情 報 保 護 學 會 誌
第21卷 第4號, 2011. 6

ID 관리 기술 및 시장 동향

조 영 섭*, 김 수 형*, 진 승 헌*

요 약

인터넷의 활용이 커짐에 따라 사용자의 식별자와 개인정보를 안전하고 편리하게 관리하는 ID 관리 기술이 필수 기술이 되고 있다. 최근 개인정보의 유출 및 해킹 사고가 국내외적으로 빈번하게 발생함에 이를 방지하기 위한 ID 관리 기술에 대한 필요성이 더욱 커지고 있다. 본 고에서는 ID 관리 기술에 대한 연구 동향을 살펴보고 ID 관리 시장에 대한 국내외 동향에 대하여 기술한다. 또한 최근 스마트폰의 확산에 따라 이슈화되고 있는 모바일 ID 관리 기술에 대하여 기술한다.

Ⅰ. 서 론

온라인 상거래, 소셜 네트워크 서비스 등 다양한 서비스를 사용하기 위해서, 사용자들은 자신을 식별할 수 있는 식별자(id, identifier)와 패스워드 등과 같은 인증정보를 등록한다. 최근 사용자가 이용하는 서비스가 다양해짐에 따라 각 서비스에서 사용하는 사용자 id와 인증정보의 수가 많아지고 이에 따라 사용자가 이러한 정보를 직접 관리하는 것이 매우 어렵게 되었다. 또한 인터넷에서 다양한 사용자 개인정보가 관리됨에 따라, 개인정보 오·남용으로 인한 피해가 증가하고 있다. 국내 조사에 의하면 일반 인터넷 이용자들이 느끼는 개인정보에 대한 불안감이 매우 커 이를 비용으로 환산하면, 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고 있다고 한다[1]. 특히, 최근 옥션, 신세계 백화점 해킹에서부터 현대캐피탈 해킹, 농협 전산장애, 소니의 해킹 등과 같이 국내외에서 지속적으로 보안 문제가 발생함에 따라 사용자들의 개인정보 보호에 대한 불안과 인식이 높아지고 있다. 따라서 사용자의 식별자, 인증정보, 신상정보, 선호도 등으로 구성된 ID(Identity)를 편리하고 안전하게 생성, 변경, 유통, 폐기하는 기술인 ID 관리 기술이 매우 중요해지고 있다.

ID 관리 시스템은 ID 관리를 서비스별로 독립적으로 수행하는 사일로(silo) ID 관리 모델로부터 진화하여, Microsoft의 .net Passport와 같이 특정 사이트에 등록된 ID 정보를 관리하는 중앙집중형(centralized) ID 관리 모델과 Liberty Alliance와 같이 연합된 사이트들 간에 ID 정보를 필요에 따라 공유하는 연합 ID 관리 모델로 발전하였다. 최근에는 ID 관리 시스템을 Invisible, Card-based, URL-based ID 관리 시스템으로 분류하고 있다[2]. Invisible ID 관리 시스템은 ID 정보 흐름이 사용자에게 인지되지 않는다는 특징을 가지고 있으며 SAML에 기반한 ID 관리 시스템이 이에 해당한다. Card-based ID 관리 시스템은 인증 및 ID 정보가 요구될 때마다, 요구 조건을 만족시키는 ID 정보를 카드 형태로 표현하여 사용자가 선택할 수 있도록 한다. WS-* 표준을 기반으로 Microsoft 윈도우에 포함된 CardSpace와 Eclipse에서 제공하는 Higgins가 대표적이다. URL-based ID 관리 시스템은 인터넷 사용자에게 가장 일반적이며 친숙한 URL 형태로 사용자 식별자를 제공하여 인증 및 ID 정보를 제공할 수 있도록 하는 특징을 가진다. OpenID가 이 유형에 속한다. 최근에는 스마트폰의 확산에 따라, 모바일 디바이스 상에서 사용자의 ID를 관리하는 모바일 ID 관리 기술에 대한 연구가 시작되고 있다.

본 고에서는 ID 관리 기술 및 시장 동향에 대하여 기술한다. 2장에서 ID 관리 기술의 국내외 연구 동향에 대하여 기술한다. 3장에서 국내외 ID 관리 시장에 대하여 기술한다. 4장에서 최근 연구가 시작되고 있는 모바일 ID 관리 기술에 대하여 기술하고 마지막으로 5장에서 결론을 맺는다.

* 한국전자통신연구원 인증기술연구팀 (yscho, lifewsky, jinsh@etri.re.kr)

Ⅱ. ID 관리 기술 동향

2.1 국내 ID 관리 기술

2.1.1 아이핀

방송통신위원회가 추진하고 있는 아이핀(i-PIN, Internet Personal Identification Number)은 대면 확인이 불가능한 인터넷 상에서 주민등록번호를 대신하여 본인임을 확인받을 수 있는 개인 식별 정보이다. 아이핀은 13자리 숫자나 영문자로 구성되며, 주민등록번호와 달리 생년월일, 출생지, 성별 등의 개인정보를 포함하지 않는다. 아이핀 발급을 위한 신원확인 방법으로는 대면확인, 공인인증서, 신용카드 정보, 휴대폰 SMS 등이 이용되고 있다[3].

사용자에게 아이핀을 발급하는 본인확인기관은 공공부분의 경우 행정안전부가 맡고 있으며, 민간 부분에는 5개의 기관이 있다. 2009년 12월 현재 3,607개 기관에 1,667,394건의 발급 건수를 기록하고 있다[4]. 특히, 2008년 6월 개정되어 2009년 1월 시행령이 공표된 정보통신망법에서 일평균 이용자 수가 5만 명이 넘는 포털 사이트, 1만 명이 넘는 일반 웹사이트에 대해서는 주민등록번호를 이용하지 않고 회원에 가입할 수 있는 수단을 의무적으로 제공해야 함을 규정하고 있어, 아이핀 도입 사이트의 수는 향후 급속히 증가할 것으로 예상된다.

아이핀은 주민등록번호 유출 위험을 최소화 하려는 목적에만 중점을 두어 실제 도입하려는 웹사이트의 내부 업무처리의 용이성이나 개인 이용자의 사용 편리성에 대한 고려가 부족한 문제를 가지고 있었다. 이와 같은 문제를 해결하기 위해, 웹사이트간 동일인 식별, 아이핀 발급기관 자동 식별, 해외거주 국민의 아이핀 발급 등이 가능한 아이핀 2.0 서비스가 개발되어 2009년 7월부터 보급 중에 있다.

2.1.2 전자ID지갑

전자ID지갑은 일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버 지갑으로 사용자의 주소, 전화번호 등과 같은 개인정보, 로그인 아이디, 비밀번호, 인증서 등과 같은 인증정보와 신용카드 등과 같은 정보를 관리한다[5]. 사용자가 인터넷 웹 사이트에서 서비스를 제공 받으면서 웹 사이트가 사용자 인증, 개인정보, 결제 정보 등을 요구하면, 자신의 전자ID지갑에서 필요한 정보를 확인하여 웹 사이트에 제공하는 방식으로 운용된다.

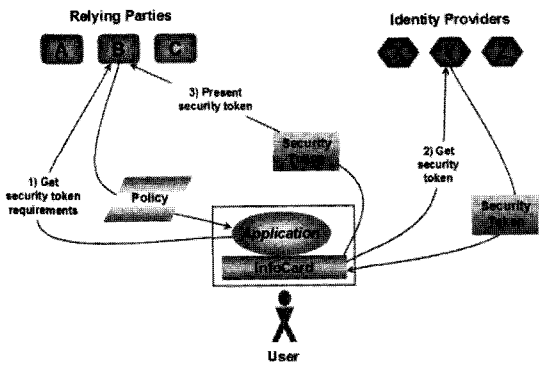
전자ID지갑은 웹 사이트 가입 및 로그인 기능, 사용자의 정보를 웹 사이트에 제공하거나 다른 웹 사이트에서 생성된 정보를 전달하는 ID 공유 기능, 사용자가 웹 사이트에서 이용한 서비스 및 물품 구입 대금을 결제하는 지불 기능 등을 제공한다.

2.2 국외 기술 동향

2.2.1 Windows CardSpace

Windows CardSpace는 다양한 ID 관리 시스템을 지원하고, ID에 대한 일관성 있는 사용자 통제가 가능하며, 패스워드 기반 웹 로그인을 대체하려는 목적으로 Microsoft에서 만든 identity selector이다[6]. Windows CardSpace .NET Framework 3.0 이상에서 동작하며 Windows Vista와 Windows 7에 포함되어 있다.

Windows CardSpace에는 사용자, ID 제공자(IP, Identity Provider), 서비스 제공자(RP, Relying Party) 역할이 존재한다. 사용자는 ID와 연관된 엔티티로 사용자, 조직, 응용, 프로그램 등이 이에 해당된다. ID 제공자는 사용자에게 ID를 부여하고 제공하는 엔티티이다. 서비스 제공자는 사용자에게 직접적인 서비스를 제공하는 엔티티로, 사용자를 인증하거나 사용자의 접근을 인가하기 위해 ID 제공자가 제공하는 사용자 ID를 의지하는 어플리케이션이다. [그림 1]은 Windows CardSpace에서 사용자, IP, RP 사이의 상호작용의 예를 보인다.

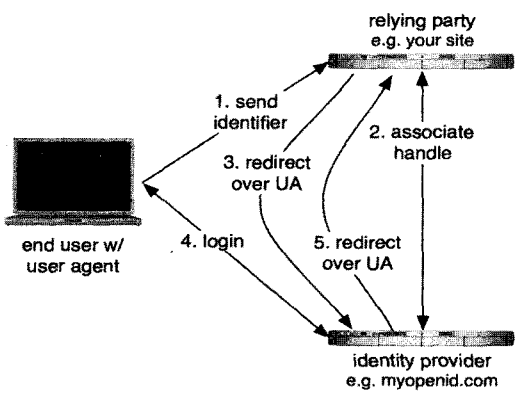


〔그림 1〕 CardSpace 상호 작용

[그림 1]에서 사용자는 먼저 서비스 제공자에게 자신이 사용할 서비스를 요청한다. 서비스 제공자는 사용자를 인증하기 위해 Windows CardSpace를 구동시킬 수 있는 태그를 가지고 있는 로그인 페이지를 사용자 브라우저에 반환한다. 사용자 브라우저는 서비스 제공자가 반환한 응답에 포함된 태그 정보를 확인하여 서비스 제공자가 요구하는 사용자 ID 정보를 확인하고 이 정보를 제공하는 ID Card들이 포함된 화면을 사용자에게 출력한다. 사용자는 화면에서 적절한 ID Card를 선택하고, 선택된 ID Card에 대응되는 ID 제공자에게 해당 ID 정보를 요청하게 된다. ID 제공자는 요청한 사용자 ID를 Windows CardSpace에게 전달하고 Windows CardSpace는 이 정보를 서비스 제공자에게 전달하게 된다. 서비스 제공자는 이 정보를 바탕으로 사용자에게 서비스를 제공할 것인지 여부를 판단한다.

2.2.2 OpenID

OpenID는 사용자들이 웹에서 쉽게 로그인할 수 있도록 해 주는 분산형 인증 프로토콜이다[7]. OpenID는 웹 블로그에 주석을 달 때, 별도의 id와 패스워드를 요구하지 않고, 주석자의 블로그 URI만 제출하면 주석을 달 수 있도록 하는데서 출발하였다. OpenID는 사용자 식별자로 사용자에게 친숙한 URI를 사용하는 등 사용자 편의성 확대에 초점을 맞추었다. [그림 2]는 OpenID에서 사용자, ID 제공자, 서비스 제공자의 상호작용 흐름을 보인다.



[그림 2] OpenID 동작 흐름도

사용자가 서비스 제공자에게 서비스를 요청하면서 OpenID 상호작용이 시작된다. 만약 서비스 제공자에서 사용자가 인증되지 않은 상태이면, 서비스 제공자는 사용자에게 사용자 식별자를 요청한다. 사용자는 자신의 사용자 식별자를 서비스 제공자에게 제공한다. 서비스 제공자는 사용자 식별자를 이용하여 ID 제공자를 확인한다. 서비스 제공자는 ID 제공자와 associate 과정을 거쳐 세션, 암호 키 등과 같은 공유 암호를 설정한다. 이후 서비스 제공자는 사용자 브라우저를 경유하여 ID 제공자에게 사용자 인증을 요청한다. ID 제공자는 사용자가 인증되지 않은 상태이면 사용자에게 패스워드 또는 인증서를 요청하여 인증한다. ID 제공자는 사용자의 인증 상태를 사용자 브라우저를 경유하여 서비스 제공자에게 전달한다. 이를 통해 서비스 제공자는 사용자 인증 사실을 확인하고 사용자에게 자신의 서비스 제공 여부를 결정한다.

현재 OpenID Authentication 2.0과 OpenID Attribute Exchange 1.0, OpenID Provider Authentication Policy Extension 1.0 등의 규격이 제정된 상태이다. OpenID는 사용자의 참여, 공유가 필수적인 웹 2.0 환경에서 많이 쓰이고 있다.

2.2.3 기타 ID 관리 기술

Higgins[8]는 2004년 Eclipse 재단에서 Eclipse Trust Framework라는 이름으로 시작되었으며, 2006년부터 IBM, Novell, Google, Microsoft 등이 참여하는 오픈소스 아이덴터티 프레임워크 프로젝트이다. Higgins는 다양한 사이트, 어플리케이션, 디바이스에 흩어져 있는 id, 프로파일, 소셜 관계 정보를 통합 제공하는 인터넷 ID 프레임워크를 지향한다. Higgins는 WS-Federation, WS-Trust, SAML, LDAP, Windows CardSpace 등과 같은 모든 주요한 ID 프로토콜과 함께 동작하면서 사용자에게 일관된 경험을 제공하는 소프트웨어 기반구조이다.

OSIS(Open-Source Identity System)은 서로 다른 다양한 ID 관리 기술 관련 프로젝트들의 상호호환성을 제공하기 위해 2006에 결성되었다[9]. OSIS에서 선언한 목적은 새롭게 등장하는 프로토콜, 프로젝트 회사들을 조정하여 중복되는 부분을 회피하고 기반구조가 상호호환되도록 하는 것이다. 현재 OSIS는 InformationCards와 OpenID이 상호호환되도록 하는 것에 초점을 맞추고 있다.

Ⅲ. ID 관리 시장 동향

3.1 국내 시장 동향

한국IDC의 2010년 조사에 따르면, 국내 ID 관리 및 접근제어 시장이 2010년 382억 원 규모에서 연평균 6.7%의 성장을 보이며 2014년 497억 원 규모의 시장으로 성장할 것으로 전망하고 있다[10].

〔표 1〕 ID 관리 및 접근제어 국내 시장 규모

(단위 : 백만원)

2010	2011	2012	2013	2014	평균 성장률
38,247	40,847	43,666	46,679	49,713	6.7%

국내 업체 중 소프트포럼은 SAML 기반의 ID 관리 솔루션인 XecureEID와 계정통합관리 솔루션인 TOUCHEN wiseaccess 제품군을 출시하고 있다. 기본적으로 SSO, 보안정책에 따른 다중 인증방식을 지원하며, 개발자 API 등을 제공하고 있다.

이니텍은 기업의 분산된 자원과 사용자에 대한 통합을 통해 일관된 관리체계를 제공하는 EAM (Enterprise Access Management) 솔루션인 INISAFE NEXESS를 출시하고 있다. 이 솔루션은 id/pw, PKI, 지문인식, OTP(One-Time Password), MOTP(Mobile OTP), Smart Card 등 다양한 인증 방식뿐만 아니라 다중 도메인에서 안전한 SSO 기능을 제공하며 RBAC 기반의 권한 관리 기능을 제공한다.

드림시큐리티는 id/pw, 인증서, 생체인식, cd-key 등과 같은 다양한 인증방식을 지원하며 인증 단계에 따른 권한을 선택적으로 부여하는 SSO 솔루션인 Magic SSO & EAM v3.0 제품을 출시하고 있다. 이 제품은 정보보호 업무의 생산성 및 효율성 증대의 방안으로 SSO와 사용자 인증을 관리하고 어플리케이션이나 데이터에 대한 사용자 접근을 결정하는 비즈니스 규칙(policy)을 구현하는 단일화된 메커니즘을 제공한다.

KSign은 SSO, 권한관리 및 계정 관리를 제공하는 KSignAccess 솔루션을 출시하고 있다. KSignAccess는 단일인증, 권한관리, 계정 관리 기능에 특화된 제품 솔루션인 KSignAccess for SSO, KSignAccess for EAM, KSignAccess for IAM으로 분류된다. 또한 기존 어플리케이션의 수정 없이도 단일 로그인으로 모든 응용프로그램에 접근할 수 있도록 해 주는 KSignPassOne을 출시하고 있다.

비티웍스는 ID 관리 솔루션으로 BTM-IDMS와 FederationWorks를 출시하고 있다. BTM-IDMS는 일괄적인 ID 관리, 카드 형태의 Identity Selector, ID Federation Bridge를 통한 신뢰 영역간 ID 연계 기능 등을 제공하며 FederationWorks는 기존 인증 체계나 DB 변경 없이 외부 서비스와 안전한 SSO를 제공한다.

이외에도 펜타시큐리티시스템은 SSO 기능을 기본적으로 제공하면서 통합 권한 관리 기능을 제공하는 EAM 솔루션인 ISign을 출시하고 있다. 티맥스소프트는 인터넷상에서 SSO 기능을 제공하는 SysKeeper SSO와 기업에게 EAM 기능을 제공하는 SysKeeper EAM 솔루션을 출시하고 있다. 알툴즈(ALTools) 사는 많은 웹사이트에서 사용자가 등록하고 있는 id와 비밀번호를 관리할 수 있는 프로그램인 알패스를 출시하고 있다.

3.2 국외 시장 동향

IDC의 2010년 3월 조사에 따르면, 전 세계적으로 모바일을 포함한 ID 관리 및 접근제어 시장 규모는 2009년 3,481백만 달러에서 연평균 8.0%의 성장을 보이며 2014년에 5,121백만 달러에 이를 것으로 전망하고 있다[11].

〔표 2〕 ID 관리 및 접근제어 국외 시장 규모

(단위 : 백만불)

2009	2010	2011	2012	2014	평균 성장률
3,481	3,775	4,090	4,402	5,121	8.0%

IBM은 2009년 ID 관리 및 접근제어 시장의 선두주자이다. IBM은 기업용 ID 제품군으로 TIM(Tivoli Identity Manager)와 TAM(Tivoli Access Manager), RACF(Resource Access Control Facility)을 출시하고 있으며 이들 제품은 PC, 유닉스, 메인프레임 등 다양한 플랫폼과 OS에서 운용된다.

EMC는 RSA Security를 합병함으로써 ID 관리 및 접근제어 시장 업계의 2위 자리를 차지하였다. OTP 토

큰 제품인 SecurID와 다양한 PKI 개발 역사를 가지고 있는 RSA는 다양한 ID 관리 및 접근제어 제품을 제공하고 있다. RSA FIM(Federated Identity Manager)는 XML, SOAP, SAML 2.0 등의 최신 웹 서비스 표준을 준용하여 다른 시스템들과의 호환성을 확보하고 있으며, RSA Access Manager는 웹 SSO를 제공한다.

CA는 웹에서부터 메인프레임에 이르기까지 다양한 ID 관리 및 접근제어 제품군을 제공한다. CA Identity Manager를 비롯하여 CA Access Control, CA SiteMinder, CA Federation Manager, CA Role & Compliance Manager 등 다양한 솔루션을 보유한다.

Oracle은 2009년 Sun 사를 합병하면서 기존 Oracle의 ID 관리 및 접근제어 제품군에 Sun의 제품을 추가하게 되었다. Oracle의 ID 관리 및 접근제어 제품군에는 Oracle Identity & Access Management Suite Plus, Oracle Access Management Suite Plus 등이 있다. 기존 Sun 사의 ID 관리 및 접근제어 제품은 주로 자바 플랫폼 스택에 병합되어 있기 때문에 아직 Oracle의 제품군에는 큰 영향을 미치고 있지는 않은 상황이다.

Microsoft는 ID 관리 및 접근제어 시장의 중추적인 업체로 인식되고 있다. ILM(Identity Lifecycle Manager) 2007은 메타 디렉토리, 인증서 및 스마트카드 관리, 사용자 provisioning 기능을 제공한다. 최근 출시된 ILM 2는 사용자의 편의성을 강화한 것으로 정책 관리, 크리덴셜 관리, 사용자 관리, 그룹 관리 기능을 제공한다. 또한 Microsoft는 기존의 .net Passport에서의 독점적인 중앙 관리에서 벗어나 여러 ID 제공자의 다양한 ID 기술들을 상호 운용하는 ID 메타시스템 개념을 제안하고, 이 개념을 Windows CardSpace로 구현하였다.

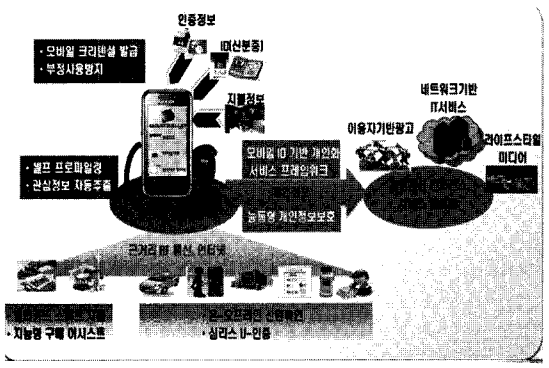
Ⅳ. 모바일 단말 ID 관리 기술

스마트폰의 급격한 활성화에 따라, 모바일 단말에서 사용자의 ID를 관리하는 모바일 ID 관리 기술에 대한 연구가 활발히 이루어지고 있으며 이에 따라 모바일 단말에서 운용되는 다양한 모바일 ID 관리 제품이 출시되고 있다.

현재 스마트폰 상의 대부분의 모바일 ID 관리 관련 제품은 모바일 단말 및 앱에 대한 접근 관리, 은행 계좌, 패스워드, 웹 계정, 신상 정보 등과 같은 개인 정보의 안전한 저장 기능 및 관리하는 개인 데이터에 대한 안전한 백업 및 복구 기능을 제공하고 있다. 안드로이드 앱인 Pocket은 사용자의 은행계좌와 패스워드와 같은 민감한 데이터를 안전하게 저장하는 기능을 제공한다. 기본적으로 다양한 정보를 암호화하여 저장하고 있으며, 일정 시간 후 self-lock 기능, 관리하는 모든 데이터를 DropBox 계정으로 백업하는 기능 등을 제공한다. 안드로이드 앱인 BioWallet Signature는 사용자 필체를 인식하여 앱에 대한 접근을 제어하는 기능을 제공한다.

모바일 ID 관리 제품으로는 현실상의 실제 지갑처럼 사용자의 신분증, 신용카드, 쿠폰, 상품권 등을 통합하여 관리하는 모바일 ID 관리 제품들이 출시되고 있다. 대표적인 제품으로는 Smart Wallet[12]이 있다. Smart Wallet은 휴대폰 하나로 다양한 멤버십 카드 적립, 조회, 사용, 지불 결제, 쿠폰과 상품권의 수신 및 사용을 가능하게 해 주는 모바일 지갑 기능을 제공한다.

또한 모바일 ID 관리뿐만 아니라, 모바일 단말에 축적되는 개인 정보를 기반으로 개인화 서비스를 제공하는 기술에 대한 연구도 진행되고 있으며 대표적인 것으로는 ETRI에서 연구 및 개발 중인 스마트지갑이다[13]. 스마트지갑은 모바일 단말에서 사용되는 모바일 ID의 보안 및 프라이버시 보호와 모바일 ID를 활용한 고부가 서비스 기반을 제공하는 퍼스널 모바일 ID 플랫폼이다. [그림 3]은 스마트지갑 서비스 개념도이다.



〔그림 3〕 스마트지갑 개념도

스마트지갑은 모바일 ID를 모바일 단말에 발급받아 안전하게 저장 관리하며 이를 통해 인증, 신원확인, 지불에 사용하고, 이 과정을 통해 발생한 개인정보를 통해 프라이버시가 침해되지 않는 개인화 서비스를 제공한다.

Ⅴ. 결 론

본 고에서는 사용자의 ID를 편리하고 안전하게 생성,

변경, 유통, 폐기하는 기술인 ID 관리 기술 및 시장 동향에 대하여 기술하였다. ID 관리 기술의 경우, 국내에서는 아이핀, 전자ID지갑 등의 기술이 개발되었으며, 국외에서는 Windows CardSpace, OpenID, Higgins 등의 기술이 개발되었다. ID 관리 시장의 경우, 국내외적으로 꾸준히 성장할 것으로 예상되었다. 또한 본 고에서는 최근 활발히 연구 개발되고 있는 모바일 ID 관리 기술에 대하여 살펴보았다.

향후 ID 관리 기술은 기존의 ID 관리 시스템인 Invisible, Card-based 및 URL-based ID 시스템이 독립적으로 발전하면서도 상호 융합을 통해 서로 간의 장점을 흡수하는 방향으로 발전할 것으로 보인다. 또한 모바일 라이프의 일상화에 따라 모바일 ID 관리 기술이 발전할 것으로 보인다.

참고문헌

[1] 한국인터넷진흥원, "개인정보의 경제적 가치 연간 약 1조 3천억원에 달해," 2007.1

[2] Johannes Ernst, "Updating The Identity Landscape of 2006," http://netmesh.info/jernst/Digital_Identity/updating-three-standards.html

[3] 한국인터넷진흥원, i-PIN 2.0 안내 & 구축 사례 소개, 2010.2

[4] 한국인터넷진흥원, 개인정보보호와 i-PIN, 2007.3

[5] 한국전자통신연구원, Digital Identity Management - 2009년 기술 백서, 한국전자통신연구원 인증기술연구팀, 2009.11

[6] Microsoft, "Introducing Windows CardSpace," http://msdn.microsoft.com/en-us/library/aa480189.aspx

[7] OpenID, http://openid.net/developers/

[8] Higgins open source identity management project, http://www.eclipse.org/higgins

[9] OSIS: Open Source Identity Systems, http://osis.idcommons.net/wiki/Main_Page

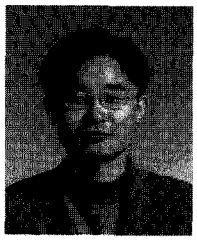
[10] 한국 IDC, 2010 Korea Security Software 2010-2014 Forecast and Analysis: 2009 Year-End Review, 2010.6

[11] IDC, Worldwide Identity and Access Management 2010-2014 Forecast : A First Look in 2010, 2010.3

[12] SKT, Smart Wallet, http://tstore.co.kr/

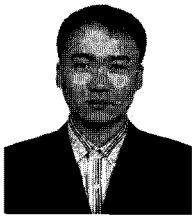
[13] 최대선, 진승헌, "모바일 ID 보안 및 프라이버시를 위한 스마트지갑," 한국정보과학회 학회지, 27(12), pp. 50-59, 2009년 12월

〈著者紹介〉



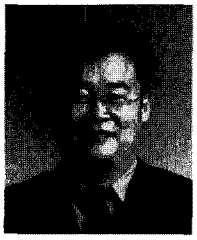
조 영 섭 (YoungSeob Cho)
정회원

1993년 2월 : 인하대학교 전자계산공학과 졸업
1995년 2월 : 인하대학교 대학원 전자계산공학과 석사
1999년 2월 : 인하대학교 대학원 전자계산공학과 박사
1998년 12월~현재 : 한국전자통신연구원 인증기반연구팀 책임연구원
관심분야 : ID 관리, 인증기술, 프라이버시 보호, 정보보호



김 수 형 (SooHyung Kim)
정회원

1996년 2월 : 연세대학교 컴퓨터과학과 학사
1998년 8월 : 연세대학교 컴퓨터과학과 석사
2011년 2월 : 한국과학기술원 전산학과 박사과정 수료
2000년 11월 : (주)한국정보통신기술연구소 연구원
2000년 12월~현재 : 한국전자통신연구원 인증기술연구팀 선임연구원
관심분야 : 정보보호(인증/인가, 프라이버시 보호), ID 관리, 모바일 지불결제



진 승 헌 (Jin Seung-Hun)
정회원

1993년 2월 : 숭실대학교 전자계산학과 학사
1995년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 전산학(정보보호) 박사
1996년 4월 : (주)대우통신 종합연구소 연구원
1999년 5월 : (주)삼성전자 통신연구소 전임연구원
1999년 6월~현재 : 한국전자통신연구원 인증기술연구팀장
관심분야 : 정보보호(PKI, 인증/인가기술, 프라이버시 보호기술), 모바일 지불결제, 컴퓨터/네트워크 보안