자바카드 기반 USIM의 보안 요구사항에 관한 연구†

정윤선°* 정영준*, 신명섭*, 임선희*, 이옥연**, 임종인*
고려대학교 정보경영공학전문대학원*
국민대학교 자연과학대학 수학과**

jys2002°*@korea.ac.kr, yz0415*@korea.ac.kr,

capsunny*@korea.ac.kr, oyyi**@kookmin.ac.kr, jilim*@korea.ac.kr

The Study on the Security Requirements of USIM based on Java Card

YunSeon Jung°*, YoungJun Jung*, MyoungSub Shin*, SunHee Lim*, Okyeon Yi**, JongIn Lim*
Graduate School of Information Management and Security, Korea University*
Department of Mathematics, Kookmin University**

요 약

3세대 이동통신 방식인 WCDMA가 상용화됨에 따라 국내에서도 GSM 방식의 SIM 카드의 역할을 하는 USIM(Universal Subscriber Identity Module) 카드가 본격적으로 도입되었다. USIM 카드는 WCDMA 단말기에 필수적으로 장착되며, 기존의 SIM 카드의 기본적인 기능 이외에도 다양한 기능이 추가될 수 있다. 본 논문에서는 자바카드의 구조 및 보안적 특징, USIM의 보안 요구사항 및 자바카드를 위한 USIM 아키텍쳐에 대해 설명한 후에 USIM의 다양한 활용을 위한 보안 고려사항에 대하여 논의한다.

1. 서 론

지금까지의 모바일 단말기는 주로 전화, 문자 메시지, 무선 인터넷 등의 통신 수단으로써 사용되어 왔다. 그러나 단말기의 성능 향상이 점차 급속화되고 1인-1단말기가 보편화됨에 따라, 모바일 단말기는 단순한 통신 기기의 의미에서 벗어나 한 개인의 일부분으로 흡수되었으며 더욱 다양한 기능의 구현과 안전한 개인정보 저장매체로서의 역할이 요구되고 있다.

WCDMA 방식의 단말기에는 USIM이라고 하는 스마트 카드가 필수적으로 장착된다. USIM은 기본적으로 사용자가 정당한 사용자인지를 인증하는 기능을 제공한다. 또한 USIM은 휴대폰, PDA, 노트북 등 단말기 종류에 상관없이 슬롯에 꽂기만 하면 이동통신 네트워크에 접속할 수 있다. 예를 들어, 사용자가 해외에서 휴대폰을 사용하고자 할 경우, SIM 카드을 체류국의 휴대폰에 장착시키면 SIM 카드는 저장되어 있는 데이터를 사용하여 사용자를 인증하고 지속적으로 서비스를 사용할 수 있도록 로밍 서비스를 제공한다.[2]

이와 같은 특징은 GSM 방식의 SIM 카드가 수행하던 기능으로써, SIM 카드는 메모리 및 데이터 처리 능력이 제한적이였으며 인증을 비롯한 단순한 몇가지 기능만을 제공하였다. 그러나 근래에 카드 한 장에 다양한 응용 프로그램을 탑재할 수 있는 개방형 플랫폼이 개발되고 스마트 카드의 메모리 및 데이터 처리 능력이 한층 향상됨으로써 USIM에 다양한 응용 프로그램을 탑재하고 많은 개인정보를 저장, 관리할 수 있게 되었다. 그리고 개방형 플랫폼은 카드가 발행된 후에도 카드에 새로운 응용 프로그램 기능을 추가할 수 있으며, 이 응용 프로그램은 카드 칩과 독립적이기 때문에 새로운 칩 기술을 적용시키는데 매우 용이하다. 따라서 개방형 플랫폼으로 구현된 USIM은 성능 및 기능, 안전성이 보다 강화되었다고 할 수 있다.

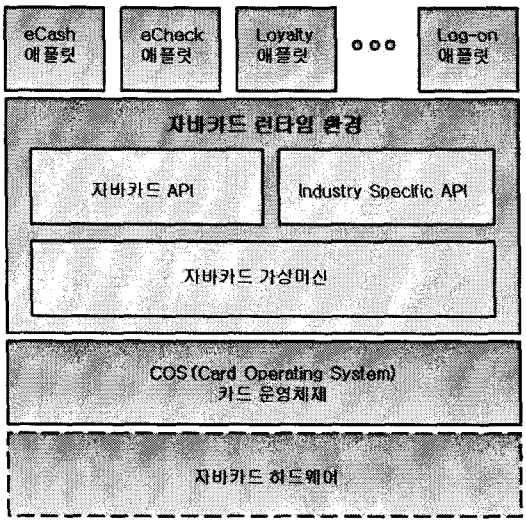
본 논문에서는 개방형 플랫폼을 제공하는 자바카드를 기반으로 하는 USIM 카드의 보안 요구사항에 대하여 논의한다.

본 논문의 구성은 다음과 같다. 2장에서는 자바카드의 구조 및 특징에 대해서 살펴보고, 3장에서는 USIM과 UICC의 보안 요구사항, 4장에서는 자바카드를 위한 USIM 아키텍쳐를 설명한다. 그리고 마지막으로 5장에서 USIM 카드에 다양한 기능을 구현하고 개인정보를 안전하게 관리하기 위한 보안 고려사항 및 향후 연구 방향을 논의한다.

2. 자바카드

자바카드는 기존 자바 기술의 특징을 기반으로 카드 상에서도 자바 언어로 쓰여진 프로그램을 실행할 수 있도록 해주는 스마트 카드이다.[1] 스마트 카드는 일반 컴퓨팅 디바이스보다 메모리가 제한적이기 때문에 자바카드는 스마트 카드에 알맞게 자바 언어의 서브셋으로써 최적화되어 있다. 따라서 자바카드는 자바 언어의 특징

† "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(IITA-2007-(C1090-0701-0025))



[그림 1] 자바카드 구조

인 객체지향 프로그래밍을 가능하게 해주고, 개방형 플랫폼에 기반함으로써 플랫폼 비종속성, 다중 응용 프로그래밍 탑재, 추가적인 응용 프로그램 설치 등이 가능하게 해준다. 또한 자바 언어 자체의 보안 특성 이외에 응용 프로그램 간의 방화벽(Firewall)을 제공함으로써 엄격한 보안성을 보장한다.

[그림 1]은 자바카드의 구조를 나타낸다. 그림과 같이 자바카드는 카드 운영체제, 자바카드 가상머신, 자바카드 API, Industry Specific API, 애플릿으로 구성된다.

- COS 영역

  COS 영역에는 메모리 액세스 및 I/O 핸들링을 위한 디바이스 드라이버와 암호 모듈 액세스 드라이버 코드가 적재된다.

- 가상머신 영역

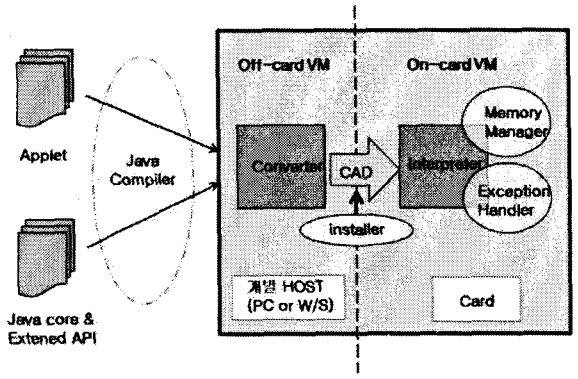
  가상머신 영역에는 자바 바이트코드 서브셋(Bytecode Subset) 지원을 위한 자바 인터프리터(Interpreter) 코드와 서명과 로그인 같은 외부 접근 통제 코드가 적재된다.

  자바카드에 탑재되는 가상머신은 SUN Microsystems사와 자바카드 포럼에 의해 제안된 가상머신으로 기존의 자바 가상머신(Java Virtual Machine) 기능 중에 일부 데이터 타입 지원과 쓰레딩(Threading) 지원과 쓰레기 수집(Garbage Collection) 지원 기능 등을 제외시킨 자바카드 가상머신(Java Card Virtual Machine)이다.

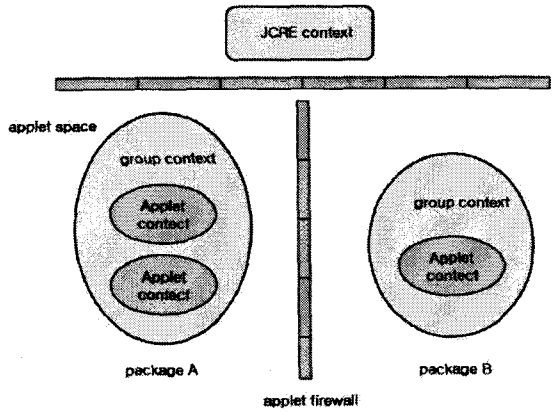
- 자바카드 API 영역

  자바카드 API 영역에는 자바카드 구현을 위한 기본 API코드가 적재된다.

- Industry Specific API 영역



[그림 2] 자바카드 가상머신



[그림 3] 자바카드 애플릿 방화벽

Industry specific API 영역에는 사용자에 의해 정의되는 암호 API 코드가 적재된다.

- 애플릿 영역

  애플릿 영역에는 전자화폐, 로열티, 그리고 신분증명 등과 같은 응용 프로그램이 적재된다.

[그림 2]는 자바카드 가상머신을 나타낸다. 자바카드 가상머신(JCVM)은 자바 가상머신(JVM)과 달리 오프-카드에서 동작하는 부분과 온-카드에서 동작하는 부분으로 분리되어 있다. 즉, 자바카드 가상머신은 분리 가상머신(Slit VM)이다. 온-카드 가상머신에는 바이트 코드 수행을 위한 인터프리터가 구현되어 있고 오프-카드 가상머신에는 클래스 로딩과 검증 그리고 바이트 코드 최적화 및 변환을 위한 컨버터가 구현되어 있다. 자바카드 가상머신을 위와 같이 분리 가상머신으로 구현하는 목적은 카드의 제한된 하드웨어 리소스를 효율적으로 활용하기 위함이다.

자바카드 애플릿이란 자바카드 플랫폼에 맞게 설계된 자바카드용 응용 프로그램을 말한다. 자바카드에는 여러 개의 애플릿이 동시에 존재할 수 있으며, 추가적으로 애플릿들이 다운로드 및 설치되어질 수 있다. 자바카드 플

랫폼은 멀티-어플리케이션 환경을 지원하기 때문에 애플릿 간에 중요한 데이터를 서로 공유하는 경우가 발생할 수 있다. 따라서 응용 간에 서로 협업할 수 있도록 지원하기 위해 자바카드에서는 객체 분리(Object Isolation) 메커니즘을 사용한다. 이러한 객체 분리는 애플릿 방화벽(Applet firewall)을 통해서 이루어진다. 이것은 하나의 애플릿을 정해진 공간에 고립시킴으로써 다른 애플릿에 의해 중요한 데이터가 빠져 나가는 것을 방지하며 해킹에 대한 보호를 제공한다. 애플릿 방화벽은 자바카드 객체 시스템을 컨텍스트(context)라고 불리는 객체 공간으로 나눈다. 컨텍스트는 애플릿을 보호하기 위한 분리된 공간을 의미한다. 이 때 방화벽은 서로 다른 컨텍스트 사이의 경계가 된다. 자바카드 방화벽은 보안을 제공할 수도 있다. 개발자의 실수나 잘못된 설계로 인해 애플릿에 민감한 데이터가 노출된 경우, 만약 객체가 방화벽에 의해 보호되는 애플릿의 소유라면 객체 참조를 요청하는 애플릿은 타겟 객체에 접근하기 위해 접근 규칙을 만족해야만 한다. 방화벽은 잘못된 코드에 대해서도 보안을 제공한다. 만약 잘못된 코드가 카드에 다운로드되면, 방화벽은 이 코드가 접근하는 객체를 보호한다. [그림 3]은 자바카드 애플릿을 나타낸다.[3,4]

3. 자바카드 보안 메커니즘

자바카드에서의 보안 문제는 애플릿 개발, 설치, 실행 등 각 단계마다 하나의 체인으로 결부되어 있다. 따라서 모든 부분이 단단하고 긴밀하게 연결되어 있어야 보안이 이루어진다.[3,4]

- 컴파일 시간 확인
  클래스 파일은 기존의 자바 컴파일러가 생성한다. 컴파일러는 클래스 파일을 생성하면서 보안과 관련된 부분을 검사한다.

- 클래스 파일 검증과 서브셋 확인
  자바카드 가상머신은 온-카드와 오프-카드 두 부분으로 나누어져 있다. 따라서 보안관 관련된 부분도 서로 분리되어 수행된다.

- CAP 파일과 export 파일 검증
  파일이 올바른 형식으로 생성되었는지 확인한다.

- 설치 확인
  설치와 관련된 보안은 인스톨러와 자바카드 런타임 환경에 의해 수행되는 표준 보안과 카드 제조사에서 정의하는 보안 정책의 두 레벨로 나누어 진다.

- 런타임 보안 강화
  애플릿 방화벽에 의한 애플릿 분리와 자바 언어의 타입 검사를 의미한다.

- 자바카드의 암호학적인 지원
카드 제조사의 허용 범위 내에서 각 애플릿은 자신만의 암호학적 정책을 가질 수 있다.

4. USIM과 UICC 보안 요구사항

본 장에서는 USIM과 UICC에 대한 보안 요구사항을 설명한다. UICC(Universal Integrated Circuit Card)는 모바일 단말기와 같은 터미널 장치로부터 장·탈착이 가능하고 물리적으로 안전한 스마트 카드를 일컫는다. UICC는 하나 또는 그 이상의 응용 프로그램을 탑재할 수 있으며, 그 중의 하나가 USIM 어플리케이션이다.

USIM은 SIM 카드를 3세대 이동통신 환경에 맞도록 단순히 적용시킨 것이 아니라 UICC와 더불어 통신, 금융, 멀티미디어 등의 다른 산업 분야에도 응용할 수 있도록 확장 개발한 것이다. SIM 카드에서는 파일들의 메모리 주소가 고정되어 있는 반면에, USIM은 디렉토리 정보를 가지고 있는 별도의 파일을 두고 파일을 관리함으로써 새로운 응용 프로그램들의 수용을 용이하게 한다. 또한 UICC는 응용 프로그램들이 종류에 관계없이 이용할 수 있는 카드 응용 툴킷을 제공한다. [그림 4]는 USIM 자바카드 아키텍쳐를 나타낸다.[5]

3.1 일반적인 요구사항

UICC는 USIM 응용을 포함하고 지원하는 물리적이고 논리적인 개체로써 단말기에서 제거 가능한 모듈이다. 3세대 이동통신 서비스에 접근하기 위해서는 유효한 UISM을 포함하는 UICC가 반드시 필요하다.

USIM은 가입자를 식별할 수 있는 신원을 포함해야 하며, 가입 정보 및 가입자와 관련된 데이터를 위한 저장 장소를 제공한다.

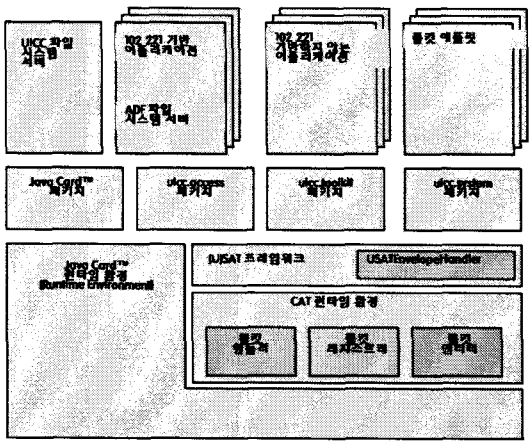
3.2 보안 요구사항

USIM은 보안 특징을 제공하기 위해 사용될 수 있다. 만약 UICC가 3세대 모바일 단말기에서 제거되면, 서비스는 즉시 종료되어야 한다. UISM은 분명하게 식별되어야 하며, 인증 키와 같이 USIM 내부에서 사용되는 데이터에는 접근할 수 없어야 한다. 그리고 도난당한 UICC가 부정 사용되는 것을 예방할 수 있어야 한다.

- 파일 접근 조건
  UICC 상의 READ, UPDATE와 같은 동작들은 접근 조건에 의해 제어되어야 한다. UICC가 3세대 응용과 비-3세대 응용 등 다중 응용을 포함할 수 있기 때문에 유연성 있는 파일 접근 방법이 제공되어야 한다.

- 사용자 인증
  USIM은 카드 도난 및 분실 등에 대비하여 사용자 인증 메커니즘을 지원해야 한다. USIM 인증은 십진수 4-8자리로 구성된 PIN 넘버를 검증함으로써 이루어진다.

  사용자가 정당한 PIN을 입력하였다면 모바일 단말기는 USIM 데이터를 사용하여 기능 및 동작을 수행할 수 있고 관련 접근 조건에 따라 보호된다.



[그림 4] USIM 자바카드 구조

만약 잘못된 PIN이 입력되면 사용자에게 지시사항을 알린다. PIN이 연속적으로 3번 잘못 입력되면 관련 PIN은 차단된다. 이렇게 PIN이 한번 차단되면 PIN 검증은 거부된다. 즉, UICC를 제거하거나 USIM 선택을 해제하거나 모바일 단말기의 전원을 끄더라도, 접근 조건에 의해 보호된 데이터에 대한 기능 및 동작은 불가능해진다.

한편 UISM은 연속적인 PIN 입력 오류로 인해 차단된 PIN을 해제시킬 수 있는 메커니즘을 지원한다. PIN 차단 해제는 PUK(PIN Unblock Key)를 사용하여 수행된다. PUK는 십진수 8자리로 구성되어 있으며, PUK가 아닌 PIN은 사용자가 변경할 수 있지만 PUK는 사용자가 변경할 수 없다. 만약 잘못된 PUK가 입력되면 사용자에게 지시사항을 알린다. UICC를 제거하거나 USIM 선택을 해제하거나 모바일 단말기의 전원을 끄더라도, PUK가 10회 연속 잘못 입력되었다면 UICC는 차단된다.

- 모바일 단말기에 저장된 사용자 데이터

네트워크 동작 중에 모바일 단말기로 전송된 사용자 관련 모든 데이터들은 UICC의 제거, USIM 선택의 해제, 모바일 단말기의 비활성화, UICC의 전자적 리셋 후에 모바일 단말기로부터 삭제된다. PIN과 같은 사용자와 관련된 보안 코드는 이 코드를 포함하는 프로시저 동안에만 모바일 단말기에 저장되었다가 삭제된다. 모바일 단말기에는 SMS처럼 보안적으로 덜 민감한 데이터를 저장할 수 있다.

- 인증

인증이란 사전에 공유된 비밀 키 K를 제시하는 USIM과 네트워크 간의 상호인증을 의미한다. 이것은 오직 USIM과 사용자의 HE 내에서만 유효하다. 인증 방법은 도전/응답(Challenge/Response) 방식과 키 수립(Key Establishment) 프로토콜로 구성되어 있다. 또한 3G에서는 AKA(Authentication and Key Agreement) 프로토콜을 정의하고 있다.

- 시그널 성분의 데이터 무결성

시그널 정보는 민감하게 고려되어야 하며 무결성이 보장되어야 한다. 무결성 기능은 모바일 단말기와 네트워크 사이에 전달되는 특정한 시그널 정보에 적용된다.

- 사용자 식별 기밀성

임시 신원을 사용함으로써 사용자 신원 기밀성이 제공되어야 한다.

- 보안 매개변수들의 길이

3G에서 사용되는 모든 보안 관련 파라미터들은 길이 지시자(Length Indicator)를 가져야 한다. 또한 USIM은 다양한 길이의 보안 파라미터를 지원해야 한다.

5. 자바카드를 위한 USIM 아키텍쳐

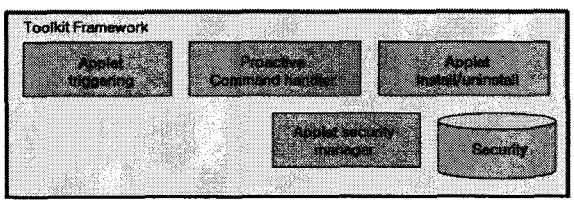
본 장에서는 자바카드를 위한 USIM API의 아키텍쳐에 대해 설명한다.

자바카드 런타임 환경(JCRE)은 카드 리소스 관리, 네트워크 통신, 애플릿 실행, 온-카드 시스템 및 애플릿 보안에 대한 책임을 가진다. 자바카드 가상머신이 자바 언어 레벨의 보안을 책임지는 반면에, 자바카드 런타임 환경은 자바카드 런타임 환경이 구현되어 있는 디바이스에서의 추가적인 실행 보안 요구사항을 제공한다. 자바카드 런타임 환경은 툴킷 레지스트리(Toolkit Registry), 툴킷 핸들러(Toolkit Handler), 파일 시스템으로 구성되어 있으며 특정 애플릿을 선택하고 APDU의 프로세스를 전달한다. 툴킷 레지스트리는 모든 툴킷 애플릿의 등록 정보와 JCRE로의 연결을 핸들링한다. 툴킷 핸들러는 시스템 핸들러와 툴킷 프로토콜의 availability를 핸들링한다.

USAT(USIM Application Toolkit)는 USIM 카드에 응용 프로그램을 운용할 수 있도록 해주는 도구이다. USAT는 UICC에서 응용이 모바일 단말기와 함께 운용되고 상호 동작할 수 있도록 메커니즘을 제공한다. [그림 5]는 USAT 프레임워크이다. USAT는 아래와 같이 각 모듈로 구성된다.[6,7]

- Applet Triggering

Applet Triggering 부분은 USIM의 어플리케이션 실행시 요구되는 Toolkit 애플릿을 실행시킨다. 자바카드 애플릿과 툴킷 애플릿의 차이점은 툴킷 애플릿은 직



[그림 5] USAT 프레임워크

접적으로 APDU를 핸들링하지 않는다는 것이다.

- Command Handler
  Proactive Command Handler는 USIM에서 기본적으로 제공하는 Proactive Command를 관리한다.

- Toolkit Registry
  Toolkit Registry 는 툴킷 애플릿들을 등록하고 관리한다.

- Applet Security
  Applet Security는 USAT 애플릿에서 사용하는 보안 메커니즘과 응용프로그램의 사용에 대한 안전성을 담당한다.

USIM은 UICC 상의 특별한 응용 프로그램이다. USIM 애플릿은 는 ETSI TS 102 241[8]에 정의되어 있다. USIM 애플릿 레벨에는 ETST TS 102 241을 기반으로 하지 않는 애플릿과 툴킷 애플릿 등도 탑재될 수 있다. 이 위치에 교통, 금융, 멀티미디어 등의 다른 산업 분야의 다양한 애플릿이 설치될 수 있으며, 툴킷 애플릿은 툴킷 서비스, 원격 관리 응용, 브라우저 응용 등이 될 수 있다.

6. USIM을 활용한 자바카드 응용

UICC는 자바카드를 기반으로 하기 때문에 USIM 애플릿 이외에도 다양한 애플릿들이 탑재될 수 있다. 또한 다른 응용 프로그램에서 USIM에 저장되어 있는 데이터를 사용하여 부가서비스를 제공할 수 있다. 부가 서비스는 금융, 교통, 멀티미디어 등 다양한 분야에 걸쳐 제공 가능하다. 또한 각 애플릿은 인증 및 사용자 정보를 공유하여 서로 협업이 가능하다.

6.1 금융

금융 관리 응용 프로그램에는 사용자의 신용카드, 계좌 번호와 같은 결제 정보 및 금융 인증서 등이 저장될 수 있다. 이를 사용하여 사용자는 실시간으로 은행, 증권, 보험 등의 다양한 금융 거래를 종합적으로 관리 및 이용 가능하다.

6.2 교통

교통 카드 및 고속도로 통행료, 주차장 사용요금 등과 같이 교통과 관련된 서비스를 제공하는 응용 프로그램을 탑재할 수 있다.

6.3 멀티미디어

무선 인터넷을 통해 멀티미디어 서비스를 이용하고자 할 때, 정당한 댓가를 지불한 사용자에 대한 인증이나 성인 인증이 필요할 때 USIM의 인증 정보를 사용할 수 있다.

6.4 컨버전스

3G를 비롯한 와이브로, 무선랜 등의 이동통식 방식과 휴대폰, PDA 등 모바일 단말기의 종류에 상관없이, USIM을 슬롯에 장착하기만 하면 USIM 내에 저장되어 있는 데이터를 사용하여 사용자를 인증을 받은 후에 서비스 사용이 가능하다.

이러한 서비스를 제공하기 위해서는 USIM의 정보를 각 이동통식 방식에 적합하게 관리, 제공해주는 응용 프로그램이 필요하다.

6.5 디지털 아이디

서비스가 고도화됨에 따라 사용자의 프라이버시를 보장하면서 개인정보를 공유할 수 있는 기술의 필요성이 증대하고 있다. 서비스 제공자의 입장에서도 운영하는 시스템이 증가하고 비즈니스 대상이 다양해짐에 따라 편리하고 안전한 사용자 아이디 관리 기술에 대한 관심이 높아지고 있다. 이러한 배경을 이유로 디지털 아이디 서비스가 등장하였으며 이것을 UICC 카드에 적용시킬 수 있다.

디지털 아이디란 안전하고 편리한 무선 전자상거래를 위하여 UICC의 디지털 아이디 응용 프로그램을 통해 사용자 신원 정보를 저장, 관리할 수 있는 서비스를 의미한다. 디지털 아이디 서비스는 사용자에 대한 단일 인증, 개인정보 보호 서비스 등을 제공하며 사용자의 개인정보, WPKI 인증서 및 기타 사용자 관련 정보가 저장되어 관리된다. 디지털 아이디 서비스는 USIM 애플릿과 협업하여 USIM에 저장되어 있는 인증 정보와 디지털 아이디 응용 프로그램에 저장되어 있는 사용자의 개인정보를 함께 사용할 수 있다.

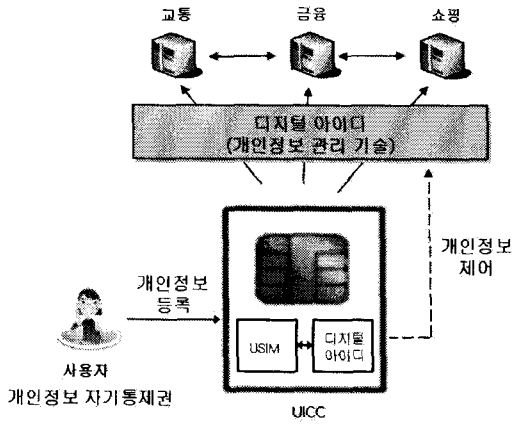
디지털 아이디를 통한 개인정보 관리 기술은 개인정보의 불법적인 접근 및 유통으로 인한 피해, 개인정보 수집과 유통에 대한 개인정보 자기 통제권 부재, 개인정보의 안전하고 편리한 유통 프레임워크의 부재를 방지한다. 따라서 디지털 아이디 서비스는 개인정보를 안전하게 유통할 수 있는 프레임워크와 개인정보 공유 제어 기술을 제공한다.[그림 6]

사용자의 개인정보를 서비스 제공자가 관리하지 않고 사용자의 UICC 카드에서 직접 관리하기 때문에 더욱 안전할 뿐만 아니라, 사용자가 자신의 개인정보를 직접 제어할 수 있다는 장점이 있다. 사용자에게는 보다 간편하고 편리한 환경이 제공되며 기존의 모든 사용자의 개인정보를 관리하던 서비스 제공자나 관리자의 업무도 감소한다. 그리고 사용자의 개인정보에 대한 보안 정책 적용이 용이해진다.

다음은 디지털 아이디가 제공하는 대표적인 서비스 유형이다.

- 아이디 관리 서비스
  사용자가 하나의 아이디를 사용하여 자신의 모든 개인정보를 등록, 수정, 관리하는 서비스를 제공한다.

- 단일 인증 서비스
  USIM의 인증 정보 및 디지털 아이디의 사용자 신



[그림 6] 디지털 아이디 서비스

원 정보를 사용하여 단 한번의 사용자 인증 후, 추가적인 인증없이 여러 서비스를 자유롭게 이용할 수 있도록 한다.

- 개인정보 보호 서비스
  가맹 서비스 간에 개인정보를 공유하고자 할 때, 사용자의 명시적인 동의를 얻도록하여 개인정보의 오남용을 방지하는 서비스를 제공한다.

- 아이디 정보 제공 서비스
  가맹 서비스가 최신의 개인정보를 유지할 수 있도록 사용자의 개인정보를 제공하고 갱신하는 서비스를 제공한다.

- 익명성 제공 서비스
  사용자가 원할 경우, 서비스 이용 초기에 정당한 사용자인지에 대해서만 인증을 받은 후에 익명으로 서비스를 제공받을 수 있도록 한다.

7. 결론

본 논문에서는 자바카드의 구조 및 보안적 특징, USIM의 보안 요구사항 및 자바카드를 위한 USIM 아키텍쳐에 대해 논의하였다.

현재 국내의 각 통신사는 자사에서 발행한 USIM 카드는 자사 가입자의 등록 휴대폰에 장착되었을 때만 동작하도록 규제하고 있다. 따라서 USIM은 모바일 단말기와 통신사에 종속적이기 때문에 제 기능을 다 발휘하지 못하고 있다.

USIM은 안전한 멀티서비스의 수단으로 사용될 수 있으며, 보다 다양하고 안전하게 이용되기 위해 USIM 응용의 유통성 확보 및 유연한 카드 운용관리가 필요하다. 최초 USIM 발급 후에 USIM 응용이 네트워크 경유로 카드 상에 안전하게 설치되기 위해서는 USIM 카드, 모바일 단말기, 서버를 포함하여 부정한 응용의 유입 방지, 응용의 개조 방지 등 보안성을 고려하여야 한다. 또한 사용자와 관리자 모두에게 편의를 제공하기 위하여 운용관리 메커니즘 구축이 필요하다. 예를 들면 네트워크 경유로 USIM 카드 장애진단이 가능하도록 해야한다.

USIM 애플릿을 비롯한 다수의 애플릿이 하나의 UICC 내에서 보안상의 충돌없이 공존할 수 있도록 해야하며, 애플릿 간의 상이한 보안 요구사항을 각각 지원해야 한다. USIM 발급 후 응용 프로그램의 로딩, 설치, 삭제에 필요한 보안 절차와 관리 기능을 제공해야 한다. 또한 로드된 파일의 무결성을 인증해야한다. 마지막으로, 응용 프로그램의 요청에 의해 암호화, 복호화, 디지털 서명 등의 보안 서비스도 제공되어야 한다.

USIM이 다양한 서비스에 응용되고 UICC에 사용자와 관련된 많은 정보들이 저장, 관리됨으로써 사용자는 보다 편리하게 다양한 서비스를 제공받을 수 있다. 그러나 사용자의 개인정보가 UICC 카드에 집중적으로 담기기 때문에 보안적인 측면에서 위험에 노출될 가능성이 많다. 그러므로 향후에는 응용 서비스 개발과 함께 USIM의 보안성 향상을 위한 연구가 함께 이루어져야할 것이다.

참고문헌

[1] 전동호, 자바 카드에서 애플릿간 안전한 객체 공유 방안, 한국정보과학회 가을 학술발표논문집 Vol. 28. No. 2, p688-690, 2001

[2] 정윤선, WPKI 기반의 3G 모바일을 위한 안전한 개인정보 제공 시스템, 한국정보보호학회 하계 학술대회, CISC '07, Vol.17, No.1, p497-501, 2007

[3] Java Card™ Platform, Version 2.2.2, Virtual Machine Specification, Sun microsystems

[4] Java Card™ Platform, Version 2.2.2, Runtime Environment Specification, Sun microsystems

[5] 3GPP TS 21.111, USIM and IC card requirements (Release 7)

[6] 3GPP TS 31.130, (U)SIM Application Programming Interface; (U)SIM API for Java ™ Card (Release 7)

[7] 3GPP TS 31.111, Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 7)

[8] ETSI TS 102 241, UICC API for Java Card™ (Release 7)