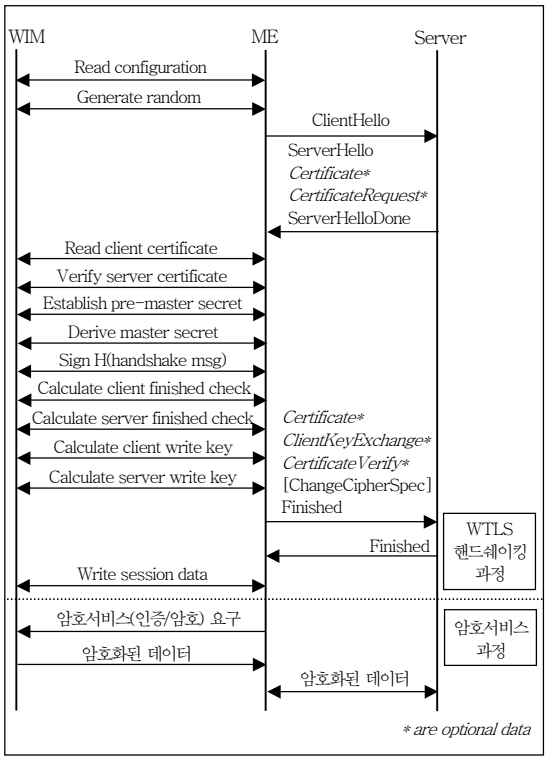
1. WIM

WIM은 무선인터넷 접속 프로토콜의 사실상 국제 표준이라 할 수 있는 WAP 포럼에서의 WAP 프로토콜에서 전송계층 또는 응용계층에서의 휴대단말 보안 서비스에 활용된다. WAP 프로토콜에서는 유선과 달리 전송계층 위에 전송계층 보안 레이어인 WTLS를 두고 보안 서비스를 제공하고, 여기에서 사용되는 키 교환 및 검증 과정에 필요한 작업은

WIM을 통해서 이루어진다. 이러한 WTLS 핸드쉐이킹 과정 이후에 전송계층에서의 데이터 암복호 서비스 제공이 가능하고, 응용계층에서의 데이터의 부인 방지를 위한 전자서명 또는 기밀성 제공을 위한 암복호를 지원할 수 있다[11],[12].

WTLS는 유선의 TLS와 유사하며, 다른 점은 암호 키의 refresh가 가능하고 RSA에 비해 연산속도에 이점을 가지는 ECC(Elliptic Curve Cryptography) 지원이 가능하며, 전체(full) 핸드쉐이킹 이외에 축약(abbreviated) 또는 최적(optimized) 핸드쉐이킹이 가능하다는 점이다. 이러한 WIM을 이용한 WTLS 전체 핸드쉐이킹과 정보보호 서비스 제공 과정은 (그림 5)에 도시하였다.

단말기(Mobile Equipment: ME)는 서버에게 연결 요청을 위한 ClientHello 메시지를 서버에게 전송하는데, 이때 필요한 랜덤수 발생은 스마트카드가 담당한다. ClientHello 메시지를 수신한 서버는 이에 대한 응답으로 ServerHello 메시지 및 서버 인증서(Certificate)와 단말기 인증서 요구(CertificateRequest)와 더불어 ServerHelloDone을 단말에게 전송한다. 이러한 인증서 및 인증서 요청 메시지 전송 과정은 생략 가능하다. 이들을 수신한 단말기는 단말기와 카드와의 명령 APDU로 원하는 서버 인증서 검증/마스터 시크릿의 계산/전송 메시지에 대한 인증을 수행하도록 한다. 이후, 인증서 및 인증서 검증을 위한 메시지(Certificate, ClientKeyExchange, CertificateVerify)를 서버에 전송하고, 서버로부터 Finished 메시지를 통해 핸드쉐이킹 과정을 종료한다. 이 과정을 마치면 단말과 서버는 카드를 이용한 암호 통신이 가능하게 된다.



(그림 5) WIM을 이용한 휴대단말 암호 서비스

2. USIM

음성 데이터의 암복호에 필요한 키 생성과 인증을 수행하는 USIM은 인증과 키 일치(Authentication and Key Agreement: AKA) 과정을 수행하고, 이 과정에서 생성된 암호키를 이용하여 단말기가 사용자 데이터에 대한 암호 및 인증 서비스를 제공한다[13].

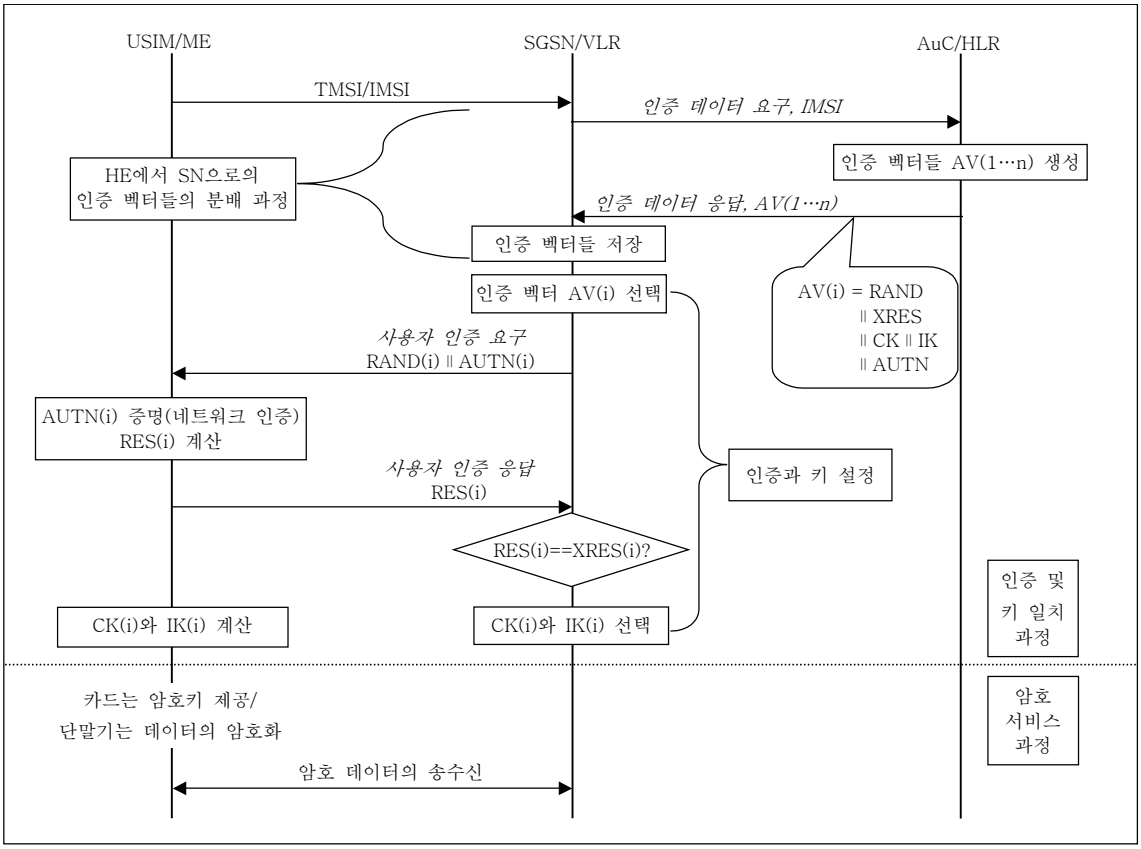
USIM은 인증 및 키 일치를 위한 난수 발생 알고리즘(f0), 네트워크 인증을 위해 XMAC을 생성하는 함수(f1), 재동기화 인증함수(f1*), RES(user RESponse) 생성을 위한 사용자 인증 함수(f2), 암호화 키 CK(Cipher Key)를 생성하는 함수(f3), 무결성 검증용 키 IK(Integrity Key)를 생성하는 함수(f4)를 반드시 제공하여야 하며, 익명키 AK(Anonymity Key) 생성 함수(f5) 및 재동기화를 위한 익명 키 유도함수(f5*)와 2세대 SIM과의 호환성 제공을 위한 함수(c2, c3)를 옵션으로 필요로 한다. 또한 단말기는 알고리즘 커널 KASUMI와 암호 알고리즘(f8) 및 인증 알고리즘(f9)을 내장하여야 한다.

먼저 단말은 인증을 위해 자신의 TMSI(Temporay Mobile Subscriber Identity) 또는 IMSI(International Mobile Subscriber Identity)를 VLR(Visitor Location Register)에게 전송하여 자신을 알리면 VLR은 인증 데이터 요구 메시지와 단

말에서 수신한 IMSI/TMSI를 인증 센터(Authentication Center: AuC)에게 전송한다. 인증 센터는 수신한 IMSI에 대한 인증벡터 AV를 생성하여 인증 데이터 요구에 대한 응답으로 VLR에게 전송한다. VLR은 저장된 인증 백터 중 하나를 선정하고 랜덤수를 생성하여 인증 벡터 내의 인증 토큰(AUTN)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. 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. 이 과정을 그림으로 도시하면 (그림 6)과 같다.

3. 휴대단말용 스마트카드의 통합 가능성

지금까지 살펴본 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 인증



(그림 6) USIM에서의 휴대단말 암호 서비스

과 키 생성 기능을 단말기에 제공하고, 다른 하나는 무선 데이터에 대한 전자 서명 및 암/복호 서비스를 단말기에 제공하므로 두 카드를 하나의 단말기로 암호 서비스를 제공받기 위해서는 다음의 몇 가지 방법으로 가능할 것이다.

첫번째 가능한 방법은 단말에 카드 장착용 슬롯을 2개 두고 USIM/WIM을 사용하는 경우이다. 하지만 최근의 단말기의 소형화/경량화 경향에 역행되는 일이며 단말 제조업체가 두 가지 디바이스에 대한 제어를 담당해야 하는 부담이 있다. 두번째는 단말 내부에 USIM/WIM 기능을 수행하는 모듈을 장착하여 카드와의 인터페이스 없이 서비스가 가능한 단말을 사용하는 방법이다. 서비스 사업자에게는 비용면에서 장점이 있지만 보안기능 강화를 위한 불법 변조 방지 장치(tamper-resistant device)로 스마트카드를 사용할 수 없으며 단말기 분실에 대한 대책을 별도로 마련하여야 한다. 마지막으로는 휴대단말에 하나의 스마트카드 슬롯을 두고 통합된 USIM/WIM 카드를 사용하는 경우이다. 즉, 하나의 카드로 독립적인 서비스의 제공이 가능하도록 하는 방식으로 스마트카드의 연산 능력 및 메모리가 매우 커야 한다. 하지만 이러한 카드의 멀티 어플리케이션화는 최근의 큰 흐름이다. 유럽의 스마트카드 제조사의 하나인 슈럼버져는 자바 기반의 SIM과 WIM 기능을 결합하여 뱅킹 등에 활용할 수 있는 스마트카드를 SWIM(Subscriber WAP Identity Module)이라는 이름으로 개발하여 출시한 바 있다[14].

IV. 결 론

본 고에서는 ISO/IEC 7816에 정의된 스마트카드 규격과 그 기술 동향에 대하여 살펴 보았다. 그리고 스마트카드 기반 휴대단말 보안 서비스가 가능한 WIM과 USIM을 이용한 휴대단말 보안 서비스 제공 방식 및 두 카드의 통합 가능성에 대하여 논하였다.

지금까지 국내에서 스마트카드의 활용은 교통카드가 일반적이며, 실질적인 카드 칩셋은 외국에 의존하고 있는 실정이다. 금융 분야에서도 2000년도에 접어들어 K-Cash, V-Cash, A-Cash 등 스마트카드 기반 전자화폐 및 신용/직불 스마트카드 서비스 개발이 진행되고 있지만, 휴대단말 분야에서 스마트카드를 응용하는 것은 매우 제한적이었다. 하지만 이동 통신 시장에서는 포화 상태에 다다른 음성 통화 이외에 새로운 수요 창출을 바라는 사업자의 요구는 절실하고, 양질의 무선 컨텐츠를 언제 어디서나 안전하게 활용하려는 사용자의 서비스 욕구가 높아지고 있다. 이러한 사업자와 사용자의 요구를 모두 만족시키는 서비스가 가능하게 하는 매체로 스마트카드는 큰 의미를 가진다. 향후 휴대단말기에 무선 데이터의 암호 및 서명에 중점을 두는 WIM과 사용자 인증과 음성 데이터의 암호에 사용되는 USIM의 기능을 동시에 가지는 멀티 어플리케이션 카드가 일반화 될 것이다. 그리고 이 카드와 휴대단말을 이용하여 자유로우면서 안전한 무선 통화는 물론 무선 결재, 뱅킹, 홈 트레이딩과 양질의 무선 컨텐츠 서비스 등이 가능할 것이다. 하지만 휴대단말 내부에서의 적절한 보안 서비스 제공을 위한 보안 프레임워크에 대한 연구가 선행되어야 한다.

참 고 문 헌

[1] Third Generation Partnership Project, http://www.3gpp.org/

[2] 3GPP TS 22.057: “MExE Service Description, Stage 1,” V4.0.0, Oct. 2000.

[3] 3GPP TS 23.057: “MExE Functional Description, Stage 2,” V4.0.0, Dec. 2000.

[4] W. Rankl and W. Effing, “Smart Card Handbook,” JOHN WILEY & SONS, Mar. 1999.

[5] WAP 포럼, http://www.wapforum.org/

[6] 전자 신문, http://www.etnews.co.kr

[7] 자바카드 포럼, http://www.javacardforum.org

[8] 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.

[9] 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.
[10] ISO/IEC 7816-8, "Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 8: Security Related Interindustry Commands, International Organization for Standardization," Oct. 1999.
[11] "Wireless Application Protocol Architecture," Version 12-July 2001, WAP 포럼, July 2001.
[12] "Wireless Application Protocol Identity Module Specification, Part: Security, Version 12-July 2001," WAP 포럼, July 2001.
[13] GPP TS 33.102: "3G Security: Security Architecture," V3.10.0, Dec. 2001.
[14] Schlumberger Homepage, http://www.slb.com/smartcards/