PKCS #15 기반의 무선인증모듈 설계 및 구현

강유성*

*한국전자통신연구원, 무선인터넷정보보호연구팀

Design and Implementation of WIM based in PKCS #15

You Sung Kang*

*Wireless Internet Security Research Team, ETRI.

요 약

무선인터넷 접속 프로토콜의 사실상 국제표준이라 할 수 있는 WAP 프로토콜의 규격을 제정하는 WAP 포럼에서는 인증서 및 비밀키의 저장, 그리고 암/복호화 및 전자서명/검증 등의 연산을 지원하기 위한 무선인증모듈 규격을 정의하고 있다. 스마트카드로 구현되는 무선인증모듈의 사용 형태를 고려할 때, 다양한 플랫폼에서의 사용과 사용자의 이동성 지원, 그리고 무선인증모듈을 이용한 정보보호 특성 보장은 필수적인 요구조건이다. 본 논문은 무선인증모듈을 스마트카드로 구현함에 있어 멀티 애플리케이션을 지원하고, 기능 확장성을 보장하기 위한 PKCS #15 기반의 무선인증모듈 설계와 구현 결과를 보인다. 본 논문에서는 접촉형 스마트카드에 대한 국제규격인 ISO/IEC 7816 시리즈 규격을 준수한 설계를 보이고, 지수승 모듈러 연산을 하드웨어적으로 지원받아 RSA 1024 비트 암/복호화 및 전자서명/검증을 처리하는 결과를 보인다.

I. 서론

WAP (Wireless Application Protocol) 포럼에서 연구중인 WAP 프로토콜과 마이크로소프트사의 ME (Mobile Explorer) 솔루션은 무선인터넷 사용의 활성화에 기여했던 대표적인 무선인터넷 접속 규격이다. 무선인터넷을 이용하는 안전한 사이버 공간을 구축하기 위해서는 기밀성(Privacy), 무결성(Integrity), 인증(Authentication), 부인방지(Non-repudiation), 접근제어(Access control) 및 신원확인(Authorization) 등 전송 정보의 정보보호 특성을 만족시키기 위한 기술개발이 병행되어야 한다.

WAP 프로토콜을 살펴볼 때, 정보보호와 관련된 요소는 WTLS (Wireless Transport Layer Security), WMLScript Crypto Library, WPKI (Wireless Public Key Infrastructure), 그리고 WIM (WAP Identity Module) 등이다. WTLS는 유선에서 사용하는 전송계층 보안 프로토콜인 SSL (Secure Socket Layer)/ TLS (Transport Layer Security)와 유사한 구조를 가지면서 무선환경에 적합하도록 구성된 프로토콜로써 무선전송계층에서 클라이언트와 서버 사이의 인증 및 세션 키 분배를 담당한다. WMLScript Crypto Library 규격에서는 전자서명을 위한 함수를 제공하고 있으며, WPKI는 공개키 기반 구조를 무선환경으로 확장한 형태로써 WTLS와 WMLScript Crypto Library 규격이 기본적으로 공개키 인증서에 기반하고 있다. WIM은 WTLS 계층에서의 데이터 암/복호화와 전자서명/검증을 지원하고 응용 계층에서의 전자서명, 암호화 키의 복호화 동작을 지원한다. 특히 WIM은 정보보호 측면에서 볼 때 비밀키와 공인 인증기관 인증서의 안전한 저장을 보장하는 장점을 지니고 있으며, 그 구현형태는 스마트카드 형태를 띠기 때문에 향후 멀티 애플리케이션 카드에 하나의 응용으로 사용되어 스마트카드 사용자에게 안전한 정보보호 서비스 제공에 기여할 수 있다.

본 논문에서는 WAP 프로토콜의 정보보호 관련 요소 중 무선인증모듈에 해당하는 WIM 내부 구조의 소프트웨어 설계에 있어 멀티 애플리케이션을 지원하며 기능 확장성이 보장되는 PKCS #15 (Public-Key Cryptography Standards #15) 기반의 효율적인 계층화 구조 설계를 제시하고 그 구현 결과에 관하여 상세히 기술한다. 본 논문의 구성은 다음과 같다. II장에서 WIM을 스마트카드 형태로 구현하기 위한 국제규격 및 관련 기술을 분석한다. 분석된 국제규격 및 관련 기술을 기반으로 WIM 모듈을 설계한 내용을 III장에서 설명하고, IV장에서는 설계된 WIM 모듈의 구현 결과 및 WIM 기능 처리 능력을 분석한다. 끝으로 V장에서 결론을 맺는다.

II. 스마트카드 구현 기술

1. WIM

보안기능을 강화하기 위하여 보안기능 처리를 위한 별도의 불법변조 방지장치(tamper-resistant device)를 사용할 수 있다. 이러한 불법변조 방지장치는 불법적인 공격자로부터 사용자의 중요 데이터를 보호하는 역할을 한다. WAP 프로토콜의 정보보

호 관련 요소 중 이러한 불법변조 방지장치 역할을 하는 요소가 WIM (WAP Identity Module)이다. WIM은 비밀키와 인증기관 인증서와 같은 중요 정보를 저장하고 있으며, 이러한 중요 정보를 이용한 암호연산을 수행하고, master secret을 계산하고 저장하는 동작을 수행한다.

WIM은 무선단말기의 보안 취약성을 보완하는 보안토큰(crypto token)으로써 기능적인 측면에서 볼 때, WTLS 계층에서의 암호연산을 지원하고, 응용계층에서의 전자서명을 지원한다[1]. 그림 1은 WIM을 포함하는 WAP 프로토콜의 아키텍처를 나타내고 있다. 그림 1에서 보이는 것처럼 WIM은 어느 특정계층만을 지원하는 것이 아니라 암호 연산과 관련된 기능을 지원하는 매체이다[1],[2]. 따라서 향후 WAP 프로토콜의 계층 구조가 SSL/TLS 계층을 포함하거나, 응용계층에서의 보안 기능 강화를 위해 발전하더라도 WIM은 다양한 보안 기능 지원을 보장할 수 있다.

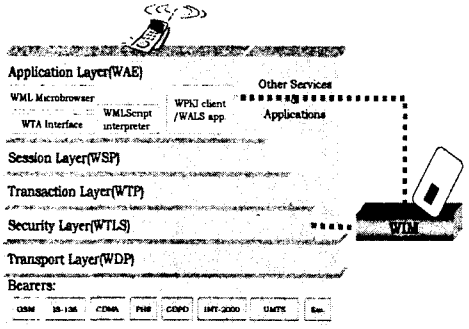

그림 1: WAP 프로토콜 참조 모델

1) WTLS 지원

WTLS 계층에서 WIM이 사용되는 시점은 핸드쉐이크 과정이다. 가입자와 서버간 핸드쉐이크는 가입자 인증과 키 설립을 위해 진행되는 과정으로써 WIM은 핸드쉐이크 과정에서의 암호연산을 수행하고 long-living WTLS 세션을 보장한다. WTLS를 지원하기 위해서 WIM이 수행하는 동작은 크게 세가지로써 첫째 비밀키의 저장 및 비밀키를 이용한 암호연산, 둘째 신뢰하는 공인 인증기관의 인증서 보관 및 인증서를 참조한 전자서명 검증, 셋째 master secret 계산과 저장 및 master secret을 이용한 주요 key material 유도 등이다.

2) 응용계층 지원

WIM은 WAP 응용계층의 요청을 받아 암호화된 데이터를 복호화하는 동작과 해쉬 데이터를 전자서명하는 동작을 수행한다. WTLS에서 제공하지 못하는 전자서명을 지원함으로써 전자상거래의 핵심 정보보호 기능인 부인방지 서비스를 보장할 수 있다. WIM은 WAP 프로토콜에서 정의하는 WMLScript를 사용한 응용뿐만 아니라 다른 모든 응용에 대한 지원을 위한 일반적인 동작을 수행한다.

2. ISO/IEC 7816

보안기능 향상을 위한 보안토큰인 WIM은 스마트카드 형태로 구현된다. 접촉형 스마트카드의 국제표준과 관련된 모든 규격은 ISO/IEC JTC1/SC17 Working Group 4에서 관리하고 있다. ISO/IEC 7816-3은 전기적 신호와 전송 프로토콜, 그리고 스마트카드와 단말기 사이에서 교환되는 정보구조를 규정하고 있다[3]. ISO/IEC 7816-4는 기본적인 산업간 명령어(Interindustry commands)를 APDU (Application Protocol Data Unit) 형태로 정의하고 있으며[4], ISO/IEC 7816-8에서는 보안기능과 관련된 산업간 명령어를 정의하고 있다[5].

접촉형 스마트카드를 구현함에 있어 ISO/IEC 7816 표준을 준용하는 것은 국제적인 호환성을 보장하기 위한 가장 중요한 부분으로써, 본 논문에서 구현하는 무선인증모듈의 소프트웨어 설계에 ISO/IEC 7816 표준을 준용하였다. 이외에도 스마트카드의 물리적 특성을 정의한 ISO/IEC 7816-1, 접점의 크기 및 위치를 정의하고 있는 ISO/IEC 7816-2, 다양한 응용의 등록 절차 및 ID 부여를 위한 규격인 ISO/IEC 7816-5가 있고, ISO/IEC 7816-6은 스마트카드와 리더 사이의 데이터 원소(Data Elements)에 관한 표준이고, ISO/IEC 7816-7에서는 SCQL (Structured Card Query Language) 데이터베이스 개념과 관련된 산업간 명령어를 정의하고 있다.

3. PKCS #15

PKCS (Public-Key Cryptography Standards) 규격은 1991년 6월에 발표되기 시작한 공개키 암호 표준의 집합으로써 RSA Laboratories가 개발, 소유 및 관리하고 있다. 특히 PKCS #15는 스마트카드와 같은 보안토큰이 저장하는 정보형식을 정의하는 공개키 암호 표준으로써 비밀키와 공인 인증기관 인증서 등을 저장하고 액세스하기 위한 방법을 정의하고 있다[6].

ISO/IEC 7816 표준은 스마트카드 구현에 있어 물리적인 특성 및 데이터 전송과 관련된 국제 호환성을 보장하는 반면, PKCS #15를 비롯한 PKCS 규격은 공개키를 사용하는 보안토큰의 정보 저장과 액세스에 대한 국제 호환성과 멀티 애플리케이션으로의 기능 확장성을 제공한다. PKCS #15에서 정의한 정보형식은 스마트카드를 비롯한 다양한 매체에 구현될 수 있으며, 스마트카드에 구현할 경우 하나의 카드에 여러 응용을 탑재할 수 있는 멀티 애플리케이션 카드 구현을 지원한다.

4. DER Encoding/Decoding

PKCS #15를 준용하는 무선인증모듈의 내부 정보형식은 ISO/IEC 7816 표준에서 정의하고 있는 DF (Dedicated Files)와 EF (Elementary Files) 개념이 적용된다. 본 논문에서 구현하는 무선인증모듈이 저장하는 중요 데이터는 EF에 저장된다. EF 내부의 데이터 구조는 ASN.1 (Abstract Syntax Notation One) 표기를 사용하여 표현할 수 있으며, 무선인증모듈에 저장되는 형태는 ASN.1 표현의 DER (Distinguished Encoding Rules) 인코딩 데이터가 저장된다[7],[8]. 따라서 무선인증모듈과 통신하는 리더는 무선인증모듈의 정보형식을 PKCS #15에 기반하여 분석하고, 분석된 결과에 따라 필요한 EF를 선택한다. EF에 저장된 DER 인코딩 데이터를 읽은 후에

DER 디코딩을 수행하여 원하는 정보를 얻게 되는데, 여기서 알 수 있듯이 DER 디코딩 동작은 리더만이 수행하므로 무선인증모듈은 DER 인코딩/디코딩 루틴을 갖고 있지 않아도 된다.

이상에서 살펴본 바와 같이 무선인증모듈을 스마트카드로 구현하기 위해서는 물리적인 특성을 비롯하여 내부 정보형식의 표현 및 저장 표준을 준수하여야 하며, 무선인증모듈이 지니는 고유의 정보보호 기능을 제공할 수 있도록 구현되어야 한다. 그림 2는 무선인증모듈을 사용하는 무선단말기와 무선인증모듈 사이의 관계를 간략하게 표현한 것이다. 본 논문에서 구현하는 PKCS #15 기반의 보안 무선인증모듈은 그림 2의 구성을 기본으로 한다.

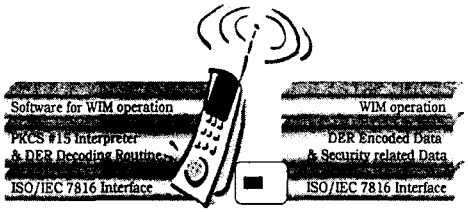

그림 2: 무선단말기와 무선인증모듈

III. 무선인증모듈 설계

1. 설계 고려사항

무선인증모듈을 구현함에 있어 기능적인 측면에서의 고려사항은 WIM 기능을 구현하는 것이고, 구현형태에서의 고려사항은 스마트카드 형태로 구현하는 것이다. 또한 상기 II절에서 밝힌바와 같이 호환성과 확장성을 고려하여 국제규격을 준수하여 설계한다.

그림 3은 이러한 기본적인 설계조건을 고려하여 구성한 스마트카드 명령어처리 설계도이다. 가장 먼저 고려해야 할 사항은 그 구현형태로써, 접촉형 스마트카드에 대한 전반적인 규격을 담고 있는 ISO/IEC 7816 표준을 준수하는 것이다. 그림 3에서 보이는 'WIM-ME contact point'에 해당하는 하드웨어적인 특성과 화살표로 표현하고 있는 스마트카드 명령어 전송 프로토콜, 그리고 스마트카드 내부 파일 구조 등이 ISO/IEC 7816 표준을 따르는 부분이다. 스마트카드가 보안토큰의 일반적인 형태인 만큼 내부 저장을 위한 정보형식은 PKCS #15를 준수하고, 정보형식의 저장형태는 DER 인코딩 데이터로 저장된다.

2. 설계 특징 및 장점

본 논문에서 구현하는 무선인증모듈의 설계 특징 중의 하나는 전송계층(Transport Layer)과 스마트카드 명령어처리 계층(Processing Layer)이 구분되는 계층화구조를 갖는다는 것이다. 그림 3에서 보이듯이 이러한 계층화구조 설계는 구현된 프로그램의 유지보수가 용이하며, 스마트카드 명령어처리 계층과는 독립적으로 데이터 전송률을 높이기 위하여 새로운 전송 프로토콜을 적용하기도 쉽다.

설계상의 또 하나의 특징은 WAP 포럼의 무선인터넷 보안모듈 규격인 WIM 규격과 PKCS #15 정보형식을 준수한 파일시스템과 파일 접근제어를 포함하고 있다는 것이다. 향후 PKCS #15 기반의 정보형식을 따르는 응용을 운용하는 멀티 애플리케이션 카드로의 확장성 및 호환성이 우수한 장점을 지닌다.

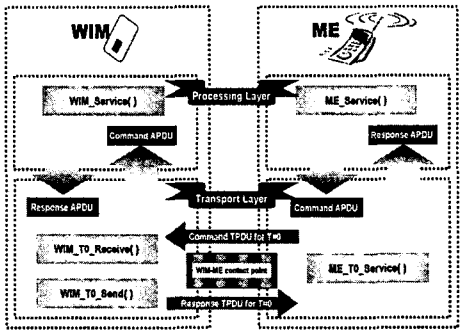

그림 3: 스마트카드 명령어처리 설계도

IV. 무선인증모듈 구현

제시된 설계에 따라 무선인증모듈을 구현하여 그 기능을 확인하기 위하여 다음과 같은 처리능력을 살펴보기로 한다. 첫째, 전송계층에서의 데이터 전송 프로토콜의 성능을 파악하는 것이고, 둘째 파일시스템에 대한 접근제어 및 정보저장 능력을 확인하는 것이며, 끝으로 정보보호 서비스 제공을 위한 정보보호 알고리즘 처리 능력을 분석하는 것이다. 본 절에서는 구현된 무선인증모듈에서의 주요 성능에 대한 분석과 그 결과를 보인다.

1. 전송계층

무선인증모듈 내부에서의 전송계층 처리는 그림 3에서 나타내고 있듯이 명령어 수신과 송신 프로토콜을 구현하는 것이다. T=0 또는 T=1 프로토콜이 사용될 수 있는데, T=0 프로토콜은 바이트 단위 전송을 기본으로 하기 때문에 요구되는 메모리의 크기가 작다는 장점이 있다. 구현된 무선인증모듈은 작은 메모리에서도 원활하게 수행되며, 대단위 데이터 전송이 요구되지 않는 WIM 기능을 고려하여 전송계층 프로토콜로써 T=0 프로토콜을 사용한다.

WIM 기능을 구현하기 위한 스마트카드 명령어는 APDU의 의미에 따라 네가지 경우로 구분할 수 있다. 전송계층에서의 T=0 프로토콜은 명령어 APDU의 길이 정보를 이용하여 네가지 경우에 따른 명령어를 구분하도록 구현되어 있다. 전송계층에서 송수신되는 데이터 유닛은 TPDU (Transport Protocol Data Unit)라 하며, 전송계층 T=0 프로토콜에서 수신된 모든 명령어 TPDU는 네가지 경우 각각에 맞게 명령어 APDU로 재구성되어 스마트카드 명령어처리 계층으로 올려진다.

따라서 그림 3에서 보이는 WIM_Service() 함수는 전송계층에서 사용되는 프로토콜에 영향을 받지 않는다. 스마트카드 명령어처리 계층이 전송계층과 독립적으로 구현되어 있기 때문에 전송계층 프로토콜의 대체가 쉬워지는 확장 가능성이 크다는 장점이

있다.

2. 정보저장 및 접근권한

무선인증모듈에 저장되는 데이터는 사용자 인증서 정보와 같은 공개 가능한 정보뿐만 아니라 전자서명에 사용되는 비밀키 정보, 사용자 인증에 사용되는 PIN (Personal Identification Number) 정보 등과 같은 중요 정보를 포함하고 있다. 구현된 무선인증모듈은 PKCS #15 규격을 준수하여 파일구조를 유지하고 있으며, 각각의 파일에 접근하기 위한 접근권한의 현재 상태정보를 무선인증모듈 내부에서 유지하고 있다. 각각의 파일에 대한 접근제어는 정보보호 서비스 측면에서 반드시 구현되어야 하는 항목이다.

파일에 대한 접근제어란 파일 내부의 콘텐츠에 접근하여 읽기 동작 또는 쓰기 동작을 수행할 수 있는 허락 여부를 의미한다. 현재 사용자가 어떤 PIN을 입력했는가에 따라 각각의 파일에 대한 접근권한이 결정된다. PKCS #15에 따른 파일시스템 구성과 내부 정보의 DER 인코딩 저장 및 파일에 대한 접근제어는 무선인증모듈을 이용한 무선인터넷 보안기능 강화에 크게 기여할 수 있으며, 호환성이 우수하여 국제표준 규격의 무선인터넷 휴대단말기에서 보안기능 수행이 가능하다.

3. 정보보호 알고리즘

무선인터넷 보안토큰으로 사용되는 무선인증모듈을 설계하고 구현함에 있어 가장 중요하게 고려되어야 하는 기능은 국제규격의 정보보호 알고리즘을 효율적으로 구현하는 것이다. 구현된 무선인증모듈이 처리하는 정보보호 알고리즘 연산은 비대칭키 연산으로써 RSA 1024 비트 암/복호화, 전자서명/검증 처리와 key material을 계산하기 위한 PRF (Pseudo Random Function) 연산이다. RSA 1024 비트 암호화 연산과 전자서명을 위한 원천데이터는 PKCS #1 규격에서 정의한 인코딩 규칙에 따라 1024 비트로 확장된다[9]. PKCS #1 인코딩은 WIM 규격에서도 정의하고 있는 내용이며, RSA 암호화를 위한 인코딩에서는 임의의 랜덤 바이트들이 첨가되기 때문에 동일한 원천데이터라 하더라도 그 결과값은 항상 달라진다.

표 1: RSA 1024 비트 연산 결과

	Data size	Key size	Time
RSA 암호화	1024 비트	24 비트	275 msec
RSA 복호화	1024 비트	1024 비트	2.55 sec
RSA 전자서명	1024 비트	1024 비트	2.68 sec
RSA 서명검증	1024 비트	24 비트	239 msec

무선인증모듈 구현에 이용한 개발툴킷은 코프로세서를 장착한 스마트카드를 고려하고 있으며, 코프로세서는 지수승 모듈러 연산을 제공하기 때문에 RSA 연산을 하드웨어적으로 처리할 수 있다. 표 1에서 RSA 1024 비트 연산에 대한 결과를 보인다. 표 1에서 보이는 시간은 호스트 PC에서 RSA 처리 명령어를 보내고 그 결과를 받을 때까지의 시간이다. 일반적인 스마트카드 개발환경과 마찬가지로 호스트 PC와 리더는 시리얼 포트로 연결되어 있으며, 무선인증모듈 내부에서 T=0 전송계층 프로토콜을 거쳐 EEPROM에 쓰기 동작을 수행하는 과정도 있기 때문에 실질적인 RSA 연산 시간은 표 1에 보인 것보다 작을 것으로 판단된다.

V. 결론

WAP 환경뿐만 아니라 유무선 통합 환경의 인터넷 공간에서도 무선인증모듈의 사용은 필수적인 보안 요소가 될 것이다. 본 논문에서 구현한 무선인증모듈은 RSA 공개키 연산을 이용한 정보보호 서비스 제공을 기본으로 하고 있다. 그 구현 기술에 있어서 전송계층과 스마트카드 명령어처리 계층을 구분하는 계층화구조로 설계하여 T=0 프로토콜이 아닌 새로운 전송 프로토콜로의 확장이 용이하다. 특히 무선인증모듈 내부의 파일시스템은 PKCS #15 규격을 준용하고 있으며, 정보형식에 대한 DER 인코딩 데이터를 저장하기 때문에 현재의 무선인증모듈을 PKCS #15 응용을 비롯한 다양한 스마트카드 응용서비스를 지닌 멀티 애플리케이션 카드로 확장하여 정보보호 서비스와 사용자의 이동성을 충실히 보장할 수 있다.

참고문헌

[1] WAP, "Wireless Application Protocol Identity Module Specification, Part: Security, Version 02-Jan-2001," WAP Forum, Jan. 2001.

[2] WAP, "Wireless Application Protocol Wireless Transport Layer Security Specification, Draft Version 02-Jan-2001," WAP Forum, Jan. 2001.

[3] 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.

[4] 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.

[5] ISO/IEC 7816-8, "Identification cards - Integrated Circuit(s) cards with contacts - Part 8: Security related interindustry commands, International Organization for Standardization," Oct. 1999.

[6] RSA Laboratories, "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard," Jun. 2000.

[7] 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.

[8] ISO/IEC 8824-1, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation," Dec. 1998.

[9] RSA Laboratories, "PKCS #1 v2.0: RSA Cryptography Standard," Oct. 1998.