

Digital Identity 관리 기술 현황 및 전망

Trend of Technology for Digital Identity Management

u-IT839의 정보보호 이슈 특집

조영섭 (Y.S. Cho)

디지털ID보안연구팀 선임연구원

진승현 (S.H. Jin)

디지털ID보안연구팀 팀장

목 차

-
- I. 서론
 - II. ID 관리 시스템
 - III. 연구 및 시장 동향
 - IV. 표준화 동향
 - V. 관련 프로젝트
 - VI. 결론

인터넷의 확산과 유비쿼터스 환경이 도래함에 따라, 사용자가 관리해야 하는 digital 형태의 identity 정보가 기하 급수적으로 증가하고 있다. 또한 이러한 identity 정보는 서비스 제공자에 의한 오남용이나 외부의 해킹 위협에 직면하고 있으며, 이는 사용자의 프라이버시를 침해하는 결과를 가져온다. 이에 따라, 사용자의 digital identity 정보를 관리하는 identity 관리 기술은 최근 그 중요성이 매우 높아지면서 국내외에서 많은 연구가 진행되고 있다. 본 고에서는 digital identity 관리 시스템에 대한 개요와 identity 관리 기술에 대한 연구 및 시장 동향, 표준화 동향 및 관련된 연구 프로젝트에 대하여 살펴본다.

I. 서론

인터넷의 확산과 발전에 따라 인터넷 전자상거래, 전자정부, 전자의료 등과 같은 다양한 전자거래가 활성화되고 있다. 이에 따라 사용자는 기존에 오프라인에서 수행하던 많은 작업과 거래를 인터넷 상에서 수행하게 되었고 이러한 전자거래는 모바일(mobile) 인터넷과 유비쿼터스(ubiquitous) 환경의 도래 등에 따라 향후에는 더욱 확대될 것으로 예상된다.

그러나 기존 인터넷 환경에서 사용자가 인터넷 서비스를 이용하기 위해서는 서비스마다 자신의 Id(Identifier)와 개인 정보를 사전에 등록하고, 서비스를 이용하기 전에 등록된 Id로 인증 받는 과정을 수행해야만 한다. 이것은 사용자가 인터넷 상에서 여러 서비스를 사용할 때 서비스마다 매번 인증 받아야 하는 불편을 초래한다. 또한, 사용자가 이용하는 인터넷 서비스의 수가 많아질수록 사용자가 기억하고 관리해야 하는 Id 수가 증가하는 문제를 발생시킨다. 일반적으로 사용자는 기억하기 쉬운 형태로 Id를 등록하거나 또는 동일한 Id를 등록하기 때문에 Id 해킹의 위험이 증대되고 하나의 Id가 해킹되면 다른 서비스의 Id도 노출되는 문제가 발생한다. 또한 현재의 인터넷 환경에서는 사용자 자신이 등록한 정보가 서비스 업체에서 어떠한 방식으로 사용되는지 확인하는 것이 어려워 서비스 제공자의 오남용에 따른 개인정보 침해문제가 발생할 수 있다[1].

본 고에서는 이와 같은 문제를 해결하기 위한 ID(Identity) 관리 시스템과 기술 및 표준화 동향에 대하여 살펴본다.

● 용 어 해 설 ●

Identity: Identity는 사전상으로 “개인의 구별되는 특징이나 개성”을 의미하며, 개인의 특징, 신상 정보, 선호도 같은 것들을 모두 포함하는 정보로 일반적으로 사용자의 Id, 신상 정보, 비신상 정보, credential로 구성된다.

II. ID 관리 시스템

1. Identity 정의

Identity는 사전상으로 “개인의 구별되는 특징이나 개성”을 의미하며, 특징, 신상 정보, 선호도 같은 것들을 모두 포함하는 정보이다. 사용자는 자신의 identity를 증명해야만 개인적인 서비스를 받을 수 있다. 따라서 identity 정보를 안전하게 유지하고 관리하는 것은 인터넷 환경에서 상호간의 신뢰를 증명하는 기본이 된다. <표 1>은 identity를 구성하는 요소에 대한 설명이다. 본 고에서는 identity의 약자로 ID를 사용한다.

Id는 인터넷 환경에서 사용자가 인터넷 사이트에 로그인하는 과정에서 사용하는 개인 식별자를 의미한다. 실 환경에서는 운전 면허증, 여권, 사원 번호나 회사 내의 인트라넷 정보와 같이 유일하게 사용자를 구분할 수 있는 식별자를 사용자 Id라고 한다.

신상 정보와 비신상 정보는 개인이 소유하는 특징들을 나타내는 정보들이다. 신상 정보는 정부나 회사 같은 기관에서 발급받거나 등록한 사용자 정보들을 의미하며, 이는 Id와 마찬가지로 개인을 유일(unique)하게 구분할 수 있다는 특징을 가지고 있다. 반면 비신상 정보는 모든 개인이 가지는 일반적인 판단 항목들로, 개인의 특성을 구분할 수 있는 취향, 종교 등과 같은 정보를 의미한다. 개인이 가질 수 있는 일반적인 정보들이기 때문에 비신상 정보만을 이용하여 사용자의 신원을 추적하는 것은 불가능하다.

Credential은 개인이 자신의 ID를 증명하기 위한 수단으로 사용하는 정보를 나타낸다. 패스워드나 인증서, 생체 정보와 같이 본인만 알고 있거나 소유하

<표 1> Identity 구성

종류	설명
Id	가입자 식별자(identifier)
신상 정보	주민번호, 주소, 전화번호, 핸드폰, 직장연락처
비신상 정보	나이, 성별, 결혼 여부, 결혼 기념일, 취미, 각종 선호도, 종교, 수입, 직업
Credential	패스워드, 인증서, 생체 정보(ID 정보 제공 대상)

고 있다고 인정되는 정보를 사용하여 자신이 정당한 사용자임을 증명할 수 있게 된다.

2. ID 관리 시스템

일반적으로 사용자 ID는 정보화기기 및 인터넷의 여러 사이트에 분산, 중복 저장되어 있다. 따라서 정보시스템 이용이 활성화됨에 따라 사용자 ID를 구성하는 정보의 양도 증가하게 되어 관리의 불편함과 함께 개인정보 유출로 인한 프라이버시 문제가 이미 발생하고 있다.

ID 관리시스템은 이와 같은 문제를 해결하기 위해 단일인증 서비스(SSO), 개인정보 소유자가 설정한 프라이버시 정책에 의한 개인정보 공유, 분산 저장된 ID에 대한 일관성 있는 관리 기능을 수행하는 시스템이다.

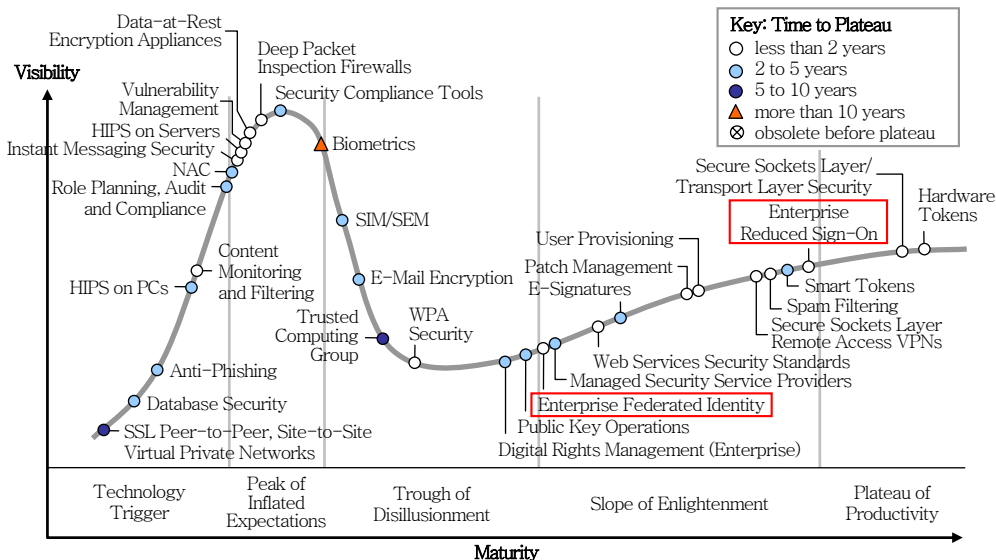
초기 ID 관리시스템은 ID 관련 모든 정보를 단일 시스템에 저장하는 중앙집중형이 대부분을 차지했으며 대표적인 사례로는 Microsoft사의 .NET Passport가 있다. 그러나 사용자의 개인정보를 한 기업에서 통합 관리하는 체계와 다른 ID 관리시스템과의 연동이 되지 않는 문제가 있다.

최근 이러한 문제점을 해결하기 위해 개인정보가 인터넷에 연결된 ID 관리시스템에 분산 저장되어 있고 서로 연동할 수 있는 ID 관리체계에 대한 연구개발이 진행되고 있다. 이러한 ID 관리시스템의 대표적 예로는 IBM과 Microsoft 등이 주도하는 WS-I, Sun이 주도하여 2001년 결성되어 현재 150여 개 회원을 가진 Liberty Alliance[2]가 있다. 국제 표준화기구인 ISO/IEC JTC1/SC27은 ID 관리시스템 연구를 위한 WG5 (privacy, identity and biometric security)를 새로 구성하였고[3], 경제협력 개발기구(OECD)에서도 정보보호작업반(WPISP)을 구성, 전자정부서비스 및 전자상거래 활성화를 위해 ID 관리프레임워크에 대한 연구를 진행하고 있다.

Ⅲ. 연구 및 시장 동향

본 장에서는 identity 관리 시스템의 연구동향에 대하여 기술한다.

(그림 1)은 시장조사기관인 Gartner에서 분석한 보안 분야의 hype cycle이다. ID 관리 기술과 밀접한 분야로는 enterprise federated identity와 en-



<자료>: Gartner, 2005. 7.

(그림 1) 보안 분야 Hype Cycle

enterprise reduced sign-on 분야를 들 수 있다.

Enterprise federated identity 분야는 여러 개체들 간에 credential을 공유할 수 있는 기술을 제공하며, 신뢰 관계를 바탕으로 신원 확인 정보와 인증 내역을 공유할 수 있도록 해주는 기술과 관련된 분야이다. 현재 이 분야는 Liberty Alliance의 SAML 기반 솔루션이 많은 관심을 받고 있다. Enterprise federated identity에 사용되는 기술은 엔터프라이즈 환경을 위한 몇 가지 사용 케이스(use case)를 가지고 있지만 BtoC 통신에서는 거의 사용되지 않고 있다. 아직은 성숙되지 못한 상태이며, 관련 기업으로는 Liberty Alliance, Microsoft, Trustgenix, Novell, Oblix, Ping Identity와 RSA Security 등이 대표적이다.

Enterprise reduced sign-on 분야는 각각의 응용 애플리케이션이 요구하는 Id/패스워드 확인 절차를 간소화시켜 로그인(sign-on) 과정의 번거로움을 줄이는 기술과 관련된 분야이다. 간소화 작업을 위해서는 통합된 패스워드 루틴과 사용자가 직접 관리하는 시스템이 가능하다. 일반적으로 SSO가 주로 쓰이는 용어지만, 여전히 정의하기 어렵기 때문에 (그림 1)에서는 'reduced'란 표현을 사용하고 있다. 이 기술은 사용자에게 편리함을 제공하지만, 전체 시스템을 한 번의 로그인 과정만으로 사용할 수 있기 때문에 보안상의 문제점을 충분히 고려해야 한다. Enterprise reduced sign-on 분야는 주류 기술로 등장하기 시작한 단계이며, 관련기업으로는 ActivCard, BNX Systems, Citrix Systems, Computer Associates, Evidian, Imprivata, i-Sprint, Novell, Passlogix, Protocom Development Systems, RSA Security, Sentillion, Version3 등이 있다.

현재 ID 관리 시장은 Liberty Alliance로 대표되는 기업들과 Microsoft가 양분하고 있다. 그러나 NetMesh의 CEO이자 YADIS 프로젝트를 운영하고 있는 Johannes Ernest는 앞으로 ID 관리 시장에서 '사용자 중심(user-controlled)의 ID 관리'가 주목을 받을 것이라고 예상했다.

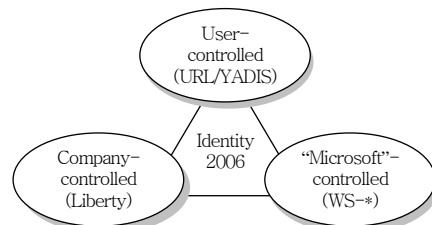
Company-controlled identity는 기업이 개인에

게 ID를 부여한 뒤 개인이 어떤 ID를 관리하고 공유할 것인가를 결정한다. Liberty Alliance 표준에 기반한 ID 관리 시스템이 대표적이며, 2006년 후반에는 Liberty Alliance 표준을 적용한 시스템이 다수 구축되어 10억 개가 넘는 ID가 존재할 것으로 예상된다.

Microsoft-controlled identity는 WS-* 표준에 기반한 ID 관리 시스템으로, Kim Cameron이 Law of Identity를 통해 주장한 ID Metasystem이 InfoCard[4] 프로젝트로 구현된 것이다. InfoCard는 OASIS 표준인 WS-Security를 기반으로 하여 X.509, Kerberos, SAML과 같은 보안 토큰 포맷을 모두 사용할 수 있으며 Windows Vista를 통해 광범위하게 적용될 것으로 예상된다.

User-controlled identity는 ID 제공자(IdP), 개인 정보, ID 사용 정책을 개인이 통제하는 시스템으로서, 기업에 속한 ID가 아니라 사용자 스스로 ID를 생성하고 관리하는 것이 특징이다. 대표적인 user-controlled identity로는 URL을 ID로 사용하는 OpenID[5], LID[6], YADIS[7]를 들 수 있다.

DIDW는 2006년의 ID 관리 시장이 확대되어 블로그, 일반 기업, RSS 리더, 위키(wiki), 사교 네트워크뿐만 아니라 검색 분야에도 ID 프로파일을 이용한 제품이 출시될 것으로 내다보았고 위험 관리(risk management) 분야에서 ID 관리가 중요하게 고려될 것으로 예상하였다. 특히 사용자 중심의 ID 관리 기술이 출현하고 그 중에서도 상용화에 한발 앞선 URL 기반의 ID 관리가 주목 받을 것으로 예상하였다. (그림 2)는 2006년 현재 ID 관리 시스템들의 현황을 도식화한 것이다.

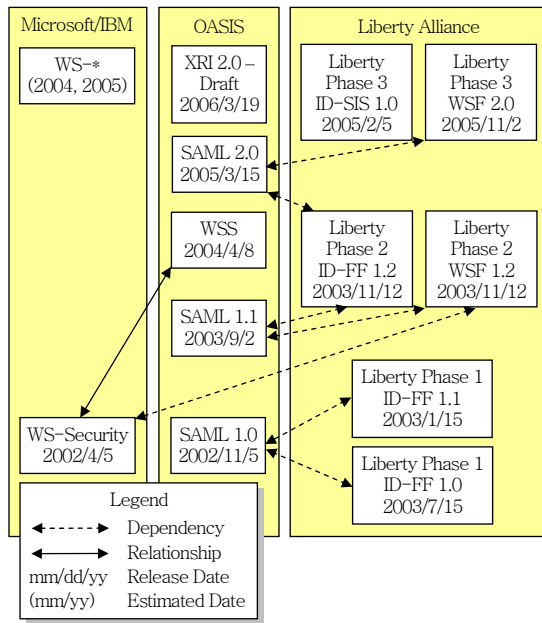


<자료>: <http://netmesh.info/jernet>

(그림 2) The Identity Landscape 2006

IV. 표준화 동향

인터넷 레벨의 identity 관리와 조직간 identity 연동을 위한 표준들이 여러 단체에서 제안되었다. 이러한 단체로는 IBM, Microsoft 등이 주도하는 WS-I, Sun이 주도하는 Liberty Alliance 그리고 XML 관련 표준을 제정하는 OASIS 등이 있다. (그림 3)은 이들 단체의 표준 및 표준 간의 관계를 나타낸 것이다.



(그림 3) Identity 관련 표준[1]

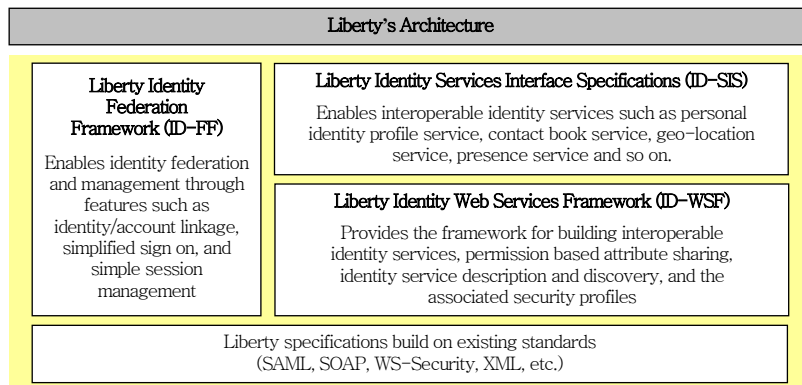
1. Liberty Alliance

Liberty Alliance는 연방화된 네트워크 identity 관리와 identity 기반의 서비스를 위한 공개 표준을 개발할 목적으로 2001년 9월에 결성되었고, 2006년 현재 150여 개의 멤버를 가진 조직으로 성장하였다. 국내에서는 ETRI가 Liberty Alliance의 affiliation member로 활동하고 있다. (그림 4)는 Liberty Alliance 표준 모듈을 나타낸다.

그림에서 ID-FF는 federated identity 관리와 인터넷 SSO에 대한 표준을 규정하고 있으며 현재 SAML v2.0으로 통합되었다. ID-WSF는 사용자가 자신의 identity 정보를 다른 시스템에 공유할 수 있도록 해주는 웹 서비스 프레임워크를 정의한다. ID-SIS는 ID-WSF를 이용하여 공유되는 사용자 identity의 표준 규격을 정의하고 있는 것으로 사용자 개인 프로파일 정보와 조직 내의 프로파일 정보를 나타내는 personal profile과 employ profile이 규정되어 있으며, presence, contact book, geo-location 등이 지속적으로 표준으로 제정되고 있다.

2. OASIS

OASIS는 XML 관련 표준을 제정하는 기관이다. OASIS가 제정하는 ID 관련 표준은 현재 WSS[8]와 SAML[9]이 있다. WSS는 WS-I에서 제안한 WS-Security를 OASIS 표준으로 받아들여 마무리할 것



<자료>: Liberty Technology Tutorials, Liberty Alliance

(그림 4) Liberty Alliance Module

으로 예상된다. SAML은 객체에 대한 인증, 인가, 속성 정보를 안전하게 교환하기 위한 프로토콜로, 현재 2.0 버전까지 발표되어 있다. (그림 5)는 OASIS SAML 표준화 진행 현황을 도식화한 것이다. 현재 SAML 2.0이 표준으로 제정된 상태이다.

SAML V2.0을 구성하는 주요 스펙은 다음과 같다.

• Core

이 스펙에서는 assertion의 구조와 SAML assertion과 관련된 요청 및 응답 프로토콜에 대하여 기술한다.

• 바인딩

SAML 요청/응답 메시지를 기존에 존재하는 하부 프로토콜로 매핑하는 방식을 기술한다. 메시지를 바인딩하는 하부 프로토콜로는 HTTP, SOAP, Reverse SOAP (PAOS)와 URI 방식이 있다.

• 프로파일

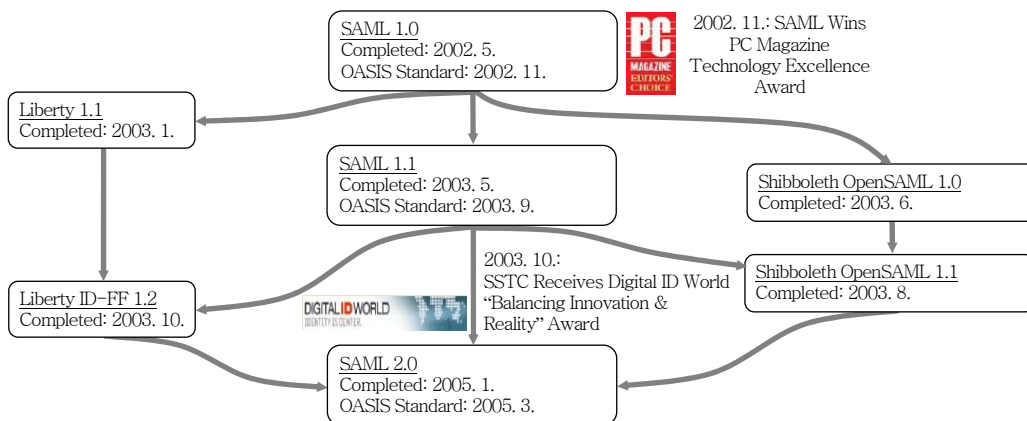
프로파일은 SAML assertion을 프레임워크나 프로토콜에 어떻게 삽입시키고, 이렇게 삽입된 메시지에서 어떻게 추출하는지에 대한 방법을 규정하는 규칙이다. 이 스펙은 SSO 프로파일, artifact resolution 프로파일, assertion 질의/응답 프로파일, 이름 식별자 매핑 프로파일, SAML 속성 프로파일 등을 규정하고 있다.

• 메타데이터 프로파일

SAML을 기반으로 IdP와 SP가 정보를 교환하기 위해서는 서로가 지원하는 프로토콜, 프로파일, 서비스 엔드포인트(endpoint), 공개키 인증서, provider ID 등과 같은 정보가 필요하다. SAML은 이와 같은 부가적인 정보를 메타데이터로 부른다. 이 스펙은 메타데이터의 구조를 규정하고 IdP와 SP의 메타데이터를 인터넷상에서 공개하는 방법과 공개된 메타데이터를 검색하는 방법을 규정한다.

• 인증 문맥(Authentication Context)

SP는 사용자에게 제공하는 서비스의 특성에 따라 IdP가 어떠한 방식으로 사용자를 인증했는지를 확인해야 할 필요가 있다. 즉, SP가 사용자에게 자금 이체와 같은 금융 서비스를 제공하는 경우, 사용자의 인증 방식이 최소한 인증서를 이용하거나 또는 인증서와 생체 정보를 이용할 것을 요구할 수 있다. 이와 같은 경우, 사용자에게 서비스를 제공할 것인지에 대한 SP의 판단은 단순히 IdP가 사용자를 인증하였는지에 대한 정보뿐만 아니라 사용자를 어떠한 방식으로 인증하였는지에 대한 부가적인 정보가 필요하다. 이 스펙은 IdP가 사용자를 어떠한 방식으로 인증하였는지를 SP에게 알려주기 위해 사용자를 인증하는 각각의 방식에 대하여 하나씩 인증 클래스를 정하고 이것이 어떠한 의미를 지니는지를 규정한다.



<자료>: Liberty Technology Tutorials, Liberty Alliance

(그림 5) SAML 표준화 진행

3. WS-I

WS-I는 SOAP, WSDL, UDDI로 구성되는 웹 서비스에 대한 표준을 제정하는 조직으로 웹 서비스의 보안과 관련된 표준 또한 제정하고 있으며 향후 표준 로드맵도 제시하고 있다. WS-Security는 SOAP 메시지의 무결성, 신뢰성, 인증을 포함하는 메시지 보호 수준(quality of protection)을 제공하기 위한 스펙이다. WS-Security는 바이너리 보안토큰을 인코딩하는 방식과 X.509 인증서 또는 Kerberos 티켓 등을 사용하는 방식 등을 정의하고 있다. 특히, 이 스펙은 OASIS에 제안되어 WSS라는 명칭으로 표준화가 진행되고 있다.

WS-Trust는 신뢰 관계를 형성하는 방법으로, 당사자간에 직접 신뢰관계를 형성하는 방법과 신뢰할 수 있는 중간 계층을 통해 신뢰관계를 형성하는 방법을 소개한다. WS-Policy는 수신자와 송신자가 보안에 대한 요구사항과 자신이 지원 가능한 보안 정도를 명시하는 방법을 제공한다. WS-Federation은 사이트 또는 조직간 ID 연동을 위한 스펙으로 WS-Security, WS-Policy, WS-Trust 및 WS-SecureConversation 기반 위에서 구현된다. 현재, WS-Federation이 SAML을 채택하여 사용할지에 대해서는 미지수이다. WS-Trust, WS-Policy, WS-Federation은 현재 버전 1.0 표준안이 나온 상태이다. WS-I는 또한 OASIS와 같은 중립적인 표준 단체에 WS-Federation을 비롯하여 WS-Trust, WS-SecureConversation, WS-SecurityPolicy를 상정할 예정이다.

V. 관련 프로젝트

본 장에서는 identity 기술에 대한 연구 및 개발을 진행하는 프로젝트에 대하여 기술한다.

1. FIDIS

FIDIS[10] 프로젝트는 유럽의 정보 사회에서 개인의 신원을 적절히 식별하기 위한 여러 계층의 이

해를 구하고, 공정한 방법으로 ID 관리를 수행한다는 비전을 가지고 있다. 이를 위해 FIDIS는 유럽의 정보 사회에서 사용할 신원을 관리하기 위한 요구사항을 정립하고, 필요한 기술과 기반구조를 개발하고 있다. 또한 ID 도용과 프라이버시 문제를 해결하고 전 유럽에서 통용될 수 있는 신원 표현 방식과 식별 방식을 제공하려는 목표를 가지고 있다.

FIDIS 프로젝트는 2004년 4월 1일부터 2009년 3월 31일까지 5년의 과제 기간을 가지고 진행되며 24개의 산·학·연 컨소시엄이 10개의 워킹 그룹을 구성하여 프로젝트를 수행한다. FIDIS는 ID 관리 시스템, ID 법안, 사용 케이스(use case)와 같은 유럽 국가들의 연구 결과를 여러 관점에서 수집한 뒤에 전문가들의 분석을 통해 전문가들의 분석을 거친다. FIDIS는 아래의 7가지 분야로 연구 분야를 구성하고 있으며, 각 분야의 결과물들은 유럽의 연구 단체, 과학 커뮤니티, 표준화 단체, 정책 결정권자와 같은 다양한 계층에게 영향력을 미칠 것으로 전망하고 있다.

- ID의 용어정리 및 파악
- 프로파일링
- 발행된 eID, ID 관리 시스템들 간의 상호운용성
- 포렌식(forensic)
- 식별 제거(de-identification)
- 최신의 식별 기술
- 이동성을 고려한 신원

FIDIS 프로젝트는 기존의 연구 결과를 통합하고, 법적, 사회-경제학적, 사용성, 응용 등의 관점에서 도출한 요구사항들, 공개 아키텍처와 스펙을 프로젝트의 결과물로 예상하고 있다. 현재 FIDIS는 3차년 과제를 수행중이다. <표 2>는 현재 도출된 FIDIS의 결과물을 보인다.

2. PRIME

디지털 사회는 모든 분야에서 이익을 가져오며, 개인화와 유비쿼터스 기술은 더욱 편리하고 효과적인 서비스를 제공하고 있다. 그러나 이 기술들은 개

〈표 2〉 FIDIS 결과물[1]

항목	내용
1차결과물 (2004/ 2005)	FIDIS Communication Infrastructure
	Inventory of Topics and Clusters
	Set of Use Cases and Scenarios
	Models
	Overview on IMS
	Study on Mobile Identity Management
	Manual of the Extended Wiki System
	A Study on PKI and Biometrics
	Workshop on ID-Documents
	Structured Account of Approaches on http://www.fidis.net/487.0.html -820 interoperability
2차결과물 (2005/ 2006)	Set of Requirements for Interoperability of Identity Management Systems
	A Survey on Legislation on ID Theft in the EU and a Number of Other Countries
	Forensic Implications of Identity Management Systems
	Descriptive Analysis and Inventory of Profiling Practices
	Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence
	Implications of Profiling Practices on Democracy
	A Specification for FIDIS Journal

인의 프라이버시와 밀접한 관련이 있기 때문에 프라이버시 법과 같은 문제들이 우선 고려되어야 한다. 이를 위해 PRIME[11] 프로젝트는 전송 레벨의 익명성을 비롯하여 최대한으로 사용자의 프라이버시를 보장하여, 디지털 사회에서 사용자들이 안전하게 자신의 개인 정보를 제어할 수 있는 방법을 제공하려고 한다. PRIME 프로젝트는 유럽 연합의 FP 6와 스위스 연방 교육과학청의 지원을 받고 IST가 프로젝트를 통합 관리하고 있으며, 프로젝트 수행기간은 4년(2004.3.~2008.2.)이고 예산은 1,600만 유로, 참가인원은 20명이다.

PRIME 프로젝트는 사용자가 직접 eID를 제어할 수 있는 시스템을 구축하려고 한다. 이론적 기술을 바탕으로 현재 유럽 연합의 IT 환경과 미래의 활용 방안을 고려하여 프라이버시가 강화된 최신의 ID 관

리 기술을 개발하는 것이 목적이다. PRIME은 프라이버시와 보안을 만족시키는 수준의 통신과 검증 방법을 개발하고, 프라이버시 문제를 현실적으로 해결할 수 있는 대안을 고려하고 있다. 또한 유럽의 프라이버시 법안과 규제를 기술적으로 지원하는 방법과 개인에게 권한을 부여하여 프라이버시를 제어할 수 있는 정보의 자기 결정권(self-determination)을 제공한다. 이 기술들을 통해 PRIME은 실세계에 활용될 ID 관리 솔루션을 개발하며 다음의 운영 원칙을 가지고 프로젝트를 진행하고 있다.

- 최대한의 프라이버시를 제공하는 설계
- 명시적인 프라이버시 규칙에 의거한 시스템 활용
- 프라이버시 규칙은 단순히 지적하는 것이 아니라 실제로 적용되어야 함
- 신뢰할 수 있는 프라이버시 정책 적용
- 사용자에게 쉽고 직관적인 추상화 레벨의 프라이버시 제공
- 프라이버시에 대한 통합된 접근
- 응용 프로그램에 통합된 프라이버시

PRIME 프로젝트는 다섯 가지의 개발 계획을 가진다. 첫째로 요구 사항을 수집하고 이에 대한 평가를 수행한다. 수집되는 요구 사항은 법적, 사회-경제학적, 일반 애플리케이션까지 다양한 범위를 포괄한다. 두번째는 애플리케이션의 프로토타입을 개발하는 것으로, 실제 환경에서 PRIME 프로젝트가 지향하는 목표와 아키텍처 기술이 제대로 동작하는지를 검증한다. 현재 진행중인 프로토타입으로는 온라인 헬스케어 시스템, 위치 기반 서비스, 프라이버시를 보호하는 고객 데이터베이스, 모바일 노동자를 위한 인프라의 익명 접근, E-Learning, 프라이버시가 강화된 유비쿼터스 기술 등이 있다. 세번째는 eID 관련 기술의 연구 개발이다. PRIME 프로젝트의 목표를 완수하기 위해서 고객의 프라이버시 요구 사항에 맞는 서비스를 보장하는 기술, HCI, 프라이버시 도메인에서 여러 프레임워크 간의 통신 고도화를 위한 온톨로지와 프라이버시 요소, 인가 모델, 암호학 기술, 통신 기반 구조, 사용자/서버측 eID 관리

가 필요하다. 네번째는 프레임워크와 아키텍처 구축이며, PRIME에서 제안하는 아키텍처를 보여준다. 그리고 다섯번째는 PRIME 아키텍처의 관리 및 확장이다.

3. e-IDMS

e-IDMS는 안전하고 편리한 전자거래를 위하여 다양한 웹사이트에 산재된 사용자 Id와 개인정보를 안전하게 보호/관리하기 위하여 ETRI에서 2004년부터 2006까지 3개년에 걸쳐서 개발하고 있는 인터넷 ID 관리서비스 시스템이다. 본 시스템은 사용자가 여러 개의 ID를 관리하는 부담을 줄이고, 사용하려는 서비스마다 매번 인증 받아야 하는 불편을 제거할 수 있으며, 자신의 개인정보에 대한 직접적인 통제를 통해 개인정보의 오남용에 대한 사용자의 우려를 해소할 수 있다. 또한 CoT 영역을 넘어서 ID 정보 공유 서비스와 SSO를 제공하며, 모바일 개인정보 제공과 권한위임을 통해 ID 관리 서비스 환경을 모바일로 확장하고 사용자 편의성을 개선하였다. e-IDMS는 2006년 2월 digital ID 웹 서비스 기능과 개인정보 보호기능을 제공하는 버전 2.0 개발이 완료되었으며 현재 대전광역시 추진중인 “공공기관 통합 ID 관리 시스템” 구축사업에 활용되고 있다. 공공기관 통합 ID 관리 시스템은 2007년 1월 구

축이 완료되어 시범 서비스를 실시할 예정이다. (그림 6)은 e-IDMS의 시스템 구성을 나타낸다. e-IDMS 시스템의 주요 특징은 다음과 같다.

- 중앙 집중적인 정책 관리 지원

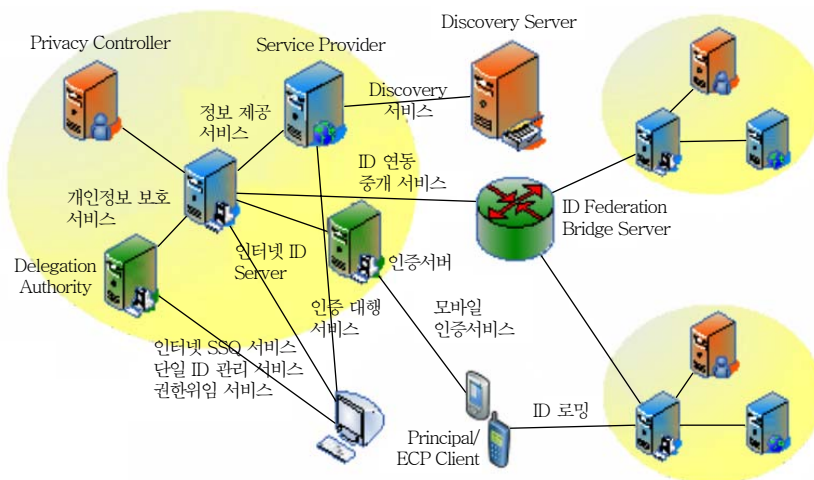
IDSP가 정책을 설정하고 사용자를 인증하는 구조로 설계되어 일관된 정책의 설정, 관리 및 적용이 쉽도록 하였다. 본 시스템은 관리자가 보다 편리하게 정책을 설정하도록 도와주고 한 번 설정된 정책이 일관성 있게 적용될 수 있도록 여러 가지 기능을 지원한다.

- 강화된 보안 서비스

본 시스템은 설계 단계부터 보안성을 고려하였으며, 보안 취약성이 예상되는 곳에 적합한 보안 메커니즘을 적용하여 기밀성, 무결성, 가용성 등과 같은 다양한 보안 요구사항을 만족시킨다.

- 표준 규격 준용

본 시스템은 표준화된 규격을 준용한다. 따라서 타 제품이나 솔루션과의 광범위한 상호연동성을 보장받을 수 있고, 보안성, 안정성, 확장성, 발전성 면에서도 검증되었다고 볼 수 있다. 본 시스템은 ID Federation과 SSO를 위해 OASIS SAML V2.0을 준용하고 있으며 ID 정보 제공을 위해 Liberty Alliance ID-WSF 2.0과 ID-SIS를 준용하고 있다. 또



(그림 6) e-IDMS 구성

한 개인정보 보호를 위해 OASIS의 XACML를 준용한다.

VI. 결론

인터넷은 일상 생활에 더욱 밀접해지고 있으며, 이에 따라 가상의 사이버공간에서 자신의 신원을 확인하며 정보를 제공하는 데 근간을 이루는 digital identity의 관리는 더욱더 중요해지고 있다. 본 고에서는 digital identity 관리 시스템과 이에 대한 연구 동향, 표준화 동향을 살펴보았다. 또한 관련된 연구 프로젝트에 대하여 살펴보았다.

약어 정리

BtoC	Business to Customer
CoT	Circle of Trust
DA	Delegation Authority
DIDW	Digital ID World
DRM	Digital Right Management
e-IDMS	ETRI IDentity Management service System
FIDIS	Future of Identity in the Information Society
FP	Framework Programme
HCI	Human-Computer Interaction
IAM	Identity & Access Management
Id	Identifier
ID	Identity
IdP	Identity Provider

● 용어해설 ●

IDMS (Identity Management System): 사용자나 객체 identity의 생성, 변경, 폐기 등을 관리하는 시스템으로 중앙집중형 IDMS, 연계형(federated) IDMS, 사용자-중심(user-controlled) IDMS로 분류될 수 있다.

IST	Information Society Technologies
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organization for Economic Cooperation and Development
PRIME	Privacy and Identity Management for Europe
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-On
WPISP	Working Party on Information and Security
WS-I	Web Service Interoperability organization
WSS	Web Service Security
XACML	eXtensible Access Control Markup Language
YADIS	Yet Another Decentralized Identity Interoperability System

참고 문헌

- [1] “인터넷 ID 관리 서비스,” 한국전자통신연구원, 디지털ID 보안연구팀, 2006.
- [2] Liberty Alliance Project, <http://www.projectliberty.org/>
- [3] ISO/IEC JTC1/SC27 WG5 N4721, Information Technology - Security Techniques - A Framework for Identity Management, Oct. 2005.
- [4] Microsoft CardSpace, <http://msdn2.microsoft.com/en-us/library/aa480189.aspx>
- [5] OpenID, <http://openid.net/>
- [6] LID, <http://lid.netmesh.org/>
- [7] SXIP, <http://www.sxip.com/>
- [8] OASIS Web Services Security, <http://www.oasis-open.org/committees/wss/>
- [9] OASIS SAML, <http://www.oasis-open.org/committees/security/>
- [10] FIDIS (Future of Identity in the Information Society), <http://www.fidis.net>
- [11] PRIME - Privacy and Identity Management for Europe, <https://www.prime-project.eu/>