4G 네트워크를 위한 LTE/SAE 기반의 모바일 전자ID지갑

준회원 정 윤 선*, 정회원 임 선 희*, 이 옥 연**, 이 상 진***

The Mobile Digital ID Wallet based on LTE/SAE for 4G Networks

Yunseon Jung* *Associate Member*,
Sun-Hee Lim*, Okyeon Yi**, Sangjin Lee*** *Regular Members*

요 약

차세대 모바일 통신 기술로 불리는 4G는 인터넷 기술의 급격한 발전 및 이기종망 간의 통합으로 인해 핸드폰, PMP, UMPC 등과 같은 모바일 단말을 사용한 무선 인터넷의 이용이 증가할 것으로 전망된다. 이로 인해 사용자는 유선 인터넷 뿐만 아니라 무선 인터넷 환경에서도 개인정보의 불법적인 사용을 예방하고 효율적으로 관리할 수 있는 전자ID(Digital ID) 기술이 필요하다.

본 논문에서는 다양한 전자ID 관리 기술을 분석하고, 사용자가 직접 개인정보를 통제할 수 있는 사용자 중심의 전자ID 관리 기술에 대한 요구사항을 정의한다. 또한 4G 표준기술로 주목받고 있는 3GPP(3rd Generation Partnership Project)의 LTE/SAE(**Long Term Evolution/System Architecture Evolution**) 네트워크에서 모바일 응용을 위한 인증 메커니즘을 제안한 후에 이와 연동이 가능한 사용자 중심의 모바일 전자ID지갑 메커니즘을 제안한다.

Key Words : 4G, LTE/SAE, Digital ID Wallet, ID Management, User-centric

ABSTRACT

In 4G environments, which is the next generation technology for mobile network, it is forecasted that the wireless Internet using a mobile devices such as a mobile phone, PDA will increase because of expansion of Internet and integration of heterogeneous networks. Therefore, we need a Digital ID management technology that can prevent illegal uses and manage private information efficiently in wired and wireless environments.

In this paper, we analyze various Digital ID management technologies, and then define requirements of user-centric Digital ID management technology. In addition, we newly propose the authentication mechanism for mobile applications in LTE/SAE network. Finally, we propose the mobile Digital ID Wallet mechanism suitable for 4G environments.

Ⅰ. 서 론

무선 인터넷의 확산과 다양한 서비스의 진화는 언제 어디서나 효율적으로 사용이 가능한 전자ID 관리 기술을 요구한다. 또한 사용자 참여 중심의 인터넷 환경인 웹 2.0 및 모바일 2.0 시대가 도래함에 따라 신원 서비스에 대한 관심이 나날이 증가하고 있다. 이미 여러 표준단체 및 기업에서 전자ID 관리에 대한 연구를 진행하고 있지만, 다가오는 4G 환경을 위한 무선 네트워크 및 유무선, 이기종 통합

네트워크에 적합한 전자ID 관리 방안에 대한 궁극적인 해답은 제시하지 못하고 있다.[1][2] 따라서 미

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))
* 고려대학교 정보경영공학전문대학원 무선이동통신연구실({jys2002,capsunny}@korea.ac.kr)
** 국민대학교 자연과학대학 수학과(oyyi@ kookmin,ac.kr) *** 고려대학교 정보경영공학전문대학원 포렌식연구실(sangjin@korea.ac.kr)
논문번호 : KICS2008-05-201, 접수일자 : 2008년 5월 2일, 최종논문접수일자 : 2008년 9월 17일

래의 통신 환경과 급속하게 발전하는 무선 서비스를 위한 전자ID 관리 방안에 관한 연구가 반드시 필요한 실정이다.

전자ID 관리 기술은 단방향의 기업 도메인 중심에서 양방향의 사용자 중심으로 진화하고 있다. 기업 도메인 중심의 전자ID 관리 기술은 각 SP(Service Provider)가 사이트마다 중복적으로 산재해 있는 개인정보를 보호해야 할 의무와 비용을 부담하고 있으며, 개인정보의 관리적 측면에서 개인정보의 주체인 사용자의 의견과 특성을 전혀 반영하지 못하고 있기 때문이다. 또한 SP가 사용자 개인정보를 정직하게 활용하고 있는지, 어떻게 관리, 폐기하는지 등의 투명성이 보장되지 않음으로써 사용자는 허술한 개인정보 관리 체계에 의한 개인정보 노출 및 프라이버시 침해에도 속수무책으로 당할 수밖에 없는 현실이다.

따라서 개인정보의 주체인 사용자가 자신의 개인정보 관리에 적극적으로 참여하고 통제할 수 있는 사용자 중심의 전자ID 관리 기술이 요구된다. 사용자가 개인정보를 스스로 통제하고 관리하기 위해서는 SP가 소유하고 있는 저장 공간이 아닌 사용자의 저장 공간에 개인정보가 안전하게 저장되어야 한다. 사용자의 저장 공간은 제 삼자에 의한 임의적인 접근은 불가능한 반면, 사용자는 언제 어디서나 사용과 접근이 가능하도록 적절한 인증과 접근제어를 제공할 수 있는 능력을 가져야 한다. 즉, 악의적인 공격자에 의한 개인정보의 오남용 및 불법적인 유통을 예방할 수 있어야 한다. 그리고 사용자가 적극적으로 나서서 전자ID를 관리하고 통제할 수 있도록 쉽고 편리한 사용자 인터페이스가 제공되어야 한다. 따라서 본 논문에서는 이와 같은 요구사항을 만족시킬 수 있는 USIM(Universal Subscriber Identity Module) 카드를 사용자 개인정보의 저장 공간으로 활용하여 사용자 중심의 전자ID 관리 메커니즘을 제안한다. USIM 카드를 개인정보의 저장 공간으로 활용함으로써 사용자는 모바일 단말기의 이동성에 의해 시간과 장소의 구애를 받지 않고 전자ID를 관리 및 통제할 수 있다. 또한 근래의 고용량 USIM은 단순히 통신 서비스를 위한 데이터 저장 공간으로써의 역할에 그치지 않고 IPSec, DRM, WPKI 등의 보안기능을 제공할 수 있으며, 암호 알고리즘을 활용한 연산도 고속으로 프로세싱이 가능할 만큼 성능이 향상되었다. 따라서 USIM 카드는 기밀성을 요구하는 데이터의 저장 공간은 물론이고 다양한 서비스를 위한 응용에 활용될 수 있다. 이 때 모바일 단말기는 사용자에게 전자ID 관리를 위한 사용자 인터페이스를 제공하고 단말플랫폼 계층에서의 보안 관련 기능을 처리한다.

본 논문의 구성은 다음과 같다. Ⅱ장과 Ⅲ장에서 다양한 전자ID 관리 기술과 관련 연구를 비교 및 분석한 후, Ⅳ장에서 기존 기술들의 한계점을 보완하고 보다 효율적인 전자ID 관리를 위해 요구되는 사용자 중심의 전자ID 관리 기술에 대한 요구사항을 정의한다. Ⅴ장에서 LTE/SAE 네트워크의 개요를 살펴보고, Ⅵ장에서 LTE/SAE 환경에 적합한 사용자 중심의 전자ID 관리 기술을 제공하기 위해 모바일 전자ID지갑 시스템과 인증 메커니즘을 제안한다. Ⅶ장에서는 Ⅳ장의 요구사항을 충족시키는 모바일 전자ID지갑 메커니즘을 제안하고, 마지막으로 Ⅷ장에서 요구사항 및 안전성에 대한 분석을 논의한 후, Ⅸ장에서 결론을 맺는다.

Ⅱ. ID 관리 시스템의 유형[3][4]

본 장에서는 ID 관리 시스템을 유형별로 분류하고 각각의 특징을 살펴본다. ID 관리 시스템은 [그림 1]과 같이 독립형, 연합형, 사용자 중심형으로 분류된다.

2.1 독립형 ID 관리(Isolated ID management)

독립형 ID 관리 모델은 가장 일반적이고 단순한

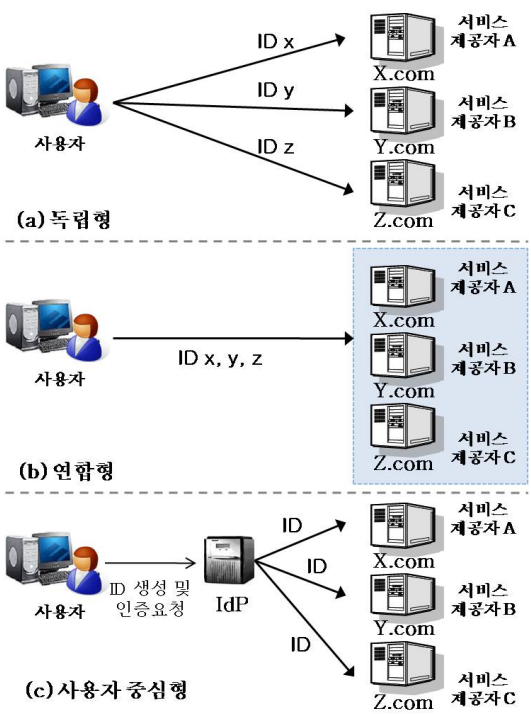

그림 1. ID 관리 시스템의 유형
Fig. 1. The Types of ID management system

방식으로써 사용자는 각 SP마다 자신의 개인정보를 등록하고 ID를 생성한다. 그러나 사용자는 SP마다 다른 서로 ID를 기억하고 관리하기 어렵기 때문에 동일한 ID와 PW를 사용함으로써 보안의 위협을 초래한다. 또한 SP가 모든 사용자의 개인정보를 소유, 관리하므로 개인정보 오남용 및 유출에 의한 프라이버시 침해가 발생한다. 그리고 서비스 가입 시마다 개인정보를 반복적으로 입력해야 하며, 이사나 핸드폰 분실 등의 변경사항이 발생하면 각 SP에 저장되어 있는 개인정보를 직접 수정해야하는 불편함이 있다.

2.2 연합형 ID 관리(Federated ID management)

연합형 ID 관리 모델은 한 번의 인증으로 동맹관계를 맺고 있는 SP들의 서비스들을 이용할 수 있는 방식이다. 이는 독립형 전자ID 관리 방식에서 나타나는 반복적인 ID/PW 입력의 불편함은 감소시켰지만, 동맹관계의 도메인 영역 내에서만 가능하다는 한계점을 가지고 있다. 따라서 사용자는 여전히 서비스 도메인마다 다른 ID와 PW를 관리해야 한다.

2.3 사용자 중심형 ID 관리(User-centric ID management)

사용자 중심형 ID 관리는 개인정보, 전자ID 관련 정책 등을 사용자가 직접 통제함으로써 기존의 전자ID 관리 방식의 한계점를 보완하고, 보다 편리하고 효율적인 개인정보 관리 방식를 제공한다. 이 방식은 사용자 통제형 전자ID 관리(User-controlled identity management)라고도 부르며, 별도의 IdP(Identity Provider)가 ID에 대한 통제 및 관리를 책임진다. 사용자는 최초에 한 번만 IdP에 ID를 등록하면 된다. 그 후 사용자가 서비스를 요청하면 SP는 IdP를 통해 사용자 인증을 받고 서비스를 시작한다. 그러나 IdP에 등록된 동일한 ID로 모든 사이트에 접속할 경우, 사용자의 행적이 노출되거나 서로 다른 사이트 간의 공모로 인한 프라이버시 침해의 문제가 발생하므로 사용자에게 익명성을 보장할 수 있는 방법이 필요하다.

Ⅲ. 전자ID 관련 연구

3.1 국내외 동향

3.1.1 FIDIS(Future of Identity in the Information Society)[5]

FIDIS는 전 유럽에서 통용 가능한 신원 관리 방식을 개발하고 ID 도용과 같은 프라이버시 문제를 해결하기 위하여 2004년부터 2009년까지 진행되고 있는 프로젝트이다. FIDIS는 유럽 국가들의 ID 관리 시스템, ID 정책 및 법률 등을 수집 및 분석하며, ID 용어 정리, 프로파일링, 기존 ID 관리 시스템 간의 상호운용성, 포렌식(forensic), 식별 제거(de-identification), 최신 식별 기술, 이동성을 고려한 신원과 같은 7가지 연구 분야로 구성되어 있다. FIDIS 프로젝트는 기존의 연구를 통합하고, 법적, 사회적, 경제학적 등 다양한 관점에서 요구사항을 도출하는 아키텍처 및 스펙 공개를 목표로 하고 있다.

3.1.2 PRIME(Privacy and Identity Management for Europe)[6]

PRIME은 유럽 연합이 지원하고 IST(Information Society Technologies)가 관리하는 프로젝트로써 프라이버시가 강화된 ID 관리 기술 개발에 초점을 맞추고 있다. PRIME 프로젝트의 개발 계획은 요구사항 수집 및 평가, 어플리케이션 프로토타입 개발, ID 관련 기술의 연구 개발, 프레임워크와 아키텍처 구축 및 확장으로 나눠진다. PRIME 프로젝트는 전송 레벨의 익명성을 비롯하여 최대한으로 사용자의 프라이버시를 보장하여, 사용자들이 안전하게 자신의 개인 정보를 제어할 수 있는 방법을 제공하려고 한다.[1] 그러나 사용자 중심의 ID 관리를 위한 구체적인 통합 프레임워크를 제시하지 못하고 있다.

3.1.3 Shibboleth[7][8]

Shibboleth는 미국의 교육 및 학술 분야를 위하여 웹 기반의 리소스 공유 및 인증 시스템을 개발하는 프로젝트이다. OpenSAML을 기반으로 Federated SSO와 사용자가 직접 속성(Attribute) 공유를 제어할 수 있는 프라이버시 기능을 제공한다.

3.2 전자ID 관련 기술

3.2.1 OpenID[9]

OpenID는 인터넷 상에서 하나의 URI(또는 URL)로 개인을 식별하는 사용자 중심 ID를 위한 공개 표준 기술이다. OpenID 기술에서는 URI가 사용자 ID가 되며 사용자 암호 및 인증서는 OpenID 서버에만 보관된다. OpenID는 사용자에게 친숙하고 무료로 이용 가능한 기술이라는 장점이 있지만 해결해야 할 보안 문제들이 아직 남아있다. 첫째, OpenID는 URI를 사용하기 때문에 기존 사용자가 자신의 홈페이지 URL을 ID로 사용하다가 탈퇴한 경우, 다른 사용자가 그 URL을 재사용할 수 있다. 둘째, OpenID는 사용자를 식별만 하기 때문에 신뢰(Trust)를 지원하

지 않는다. 따라서 피싱 사고 등이 발생할 수 있다. 셋째, OpenID는 유일한 ID이기 때문에 사용자의 행동 패턴을 추적할 수 있다. 즉, OpenID를 지원하는 사이트들 간의 공모를 통해 사용자 행동이 감시당할 우려가 있다. 넷째, ID 정보 공유 등 개인정보 관리에 대한 한계가 있다.

3.2.2 CardSpace[10]

CardSpace는 마이크로소프트(Microsoft)사가 Window Vista 운영체제에 탑재한 인증/지불 정보 통합 관리 프로그램이다. 즉, CardSpace는 IdP에게 정보를 제공하는 ID 메타시스템 역할을 수행한다. CardSpace는 InfoCard라는 카드 형태로 사용자에게 ID 정보를 시각적으로 제공한다. InfoCard는 신뢰 사이트가 만든 managed 카드와 사용자가 만든 self-issued 카드 두 종류가 있다. 그러나 self-issued 카드에는 이름, 집주소, 전화번호, 성별 등 한정된 정보만이 포함된다.

Ⅳ. 보안 요구사항

본 장에서는 LTE/SAE 환경에서 사용자 중심의 전자ID 관리 기술이 충족시켜야 할 보안 12가지 요구사항을 아래와 같이 정의하고 분석한다.[11]

① 사용자의 개인정보 통제권
사용자는 자신의 개인정보를 직접적으로 통제함으로써 자신의 개인정보가 어떻게 생성, 이용, 폐기되는지 알 수 있어야 한다. 또한 신뢰할 수 없는 서비스의 경우, 개인정보를 전혀 제공하지 않을 수도 있어야 한다.

② 신뢰할 수 있는 사용자 식별
SP는 주민등록번호와 같은 민감한 개인정보를 소유하지 않더라도 각 사용자를 유일하게 식별할 수 있어야 하며, 식별방식은 신뢰성이 보장되어야 한다.

③ 개인정보 노출의 최소화
서비스 제공을 위하여 사용자의 개인정보가 필요한 경우, 반드시 필요한 정보만이 제공되어야 하며, 사용자가 공유되거나 제공되기를 원하지 않는 민감한 정보는 보호되어야 한다.

④ 개인정보보호 정책 수립 및 협상
SP는 사용자로부터 개인정보 사용에 대한 동의를 얻어야 하며, 사용자는 직접 개인정보보호 정책을 설정할 수 있어야 한다. 즉, 사용자의 의도에 따른 개인정보 공유가 가능해야 한다.

⑤ 안전한 개인정보 저장
사용자의 개인정보는 SP나 IdP와 같은 제 삼의 장소가 아닌 사용자의 데이터 저장소에 안전하게 저장되어야 한다.

⑥ 익명성 제공
공격자가 사용자의 유일한 식별자에 의해 선호도와 같은 프라이버시 관련 정보나 행동패턴 등을 추적할 수 없도록 익명성이 제공되어야 한다.

⑦ 사용자 추적가능성 제공
사용자는 익명성을 보장받아야 하는 반면에, ID 도용 등을 대비하여 사용자 로그의 유지가 필요하다. 프라이버시 보호를 위하여 로그파일은 안전한 데이터 저장소에 저장되어야 한다.

⑧ 사용자 개인화 서비스 제공
관리와 통제의 대상이 되는 개인정보에는 이름, 주민번호, 주소, 전화번호 등과 같은 추적 가능한 신상정보 및 PW, 인증서와 같은 인증정보(Credential) 뿐만 아니라 나이, 성별, 취미, 종교, 각종 선호도와 같이 추적 불가능한 비신상정보도 자유롭게 포함시킴으로써 개인화 서비스를 제공받을 수 있어야 한다. 이와 같은 개인화 서비스는 사용자의 성향에 따른 적절하고 효과적인 서비스를 제공함으로써 사용자의 만족도를 높이고 편의성을 보장한다.

⑨ 개인정보 동기화 서비스 제공
온라인상에서 산재되어 관리되고 있는 개인정보를 동기화할 수 있어야 한다.

⑩ 개체 간 상호인증
사용자가 서비스를 이용하기 전에 사용자의 모바일 단말기가 SP 및 IdP 등 응용 서비스를 위한 각 개체들과 상호 인증될 수 있어야 한다.

⑪ 접근제어
정당한 사용자만이 개인정보에 접근하고 사용할 수 있어야 한다.

⑫ 네트워크 통신 보안
악의적인 공격자로부터 사용자의 개인정보를 보호하기 위하여 네트워크상의 모든 개체 사이의 통신은 안전해야 한다.

Ⅴ. LTE/SAE 네트워크의 개요

본 장에서는 3GPP TR 33.821에 정의된 LTE/SAE 네트워크에 대하여 분석한다.[12]

LTE/SAE는 3GPP가 4G 이동통신의 표준으로 제

시하고 있는 기술이며, 고속의 데이터 전송 속도와 낮은 지연율을 특징으로 한다. 또한 최적화된 패킷 기반의 네트워크 구조를 가짐으로써 다양한 서비스를 쉽게 적용시킬 수 있고, 이기종 네트워크 간 핸드오버를 지원하는 유연성을 가진다. LTE/SAE에는 처리율 향상과 지연율 감소를 위하여 다양한 객체가 추가되었으며, 핵심망은 크게 MME / UPE(Mobility Management Entity / User Plane Entity), 3GPP anchor, SAE anchor로 구성된다. 3GPP anchor와 SAE anchor 기능을 통합하여 IASA(Inter Access System Anchor)라고 한다.

- **MME /UPE :** 네트워크의 이동성을 관리하며 LTE / SAE 게이트웨이 역할을 하는 기능상의 객체
- **3GPP anchor:** GSM(Global System for Mobile communications), UMTS(Universal Mobile Telecommunications System)와 같은 기존 2G/3G 시스템과 LTE 시스템 사이의 이동성을 지원하는 객체
- **SAE anchor:** 3GPP 시스템(2G / 3G / LTE / SAE)과 non-3GPP 시스템(WLAN, WiMax 등) 사이의 이동성 지원을 위한 객체

LTE / SAE에서는 키 관리를 위하여 HSS로부터 접근 네트워크의 최상위 키를 받는 ASME(Access Security Management Entity)라는 객체를 정의하고 있다. 일반적으로 MME가 ASME의 역할을 수행한다. 3G 네트워크 인 UMTS는 AKA 과정을 통하여 비밀키 K로부터 CK와 IK를 생성함으로써 기밀성과 무결성을 제공하는 반면에, LTE/SAE는 CK 및 IK를 유도하여 생성한 키 K_{ASME}를 ASME(MME)에 전송하여 추가적으로 필요한 키들을 생성한다. 이처럼

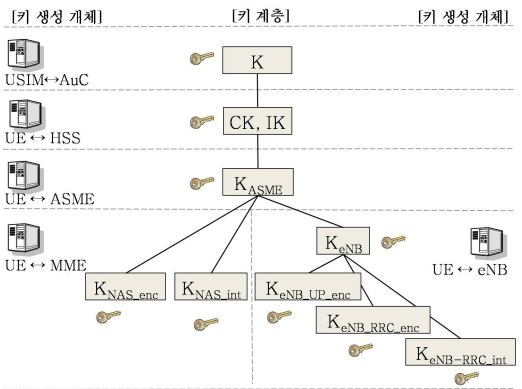

그림 2. LTE/SAE 키 계층
Fig. 2. LTE/SAE Key Hierarchy

LTE/SAE 네트워크에서의 CK, IK는 HSS 이외의 객체에는 노출되지 않으며 다른 객체나 네트워크의 키 설립 과정에서 직접 이용될 수 없다. [그림 2]는 LTE/SAE의 키 계층 구조를 나타낸다.

Ⅵ. LTE/SAE 기반의 모바일 전자ID지갑 제안

All-IP 기술을 기반으로 하는 LTE / SAE 네트워크에서는 SP가 기존과 같이 동일한 네트워크뿐만 아니라 다른 영역의 네트워크에 존재할 수 있다. 따라서 모바일 응용 서비스에 대하여 상이한 영역에 존재하는 SP와 사용자 사이에서 어떻게 상호인증과 키 일치를 제공할 것인지가 매우 중요하다. 그러므로 LTE / SAE 환경에서 사용자 중심의 전자ID지갑을 사용한 모바일 응용 서비스의 제공을 위하여, LTE / SAE에 적합한 상호인증 및 키 일치 메커니즘이 반드시 필요하다. 그러나 아직까지 이러한 인증 메커니즘이 제시되지 않은 상태이다. 따라서 본 장에서는 LTE / SAE 네트워크에 기반한 모바일 전자ID지갑 시스템과 모바일 응용 서비스를 위한 상호인증 및 키 일치 메커니즘인 LTE/SAE Boot- strapping을 제안한다.

6.1 LTE/SAE 상의 모바일 전자ID지갑 시스템

LTE/SAE 상에서 모바일 전자ID지갑을 사용한 전자ID 관리 시스템을 [그림 3]과 같이 제안한다. IASA는 3GPP 및 non-3GPP 네트워크에 존재하는 서비스

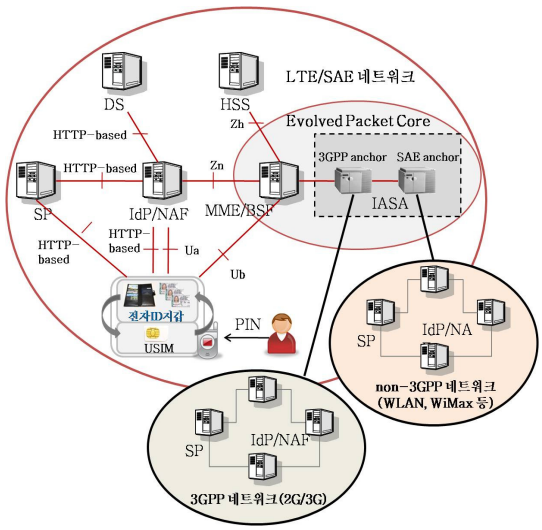

그림 3. LTE/SAE 기반의 사용자 중심의 모바일 전자ID지갑 시스템
Fig. 3. User-centric Mobile Digital ID Wallet system based on LTE/SAE

를 위한 이동성 관리를 담당하므로, 사용자는 전자ID지갑을 사용하여 타 네트워크의 서비스도 제공받을 수 있다. 다음은 모바일 전자HD지갑 시스템의 구성요소에 대한 설명이다.

- **HSS(Home Subscriber Server):** 호/세션 제어를 위한 가입자 데이터를 책임지는 마스터 데이터베이스이다.[13] HSS는 가입자 식별번호, 네트워크 접근제어 정보, 가입자의 위치 정보 및 서비스 프로파일 정보 등 가입자와 관련된 네트워크 기본 정보를 가지고 있다. 사용자 등록 과정과 AKA(Authentica- tion and Key Agreement) 과정을 지원한다.
- **BSF(Bootstrapping Server Function):** HSS와 UE(User Equipment) 사이의 인증 정보를 전달하고, 응용 서비스와 UE 사이의 키 공유를 중계한다.[14] LTE/SAE 네트워크 전반의 이동성을 관리하는 MME가 UPE이므로 BSF 역할을 수행하도록 한다.
- **NAF(Network Application Function):** 원격장치와 UICC(Universal Integrated Circuit Card) 호스팅 장치 사이의 키 센터이다.[14] IdP가 NAF 역할을 수행한다.
- **IdP:** 사용자의 신원을 밝히고 인증, 개인정보 관리, 개인정보 열람 등의 신원 서비스를 제공하는 사업자이다. IdP와 SP는 사전에 협약 등을 통해 신뢰관계를 형성하고 있으며, 기존에 별도로 가입된 SP도 IdP와 연계시킬 수 있다.
- **SP:** 사용자가 최종적으로 받기 원하는 서비스를 제공하는 사업자이다.
- **DS(Discovery Service)**: 신원과 연관된 신원 서비스를 찾기 위해 제공되는 신원 서비스의 한 종류이다.[14] 사용자의 개인정보가 등록되어 있는 IdP의 주소를 DS에 게시해 두고, 사용자의 개인정보를 필요로 하는 다른 IdP나 SP가 DS를 통해 자신들이 필요로 하는 정보를 제공하는 IdP를 검색한다.
- **UE:** USIM 응용과 전자ID지갑 응용이 탑재되어 있는 UICC가 장착된 ME(Mobile Equipment)이다.
- **전자ID지갑:** USIM으로부터 획득한 사용자 데이터 및 개인정보를 관리하고 전자ID카드를 생성, 제공 및 유지함으로써 사용자가 직접 개인정보를 통제할 수 있게 해주는 응용이다.
- **USIM:** 3G UMTS 및 4G LTE/SAE 네트워크의 인증 정보, 사용자의 식별자 및 개인정보를 저장하고 지원하는 응용으로써 AKA를 지원한다.[13] USIM 카드는 UICC에 USIM 응용이 탑재된 구조이며, 전자ID지갑을 비롯한 다양한 응용이 탑재될 수 있다. [그림 4]는 전자ID지갑이 탑재된 USIM의 구조를 나타낸다.[15]

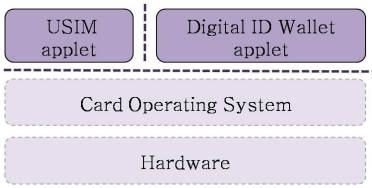

그림 4. 전자ID지갑이 탑재된 USIM
Fig. 4. USIM loaded with Digital ID Wallet

6.2 상호인증 및 키 일치 메커니즘(LTE/SAE Bootstrapping)

기존의 3G 네트워크인 UMTS는 네트워크의 보안을 위하여 암호화키 CK와 무결성키 IK를 사용하였으나 LTE/SAE 네트워크에서는 UMTS 네트워크와 다른 종류의 계층화된 키를 사용함을 5.1절에서 살펴보았다. 그러나 현재 LTE/SAE의 모바일 응용을 위한 상호인증 및 키 일치를 위한 메커니즘이 아직 제시되지 않은 상태이기 때문에 이에 적합하도록 새롭게 제안할 필요성이 있다. 따라서 본 절에서는 3GPP TR 33.980에 정의된 UMTS를 위한 인증 메커니즘을 기반으로 LTE/SAE에 적합한 UE와 HSS 및 MME/BSF 간의 상호인증 및 키 일치 메커니즘인 Bootstrapping을 제안한다.[14] 본 논문에서 제안하는 Bootstrapping 과정은 [그림 5]와 같으며, 본 과정을 통하여 UE와 HSS 사이의 상호인증이 이루어지고, 최종적으로 MME/BSF와 UE는 세션키 Ks_NAF를 공유한다.

다음은 LTE/SAE Bootstrapping 과정을 설명한다.

① UE가 BSF에 사용자 신원을 보내서 요청을 한다.
② BSF는 HSS로부터 사용자 이름에 대응하는 GUSS (Generic Bootstrapping architecture user Security Settings)와 인증 벡터를 가져온다.
③ BSF는 RAND와 AUTN을 보낸다.
④ UE는 AKA를 수행하여 CK, IK와 RES를 계산한다. CK, IK로부터 K_{ASME}를 생성한 후, K_{ASME}로부터 K_{NAS_enc}와 K_{NAS_int}를 생성한다. UE는 BSF에게 다른 HTTP 요청을 통해 Digest AKA response를 보낸다. BSF는 Digest AKA response를 검증함으로써 UE를 인증한다.
⑤ BSF는 RAND값과 BSF name을 이용하여 B-TID

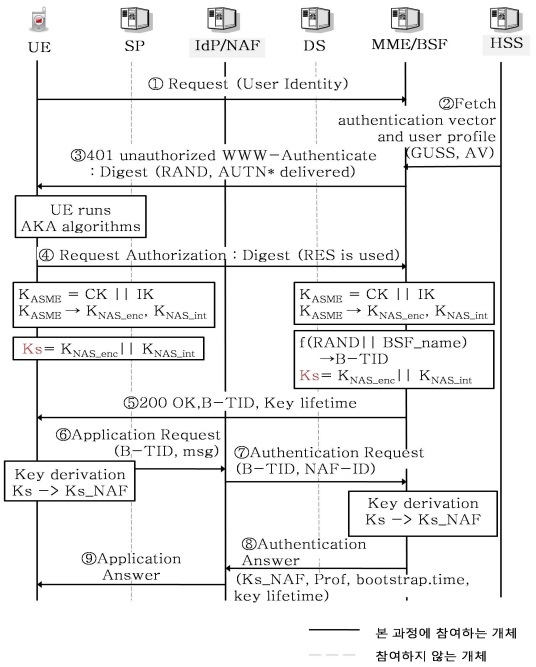

그림 5. LTE/SAE에서 인증 및 키 일치를 위한 Bootstrapping
Fig. 5. Bootstrapping for Authentication and Key Aggrement on LTE/SAE

를 생성하고 키 유효시간과 함께 UE에게 전송한다. UE와 BSF는 K_{NAS_enc}와 K_{NAS_int}를 연결함으로써 키 Ks를 만들 수 있다. 그러나 실제 키 Ks_NAF는 필요에 의해 Ks로 부터 만든다.

⑥ UE는 NAF에 B-TID를 가지고 응용 요청 메시지를 보낸다.

⑦ NAF는 BSF에 B-TID에 대응하는 키 물질을 얻기 위하여 B-TID, NAF-ID를 포함한 인증 요청 메시지를 보낸다.

⑧ BSF는 주어진 호스트 이름을 사용하여 NAF가 권한이 있는지 확인한다. 만약 검증이 성공적이면 주어진 B-TID가 가진 키를 찾는다.

⑨ BSF는 Bootstrapping 시간을 가진 Ks_NAF와 NAF의 유효시간을 보낸다. NAF는 Ks_NAF에 추가로 BSF로부터 일부 응용에 대한 특정 정보를 요청할 수 있다. 그러나 만약 B-TID에 대응되는 키가 없으면 BSF는 NAF에게 UE와 Bootstrapping 재협상 할 것을 요청한다.

Ⅶ. USIM을 활용한 모바일 전자ID지갑

모바일 전자ID 지갑은 마치 현실세계의 실제 지갑처럼 평소에는 서비스 유형, 보안레벨 등 각 목적

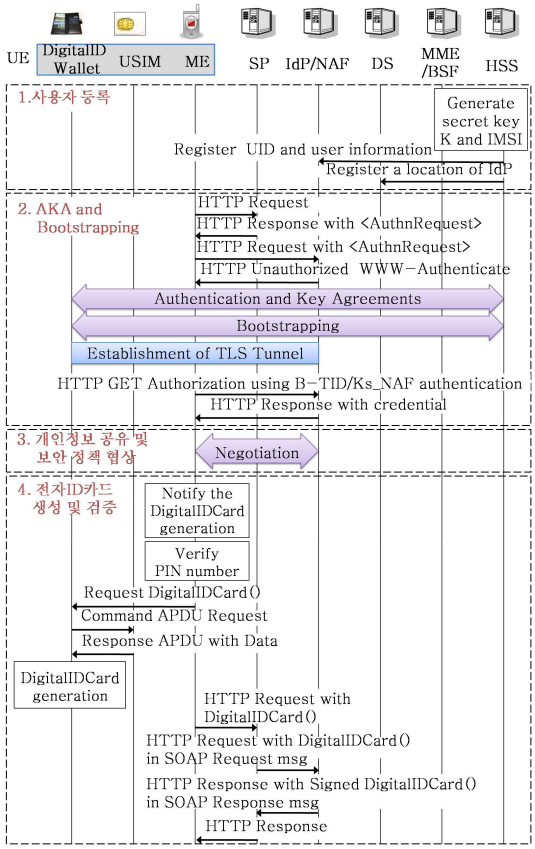

그림 6. 모바일 전자ID지갑 메커니즘
Fig. 6. The Mobile Digital ID Wallet Mechanism

에 따라 생성된 전자ID 카드를 보관하고 있다가 서비스 필요시 인증 및 개인정보 활용을 위해 꺼내어 사용할 수 있도록 한 것이다. 전자ID 카드는 필요시마다 사용자가 생성할 수도 있고 유효기간 내의 기존 전자ID카드를 재사용하거나 새로운 정보를 추가하여 발급할 수도 있다. 따라서 모바일 전자ID지갑은 사용자 인증 기능에 국한되지 않고 다양한 서비스에 응용 및 활용될 수 있다.

모바일 전자ID 지갑 메커니즘은 [그림 6]과 같이 사용자 등록, 키 일치를 위한 AKA와 Bootstrapping, 개인정보 공유 및 보안 정책 협상, 전자ID카드 생성 및 검증 과정으로 구성된다. 본 장에서는 각 과정을 정의하고 전자ID카드를 사용한 단일 인증 로그온 절차를 예제로써 설명한다.

7.1 사용자 등록

사용자가 LTE/SAE 네트워크에 가입하면 HSS는 비밀키 K와 가입자 신원확인을 위한 IMSI(International Mobile Subscriber Identity)를 생성한다. IMSI는 네트

워크에서 사용자를 유일하게 나타내는 15자리 식별 번호로써 USIM에 저장된다. IMSI가 직접적으로 노출되면 사용자에 대한 통신정보가 유출되고 인증서버에 대한 인증요청 서비스거부 공격 등에 악용될 수 있으므로 IMSI는 보호되어야 한다. 따라서 Air 인터페이스 상에서 IMSI의 노출을 최소화하기 위해 최초 위치 등록시 VLR(Visitor Location Register)이 IMSI 대신 TMSI를 할당한다. 반면에 전자ID지갑 시스템에서는 사용자 식별을 위해 UID(User Identity)를 사용도록 정의한다. UID은 IMSI로부터 유도되며 최초에 HSS가 IdP에 사용자 데이터 및 개인정보와 함께 등록한다. 그리고 UID 및 사용자의 개인정보가 등록된 IdP의 위치를 DS에 등록한다.

7.2 AKA와 LTE/SAE Bootstrapping

AKA와 Bootstrapping 과정은 6.2에서 정의한 바와 같이, UE와 HSS가 상호인증을 하고, UE가 SP 및 IdP와 세션키를 일치시키는 과정이다. UE는 HSS와 IdP에 의해 개체 인증되어야 하며 세션키는 freshness를 만족해야 한다. 본 과정을 통해 생성되는 세션키 KS_NAF는 전자HD카드의 기밀성 및 무결성을 제공하기 위해 사용된다. 다음은 사용자의 서비스 요청을 시작으로 세션키를 공유하기까지의 과정이다.

- **UE→SP:** UE는 SP의 서비스에 접근하기 위해 HTTP Request를 전송함으로써 SP에 접속한다.
- **SP→UE:** UE는 HTTP Request에 대한 응답으로써 IdP의 주소와 <AuthnRequest>를 얻는다.
- **UE→SP:** UE는 Lacation Header Field에 주어진 URL 하의 IdP에 접속한다. UE는 <AuthnRequest> 정보를 가지고 IdP/NAF URL에 접근해야 한다.
- **SP→UE:** UE가 아직 IdP로부터 인증되지 않았다면 인증 과정의 실행이 필요하다. IdP는 UE에 대한 Unauthorized 상태의 HTTP Response를 전송한다. NAF안에 어떤 유효한 키 물질이 없거나, freshness가 IdP/NAF에 의해 만족되지 않는다면, 6.2에서 정의한 바와 같이 Bootstrapping을 실행한다.
- **UE↔IdP/NAF:** UE와 IdP/NAF는 TLS 터널을 설정한다. 이것은 IdP/NAF에 대한 전송을 위한 요청을 준비하기 위한 것이다. UE는 IdP/NAF에 의해 선택된 TLS Ciphersuite를 확인한다. UE와 IdP/NAF가 안전하게 Bootstrapping 과정을 거쳤다면 일치된 세션키를 공유하고 있을 것이며, UE는 TLS 터널을 설정하기 위한 모든 필요한 데이터를 처리한다. 위의 과정을 통해 다음 접속에서는 Bootstrapping 과정을 실행하지 않고 곧바로 접근할 수 있다.
- **UE→IdP/NAF:** UE는 식별자로서 B-TID와 비밀값으로서 Ks_NAF를 Authorization Header에 포함하여 HTTP GET Authorization을 전송한다.
- **IdP/NAF→UE:** IdP는 Credential을 포함하여 HTTP Response를 전송한다. Credential은 추후에 인증을 위하여 전자HD카드에 포함된다.

7.3 개인정보보호 정책 수립 및 협상

기존 네트워크에서는 각각의 SP가 일방적으로 미리 설정한 개인정보보호 정책에 의해서만 사용자의 개인정보가 보호받을 수 있었다. 그러나 사용자가 주도적으로 자신의 개인정보를 관리하기 위해서는 사용자가 설정한 정책에 의해서 개인정보를 제공하고 관리할 수 있어야 한다. 또한 중요하거나 민감한 개인정보의 경우, SP는 사용자에게 동의를 구하는 과정을 거쳐서 사용자의 개인정보가 어떤 목적으로 사용되는지 알려야 한다. 그러므로 전자HD지갑은 사용자의 개인정보 노출 및 공유를 최소화하기 위해 보안정책을 설정하고 협상하는 과정을 제공한다. [표 1]은 개인정보의 중요도 및 민감도에 따른 보안레벨을 나타낸다. 사용자의 개인정보는 중요도 및 민감도에 따라 적절한 보안레벨로 분류되어 관리될 수 있어야 하며, 필요시마다 재설정 및 재협상 과정을 가질 수 있다. 이는 SP가 사용자의 민감한 정보를 과도하게 수집하지 않도록 예방하며 사용자가 개인정보에 대한 직접적인 관리 및 통제에 참여할 수 있도록 한다.

표 1. 보안레벨에 의한 개인정보의 분류
Table 1. The classification of Private Information by security levels

레벨	개인정보	특성
1	주민등록번호, 결제정보, 인증서, ID/PW 등	유출 즉시 심각한 피해가 발생할 수 있는 신상정보 및 인증정보
2	주소, 전화번호, 직장 등	즉각적인 피해 우려는 적지만 2차 범죄에 악용될 수 있는 신상정보
3	진료기록 등	추적은 불가능하지만 프라이버시 침해 가능성이 있는 비신상정보
4	취미, 종교, 관심분야 등	추적도 불가능하고 프라이버시 침해 가능성도 비교적 적은 비신상정보

7.4 전자ID카드 생성 및 검증

7.3의 협상과정이 완료되면 SP는 인증 및 개인정보 획득을 위하여 사용자에게 전자ID카드를 요청한다. 전자ID카드는 매번 새로 생성할 수도 있고 유효기간 내의 전자ID카드를 재사용하거나 추가적인 정보를 포함하여 재발급할 수도 있다. UE와 SP, IdP 사이의 통신은 TLS 상의 HTTP 프로토콜을 통해 이루어지며, Bootstrapping 과정에서 생성된 키 Ks_NAF를 사용하여 메시지 기밀성 및 무결성을 제공할 수 있다. 다음은 사용자가 전자ID카드를 생성하고 IdP가 검증하는 과정을 설명한다.

- **ME:** 사용자에게 전자ID카드 생성에 대한 동의 및 PIN 입력을 요청한다.
- **ME→전자ID지갑:** ME를 통하여 전자ID카드 생성 요청이 전달된다.
- **전자ID지갑→USIM:** 전자ID지갑은 UID를 생성하기 위한 IMSI 등 필요한 데이터를 얻기 위해 USIM에게 Command APDU Request를 전송한다.
- **USIM→전자ID지갑:** USIM은 요청받은 데이터를 Response APDU에 포함하여 전자ID지갑에게 전송한다.
- **전자ID지갑:** 전자ID지갑은 SP와 Negotiation 과정에서 협상한 정책에 따라 전자ID카드를 생성한다.
- **전자ID지갑→SP:** 생성한 전자ID카드를 SP에게 제출한다. 전자ID카드는 Ks_NAF로 암호화된다.
- **SP→IdP/NAF:** SP는 UE로부터 전송받은 HTTP Response로부터 전자ID카드를 추출하여 IdP에게 HTTP Request를 보낸다. 이 메시지는 전자ID카드에 대한 검증을 요청한다.
- **IdP/NAF→SP:** IdP는 요청에 대한 응답으로서 IdP의 서명이 포함된 전자ID카드를 SP에게 전송한다.
- **SP→UE:** SP는 전자ID카드에 사용된 IdP의 서명을 검증하여 메시지를 처리한다.

[그림 7]은 SP와 IdP가 전자ID카드에 대한 검증을 위해 주고 받는 요청 및 응답 메시지의 형식(a,b)과 전자ID카드의 데이터 형식(c)을 나타낸다. 증요청 메시지에서 RequestID는 메시지를 식별하기 위한 식별자이며, Version No.는 버전 정보이다. IssueInstant는 메시지가 생성된 시간이고, Consent와 Policy는 Negotiation 과정에서 사용자의 동의를 얻었는지의 여부와 어떤 정보를 공유하기로 했는지 등의 개인정보보호 정책 협상 내용을 포함한다. CipherSuite은 전자ID카드를 보호하기 위해 사용된 인증 및 암호 알고리즘 등의 보안 집합이며, SPID는 사용자가 서비스를 요청하는 SP의 ID이다. RequestAuthnContext는 SP가 요구하는 인증 수준을 나타낸다. 왜냐하면 모바일 응용 서비스에 따라 SP가 다른 인증 방식을 요구할 수도 있기 때문이다. 즉, 높은 보안성이 필요한 응용 서비스는 보안성이 높은 인증 방식을 요구한다. AuthnContextClassRef는 인증 방법을 나타내고, AuthnContextComparison은 인증 방법 비교를 나타낸다. 그리고 검증요청 메시지의 RelayState는 검증응답 메시지에서 재전공되기를 원하는 상태정보를 나타낸다.

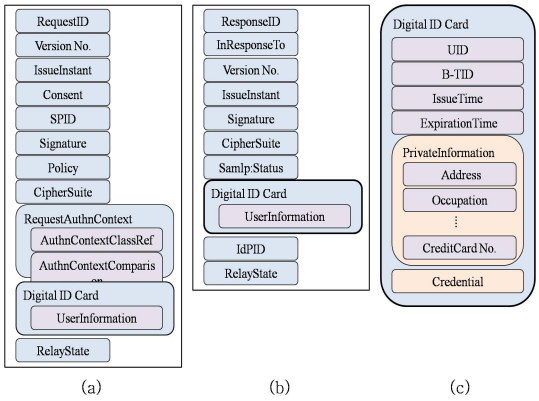

그림 7. 전자ID카드 검증요청 메시지(a) 및 검증응답 메시지(b)와 전자ID카드 데이터 형식(c)
Fig. 7. Verification Request Message(a) and Verification Response Message(b) for Digital ID Card, Data Type of Digital ID Card

검증응답 메시지도 검증요청 메시지처럼 식별자인 ResponseID와 Version No., IssueInstant 정보 등을 포함한다. 검증응답 메시지의 ResponseID는 응답 메시지임을 식별하기 위한 식별자로써 InResponseTo는 검증요청 메시지의 RequestID가 된다. IdPID는 사용자의 개인정보가 등록되어 있고 전자ID카드를 검증하는 IdP의 ID이다. 마지막으로, 검증응답 메시지의 RelayState는 검증요청 메시지의 RelayState가 된다.

7.5 전자ID지갑을 통한 단일 인증 로그온(Single Sign On)

단일 인증 로그온은 사용자가 IdP로부터 인증을 받은 뒤 SP를 이용할 때 유효한 인증 세션이 설정되어 있으면 추가적인 인증절차를 거치지 않고도 서비스를 받을 수 있도록 해준다. 이 때 사용자가 AKA 및 Bootstrapping을 통하여 이미 인증된 상태이면, 단순히 SP에게 전자ID카드를 제출하고 IdP에게 검증

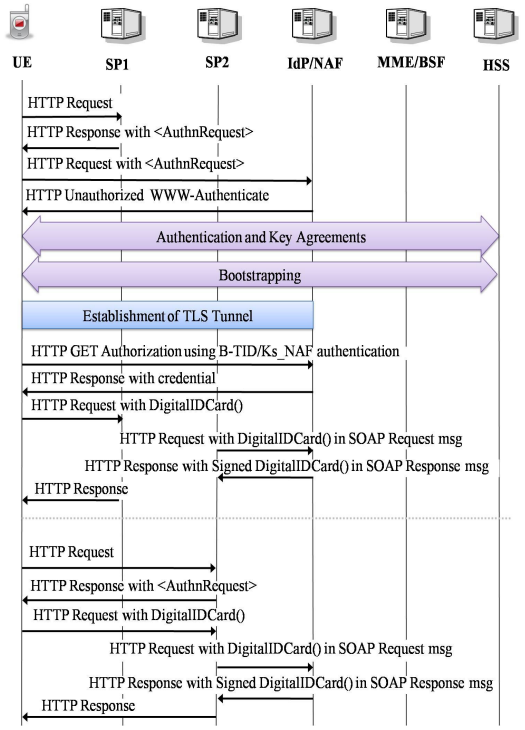

그림 8. 전자ID카드를 사용한 단일 인증 로그온 절차
Fig. 8. Sing Sign On using Digital ID Card

받음으로써 단일 인증 로그온을 수행할 수 있다. 예를 들어, 사용자가 전자ID지갑을 통해 전자HD카드를 제출하기만 하면 주민등록등본, 대학졸업증명서 및 성적증명서, 어학증명서, 경력증명서 등 각종 서류를 발급받기 위해 전자정부싸이트, 대학싸이트 등 모든 싸이트에 일일이 가입하고 인증받을 필요없이 한 번에 서류를 발급받을 수 있다.[16]

[그림 8]은 SP1을 이용하기 위해 IdP/BSF, HSS 등과 AKA 및 Bootstrapping 과정을 수행하고 전자ID카드로 사용자 인증을 받았던 사용자가 SP2를 이용하기 위해 단순히 전자HD카드를 제출함으로써 사용자 인증을 받는 간단한 단일 인증 로그온 절차를 나타낸다.

Ⅷ. 분 석

8.1 요구사항에 대한 분석

모바일 전자HD지갑은 4장에서 정의하였던 사용자 중심의 전자HD 기술이 만족해야 할 요구사항에 따라 설계되었다. 본 절에서는 각 요구사항에 대한 모바일 전자ID지갑의 분석 내용을 논의한다.

분석 1. 사용자는 자신의 개인정보를 USIM 카드에 저장하고 직접 소유함으로써 개인정보 통제권을 가진다. 사용자는 개인정보보호 정책 수립 및 협상 과정에 직접 참여하고 SP에게 제공할 개인정보 항목을 선택함으로써 개인정보 관리 및 통제의 주체가 된다.

분석 2. 전자HD지갑은 사용자 식별을 위하여 UID를 사용한다. UID는 HSS가 IMSI를 기반으로 생성하기 때문에 사용자를 유일하게 식별할 수 있다. 또한 사용자가 서비스 가입을 위해 ID/PW를 결정해야 하는 어려움을 해결한다. 각 서비스마다 다른 ID와 비밀번호는 관리가 어렵고, 편의를 위해 유일한 ID와 비밀번호를 사용하는 것은 보안상 위협을 초래하기 때문이다.

분석 3. 사용자는 개인정보보호 정책 수립 및 협상 과정에 참여함으로써 개인정보 노출 수준을 설정하고 SP의 과도한 개인정보 수집을 예방한다. 또한 사용자가 자신의 개인정보 항목과 내용을 직접 선택함으로써 개인정보 공유 과정에 사용자의 의견을 반영할 수 있다.

분석 4. 사용자 중심의 전자ID 관리 기술은 개인정보가 SP가 아닌 사용자의 데이터 저장소에 안전하게 저장될 것을 요구한다. 따라서 모바일 전자HD지갑은 사용자의 개인정보를 USIM 카드에 저장한다. USIM 카드는 스마트카드의 일종으로써 Tamper resistant한 성질을 가진다.[17] 사용자는 USIM 카드에 접근하기 위해 반드시 LTE/SAE-네트워크로부터 사용자 인증을 받아야 한다.

분석 5. SP는 사용자의 개인정보를 보유하지 않음으로써 개인정보를 안전하게 관리하기 위한 관리 비용 및 부담이 감소한다.

분석 6. 사용자는 Bootstrapping 과정에서 RAND 값과 BSF name을 이용하여 생성된 B-TID를 UID 대신 ID로 사용함으로써 익명성을 제공받을 수 있다. B-TID는 Bootstrapping 과정을 수행할 때마다 새로운 값으로 생성되며 Bootstrapping time만큼 유지된다. 익명성은 사용자의 선호도와 같은 프라이버시 관련 정보나 행동패턴 등이 노출되지 않도록 한다.

분석 7. 사용자는 원할 시 익명성을 제공받을 수 있어야 하지만, 한편으로 ID 도용 등을 대비하여 행적추적을 위한 로그도 기록되어야 한다. 그러나 프라이버시 보호를 위하여 로그파일은 SP가 아닌 사용자의 데이터 저장소인 USIM과 IdP에만 저장된다.

분석 8. 모바일 전자HD지갑은 이름, 주민번호, 주소, 전화번호 등과 같은 신상정보 및 PW, 인증서와 같은 인증정보(Credential) 뿐만 아니라 나이, 성별,

표 2. 관련 연구와의 장단점 비교
Table 2. Comparison between Digital ID Studiees

분류	전자ID 관련 프로젝트			전자ID 관련 기술		제안 기술
	FIDIS	PRIME	Shibboleth	OpenID	CardSpace	전자ID지갑
관리 유형	사용자 중심					
목적	전 유럽에서 통용 가능한 신원 관리 방식의 개발	프라이버시를 강화한 ID 관리 시스템의 개발	속성 기반의 식별 기술 및 인증시스템 개발	URL 기반의 식별 기술	인증 및 지불 프로그램	4G 이동통신에 적합한 개인정보 통제 강화 기술
장점 및 단점	기존 연구의 통합 및 다양한 관점에서의 요구사항을 도출한다.	구체적인 솔루션을 제안하지 못하고 있으며, 연구 분야가 너무 광범위하다. 특정 응용 시나리오에 대해서만 적용하고 있다.	공격자가 사용자의 모든 계정에 무제한으로 접근할 수 있는 위험이 있다. 인증 및 인가만 지원한다.	피싱, 신뢰성 문제, 사이트간 공모 등 아직 해결해야 할 보안위협이 남아있다.	Self-issued 카드에 한정적인 개인정보만 담을 수 있기 때문에 사용자별 개인화 서비스가 불가능하다.	USIM을 활용함으로써 모바일 단말기의 이동성에 의해 시간과 공간의 제약없이 개인정보 통제가 가능하다. 또한 다양한 서비스에 응용 가능하다.

취미, 종교, 각종 선호도와 같은 비신상정보도 전자ID카드에 자유롭게 포함시킴으로써 개인화 서비스를 제공받을 수 있다. 즉, 전자ID카드는 사용자 인증의 기능뿐만 아니라 개인정보 활용을 위한 수단으로써도 안전하게 사용될 수 있다. 모바일 전자ID지갑은 사용자의 성향에 따른 적절하고 효과적인 서비스에 이용됨으로써 사용자 참여 중심의 인터넷 환경에서 매우 유용하다.

분석 9. 기존의 온라인 네트워크에서는 개인정보의 변경 시, 사용자가 각 사이트를 방문하여 개인정보를 직접 수정해야 했다. 따라서 수 많은 사이트에 저장된 개인정보를 최신으로 유지하고 관리하기가 번거롭고 어려웠다. 따라서 모바일 전자ID지갑을 사용하여 SP마다 산재되어 있는 개인정보를 동기화할 수 있다. 즉, 전자ID지갑에 추가되거나 수정된 최신의 개인정보를 IdP에 반영함으로써 사용자는 개인정보의 동기화를 위하여 각 사이트를 직접 방문할 필요가 없다.

분석 10. 사용자가 전자ID지갑을 사용하기 전에 모바일 단말기, HSS, SP 및 IdP 등 네트워크 개체 간의 상호인증이 이루어진다. 모바일 전자ID지갑 시스템은 LTE/SAE 네트워크의 AKA 과정에서 공유된 키를 기반으로 LTE/SAE Bootstrapping을 수행하여 개체 간 상호인증 및 세션키 일치를 수행한다.

분석 11. 모바일 전자ID지갑에는 정당한 사용자만이 접근하고 사용할 수 있다. 공격자가 USIM을 획득하여 타 단말기에 장착하거나 단말기와 USIM을 모두 획득하여 정당한 사용자를 가장하는 경우, PIN을 입력받는 등 정당한 사용자임을 인증받아야 한다.

분석 12. 악의적인 공격자의 도청, 위장 공격, 메시지 위조공격, 피싱 공격, 재사용 공격 등으로부터 사용자의 개인정보를 보호하기 위하여 네트워크 개체 간의 통신은 TLS 상의 HTTP 프로토콜을 사용한다. 또한 Bootstrapping을 통하여 생성된 키 Ks_NAF를 사용하여 메시지를 암호화함으로써 기밀성 및 무결성을 제공한다.

[표 2]는 3장에서 살펴보았던 관련 연구들과 제안된 전자ID지갑의 장단점을 비교하여 나타낸 것이다. 전자ID지갑은 사용자 중심의 전자ID 관리를 위한 요구사항을 모두 충족시킴을 위에서 보였으며, 기존 전자ID 관리 기술들의 한계점을 보완하고 변화하는 네트워크 환경에서 사용자에게 보다 강화된 개인정보 관리 방안을 제공하기 위해 제안되었음을 모두 설명하였다.

[표 3]는 관련 기술들과 제안된 전자ID지갑의 효율성을 비교하였다. OpenID, CardSpace, 전자ID지갑 모두 사용자 중심의 ID 관리를 위한 기술이지만, 다음과 같은 차이가 있다. 첫째, OpenID는 OpenID 서버에 개인정보를 저장하는데 OpenID 서버는 사용자가 직접 운용할 수도 있고 OpenID 서비스 제공업체가 운용할 수도 있다. 그러나 OpenID 서버를 사용자가 운용하는 것은 번거롭고 어려운 일이며 OpenID 서비스 제공업체가 혼자 운용하는 것은 제 3자에게 전적으로 개인정보 관리를 위임하는 것이다. 전자ID지갑도 최초에 한 번은 IdP에 개인정보를 등록해야 하지만 전자ID지갑이 개인용 IdP의 역할을 하기 때문에 OpenID 서비스 제공업체의 서버 운용에 비해 신뢰도가 높다. CardSpace는 Window Vista 운영체제가 탑재된 PC에서만 사용 가능하기 때문에 제한

표 3. 전자ID 관련 기술과의 효율성 비교
Table 3. Comparison of proposed Digital ID Wallet system and existing systems

	OpenID	CardSpace	제안하는 전자ID지갑
개인정보 저장위치	OpenID 서버(IdP)	Window vista가 탑재된 PC 및 IdP	USIM 및 IdP
개인정보 관리의 주체	사용자	사용자	사용자
IdP 의존도	높음	높음	낮음
개인정보 관리	×	△	○
개인정보 통제	△	△	○
이동성	×	×	○

적이며 PC는 사용자가 아닌 제 3자도 접근이 가능하다. 반면에 전자ID지갑은 사용자만 접근 가능한 USIM에 개인정보를 저장하므로 휴대 및 접근이 용이하여 사용자 중심의 전자ID 관리에 더욱 적합하다. 둘째, OpenID 서버에 개인정보를 저장하는 OpenID는 평상 시에 개인정보를 관리하기 어려우며, CardSpace는 self-issued 카드에 포함되는 개인정보가 한정적이고 CardSpace가 본래 인증 및 지불을 위한 프로그램으로써 개인정보 관리에 대한 기능은 미약하기 때문에 개인정보 관리의 목적으로써는 제한적이다. 그러나 전자ID지갑은 사용자가 USIM이 탑재된 모바일 단말기를 소지하고만 있으면 서비스를 이용하지 않을 때에도 직접 개인정보를 관리할 수 있다. 셋째, OpenID는 서비스 이용 도중, SP로부터 e-mail과 같은 개인정보를 요청받으면 사용자가 전달여부를 결정할 수 있으며 CardSpace도 결제정보 중 어떤 정보를 전송할 것인지 사용자가 선택할 수 있다. 그러나 전자ID지갑은 위와 같은 개인정보 전송여부의 결정 뿐만 아니라 개인정보보호 정책 설정에도 직접 참여함으로써 보다 적극적이고 강력한 개인정보의 통제가 가능하다. 따라서 세 가지 기술 모두 신뢰할 수 있는 IdP의 관여가 필요하지만 전자ID지갑은 OpenID 및 CardSpace에 비해 IdP에 대한 의존도가 낮다. 마지막으로 전자ID지갑은 USIM을 개인정보의 저장소로 활용함으로써 언제 어디서나 사용이 가능하고 모바일 단말기를 통해 편리한 인터페이스를 제공받을 수 있을 뿐만 아니라 모바일 단말기를 통한 인터넷 접속이 급속도로 증가하는 현실정에 매우 유용하다.

8.2 안전성 분석

본 절에서는 가장 위협적인 도청 공격, 위장 공격, 재전송 공격, 메시지 위조 공격, 방향재설정 공격의 5가지 공격에 대한 전자ID지갑의 안전성을 논의한다.

8.2.1 도청 및 정보누출(Eavesdropping and Information leakage)

수동적인 공격자는 UE와 SP 사이의 통신을 도청하는 공격을 시도할 수 있다. 그러나 전자ID카드는 UE와 SP가 LTE/SAE Bootstrapping 과정을 통해 공유한 세션키로 암호화될 뿐만 아니라 모든 전자ID지갑 메시지는 TLS 터널 상에서 전송되므로 공격자는 전자ID지갑 프로토콜에서 어떠한 정보도 얻을 수 없다.

8.2.2 위장 공격(Impersonation attack)

위장 공격은 악의적인 공격자가 정당한 SP로 위장하여 사용자의 전자ID카드를 요구하거나, 정당한 UE로 위장하여 위조된 전자ID카드를 제출하는 능동적인 공격이다. 따라서 공격자는 정당한 참여자들과 세션키를 설정하려고 시도할 것이다. 그러나 공격자는 네트워크 비밀키 K를 가지고 있지 않으므로 AKA를 통해 HSS로부터 인증을 받을 수 없고 LTE / SAE Bootstrapping에도 참여할 수 없다. 따라서 공격자는 정당한 UE에게 전자ID카드 요청 메시지를 보내거나 SP에게 암호화된 전자ID카드를 보낼 수 없다. 따라서 위장 공격은 불가능하다.

8.2.3 재전송 공격(Replay attack)

악의적인 공격자는 UE와 SP 사이의 전송 메시지들을 도청하여 저장해두었다가 다음 세션에서 재전송하는 능동적인 공격을 할 수 있다. 그러나 Bootstrapping에서 인증 응답 메시지에 Bootstrap time과 Key lifetime이 포함되기 때문에 재전송 공격은 불가능하다. 또한 모든 메시지에는 메시지 생성시간이 포함된다.

8.2.4 메시지 위조 공격(Message forgery attack)

공격자는 임의로 USIM에 접근하여 저장된 정보를 읽을 수 없다. 즉, 전자ID카드를 생성하거나 사용하기 위해서는 PIN 번호 등 접근제어를 위한 인증과정을 거친 후 LTE/SAE Bootstrapping 을 통하여 세션

키 Ks_NAF를 가져야 한다. 또한 전자HD카드의 위조가 성공하더라도 IdP에 의한 검증 과정에서 IdP에 저장된 정보와 불일치하므로 메시지 위조 공격은 실패한다.

8.2.5 방향재설정 공격(Redirections attack)

방향재설정 공격은 공격자가 SP로 전송되는 전자ID카드를 가로챈 다음, UE에게 악의적인 SP로 접속하도록 방향을 재설정하는 공격이다. 그리고 악의적인 SP는 가로챈 전자HD카드를 IdP에게 제출하여 검증을 요청할 것이다. 그러나 전자HD카드 검증요청 메시지에 SP의 서명이 포함되므로 IdP가 악의적인 SP를 탐지할 수 있다.

Ⅸ. 결 론

최근 대형 포탈싸이트 및 쇼핑싸이트에서 연이어 발생한 개인정보 유출 사건이 심각한 사회 문제로 대두되었다. 일부 SP들이 서비스 가입을 통해 수집한 사용자들의 개인정보를 가입자 몰래 재판매하는 등의 악행으로 부가적인 수입을 얻고 있었음이 밝혀졌으며, 이를 규제할 법률이 미비함이 드러났다. 더구나 모바일 단말기를 통한 무선 인터넷의 이용이 급증하고 있기 때문에 하루빨리 변화하는 네트워크에 적합한 전자ID 관리 기술의 도입이 필요하다. 그러므로 이와 같은 문제를 해결하기 위하여 모바일 전자ID지갑과 같은 신뢰할 수 있는 전자HD 관리 서비스를 통해 개인정보를 관리하는 것이 사용자와 SP 모두에게 이익이 될 것이다.

본 논문에서는 4G LTE/SAE 환경에 적합한 사용자 중심의 전자ID 관리 방안을 제공하기 위하여 모바일 전자HD지갑 시스템을 정의한 후, 모바일 응용서비스를 위하여 상호인증 및 키 일치를 위한 LTE/SAE Bootstrapping과 모바일 전자HD지갑 메커니즘을 제안하였다. 제안된 LTE/SAE Bootstrapping은 LTE/SAE 네트워크 개체들 간의 상호인증을 제공함으로써 신뢰성을 높였으며, 공유된 세션키는 모바일 전자ID지갑 메커니즘에서 기밀성 및 무결성을 제공하기 위해 사용되었다. 그리고 사용자 중심의 전자HD 관리를 위한 요구사항을 정의하고 모바일 전자HD지갑이 각 요구사항을 만족하도록 설계하였다. 다시 말하면, 전자HD지갑은 USIM을 개인정보의 저장소로 활용함으로써 사용자가 시간과 공간의 제약없이 자신의 개인정보를 관리할 수 있도록 하였으며 기존의 사용자 중심의 전자ID 관리 기술보다 개인정보 통제 기능을 강화시키고 IdP에 대한 의존도를 낮추었다. 또한 사용자가 직접 설정한 개인정보보호 정책에 따라 개인정보를 관리할 수 있도록 하였다. 마지막으로, 모바일 전자ID지갑이 도청 및 정보누출, 위장 공격, 재전송 공격, 메시지 위조 공격, 방향재설정 공격 등으로부터 안전함도 증명하였다.

다가오는 4G 환경은 다양한 네트워크가 융합된 통합 네트워크로서 사용자의 참여를 요구하고 사용자별 맞춤 서비스를 제공하는 환경이 될 것으로 예측된다. 따라서 향후에는 전자ID지갑의 활용도를 높이고 사용자에게 최대한의 편의성을 제공하기 위하여 사용자 참여 중심의 다양하고 유용한 서비스도 함께 개발되어야 할 것이다. 또한 개인정보 관리의 중요성에 대한 인식 개선 및 강화된 법률 제정이 반드시 뒷받침되어야 할 것이다.

참 고 문 헌

〔1〕 조영섭, 진승헌, "Digital Identity 관리 기술 현황 및 전망", *한국전자통신연구소*, 전자통신동향분석, 제22권 제1호, 2007.

〔2〕 조영섭, 진승헌, "인터넷 ID 관리 시스템 개요 및 비교", *한국전자통신연구소*, 전자통신동향분석, 제22권 제3호, 2007.

〔3〕 A. Josang, S. Pope, "User Centric Identity Management," *AusCERT Conference 2005*, 2005.

〔4〕 정책개발단 기술정책팀, "웹 2.0과 아이디 관리", *한국정보보호진흥원*, 월간 정보보호뉴스, Vol.119, 2007.

〔5〕 FIDIS, "Future of Identity in the Information Society," http://fidis.net.

〔6〕 PRIME. "Privacy and Identity Management for Europe," http://www.prime-project.eu.org.

〔7〕 S. Carmody, "Shibboleth Overview and Requirements," http://shibboleth.internet2.edu, 2001

〔8〕 김승현, 진승헌, "오픈소스 ID관리 프로젝트 동향" *IITA기술정책정보단*, 동향분석자료, 2007.

〔9〕 OpenID, http://openid.org.

〔10〕 CardSpace, http://msdn2.microsoft.com/en-us/library/aa480189.aspx.

〔11〕 A. Jøsang, J. Fabre, B. Hay, "Trust Requirements in Identity Management," *Australasian Information Security Workshop*, 2005.

〔12〕 3GPP TR 33.821, "Rationale and track of security decisions in Long Term Evolved(LTE) RAN

/ 3GPP System Architecture Evolution(SAE)," Release 8, 2007.
〔13〕 3GPP TS 33.102, "3G Security; Security architecture," Release 7, 2006.
〔14〕 3GPP TR 33.980, "Liberty Alliance and 3GPP security interworking; ID-FF, ID-WSF and GAA," Release 7, 2007.
〔15〕 3GPP TS 31.102, "Characteristics of the Universal Subscriber Identity Module(USIM) application," Release 8, 2008.
〔16〕 조상래, "Present and Future Trends of Digital Identity in Korea," *한국전자통신연구원*, Workshop on "Digital Identity for NGN, 2006.
〔17〕 O. Benoit, N. Dabbous, "Mobile Terminal Security," *Cryptology ePrint Archive*, 2004.

정 윤 선 (Yunseon Jung) 준회원

2006년 8월 고려대학교 컴퓨터정보학과 학사
2008년 8월 고려대학교 정보경영공학전문대학원 석사
<관심분야> 무선통신, 정보보호, 3G, USIM, ID관리

임 선 희 (Sun-Hee Lim) 정회원

1999년 2월 고려대학교 컴퓨터학과 학사
2005년 2월 고려대학교 정보보호대학원 석사
2007년 2월 고려대학교 정보경영공학전문대학원 박사과정 수료
<관심분야> 무선통신, 정보보호

이 옥 연 (Okyeon Yi) 정회원

1988년 2월 고려대학교 수학과 학사
1990년 2월 고려대학교 수학과 석사
1996년 8월 University of Kentucky 수학과 박사
1999년~2001년 한국전자통신연구원 선임연구원, 팀장
2001년~현재 국민대학교 수학과 부교수
<관심분야> 정보보호, 이동통신, 암호, 컴퓨터보안

이 상 진 (Sangjin Lee) 정회원

1987년 2월 고려대학교 수학과 학사
1989년 2월 고려대학교 수학과 석사
1994년 2월 고려대학교 수학과 박사
1989년 2월~1999년 2월 한국 전자통신연구원 선임 연구원
1999년 2월~2001년 8월 고려대학교 자연과학대학 조교수
2001년 9월~현재 고려대학교 정보경영공학전문대학원 교수
<관심분야> 대칭키 암호, 정보은닉이론, 컴퓨터 포렌식