논문 2006-43TC-7-11

ID 연계 기반의 인터넷 ID Management System: e-IDMS

(Internet ID Management System based on ID Federation: e-IDMS)

조 영 섭*, 진 승 헌*, 문 필 주**, 정 교 일***

(YeongSub Cho, SeungHun Jin, Philjoo Moon, and Kyoil Chung)

요 약

인터넷 서비스를 이용하기 위해서 사용자는 일반적으로 가입절차를 수행하고 서비스를 위한 id(identifier)를 등록하게 된다. 그러나 인터넷의 활용이 증가함에 따라, 사용자는 많은 id를 가지게 되었으며 이것은 사용자가 인터넷 서비스를 이용할 때마다, 매번 인증을 받아야 한다는 문제를 발생시키고 있다. 또한 여러 사이트에 산재되어 관리되지 않은 id들은 사용자 개인정보의 침해 가능성을 높이고 있다. 본 논문에서는 이와 같은 문제를 해결하기 위해 ETRI에서 개발한 ID(IDentity) 연계 기반의 인터넷 ID 관리 시스템인 e-IDMS에 대하여 기술한다. e-IDMS는 ID 연계를 기반으로 복합 인증, 인터넷 SSO, ID 정보 관리, ID 정보 공유, 개인정보 보호 및 대화형 질의 기능을 제공한다. e-IDMS는 공공기관 통합 ID 관리 시스템 구축에 활용되고 있다.

Abstract

In order to use an Internet service, it is a general procedure that user subscribes to the service and then registers her or his id(identifier). As Internet has been more widely used, however, user has more and more ids than ever before. In this environments, whenever user uses an Internet service, she or he must authenticate to the service provider, which makes her or him inconvenient. As user's data is scattered and unmanaged on various web sites, user privacy has been revealed more often. This paper specifies e-IDMS which ETRI has been developing to solve such problems. e-IDMS is an Internet ID(IDentity) management system based on ID Federation Mechanism. e-IDMS provides ID Federation-based facilities such as composite authentication, Internet SSO, ID information management, privacy protection and interactive query. e-IDMS is used in establishing integrated ID management system for public institutions.

Keywords : Identity, Identity Federation, IDMS

I. 서 론

인터넷의 급속한 보급으로 사용자들은 기존에 오프라인으로 수행하던 많은 서비스를 인터넷 상에서 수행하게 되었다. 사용자들은 이러한 서비스를 제공받기 위해서는 일반적으로 인터넷 서비스 제공자에 회원 가입 절차를 수행하여, 서비스 이용시 사용자 인증을 위해 자신의 id(identifier)와 패스워드를 등록하게 된다. 그러나 인터넷의 활용의 폭이 넓어짐에 따라 사용자들은 많은 서비스에 회원 가입을 하게 되었고 이것은 사용자가 가지고 있는 id의 수가 매우 많아지는 결과를 초래하게 되었다[1,2]. 2005년 개인정보 보호 사이트인 이지스의 조사에 의하면, 개인마다 평균 27개 웹 사이트의 회원으로 가입되어 있으며, 10여 개의 ID(Identity)를 보유하고 있는 것으로 나타나고 있다[3].

대부분의 인터넷 서비스들은 사용자에게 서비스를 제공하기 전에 사용자를 인증하는 것이 일반적이다. 사용자가 하나의 사이트에서 인증을 받더라도 다른 사이트의 서비스를 이용하기 위해서는 다시 재 인증을 받아

* 정회원, 한국전자통신연구원 정보보호연구단 디지털 ID보안연구팀
(Digital ID Security Research Team, Information Security Research Division, ETRI)
** 정회원, 평택대학교 정보통신학과
(Dept. of Information & Communication, PyeongTaek University)
*** 평생회원, 한국전자통신연구원 정보보호연구단 정보보호기반 그룹
(Information Security Infrastructure Group, Information Security Research Division, ETRI)
접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

야 한다. 이것은 사용자의 편의성을 떨어뜨린다. 또한 사용자가 이용하는 서비스가 증가하면 할수록, 사용자가 기억하고 관리해야 하는 id의 수가 증가하는 문제가 발생한다[1,2].

또한, 사용자가 id 등록을 할 때, 사용자의 정보를 함께 등록하도록 하는 현재의 인터넷 서비스 환경에서는, 사용자의 개인정보가 여러 사이트에 산재하는 결과를 초래한다. 이것은 사용자의 프라이버시를 침해할 가능성을 높이며, 사용자가 자신의 ID를 관리하지 않고 방치함에 따라 ID가 도용될 가능성이 높이지게 된다. Aberdeen Group은 ID 도용으로 인한 경제적 손실이 2003년 한 해에만 전 세계적으로 약 2,210 억 달러에 이르고, 그 피해가 연평균 300% 증가할 것으로 예측할 정도로 ID 도용 문제를 매우 심각한 실정이다[4]. 또한, 주소와 같은 사용자의 개인정보가 변경되면, 사용자는 자신이 가입한 모든 웹 사이트에 개별적으로 자신의 정보 변경 작업을 수행해야하는 불편 또한 매우 심각한 문제이다.

이와 같은 문제를 해결하기 사용자의 ID를 통합하거나 연계하여 관리하는 ID 관리 시스템(IdM, Identity Management)에 대한 연구가 진행되고 있다. IdM에 대한 연구 개발은 주로 조직 내에서 ID 통합과 접근제어를 제공하는 IAM(Identity & Access Management)과 ID 연계 기술을 기반으로 여러 기관의 ID를 연계하는 FIM(Federated Identity Management)로 진행되고 있다. IAM은 몇몇 선도 외국 업체들에 의해 초기 제품이 출시되고 있는 상황이다. 그러나 FIM은 많은 기업과 연구소에서 현재 연구가 진행되고 있다. 특히, 국내에서의 IAM과 FIM에 대한 연구 개발은 매우 미흡한 실정이다[2].

본 논문에서는 이와 같은 문제를 해결하기 위해 사용자의 재 인증 불편을 경감시키면서, 정보 공유를 통해 사용자 프라이버시를 보호하는 ID 연계 기반의 인터넷 ID 관리 시스템인 e-IDMS(ETRI IDentity Management System)에 대하여 기술한다. e-IDMS는 ID 연계를 기반으로 복합 인증, 인터넷 SSO(Single Sign-On), ID 정보 관리, ID 정보 공유, 개인정보 보호 및 대화형 질의 기능을 제공하며 공공기관 통합 ID 관리 시스템 구축에 활용되고 있다.

본 논문은 다음과 같이 구성된다. II장에서 인터넷 ID 연계 기술과 관련 연구에 대하여 기술하고 III장에서 e-IDMS에 대하여 기술하고 마지막으로 IV장에서 결론을 맺는다.

II. ID 연계 기술 & 관련 연구

1. ID 연계 기술

본 절에서는 ID 연계를 설정하는 단위 도메인인 CoT(Circle of Trust)의 개념과 예를 통해 ID 연계 기술을 설명한다.

가. CoT 개요

CoT[5]는 사용자의 ID를 연계할 수 있는 단위 신뢰 영역을 의미한다. CoT는 사용자에게 ID 관리 서비스를 제공하는 IDSP(IDentity Service Provider)와 사용자에게 다양한 서비스를 제공하는 SP(Service Provider) 그리고 서로 연관된 SP들이 연합한 Affiliated SP로 구성된다. 그림 1은 CoT의 개념도를 나타낸다.

그림 1에서 보이듯이 IDSP는 사용자가 신뢰하는 기관으로 사용자를 인증하고 인증된 사실을 assertion으로 발급하여 SP들에게 전달함으로써, SP들이 사용자를 직접 인증하지 않고도, 사용자의 인증 여부를 판단할 수 있도록 해 준다. SP 또는 Affiliated SP는 사용자에게 일반 인터넷 서비스를 제공하는 기관으로 사용자 인증을 IDSP에게 의존할 수 있기 때문에 인증을 위해 추가적인 기능을 설치하는 비용이 발생하지 않는다. 이러한 CoT는 IDSP와 SP들 간의 비즈니스 협약을 통해 구성되며 사용자 인증 정책, Assertion 발급 정책 등 다양한 정책과 가이드라인을 가지고 있게 된다.

나. ID 연계 예

ID 연계[5]는 IDSP와 SP가 한 사용자에 대하여 자신들이 기존에 소유하고 있는 사용자 id를 서로 연관시키는 과정이다. IDSP와 SP는 ID 연계를 위해 사용자 이

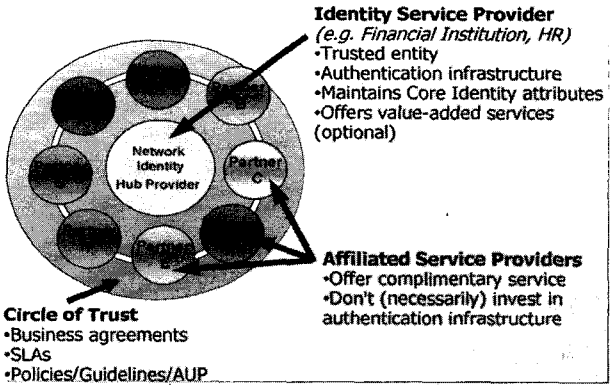


그림 1. CoT 개념도(출처: Liberty Alliance)
Fig. 1. CoT Concept(Orig.: Liberty Alliance).

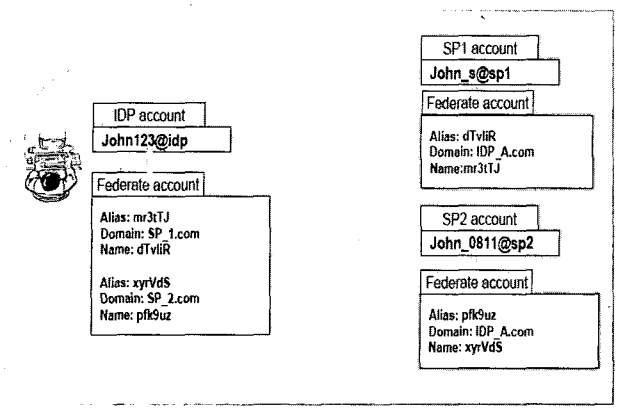


그림 2. ID 연계 예(출처: Liberty Alliance)
Fig. 2. An Example of ID Federation. (Orig.: Liberty Alliance)

름 식별자를 생성하고 서로 교환하여 사용자 이름 식별자 정보를 관리한다. 사용자 이름 식별자는 의사난수(pseudo-random) 값으로 중복되지 않도록 생성한다.

그림 2는 "Joe"라는 사용자가 IDSP에는 "John123"라는 id로 등록되어 있고, SP1에는 "John_s"라는 id를 사용하고 있으며, SP2에서는 "John_0811"이란 id를 사용하는 경우에, IDSP와 SP1 그리고 IDSP와 SP2의 ID 연계 예를 보인다. 그림 2에서 표시된 IDP(IDentity Provider)는 IDSP와 동일한 의미를 가진다.

IDSP와 SP의 연계에서는 둘 사이에서만 인식될 수 있는 사용자 alias를 각각 생성하고, 이들을 서로 교환하여 관리함으로써 사용자 id를 연결시킨다. 그림 2에서는 IDSP와 SP1은 "Joe"에 대하여 ID를 연계시키기 위해, IDSP는 "mr3tTJ"라는 alias를 생성하고 SP1은 "dTvliR"을 생성한다. 그리고 서로 이들 alias를 교환하고 각각 사용자 계정에 저장하여 관리한다. 즉, IDSP는 "Joe"가 SP1 도메인에서 "dTvliR"로 인식된다는 사실을 alias "mr3tTJ"에 기록하고, SP1은 "Joe"가 IDSP 도메인에서는 "mr3tTJ"로 인식된다는 사실을 alias "dTvliR"에 기록한다. 이와 같은 방식으로 "Joe"에 대하여 IDSP와 SP1 사이의 ID 연계가 이루어진다. IDSP와 SP2에서의 "Joe"에 대한 연계도 역시 같은 방식으로 이루어진다.

이와 같은 ID 연계를 이용하면, SP는 사용자에 대한 인증이 필요할 때, 자신과 CoT를 구성하는 IDSP에게 사용자 인증을 요청할 수 있다. IDSP는 SP의 요청에 따라 사용자를 인증하고, 요청한 SP에서 사용자가 식별되는 이름을 확인하여 그 이름으로 사용자 인증 사실을 assertion으로 생성하여 SP에게 전달한다. ID 연계 방식에서는 사용자가 IDSP에 한번만 인증받게 되면, SP들에서는 추가적인 사용자 인증이 필요 없게 되어 SSO 서비스가 제공되는 효과를 얻을 수 있다.

ID 연계는 또한 사용자가 가지고 있는 기존 id를 연계하는 방식을 채택하기 때문에 하나의 id 만을 사용하는 방식보다 보안성을 향상시킬 수 있다. 즉, 어떤 id가 유출되더라도, 해당 id를 사용하는 IDSP와 SP만 영향을 미치고 다른 SP들에게는 영향을 미치지 않는다.

2. ID 관련 표준

본 절에서는 ID 관리와 관련된 대표적인 표준인 Liberty Alliance와 SAML(Security Assertion Markup Language) V2.0에 대하여 기술한다.

가. Liberty Alliance

Liberty Alliance[6]는 연계된 네트워크 ID 관리와 ID 기반의 서비스를 위한 공개 표준을 개발할 목적으로 2001년 9월에 결성되었다. 2001년에 20개의 기관으로 출발한 Liberty Alliance는 2006년 5월 현재 150 여개의 멤버를 가진 조직으로 성장하였다. 이 기관들은 교육기관, 정부 조직, 서비스 제공자, 금융기관, IT 업체, 무선 서비스 제공자 등 그 영역 범위가 상당히 넓다.

Liberty Alliance는 ID 연계를 통해 여러 사이트에 분산된 사용자의 계정을 연결시키고 이를 이용해서 한 번의 사용자 인증으로, 사용자가 추가적인 인증 없이 여러 사이트를 이용할 수 있게 하는 SSO 서비스를 제공한다. 또한, 사용자는 자신의 계정들이 어떻게 연결되고, 서비스 제공자에게 사용자 정보가 어떻게 공유되는지 관리할 수 있어 자신의 정보에 대해 보다 많은 제어권을 확보할 수 있다.

또한 사용자가 자신의 정보를 다른 사이트에 제공할 것인지를 선택할 수 있도록 하여, 사용자의 허가에 기반한 사용자 정보 공유가 가능하도록 하며, 이것은 사용자의 개인정보가 산재되는 것을 방지하는 효과가 있다.

그림 3은 Liberty Alliance에서 단계적으로 제정하고 있는 표준 스펙들을 보이고 있다.

Liberty Alliance의 표준은 3개의 단계로 나누어 진행되고 있다. 단계 1인 ID-FF(Identity Federation Framework)은 ID를 연계하는 메커니즘과 이를 기반으로 하여 SSO 제공을 위한 표준을 제정하였다. 단계 2인 ID-WSF(Identity Web Service Framework)는 사용자의 ID 정보를 사용자의 허가 하에 웹 서비스 방식을 이용하여 다른 사이트와 공유할 수 있도록 하는 프레임워크를 규정하고 있으며, 단계 3인 ID-SIS(Identity

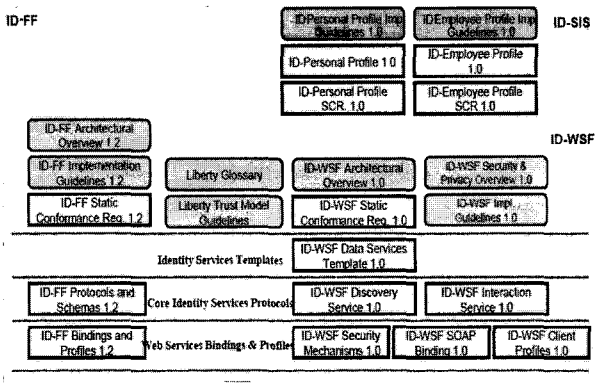


그림 3. Liberty Alliance 스펙(출처 Liberty Alliance)
Fig. 3. Liberty Alliance Specification.
(Orig.: Liberty Alliance)

Service Interface Specification)는 사용자 프로파일, contact, Geolocation 등과 같은 사용자 Identity 서비스 프로파일을 정의한다.

나. SAML V2.0

OASIS(Organization for the Advancement of Structured Information Standards)[7]에서는 2002년 11월에 SAML V1.0 표준을 제정하였고 2003년 9월에는 V1.0을 보완한 V1.1을 제정하였다. SAML V1.1은 많은 업체에 의해 구현되어, 공공, 교육, 산업 분야에서 큰 성공을 거두었다. SAML V2.0은 Liberty Alliance와 Shibboleth[8]의 연구 결과물을 수용하여 SAML V1.1에 ID 연계 기능을 통합하여 2005년 3월에 제정된 통합 표준이다.

SAML V2.0은 IDSP가 사용자를 인증한 후, 사용자의 인증 사실을 assertion으로 생성하여 SP에게 전달하고 이를 통해 SP가 사용자의 인증 사실을 확인하는 수단을 제공한다. SAML V2.0의 주요 표준 스펙은 다음과 같다.

■ Core

이 스펙에서는 assertion의 구조와 SAML assertion과 관련된 요청 및 응답 프로토콜에 대하여 기술한다. assertion은 IDSP와 SP가 사용자에 대하여 ID를 연계할 수 있도록 해주며, IDSP가 사용자를 어떠한 방식으로 인증하였는지에 대한 정보를 제공한다. 또한 assertion은 자신의 수신자 SP가 누구인지, 자신의 유효기간이 얼마인지 등에 대한 정보를 담을 수 있다. 요청 및 응답 프로토콜은 SP가 IDSP에게 사용자 인증, 사용자 ID 연계, 단일 로그아웃 등을 요청하고 응답하는 프로토콜 메시지에 대하여 기술하고 있다.

■ 바인딩

이 스펙에서는 SAML 요청/응답 메시지를 기존 통신 프로토콜에 어떻게 매핑시켜야 하는지에 대한 방법을 기술한다. 프로토콜 메시지를 바인딩 하는데 사용되는 하부 프로토콜로는 HTTP, SOAP(Simple Object Access Protocol), Reverse SOAP(PAOS)와 URI가 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

SAML을 기반으로 IDSP와 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 IDSP와 SP의 메타데이터를 인터넷 상에서 공개하는 방법과 공개된 메타데이터를 검색하는 방법을 규정한다.

■ 인증 문맥(Authentication Context)

사용자에게 서비스를 제공할 것인지에 대한 SP의 판

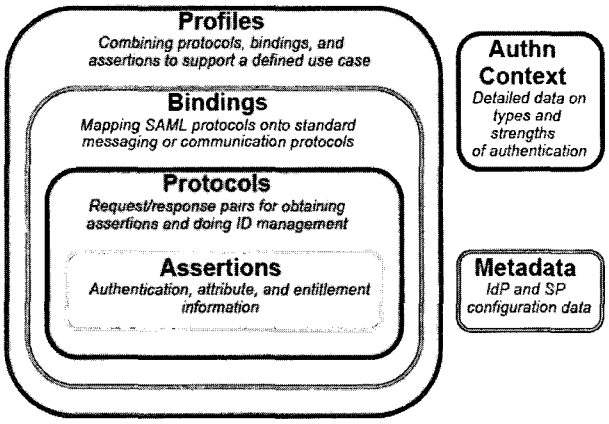


그림 4. SAML Protocol Stack(출처. SAML V2.0 Basics from Sun)
Fig. 4. SAML Protocol Stack.
(Orig.: SAML V2.0 Basics from Sun)

단은 IDSP가 사용자를 인증하였는지에 대한 정보뿐만 아니라 사용자를 어떠한 방식으로 인증하였는지에 대한 부가적인 정보를 필요로 할 때가 있다. 이 스펙은 IDSP가 사용자를 어떠한 방식으로 인증하였는지를 SP에게 알려주기 위해, 사용자를 인증하는 각각의 방식에 대하여 하나씩 인증 클래스를 정의하고 이것이 어떠한 의미를 지니는지를 규정한다.

그림 4는 앞에서 설명한 SAML V2.0의 스펙들의 연관성을 도식화한 것이다.

3. 관련 연구

본 절에서는 IdM과 관련된 기존 연구에 대하여 기술한다.

가. PRIME

PRIME(Privacy and Identity Management for Europe)[9]은 유럽의 주요한 연구 단체들을 중심으로 W3C 등 주요 표준화 기관과 연계하여 개인의 프라이버시를 보호하는 방법에 대하여 연구하는 프로젝트이다. PRIME은 개인들이 정보화 사회에서 스스로 개인정보를 제어하여 그들의 프라이버시를 보호하는 것을 목적으로 하고 있다. 또한 편리한 컴퓨터 사용자 인터페이스, 온톨로지, 인증, 인가, 암호화 기술을 기초로, 최신의 ID 관리 기술과도 상호 동작하면서 프로그램 개발자나, 서비스 제공자, 애플리케이션 운용자 등 특정 산업과 연관되는 여러 응용들과 관련된 전문가들을 위한 프라이버시 보호 지침에 해당하는 표준 기술의 제공을 목표로 한다. 정부, 사회, 경제, 전문적인 분야를 총괄하는 정보화 사회 전반에 걸쳐 프라이버시를 제공하는 ID관리에 초점을 맞추고 연구가 진행되고 있다.

PRIME은 ID 관리와 사용자의 프라이버시 보호를 위한 프레임워크를 제안하기 위해 2004년에 시작해서 4년 동안 5단계로 나누어 수행되고 있다. 그림 5는 PRIME 프로젝트의 구조와 연관성을 보인다.

나. RAPID

RAPID(Roadmap for Advanced research in Privacy and Identity management)[10]는 PIM(Privacy and Identity Management) 분야의 연구 주제를 결정하고 이 분야의 연구 주제들을 확인함으로써 EU 연구 커뮤니티를 활성화하는 것을 목표로 하는 프로젝트이다. RAPID의 목표들을 지원하기 위하여, 기반 구조에서의 프라이버시 강화 기술들, 기업 시스템들에서의 PIM, 다양하고 신뢰할 수 있는 신원 관리, 적법한 PIM 이슈들, 사회 경제적인 PIM 이슈들 등 5개의 세부적인 PIM 테마들이 연구되었다. 그림 6은 RAPID의 개념도를 보인다.

RAPID의 프라이버시 강화 기술과 ID 관리 방법은 기술적 측면과 사회·경제·법률적 측면을 모두 고려하고 있다. 기술적 측면에는 개인정보 보호에 사용되는 보안 메커니즘을 활용하는 인증, 접근 통제, 암호, 보안 관리 기술 등이 고려되며, 서비스 제공자에 의한 ID 보호 기술로는 익명의 웹 서핑, 계정과 가명의 프로비저

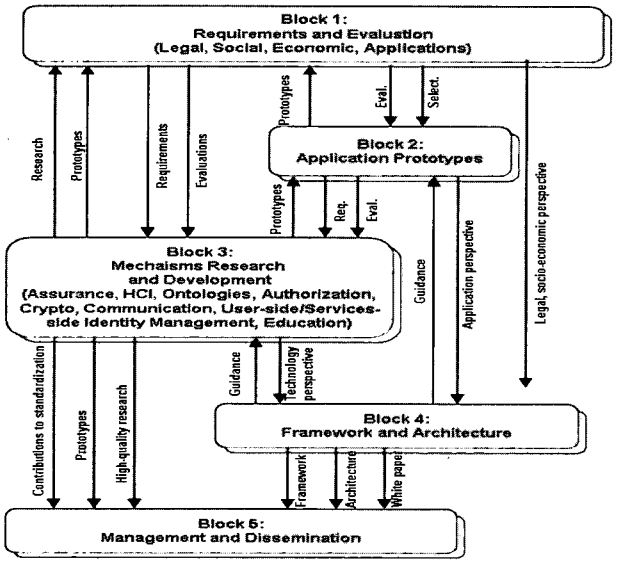


그림 5. PRIME 프로젝트 구조 및 연관성
Fig. 5. Structure & Relationship of PRIME Project.

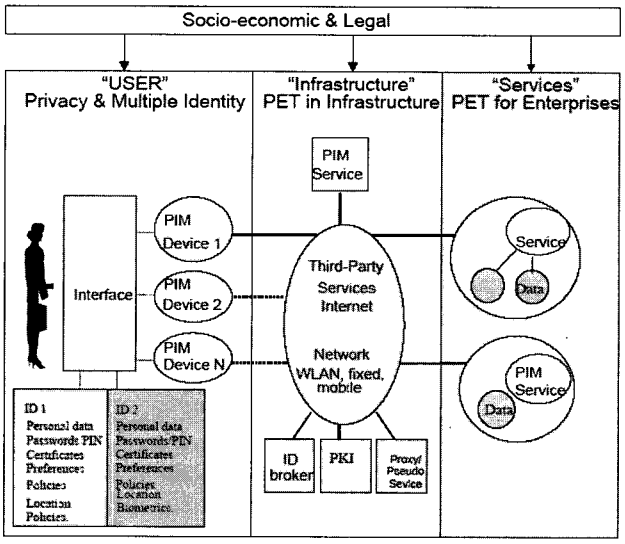


그림 6. RAPID 개념도
Fig. 6. Conceptual Structure of RAPID.

닝이 고려된다.

Ⅲ. e-IDMS

본 장에서는 ETRI에서 개발하는 ID 관리 시스템인 e-IDMS에 대하여 기술한다. e-IDMS는 단계별로 시스템이 개발되고 있으며, version 2의 개발이 완료되었고 현재 version 3의 개발이 진행되고 있다. 본 장에서는 e-IDMS version 2를 중심으로 시스템의 특징, 시스템 구성과 주요 기능에 대하여 기술한다. 그리고 e-IDMS의 활용 예를 설명한다.

1. 개요

e-IDMS는 다음과 같은 특징을 가지고 있다.

■ 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 한번 설정된 정책이 일관성 있게 적용될 수 있도록 여러가지 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. 또한 개인정보 보호를 위해 OASIS의 XACML(eXtensible Access Control Markup Language)를 준용한다.

2. 시스템 구성

가. 시스템 아키텍처

e-IDMS은 그림 7과 같이 구성되어 있다.

그림 7에서 보듯이 각각의 구성 요소와 그것이 제공하는 기능은 다음과 같다.

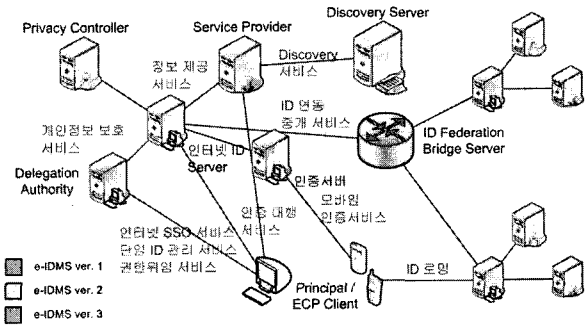


그림 7. e-IDMS 구성
Fig. 7. e-IDMS Structure.

■ IDSP

인터넷 ID 관리 서비스를 제공하는 메인 시스템으로 인증, 개인정보 관리, 개인정보 열람 등의 서비스를 제공한다. 타 도메인의 서비스 제공자가 운영하는 인터넷 ID Server와 연결되어 로밍 서비스를 제공하기도 한다.

■ Privacy Controller

인터넷 ID 관리 서비스에서 개인정보 유통을 제어하는 서버이다. 개인정보 제공자는 공개되는 정보에 대한 허가를 Privacy Controller에게 질의한다. Privacy Controller는 가입자가 자신의 개인정보 제어 정책을 쉽게 관리할 수 있도록 해주는 인터페이스를 제공한다. 프라이버시 도메인 관리자 또한 정보의 유통을 제어할 수 있다.

■ 가입자 웹 브라우저

가입자는 IE나 Mozilla 등과 같은 기본 브라우저만으로 e-IDMS에 접근하며 서비스를 제공받을 수 있다. 가입자는 브라우저를 통해, 가입, 개인정보 관리, 개인정보 보호 정책 관리 등의 기능을 수행하게 된다.

■ Discovery Server

ID 정보를 제공하는 AP(Attribute Provider)가 제공하는 정보를 등록하고, ID 정보를 소비하는 AC(Attribute Consumer)가 ID 정보 제공자를 검색하는 기능을 제공한다. SP는 자신이 ID 정보를 제공할 때는 AP 역할을 수행하고, 다른 AP에서 제공하는 ID 정보를 사용할 때는 AC의 역할을 수행한다.

■ ID Federation Bridge Server

여러 CoT가 존재할 때 이들 간의 ID Federation을 통해, SSO와 ID 정보 서비스를 제공하려면, 개별 CoT 간 신뢰 관리와 ID 연계가 선행되어야 한다. CoT가 여러 개 존재하면, CoT간 신뢰 관리와 ID 연계가 매우 복잡해지게 된다. ID Federation Bridge Server는 이들 신뢰 관리와 ID 연계가 쉽게 제공할 수 있도록 하여 시스템의 확장성을 제공한다.

나. 소프트웨어 구조

그림 8은 e-IDMS의 소프트웨어 구조를 보인다.

IDSP는 ID-FF를 위한 구성 요소와 ID-WSF를 위한 구성 요소를 모두 갖고 있으며, IDSP Admin과 사용자를 위한 관리 모듈도 갖고 있다. SP는 ID-FF를 위한 모듈과 ID-WSF 서비스를 위한 모듈을 포함한다. Privacy Controller와 Discovery Server는 데이터 저장소와 이를 처리하는 서비스 엔진으로 구성된다. Privacy Controller에서 PDP(Policy Decision Point)는 자원 접근 요청이 정책에 부합되는지 여부를 판단하는 모듈이며, PAP(Policy Adminstration Point)는 PDP에서 사용되는 정책을 생성하고 관리하는 모듈이다.

IDSP와 SP는 SAML V2.0 Service 모듈을 이용하여 SSO 기능을 제공한다. SP가 사용자를 인증할 필요가 있을 때마다 IDSP에게 사용자 인증을 요구하고, IDSP는 사용자를 인증한 후, 사용자 인증 사실을 해당 SP에게 Assertion으로 전달한다. IDSP는 사용자를 인증하면, 자체적으로 cookie 등을 이용하여 사용자 인증 세션을 관리한다. 이것은 여러 SP에서 사용자 인증을 요구하더라도 IDSP는 한번만 사용자를 인증하면 된다는 것

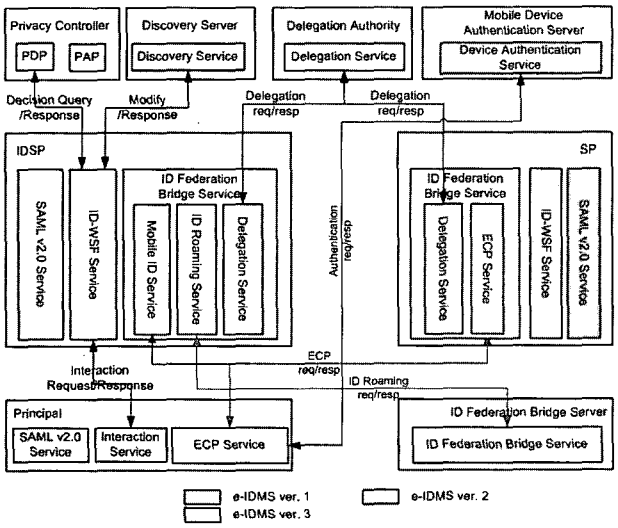


그림 8. e-IDMS 소프트웨어 구조
Fig. 8. e-IDMS Software Structure.

을 의미한다. 이를 통해 IDSP는 사용자에게 SSO 기능을 제공한다.

또한 IDSP와 SP는 ID-WSF Service 모듈을 이용하여 Discovery Server에 ID 정보 공유 사실을 등록하거나 또는 등록된 정보를 검색한다. AC는 DS로부터 검색된 정보를 이용하여 AP에 ID 정보를 요청하고 응답을 받는다. AP는 AC에 정보를 제공할 때, PDP에게 정보 제공에 대한 허가를 받도록 하여 사용자 개인정보 보호 기능을 제공한다.

3. 시스템 기능

e-IDMS에서 구현된 주요 기능은 다음과 같다.

가. 복합 인증 기능

가입자가 처음에 시스템에 접근하면 시스템은 인증서 또는 패스워드 방식의 인증 메커니즘 중에 하나를 선택하여 가입자에게 Credential을 제출할 것을 요구한다. 가입자가 Credential을 제출하면 시스템은 검증하여 가입자를 인증한다. 시스템을 사용하기 위해 반드시 거쳐야 하는 기본 기능으로 제공된다.

e-IDMS는 현재 PW 인증, PW-SSL 인증, PKC(Public Key Certifcate) 인증 세 가지 방식을 제공한다.

나. 인터넷 SSO 기능

가입자가 SP에 접근하면 SP는 IDSP에게 가입자의 인증을 요청한다. 가입자의 인증이 필요하면 IDSP는 앞에서 설명한 복합 인증 기능을 이용하여 인증한다. 만약 가입자가 이미 인증을 받은 경우에는 추가적인 인증을 수행하지 않는다. 이와 같은 인증 확인 후, IDSP는 가입자 인증 확인 정보를 SP에 전달함으로써, 가입자가 한번의 IDSP 인증 후 여러 SP의 서비스를 이용할 수 있도록 하는 SSO 기능을 제공한다. 만약 가입자가 IDSP에서 이미 인증을 받았지만 SP가 다른 인증 메커니즘으로 가입자를 인증할 것을 요구할 경우, IDSP는 가입자를 재인증한다. IDSP들 간의 SSO도 본 기능을 이용한다.

다. ID 정보 관리 기능

IDSP를 통해 가입자의 ID 정보를 관리하는 기능이다. 가입자는 IDSP에 가입 후 IDSP의 ID와 별도로 가입된 SP의 ID를 연계한다. ID 연계가 완료되면 가입자

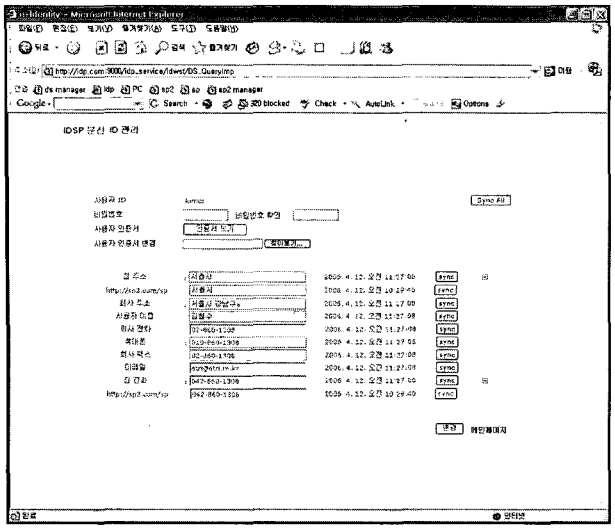


그림 9. ID 정보 관리
Fig. 9. ID Information Management.ID Information Sharing Selection.

는 IDSP를 통해 SP에 산재한 자신의 ID 정보를 조회하고 관리할 수 있게 된다.

그림 9는 ID 정보 관리 기능이 수행되는 예를 보인다. IDSP에 저장된 정보뿐만 아니라 SP들에 저장된 정보를 함께 조회할 수 있으며, 정보의 수정도 가능하다. 특히 "sync" 기능은 특정 SP나 IDSP의 정보를 다른 SP나 IDSP에 반영하도록 함으로써, 분산된 데이터에 대한 동기화 기능을 제공한다. 변경일자를 기준으로 "sync" 기준을 추천하는 기능도 제공한다.

라. ID 정보 공유 기능

IDSP나 SP가 보유한 가입자의 ID 정보를 공유하는 기능이다. 공유되는 가입자 정보는 가입자에게 맞춤형

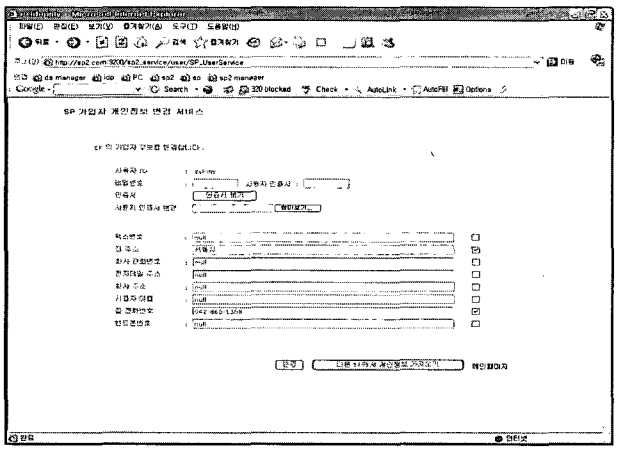


그림 10. ID 정보 공유 선택
Fig. 10. ID Information Sharing Selection.

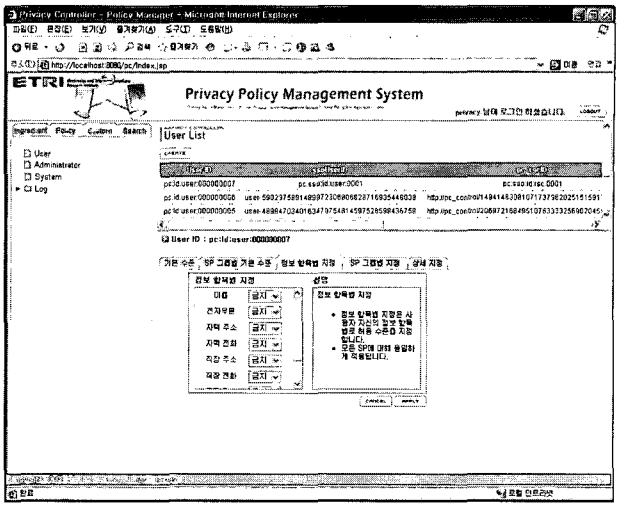


그림 11. 개인정보보호 정책설정
Fig. 11. Privacy Protection Policy Setting.

서비스를 제공하기 위해 사용된다. 가입자 정보를 공유하여 사용하면 가입자에게 직접 정보 입력을 요구하지 않아도 되고, 중복된 정보의 불일치성 문제나 최신성 유지 문제를 해결할 수 있다. 그림 10은 SP 이용시 ID 정보 공유 기능을 이용하는 예를 보여준다.

마. 개인정보 보호 기능

Privacy Controller는 가입자의 개인정보 유통을 제어한다. 개인정보 제공자는 가입자의 정보를 공개하기 전에 Privacy Controller에게 질의하여 허가를 받은 후 정보를 제공한다. Privacy Controller의 개인정보 제어 정책은 개인정보의 실소유자가 직접 관리할 수 있다. 또한 가입자의 편의를 도모하고 정보 노출의 위험을 제거하기 위해 관리자가 정책을 생성할 수 있다.

가입자는 개인정보 항목에 따라 또는 정보를 사용하려는 주체에 따라 개인정보 공개를 제어할 수 있다. 또한 개인정보 공개 시점에 가입자에게 공개 허가를 직접 질의하도록 할 수 있다. 그림 11은 Privacy Controller를 이용하여 사용자가 개인정보보호 정책을 설정하는 예를 보인다.

바. 대화형 질의 기능

대화형 질의 기능은 가입자가 본인 정보의 공유 여부를 '질의'로 설정한 경우에 발생한다. SP가 작업을 처리하기 위해 가입자의 정보를 요구할 경우, SP는 IDSP에 해당 정보를 요청하게 된다. 이 때 정보의 공유 여부는 사용자의 정책에 달려있다. 해당 정보에 대한 정책이 '질의'로 설정되었다면, IDSP는 해당 정보를 SP에게 제

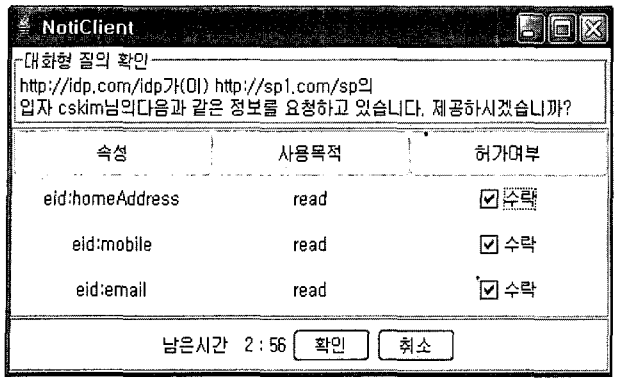


그림 12. 대화형 질의
Fig. 12. Interactive Query

공하기 전에 가입자로부터 직접 해당 정보의 공유를 동의하는지 여부를 질의해야 한다.

대화형 질의 기능은 두 가지 방식으로 동작할 수 있다. 첫 번째는 가입자가 현재 시스템에 접근해 있는 상태이다. 이 경우에는 정보제공 동의 여부를 질의하는 페이지로 가입자를 이동시켜 가입자의 동의를 얻도록 한다.

두 번째는 가입자가 현재 시스템에 접근하지 않은 상태이다. 이 경우에는 가입자가 다른 서비스를 이용하고 있거나, 웹 환경을 이용하지 않을 때이다. 본 시스템에서는 이와 같은 경우를 대처하기 위해 가입자가 IDSP에 로그인할 때, Noti 프로그램을 가입자 PC에 구동시킨다. 이 경우 IDSP는 Noti에게 해당 질의 메시지를 전송한다. Noti 프로그램은 항상 IDSP의 응답을 대기하고 있으며, 메시지를 받으면 사용자로부터 응답을 받아서 IDSP로 다시 전달한다. 그림 12는 Noti 프로그램이 동작하는 모습을 보여준다.

4. e-IDMS 적용 사례

본 절에서는 e-IDMS를 적용하여 현재 구축이 진행되고 있는 공공기관 통합 ID 관리 시스템에 대하여 기술한다.

공공기관 통합 ID 관리 시스템은 행정업무 효율화와 민원서비스 개선 등을 위한 전자정부의 자치단체 정보화사업의 일환으로 대전광역시에서 현재 진행되고 있다. 이 시스템은 다음과 같은 필요성에 따라 개발되고 있다.

- 공공기관의 홈페이지에 대한 개인정보 유출방지
- 인터넷상의 주민번호 보호(대체) 기술 필요
- 개인화된 맞춤형 서비스의 요구증가

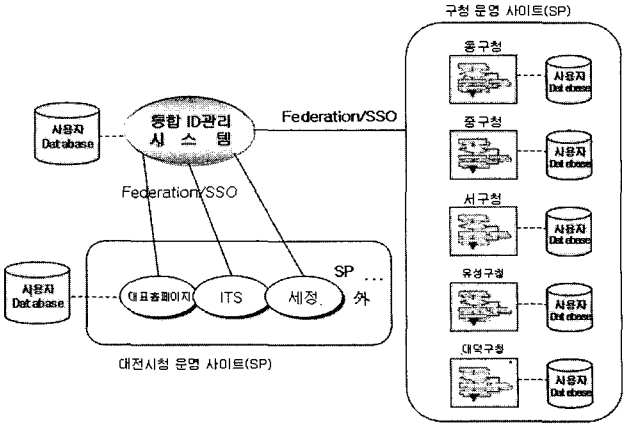


그림 13. 공공기관 통합ID 관리시스템 구축 개념도
Fig. 13. Conceptual Structure of Integrated ID Management System for Public Institution.

- 공공기관 개인정보보호정책의 체계적 관리 필요

즉, 이 시스템은 공공기관의 홈페이지를 통해 사용자의 정보가 유출되는 것을 방지하며, 현재 널리 활용되고 있는 주민번호를 사용하지 않고도, 사용자 본인을 확인할 수 있는 수단을 제공하는 것을 목적으로 하고 있다. 또한, 사용자 개인의 취향이나 서비스 사용 문맥(Context)에 따라, 사용자에게 최적화된 서비스를 제공하는 것을 목적으로 한다.

그림 13은 공공기관 통합ID 관리시스템 구축의 개념도이다. 이 시스템은 현재 관내 5개 구청을 포함한 21개 사이트를 연계하여 구축하고 있으며 다음과 같은 서비스를 제공한다.

- ID 관리 서비스
- ID 정보 제공 서비스
- 인터넷 SSO 서비스
- 개인정보 보호 서비스
- 인터넷 민원접수 실명제 서비스

공공기관 통합ID 관리시스템은 인터넷 민원접수 실명제 서비스를 제공한다. 그림 14는 인터넷 민원접수 실명제 서비스의 동작 흐름도를 나타낸다.

서비스를 이용하기 위해서 사용자는 먼저 IDSP에 가입을 한다. IDSP 가입을 위해 사용자는 먼저 동사무소, 학교 등과 같은 대면확인 기관에 실명확인 정보를 등록하며 이들 정보는 IDSP에 등록된다. 사용자는 대면등록 후, IDSP에 실명 인증 등록을 수행함으로써 IDSP에 가입을 완료하게 된다.

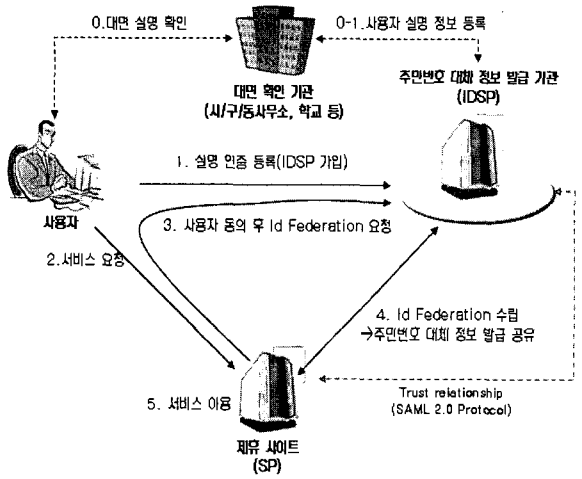


그림 14. 인터넷 민원접수 실명제 서비스
Fig. 14. An Enhanced Internet-based Civil Service.

IDSP 가입 후, 사용자는 SP를 통해 서비스를 이용하게 된다. SP는 사용자에게 서비스를 제공하기 전에 사용자의 실명 확인을 위해 IDSP에게 사용자 실명확인 정보를 요청하게 되고, IDSP는 사용자의 실명을 확인한 후, 이 정보를 SP에 전달한다. SP는 IDSP의 정보를 이용하여 사용자의 실명을 확인한 후, 사용자에게 서비스를 제공한다.

IV. 결 론

본 논문은 ETRI에서 개발한 ID 관리 시스템인 e-IDMS에 대하여 기술하였다. e-IDMS는 ID 연계 기술을 기반으로 다양한 ID 관리 기능을 제공하는 ID 관리 시스템이다. ID 관리, ID 정보 공유, 개인정보 보호, ID 로밍 등과 같이 기능을 제공한다. 본 논문은 이들 기능을 제공하는 e-IDMS의 특징과 시스템 구조 및 소프트웨어 구조에 대하여 기술하였다. 또한 e-IDMS의 기능 구현에 대하여 기술하였으며, 현재 e-IMDS가 활용되고 있는 공공기관 통합ID관리 시스템에 대하여 기술하였다.

향후, 현재의 유선 인터넷 환경뿐만 아니라 모바일 환경과 유비쿼터스 환경에서 효과적으로 ID 관리 기능을 제공하기 위한 ID 관리 연구가 필요하다.

참 고 문 헌

[1] 최대선, 진승헌, 정교일, "인터넷 ID 관리 서비스", *한국전자통신연구원 전자통신동향분석*, 20권, 1호, 73~83쪽, 2005년 2월

[2] 한국전자통신연구원, "인터넷 ID 관리 서비스 기술 백서", 2005년 6월

[3] 이지스, "대한민국 누리꾼 현황 보고서", 2005년 2월, http://egis.onoffkorea/

[4] Aberdeen, Aberdeen Group, "Identity Theft: A $2 Trillion Criminal Industry in 2005", May 2003

[5] Thomas Wason, "Liberty ID-FF Architecture Overview", Liberty Alliance Project, 2004. http://www.projectliberty.org/specs

[6] Liberty Alliance, http://www.projectliberty.org/

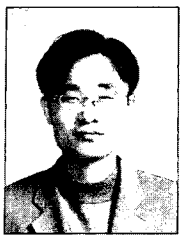
[7] OASIS SAML, http://www.oasis-open.org/ committees/security/

[8] Shibboleth, http://shibboleth.intenet2.edu/

[9] PRIME Project, "PRIME : Privacy and Identity Management for Europe Date of preparation," February 2004, http://www.prime-project.eu.org/

[10] RAPID Project, "RAPID : Roadmap for Advanced Research in Privacy and Identity Management," 2001, http://www.ra-pid.org

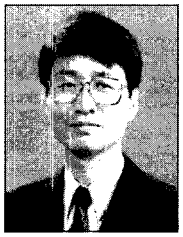
저 자 소 개



조 영 섭(정회원)
1993년 인하대학교 전자계산공학과 학사
1995년 인하대학교 대학원 전자계산공학과 석사
1999년 인하대학교 대학원 전자계산공학과 박사
1998년~현재 한국전자통신연구원 디지털ID보안연구팀 선임연구원
<주관심분야 : Digital Identity Management, 인증인가, 정보보호, EC>

진 승 헌(정회원)
1993년 숭실대학교 전자계산학과 학사
1995년 숭실대학교 대학원 전자계산학과 석사
2004년 충남대학교 대학원 컴퓨터과학과 박사
1994년~1996년 (주)대우통신 종합연구소 연구원
1996년~1999년 (주)삼성전자 통신연구소 전임연구원
1999년~현재 한국전자통신연구원 디지털ID보안연구팀장/선임연구원
<주관심분야 : Digital Identity Management, PKI, PMI, 인증인가>

문 필 주(정회원)
1988년 숭실대학교 전자계산학과학사
1991년 숭실대학교 대학원 전자계산학과 석사
1998년 숭실대학교 대학원 전자계산학과 박사
1988년~2001년 한국전자통신연구원, 팀장
2001년~현재 평택대학교 정보통신학과 교수
<주관심분야 : 가입자망기술, 네트워크 보안, 무선통신망>



정 교 일(평생회원)
1981년 한양대학교 전자공학과 학사
1983년 한양대학교 산업대학원 전자계산학과 석사
1997년 한양대학교 대학원 전자공학과 박사
1980년~1981년 엠시스템즈 사원
1981년~1982년 한국전기통신연구소 위촉연구원
1982년~현재 한국전자통신연구원 정보보호기반그룹장/책임연구원
<주관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리>