6

모바일 ID 보안 및 프라이버시를 위한 스마트지갑

한국전자통신연구원 ▌최대선 · 진승헌

1. 서 론

"휴대폰이 당신의 미래 지갑이며 5년 이내에 필수 소지품인 지갑, 휴대폰, 열쇠를 모바일 지갑 하나로 통합하게 될 것"이라는 보도가 나오고 있다[1]. 세계 각국의 이동통신사나 신용카드회사는 신용카드를 휴대폰에 발급, 저장하고 NFC[2] 통신을 이용하여 지불할 수 있는 모바일 신용카드 서비스를 시작하고 있다[3]. 애플의 아이폰에 자동차 시동키를 저장하고 이를 이용해 자동차 문의 개폐와 시동을 수행하는 시연이 보도되었다[4]. 이렇게 휴대폰에 지불 기능과 인증 기능을 포함하는 추세는 앞으로 더욱 가속화될 것으로 예상된다.

휴대폰이 지갑으로 이용되게 되면 여러 가지 문제가 발생할 것이다. 우선 휴대전화 분실이나 도난이 더욱 큰 문제가 될 것이다. 또한, 서비스 제공자에 따라 각기 다른 지불이나 인증매체가 사용되게 되는데 매체의 발급 및 관리가 서비스에 따라 다른 방식으로 이루어진다면 사용자는 매우 불편할 것이며, 관련 모듈이 각기 따로 휴대폰에 설치되어야 하므로 오버헤드가 발생하게 된다. 한편, 지불이나 인증매체 사용 시에도 일관된 사용자 인터페이스의 부재는 큰 불편을 초래한다. 현재의 지갑은 지폐, 카드 신분증을 각각 종류별로 구분해서 보관하고, 사용시 원하는 대로 꺼내 사용할 수 있다. 이러한 직관적이고 편리한 사용체계가 없다면 여러 가지 매체가 탑재되어 보편적으로 이용되기 어려울 것이다.

한편, 스마트폰을 비롯해 휴대폰은 컴퓨팅 능력을 갖고 있으므로 기존 지갑과는 다른 지능형 서비스를 제공할 수 있다. 다양한 지불 수단 중 할인 등을 고려한 최적의 조합을 추천해 줄 수 있으며, 구입할 상품의 태그를 휴대폰으로 스캔한 뒤 계산된 금액을 일괄 지불하는 것도 가능하다. 또한 개선된 ID 기능을 수행할 수 있다. 휴대폰이나 보험 가입 신청서 등에 기입한 개인정보와 주민등록번호를 도용해서 이용자 몰래 추가 가입을 하는 등의 문제가 발생하고 있는데, 휴대폰에서 1회용 주민등록번호를 생성하여 제공한다면 이러한 재사용 문제를 막을 수 있다.

휴대폰은 개인의 컨텍스트를 반영하므로 휴대폰을 이용한 개인화서비스가 부각되고 있다. 가장 대표적인 것이 위치기반 서비스로, 사용자의 위치에 가까운 상점이나 친구의 위치를 알려주는 서비스를 통해 커다란 부가가치를 창출할 것으로 예상된다[5]. 휴대폰을 통해 인증과 지불을 수행하게 되면, 위치 이외에도 다양한 사용자의 동태정보가 생성된다. 어디에 출입하고, 어떤 서비스를 이용하며, 어떤 물품을 구입하는지 등과 같은 동태정보가 휴대폰에서 생성 및 집계될 수 있다. 이러한 동태적 개인정보는 고부가 개인화서비스를 위한 기반이 될 수 있는 동시에 민감한 프라이버시 문제를 발생시킨다.

한국전자통신연구원에서는 휴대폰 지갑 시대에 대응하여 발생 가능한 문제점을 방지하고 지능형 기능과 고부가 서비스를 가능하게 할 수 있는 스마트지갑 기술을 개발할 예정이다. 스마트지갑은 여러 가지 인증, 지불 매체를 일관된 체계로 관리하고 안전하게 이용할 수 있도록 해주는 매니저 기능과 휴대폰의 컴퓨팅 능력을 이용한 여러 가지 편리하고 고도화된 지능형 기능을 제공하며, 휴대폰에서 발생한 동태적 개인정보를 효과적으로 사용해 고부가 개인화 서비스를 구성할 수 있도록 해주며, 이 과정에서 개인의 프라이버시를 보호할 수 있는 기능도 제공한다.

본 고에서는 스마트지갑을 소개한다. 2장에서 스마트지갑의 개념과 필요성을 설명하고, 3장에서 스마트지갑을 구성하는 핵심기술을 설명한다. 4장에서는 스마트지갑을 통해 제공할 수 있는 서비스 시나리오를 소개한다. 5장에서는 스마트지갑에 관련된 기술 및 시장 동향을 소개하고 6장에서 결론을 맺는다.

† 본 연구는 지식경제부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행하였음[2007-S-601-03, 자기통제 강화형 전자ID지갑 시스템 개발].

2. 스마트지갑 개념

2.1 개념

스마트지갑은 휴대폰 등 모바일 단말용 클라이언트 S/W와 이를 위한 지원 서버군으로 구성되는 시스템이다. 휴대폰 등 모바일 단말기에 저장, 이용되는 개인정보를 모바일 ID라고 한다[12]. 모바일 ID의 구성은 표 1과 같다.

표 1 스마트지갑에 저장되는 모바일 ID의 구성

종류	내용
온 · 오프라인 ID	주민등록번호, 신분증
온 · 오프라인 인증 수단	출입증, id, pw, 인증서, 스마트키 등
정태적 개인정보	구매기록, 이동기록, 출입 기록
퍼스널 컨텍스트	사용자의 위치, 시간, 주변 환경
관심정보	선호도, 관심 분야

스마트지갑의 서비스 개념은 다음과 같다.

- 모바일 ID를 통신을 통해 모바일 단말에 발급받아 안전하게 저장, 관리
- 모바일 ID를 온 · 오프라인 환경의 인증, 신원 확인, 지불에 안전하고 편리하게 사용
- 이 과정에서 자체 프로파일링된 동태적 개인정보를 개인화 서비스를 위하여 프라이버시를 보호하며 제공

이러한 서비스 개념은 그림 1에 표현되어 있다.

스마트지갑 클라이언트(별도 표기가 없는 경우 이후 스마트지갑으로 표기)에서 통신 채널을 통해 인증정보, ID, 지불정보와 같은 모바일 크리덴셜을 발급받는다. 이러한 모바일 크리덴셜은 스마트지갑의 부정사용방지 기능에 의해 안전하게 유지된다. 스마트지갑을 이용해 스마트지불, 온, 오프라인 ID 증명, 통합인증을 수행한다. 이때 사용되는 통신 채널은 NFC와 같은 근거리 RF 통신이 주종을 이루는데, 스마트지갑은 이 근거리 RF 통신의 보안을 유지해 준다. 또한 사용 과정의 개인의 활동 기록은 스마트지갑 자체에서 자체 프로파일링되어 축적된다. 축적된 개인정보는 사용자가 원하는 범위 만큼만 개인화서비스에 제공된다. 개인정보를 이용한 개인화 서비스 구축을 용이하게 하기 위해 개인정보 이용 API를 제공한다. 이를 이용하는 개인화 서비스의 예는 이용자기반광고, 라이프스타일미디어, 네트워크 기반 IT서비스 같은 것들이 있다.

2.2 필요성

스마트지갑의 필요성은 기술적, 경제적, 사회적인 면에서 제시될 수 있다.

- 기술적 필요성
  - 온 · 오프라인 지불 및 인증수단과 관계정보, 관심정보, 구매정보 등 다양한 개인정보를 포함한 모바일 ID를 이용한 서비스가 급속히 확대될 전망으로, 이에 따른 모바일 ID 보안 및 프라이버시 문제들이 제기되고 있다.
  - 고도화된 ID 연계 및 ID기반 개인화 서비스 기술 수요가 제기되고 있다. 이용자 동의하에 이용자의 특성에 따른 다양한 정보를 수집하고 분석하여 IT자원, 콘텐츠, 광고 등을 맞춤형으로 패키징하여 제공하기 위한 개인중심 컨버전스 플랫폼 개발이 필요하다는 주장이 제기되고 있다[6].
- 경제적 필요성 : 모바일 인증, 지불, 개인화 서비스 구축을 위한 핵심 요소 기술로서 2013년 세계적으로 336억 달러[1]에 달할 것으로 예상되는 관련 솔루션 시장에 대응할 필요가 있다.

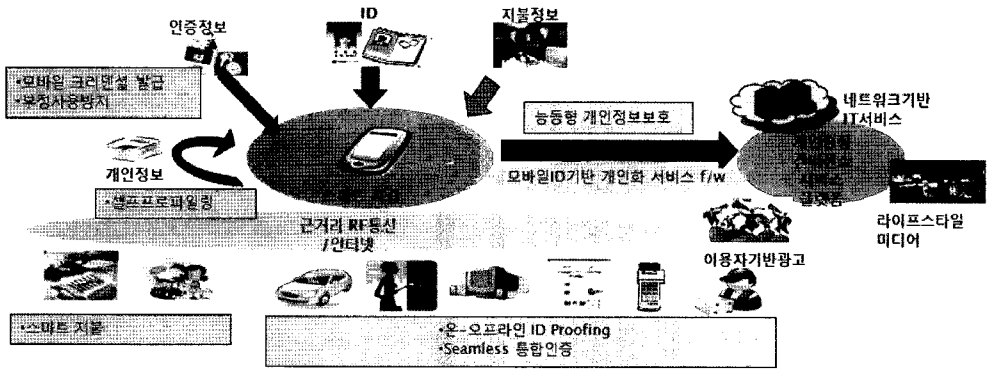

그림 1 스마트지갑 서비스 개념

1) IT인증 [7], 모바일 지불결제 솔루션[8], 모바일 개인화 서비스 [9] 3개 시장 규모합산, CAGR은 10%로 산정

· 국가 사회적 필요성
  - 다양한 발급 주체를 갖는 모바일 ID가 상호 운용성을 갖고 사용되기 위해서는 특정 기업에 독점적 지위를 부여하지 않는 오픈된 플랫폼이 요구된다.
  - 온라인 상의 주민등록번호 대체수단인 아이핀[17] 형태의 개인식별체계를 오프라인으로 확대하는 방안 필요하다.
  - 개인들이 매일 방문하는 인터넷 웹 페이지 등 통신 내용을 서비스 제공자 측에서 추적해 맞춤형 웹 등 개인화 서비스를 제공하는 경우 사생활을 심각하게 침해할 우려가 있다[18]. 개인의 활동을 모니터링하여 획득된 동태적 개인정보를 활용한 다양한 고부가 맞춤형 서비스가 활성화되기 위해서는 이러한 프라이버시 우려를 해소할 수 있는 기술이 필요하다.

3. 핵심기술

3.1 특성

모바일 ID는 기존의 온라인 상에서 이용되던 디지털ID의 확장 개념으로 볼 수 있다. ID 개념 확장은 다음과 같은 측면으로 정리할 수 있다.

· 서비스 공간의 확장
  - 온라인 환경 → 온·오프라인 연계 모바일 환경
· 처리하는 개인정보의 확장
  - 온라인 인증 정보 → 물리적·논리적 인증정보, 오프라인 지불정보
  - 정태적 개인정보 → 동태적 개인정보, 퍼스널 컨텍스트, 선호정보

따라서 모바일 ID 관리에 있어서도, 기존의 ID관리와 다른 기능적, 기술적 요구사항이 존재한다. 이러한 모바일 ID의 특성과 이에 따라 신규로 요구되는 기능 및 기술은 다음과 같다.

· 휴대성: 모바일 단말에 ID를 저장하고 다니며 이용하기 때문에, 단말의 분실이나 도난 가능성이 있다. 따라서 분실, 도난시의 개인 정보 유출이나 도용을 방지해야 한다. 또한, 모바일 단말은 작은 스크린으로 PC와는 다른 UI 체계를 갖고 있다. 따라서 여기에 적합한 ID관리 및 이용 UI가 필요하다.
· 이동성: 모바일 단말이 이동성을 가짐에 따라 생성되는 ID 정보가 다이나믹해진다. 위치정보가 대표적 예다. 새로운 물리적 서비스 환경과 안전하게 상호작용할 수 있도록 사용자 부담을 최소화하며 초기 신뢰를 수립하는 기술이 필요하다.
· 항시성: 언제 어디서나 휴대하고 사용하므로 모바일ID는 사용자의 컨텍스트를 광범위하게 반영한다. 또한 사용자의 건강 상태나 주변환경을 모니터링 할 수도 있다. 따라서 이러한 정보를 수집, 생성, 전달하는 체계가 필요하다. 이 과정에서의 ID의 보안성과 프라이버시를 보장하는 기술이 필요하다.
· 오프라인 상호작용: 오프라인 환경에서 모바일 단말과 상호작용하는 디바이스들은 지불 단말, 출입 통제 단말, 신분증 확인 단말 등이 있을 수 있으며, 헬스모니터링 등 모니터링 용도로 사용될 경우 해당 센서 네트워크 등이 여기에 포함된다. 이러한 오프라인 인프라 디바이스들과는 근거리 RF 통신을 통해 상호작용하게 된다. 이때 모바일 ID를 사용하는 과정에서 보안과 프라이버시를 보장하는 기술이 필요하다.
· 고부가가치: 모바일 ID 중 지불정보, 인증정보는 매우 중요한 가치를 갖는 정보이다. 또한 동태적 개인정보나 퍼스널 컨텍스트는 이를 바탕으로 고부가 맞춤형 서비스를 창출할 수 있는 고부가 정보이다. 따라서 이러한 귀중한 정보를 안전하게 관리할 필요성이 있으며 개인정보에 대한 프라이버시 보호도 매우 필요하다.

3.2 문제점 및 기존 기술

스마트지갑이 해결해야 될 기술적 과제가 표 2에 정리되어 있다.

3.3 스마트지갑의 요소기술

3.2절에 언급된 기술적 과제를 해결하기 위한 스마트지갑의 요소 기술은 모바일 ID 보안기술, 고도화된 모바일 ID 오퍼레이션 기술, 모바일 ID 기반 개인화서비스 기술로 구성되며 표 3에 정리되어 있다. 모바일 ID 보안 기술은 다음과 같다.

· OTA 모바일 크리덴셜 발급 기술 : 무선인터넷을 통해 모바일 크리덴셜을 안전하고 효율적으로 발급하는 기술이다.
· 사용자 친화형 모바일 단말 접근 제어 기술 : pin이나 지문이외에 편리한 단말 사용자 인증 방법으로, 햅틱이나 터치 등을 이용한 기술이 있다.
· 거리기반 모바일 단말 locking 기술 : 휴대단말

표 2 문제점과 기존 기술의 한계 및 신기술요구사항

문제점	기존기술 (ID 2.0)	신기술 요구사항
- 다양한 모바일 ID 발급 및 관리 과정의 보안 위협 - 사용자 불편 및 성능 부족	- 응용 별로 크리덴셜 발급 및 관리, 보안 - OTA 발급 시간이 오래 걸림 (카드1장 25초 이상)	- 관리 편리성, 일관된 보안성 유지를 위한 모바일 ID 통합관리 기술 - OTA 발급 시간 단축 기술
- 휴대폰 분실로 인한 부정사용 및 개인정보 유출 피해 영향 확대	- PIN 기반 접근제어 - 분실시 원격제어나 소거하는 기술의 국내 적용 사례 제한적임	- 사용자 개입없는 거리기반 locking 기술 - 분실시 원격 제어 및 데이터 소거
- 휴대폰에서 근거리 RF 통신을 사용한 지불, 인증, 개인정보 전송 구간 보안 위협(부정사용, 정보노출, MITM 공격 대응)	- 블루투스 Pairing 식의 binding 기술	- 이용자 개입 최소화하며, MITM 공격에 안전한 바인딩 기술
- 지불수단 선택 및 사용 불편 - 광고/쿠폰 연계 및 태깅기반 구매 지불 기술 수요 제기	- 개별 카드 NFC채널 지불	- 멀티 지불 수단 탑재 및 사용 기술 - LBS 연계 쿠폰 수신 및 관리 기술
- 물리, 기기, 서비스 인증의 사용자 및 정책 관리 분산으로 인한 관리 부담 및 보안 위협	- 물리, 기기, 서비스 통합인증 국내 개발 사례 제한적임 - 전자ID지갑의 온라인서비스 인증	- 물리, 기기, 서비스 통합인증 기술 : 통합프로비저닝 및 컨텍스트 (위치, 시간, 동작이력) 기반 접근제어 기술
- 오프라인 주민등록번호 도용 사례 (재사용 등) 빈발	- 온라인에서만 사용되는 I-PIN - 전자ID지갑 기반 I-PIN 서비스	- 오프라인 환경에서 사용되는 재사용 및 도용 불가 ID
- 동태정보 처리 기술 수요 제기 - 개인이 이익을 공유하는 롱테일 서비스 수요 제기	- 웹검색 현황 모니터링 기술	- 전자지갑폰 사용의 동태적개인정보 모니터링 및 선호정보 자동 추출 기술
- 개인정보 제공 조건에 대한 동의가 포괄적이고, 민감정보를 따로 보호할 수 없어 프라이버시 침해가 빈발	- 익명화, 민감정보 암호화 - 전자ID지갑의 사용자 직접 통제	- 개인정보 제공 조건 협상 및 자동 판단 기술 - 전송 개인정보 자동 익명화, k-anonymity 보장
- 개인화 서비스를 제공하기 위한 사용자 검색과정에서의 프라이버시 침해	- 데이터 마이닝에서 통계값 계산시 사용되는 원시값의 노출 방지 목적	- 개인화 서비스 대상을 검색하는 과정에서 프라이버시 침해 방지 목적 (가상개인이미징 기술)
- 개인화 서비스를 위한 개인정보 및 크리덴셜의 상호연동성 부족 및 개발 생산성 저하, 불균일한 보안성, 관리 부담	- 개별적 개인화 서비스	- 상호연동, 생산성제고, 보안 및 프라이버시가 보장되는 프레임웍 기술

이 사용자로부터 멀어지면 자동으로 locking되게 하는 기술이다.

고도화된 모바일 ID 오퍼레이션 기술은 다음과 같다.

- 근거리 RF 채널 시큐어 바인딩 기술 : 근거리 RF 채널에서 사용자 인터페이스의 제약이 있는 스마트지갑과 인프라 디바이스들 간에 빈번히 요구되는 보안채널의 효율적 수립 기술로, 사용자 친화형 초기신뢰 수립, 효율적 인증 및 키 교환 기술을 포함한다.
- 멀티 지불 수단 기반 구매/지불 최적화 기술 : 스마트지갑에 저장된 다양한 지불 및 할인 수단 간의 상호운영성을 확보하기 위한 구매/지불 서비스 플랫폼 및 프로토콜과 보유 지불 수단 중에 최적 할인 수단을 찾는 기술로 구성된다. 또한 인터넷 쇼핑의 경우처럼 가격 비교와 구매 도움을 오프라인 구매 환경에서 제공하는 지능형 구매지불 agent도 포함된다.
- 물리, 기기, 서비스 연계 seamless 인증 기술 : 스마트지갑에 저장된 인증 정보를 이용하여 근거리 RF 통신을 통해 출입통제, 기기 사용자 인증, 서비스 사용자 인증을 수행한다. PC등 기기의 사용자 인증 세션과 서비스 Id 들을 연계하여 심리스 인증을 수행하는 기술이다.
- 목적별 ID 발급 및 관리, 검증 기술 : 온·오프라인 환경에서 주민등록번호를 대체하는 안전한 ID를 제공하기 위해, 스마트지갑을 통해 마스터 ID를 발급받고 필요 시 목적별 ID를 생성해서 사용하는 기술이다. 목적별 ID는 인터넷, 근거리 RF 채널로 전송될 수도 있고, 몇 자리 숫자형태로 생

표 3 스마트지갑 요소기술

구분		요소 기술
모바일 ID 관리 및 보안 기술	라이프싸이클 관리	- OTA 모바일 크리덴셜 발급 기술 - 모바일 ID 통합관리 기술 - 모바일 ID 관리 및 사용 인터페이스
	부정사용방지	- 사용자 친화형 모바일 단말 접근 제어 기술 - 거리기반 모바일 단말 locking 기술
	이용채널 보안	- 근거리 RF 채널 시큐어 바인딩 기술
모바일 ID 오퍼레이션 기술	스마트 지불	- 멀티 지불 수단 기반 구매/지불 최적화 기술 - 태깅 기반 모바일 쇼핑 기술 - 쿠폰 LBS 연계 기술
	seamless 통합 인증	- 물리, 기기, 서비스 연계 seamless 인증 기술 - 통합프로비저닝 기술 - 컨텍스트 (위치, 시간, 동작, 이력) 기반 접근제어 기술
	ID Proofing	- 목적별 ID 발급 및 관리 기술 - 온오프라인 목적별 ID 이용 및 검증 기술
모바일 ID 기반 개인화 서비스 기술	셀프 프로파일링	- 동태적 개인정보 셀프 모니터링 기술 - 관심정보 자동 추출 기술
	능동형 개인 정보 보호	- 사용자 친화형 개인정보 정책관리 - 정책기반 개인정보 협상 기술 - 동태적 개인정보 익명화 및 가상화 기술
	개인 정보 디스커버리	- 프라이버시 보존형 개인정보 디스커버리 및 브로커 기술 - 가상 개인 이미징 기술
	개인화 서비스 F/W	- ID기반 서비스 개발 프레임웍 기술 - ID기반 서비스 오픈 API 기술

성되어 주민등록번호와 마찬가지로 수기 또는 구두로 이용될 수 있다. 전송된 목적별 ID는 검증을 통해 도용을 방지하며, 재사용 또한 불가능하다.

모바일 ID 기반 개인화 서비스 기술은 다음과 같다.

- 동태적 개인정보 셀프 모니터링 기술 : 스마트지갑 사용 과정에서 생성된 동태적 개인정보(출입, 인증, 구매, 지불, 이동 내역)를 기록한다. 또한 사용자의 위치, 주변환경 등 스마트지갑을 통해 모니터링한 퍼스널 컨텍스트를 기록한다.
- 관심정보 자동 추출 기술 : 축적된 기록을 분석하여 개인의 선호도나 관심분야를 추출하고 동태적 개인정보 및 퍼스널 컨텍스트를 정형화한다.
- 정책기반 개인정보 협상 기술 : 스마트지갑에서 생성된 셀프 프로파일과 정태적 개인정보를 사용자의 선택에 따라 프라이버시 침해없이 전달하는 기술이다. 스마트폰의 인터페이스를 고려한 사용자 개인정보 정책 관리 기술, 사용자와 정보 수요자의 정책 간의 협상을 통해 개인정보 제공 여부를 자동으로 판단하는 기술이다.
- 동태적 개인정보 익명화 및 가상화 기술 : 개인정보 중 신원확인이 가능한 정보를 제거하는 익명화 기술과 신원은 알 수 없지만 지속적으로 관리가 가능한 가상화된 신원을 생성, 이용할 수 있도록 하는 기술이다.
- 프라이버시 보존형 개인정보 디스커버리 및 브로커 기술 : ID기반 맞춤형 서비스를 위해 서비스 제공자가 특정한 개인정보 속성 값을 갖는 개인을 검색하거나(디스커버리), 특정 사용자와 특정 서비스 제공자를 중개해(브로커) 주는 서비스가 필요하다. 이때 개인의 신원이 노출되지 않는 검색과 중개기술이 모바일 ID 기반 서비스 개발 프레임워크에 포함된다.
- 모바일 ID기반 서비스 오픈 API 기술 : 모바일 ID 기반 서비스 구현을 용이하도록 하기 위해 개인정보의 획득을 위한 API를 제공한다.

4. 스마트지갑 시스템

4.1 시스템 구성

스마트지갑 시스템 구성 예가 그림 2에 나타나 있다. 시스템 구성 요소는 다음과 같다.

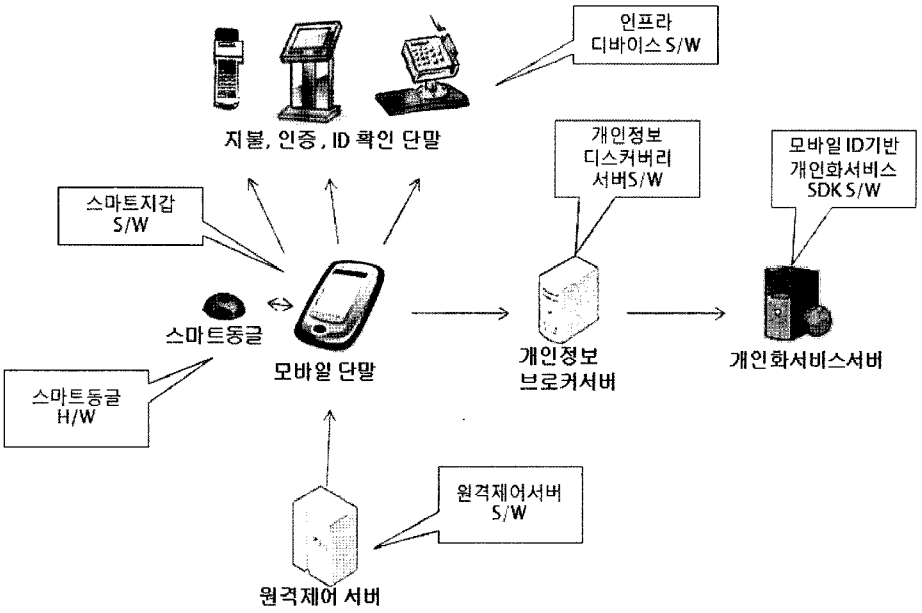

그림 2 스마트지갑 시스템 구성도

- 스마트지갑 클라이언트 : 모바일단말에 탑재되는 스마트지갑 S/W와 별도로 휴대할 수 있는 스마트동글 H/W로 구성된다. 스마트동글은 옵션으로, USB 동글형태를 가지며, PC에 장착하여 모바일 단말과의 통신 채널을 형성해 주는 역할을 한다.
- 지불, 인증, ID 확인에 사용되는 인프라 디바이스(H/W+S/W) : 스마트지갑 S/W가 탑재된 휴대단말을 사용하여 지불, 인증, ID 확인을 수행하는 경우에 근거리 RF 통신을 통해 이와 상호작용하는 인프라 단말이다.
- 개인정보 디스커버리서버 : 서비스 제공자가 원하는 내용의 개인정보 제공자를 찾기 위한 디스커버리 서비스를 제공하는 서버이다.
- 개인화 서비스 서버 : 모바일 ID 기반 개인화 서비스 프레임워크가 설치되어 개인정보의 조회, 이용, 가상화된 개인과 상호 작용 등을 지원해주며, 이러한 개인정보를 이용한 개인화 서비스 API를 이용하는 응용서비스가 설치 운영된다.

스마트지갑의 논리적 구성은 그림 3과 같다.

4.2 활용 범위 및 서비스 시나리오

스마트지갑은 여러 가지 분야에서 활용될 수 있다.

- 온·오프라인 신원확인 : 주민 번호 대체 수단과 신분증(운전면허증, 여권, 의료보험증 등)을 탑재하여 사용할 수 있으며, 수요자는 정부이다.
- 구매, 지불 : 신용카드, 교통카드, 할인카드, 로열티 카드를 탑재하여 구매·지불 시 사용하며, 수요자는 카드회사와 로열티 회사 등이다.
- 심리스 인증 : 각종 출입 통제와 자동차, PC 등 기기의 사용자 인증 시 사용하며, IT 서비스 사용자 인증에도 사용할 수 있다. 수요자는 인증 솔루션 공급회사, 자동차, PC 등 기기 제작사가 될 수 있다.
- 기업 보안 : 기업 구내 물리적 출입통제와 IT시스템 인증에 활용할 수 있다. 수요자는 기업 보안 회사 및 각종 기관이다.

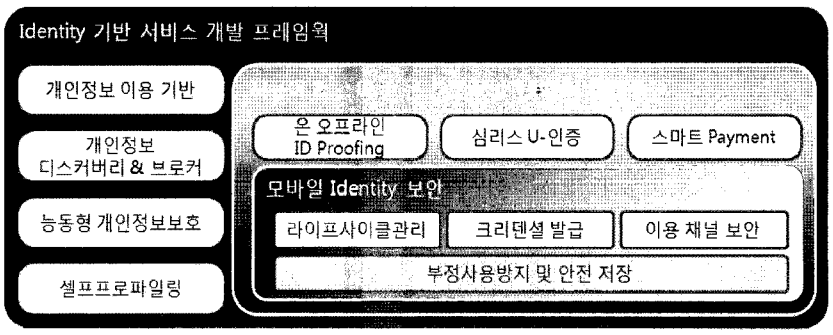

그림 3 스마트지갑 논리적 구성도

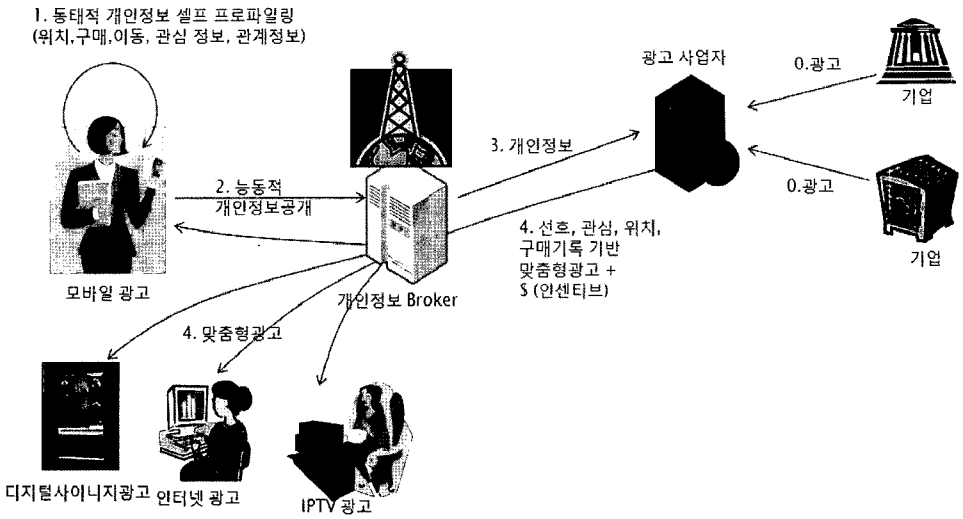

그림 4 스마트지갑 맞춤형 광고 서비스 시나리오

- 맞춤형 광고/쿠폰 : 맞춤형 광고를 위한 선호, 관심 정보 수집 기반으로 사용될 수 있으며, 수요자는 광고회사 및 인터넷 포털이 될 수 있다.
- 맞춤형 의료, 교육, 자산관리 서비스: 맞춤형 서비스를 위한 개인정보 획득 기반으로 사용되며, 수요자는 맞춤형 서비스 제공자 및 솔루션 구축자가 될 수 있다.

스마트지갑을 이용한 구체적 서비스 시나리오는 다음과 같다. 그림 4는 스마트지갑을 적용한 모바일 지불 결제 시나리오를 보여준다. 카드의 발급과정에서 사용, 그 이후의 CRM과 지출관리 과정까지 포함된다. 스마트지갑을 이용하면 모바일 지불을 안전하고 편리하게 이용할 수 있고, 이후 포인트 적립 및 할인 혜택 등과 같은 인센티브로 받을 수 있다.

그림 5는 스마트지갑을 적용한 맞춤형 광고 시나리오를 보여준다. 동태적 개인정보를 셀프 프로파일링 하여 개인의 선택에 따라 제공하면, 개인의 선호도, 관심, 위치, 구매이력 등에 기반한 정밀한 맞춤형 광고를 이용하고 광고를 보는 대가로 인센티브를 획득하게 된다. 맞춤형광고는 웹 서핑, IPTV 시청, 오프라인 사이니지(signage) 등 사용자가 현재 이용하는 매체를 통해 제공될 수 있다.

이외에도 스마트지갑을 이용한 심리스인증, 역경매 등 다양한 시나리오가 존재할 수 있으며, 스마트지갑은 여러 가지 지불, 인증 상황에서의 편리함을 제공하고, 고부가가치 개인화 서비스를 가능하게 해준다.

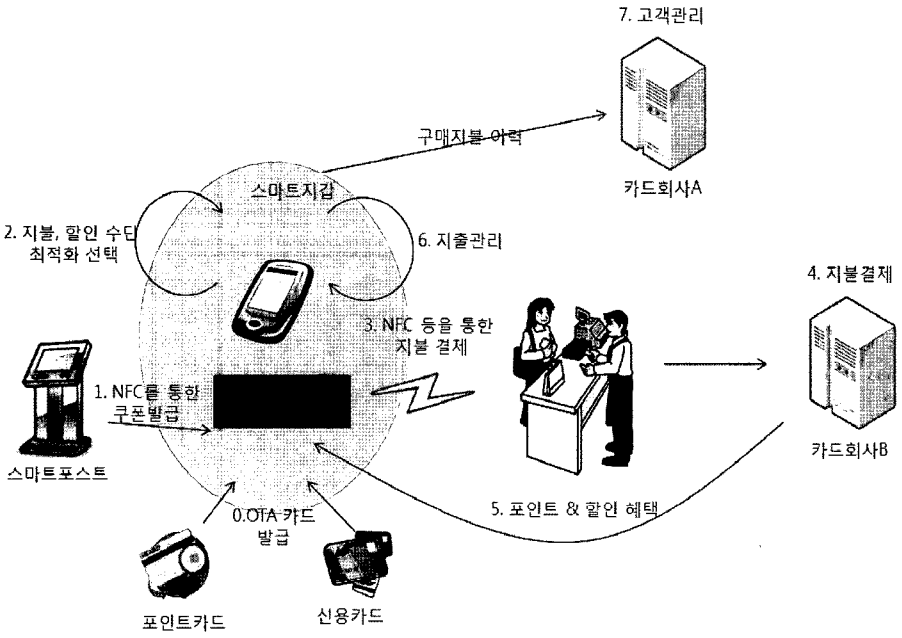

그림 5 스마트지갑 구매/지불 서비스 시나리오

5. 관련동향

5.1 기술 동향

국내외 스마트지갑 관련 기술개발 동향은 다음과 같다.

- 국내에서는 모바일 지불 결제 기술이 일부 개발되어 있다.
  - KB에서 단일 카드를 탑재한 앤디카드가 제품화되어 있다[10].
  - 복수의 지불매체를 탑재하고 이들 정보를 연계한 지능형 지불 및 구매를 제공하는 기술은 없는 것으로 파악된다.
- EU에서 진행 중인 PrimeLife 프로젝트(2008.3~2011.2)에서는 온·오프라인 환경의 Identity 관리 및 프라이버시 보호 기술을 연구 중이다[11]. 실생활에 관련된 프라이버시 강화형 Identity 관리 기술을 연구하며 프라이버시 친화형 Identity 관리 도구를 개발하고 있다.
- FIDIS의 WP3 "Study on Mobile Identity Management" 프로젝트에서 모바일 Identity 관리 및 보안 요구사항과 기술을 연구하였다[12].
  - iManager는 독일의 Univ. of Freiburg에서 개발한 모바일 Identity manager로서 partial identity 관리와 프라이버시 보호 기능을 갖고 있다.
  - AXS ID-Card는 AXS-authentication scheme을 기반으로 한 휴대용 인증 디바이스이다. 대규모 id federation과 EAM 등 온라인 용도는 물론, 물리적 인증에도 대응하도록 개발하였다.
- Sony는 비접촉식 IC카드로서 핸드폰에 탑재되는 Felica 칩을 개발하였다[13]. 최대 16개의 서비스가 동시 사용하며 교통카드, 신용카드, 멤버십카드 등 다양한 종류의 카드를 탑재할 수 있으며 휴대폰에서 구동되는 프로그램을 통해 다양한 응용 서비스 개발할 수 있다.
- DoCoMo는 iD 플랫폼을 탑재한 전자지갑폰을 제공하고 있다. 다수의 신용카드와 할인쿠폰을 탑재하여 NFC 통신을 통해 이용할 수 있으며 원격잠금기능을 통한 보안성을 제공한다[14].
- Apple의 아이폰에서 동작하는 전자지갑 어플리케이션들이 개발되었다[15]. eWallet S/W는 지불, 인증 수단을 저장, 필요시 조회하는 수준의 기능을 제공하며, 항공티켓을 아이폰으로 전송하여, 아이폰 화면에 출력된 바코드를 사용하는 기능이 개발되었다. 단말 위치 조회와 원격제어를 통한 분실 보안 기능도 제공된다.

5.2 시장 동향

우리나라를 포함하여 주요 선진국들의 인구대비 모바일 보급률은 80%대를 넘었고, 2008년 6월 기준으로 신흥경제국(BRIC)인 러시아는 123.7%, 브라질 73%, 중국 44.7%, 인도 25.3%를 기록하고 있다.

시스템, 단말 및 서비스의 모바일 시장은 2007년 9,911억 달러의 매출을 기록하였으며, 2006~2011년까지 연평균 8.7% 성장률로 증가하여 2011년에는 1조 3,314억 달러에 이를 것으로 전망하고 있다. 이중 스마트지갑을 필요로 하는 서비스 시장이 자치하는 비율이 9.2%의 연평균 성장으로 2011년에는 1조 262억달러를 기록할 것으로 보여 가장 높으며, 시스템 시장이 낮은 증가율을 보여 2011년에는 608억 달러를 기록할 것으로 나타났다.

국내의 경우, 미래에셋증권사의 보고서에 의하면 2010년까지의 국내 휴대폰 수요 전망치를 보면 2009년에 4,649만대에서 2010년에는 4,839만대로 내수가 될 것으로 보이며 이는 연평균 4.7%의 성장률에 해당한다. 한국 IDC코리아의 '국내 모바일 서비스 시장 현황 및 전망 보고서'에 따르면, 모바일 데이터 및 부가 서비스 등 비음성 부문의 매출액은 연평균 18.3%의 고속 성장을 구가, 2004년 2조 6,035억 원에서 2009년 6조 원 규모로 성장할 것으로 예상하고 있다.

세계 휴대폰 시장은 노키아, 모토롤라, 삼성전자, 소니에릭슨, LG전자의 5개 업체가 주도하고 있으며, 전체 시장의 80.2%(2006년 기준)을 점유하고 있다. 스마트폰 시장의 경우에는 노키아가 50% 내외의 점유율을 차지하고, 이어서 캐나다의 RIM사가 19.5%, 애플사가 10.7% 순으로 점유율을 나타내고 있다.

2007년 이후 인터넷, 멀티미디어 구현 등 정보기기의 성격이 강화된 스마트폰이 각광을 받으면서 스마트지갑 ID 플랫폼의 시장구조는 휴대폰과 스마트폰의 시장점유율에 따라 연관되고 있다. 스마트폰은 휴대폰 대비 2007년 1.2억대(10.4%)에서 2010년 4.2억대(27.1%)로 비중이 증대하고 있다. 스마트폰 이용자들은 하기의 그림에서 보인 바와 같이 이용시간 대부분을 메시지, 멀티미디어, 인터넷, 개인정보 관리 등의 정보처리를 위해 사용하고 있다.

노키아의 경우 수년전부터 모바일 콘텐츠를 신규 사업영역으로 설정하여 준비하고 있으며, 자사의 OS인 심비안의 보급 확대를 통해 자사 모바일 콘텐츠의 시장점유율 확대를 모색하였고, 이 결과 휴대인터넷인 스마트폰에 대하여 1위의 시장점유율로 결실을 맺고 있다.

애플의 경우 풀 브라우징을 구현할 수 있는 '아이폰'과 아이폰용 응용소프트웨어를 유통시킬 수 있는 '앱스토어'를 출시하면서 스마트폰과 모바일 응용소프트웨어 부문을 선도하고 있고, 구글은 개방형 운영체제인 '안드로이드'를 개발하여 모바일 인터넷시장을 주도하려 하고 있다.

우리나라의 경우 고객 개개인의 개성과 니즈를 반영한 맞춤형 휴대폰을 공급하고 있다. 즉 개인정보가 축적된 휴대폰을 활용해 인터넷 기반의 다양한 개인 맞춤형 생활정보 서비스를 창출하여 시장선점을 꾀하고 있다.

스마트폰의 시장 성장과 함께, 이동 중에도 다양한 정보를 얻고자 하는 소비자의 잠재적 니즈를 겨냥한 모바일 서비스 시장은 단순한 문자, 음성메세지 서비스에서 개인정보 서비스 위주로 급속히 확대되어 2006년 695억달러에서 2010년에는 1,568억 달러(연평균 22.6%성장)에 이를 것으로 예측하고 있다.

휴대폰과 스마트폰은 개인생활에 가장 밀접한 기기로서 PC(데스크탑, 노트북)와는 차별화된 개인형 정보서비스 위주로 지속적으로 발전될 전망이다. 개인형 정보서비스는 스마트지갑을 탑재시킴으로써 구현이 가능하게 되므로, 스마트폰을 포함한 퍼스널 모바일의 시장과 함께 성장할 것이다.

스마트지갑은 휴대폰에 축적된 금융결제, 의료처방, 콘텐츠 이용내역 등 각종 개인 생활정보를 관리 및 분석할 수 있다. 차후 스마트지갑이 탑재된 휴대폰의 구매시, 이용자에게 최적화된 휴대폰을 제안하거나 다양한 파생 비즈니스를 창출할 있어 향후 3년 내에 휴대폰 시장구조의 주도권을 가질 수 있고, 선도적 지위에서 휴대폰의 시장점유율을 확대할 수 있어 글로벌 경쟁력의 확보가 가능할 것으로 전망된다[16].

6. 결 론

스마트지갑의 기대 효과는 매우 다양하다. 첫째, 국가적 아젠다를 해결한다. 온·오프라인을 망라하는 주민등록번호 대체 기술을 확보하여 주민등록번호 유출 및 도용으로 발생하는 문제를 해결할 수 있다. 스마트지갑은 재사용 및 도용이 불가능한 주민등록번호 대체 ID를 온·오프라인 환경의 다양한 전달 수단을 통해 사용할 수 있도록 해준다. 또한 최근 이슈가 되고 있는 사용자 맞춤형 서비스에서의 프라이버시 문제를 해결할 수 있다. 사용자 맞춤형 서비스를 위해 사용자의 동태정보를 모니터링하고 집적하는 것이 프라이버시 관점에서 문제가 되고 있는데, 스마트지갑은 사용자 단말에서 이들 정보를 모니터링하고 집적한 뒤, 사용자의 선택에 따라 프라이버시를 보존하며 제공할 수 있도록 해주므로 정보집적에 따른 프라이버시 문제를 해결할 수 있다.

둘째는 경제적 기대효과이다. 온·오프라인 환경의 인증, 지불, 출입, 개인정보기반 서비스 구축 등 다양한 활용분야가 있고 이들 솔루션의 시장 규모만 2013년 336억 달러 규모에 달한다. 관련 경제 효과는 솔루션 시장에 그치지 않는다. 스마트지갑을 통해 프라이버시 및 보안 우려를 해소한 맞춤형 광고, 교육, 의료, 자산관리 서비스 등의 다양한 맞춤형 서비스가 활성화될 수 있으며, 이들 시장 규모는 솔루션 시장보다 훨씬 클 것으로 예상된다.

셋째, 스마트지갑을 기반으로 다양한 신규 융·복합 서비스를 창출할 수 있다. u-헬스모니터링의 개인 단말로 사용되어 헬스케어 정보의 프라이버시 보호 및 타 개인정보와의 연계서비스를 제공할 수도 있고, 자동차의 사용자 환경을 저장하였다가, 사용자 맞춤형 환경 구성을 제공할 수도 있다. 또한 유비쿼터스 센서 및 인프라 디바이스 등과 연계하여 지능형 관광 서비스 등에 이용될 수도 있다.

따라서 스마트지갑은 다양한 국가적, 기술적, 사회적, 경제적 파급효과를 가져오는 기술로서 지속적인 연구개발이 필요한 기술이다.

참고문헌

[1] J.D. Sutter, "Wallet of the future? Your mobile phone", CNN, 2009. 8.

[2] NFC, http://www.nfc-forum.org

[3] 천성록, "비접촉식 신용카드 기술의 동향과 시사점", 디지털타임스, 2009. 10.

[4] 이정환, "아이폰으로 시동거는 자동차 등장", 전자신문, 2009.2.

[5] http://en.wikipedia.org/wiki/Location-based_service

[6] "IT 컨버전스의 진화", SERI 경제포커스, 2009.2.

[7] "Worldwide I&AM 2008-2012 Forecast", IDC, 2008.

[8] "Mobile Payment Markets Strategies & Forecasts 2008-2013", Juniper Research, 2008.

[9] "Service Personalization", ABIresearch, 2007.

[10] 앤디카드, http://www.kbndcard.com

[11] PrimeLife, http://www.primelife.eu/about/factsheet

[12] FIDIS Deliverable D11.1 : Collection of Topics and Clusters of Mobility and Identity - Towards a Taxonomy of Mobility and Identity, 2006.

[13] Felica, SONY, http://www.sony.net/Products/felica/

[14] Docomo, http://wirelesswatch.jp/2009/08/03/docomo-

id-for-summer-sonic/
[15] eWallet, iLium Software, http://www.iliumsoft.com/site/iphone/products_ewallet.php
[16] "모바일 ID 시장동향 분석 보고서", 2009.8.
[17] "i-PIN 2.0 소개", http://www.kisa.or.kr/kisa/ipin/jsp/ipin_0000.jsp
[18] "쿡 스마트웹은 당신이 한 일을 알고 있다?", 오마이 뉴스, 2009.9.

최 대 선

1995 동국대학교 컴퓨터공학과(학사)
1997 포항공과대학교 컴퓨터공학과 (석사)
2009 한국과학기술원 전산학과(박사)
1997~1999 현대전자/정보기술
1999~현재 한국전자통신연구원 지식정보보안 연구부 인증기술팀 선임연구원
관심분야 : 정보보호, 디지털ID관리, 개인정보보호
E-mail : sunchoi@etri.re.kr

진 승 헌

1993 숭실대학교 전자계산공학과(학사)
1995 숭실대학교 전자계산공학과(석사)
2004 충남대학교 컴퓨터과학과(박사)
1994~1996 대우통신
1996~1999 삼성전자
1999~현재 한국전자통신연구원 지식정보보안 연구부 인증기술연구팀장/책임연구원
관심분야 : 컴퓨터/네트워크 보안, 정보보호(PKI), ID 관리
E-mail : jinsh@etri.re.kr