情 報 保 護 學 會 誌
第 14 券 第 5 號, 2004. 10

인터넷 ID 관리 서비스

최 대 선*, 조 상 래*, 김 승 현*, 진 승 헌*, 정 교 일**

요 약

인터넷에 산재한 id와 개인정보들은 적절한 관리와 보호를 필요로 한다. 인터넷 ID 관리 서비스는 가입자의 id와 개인정보를 관리해 주는 서비스이다. 가입자는 인터넷 ID 관리 서비스에 가입해 id와 개인정보를 등록하면, 이 id로 한번의 로그인 만으로 모든 가맹 웹사이트를 이용할 수 있고, 개인정보의 활용에 대한 통제도 할 수 있다. 인터넷 ID 관리 서비스가 도입되면 인터넷 이용이 편리해지고 id 도용을 크게 줄이며, 개인정보 보호를 강화할 수 있다. 해외에서도 ID 관리 분야에 대한 기술 개발과 표준화, 실환경 도입이 활발히 진행되고 있다. ETRI에서는 Liberty 규격을 준용한 인터넷 ID 관리 서비스 시스템을 개발 중에 있다.

Ⅰ. 서 론

인터넷의 급속한 보급으로 누구나 여러 웹 사이트에서 제공하는 서비스들을 이용하고 있다. 서비스를 이용하기 위해서는 사용자 개인 정보 등록을 포함하는 가입 절차가 요구된다. Id와 패스워드를 등록하고 주소, 전화번호 등 개인 신상정보를 입력하여 가입하게 된다. 사용자들은 이렇게 새로운 사이트에 가입할 때 마다 id를 정하고 개인정보를 입력하는 것을 매우 불편하게 느끼고 있다. 새로 가입한 사이트에서는 기존에 다른 사이트에서 사용하던 id가 이미 다른 사람에 의해 사용되고 있는 경우가 있으므로 여러 사이트에 가입하다보면 여러 개의 id를 갖게 되는 경우가 많다. 웹 사이트를 이용하기 위해서는 가입 시 등록한 id와 패스워드를 사용해 로그인 절차를 거쳐야 하는데 한번 컴퓨터를 이용할 때 여러 개의 웹 사이트를 방문하는 것이 일반적인 상황에서 매 사이트 마다 로그인 하는 것은 매우 불편한 일이다. 또한 각 사이트마다 id와 패스워드가 다른 경우가 많은데 자주 이용하지 않는 사이트를 방문할 경우 id와 패스워드를 망각하는 일은 흔하게 발생한다. 또한 웹 사이트마다 개인 정보를 따로 등록하기 때문에 주소 변경 등 개인정보가 변경되었을 때는 가입한 모든 웹 사이트를 방문하여 이를 변경하여야 한다. 한편 웹 사이트에 등록된 개인 정보 유출에 대한 우려가 증폭되고 있는 상황이다. 이 때문에 사용자들은 틀린 정보를 입력하는 경우가 많다. 이러한 상황은 단순한 사용자의 불편을 넘어서 서비스 이용의 확산을 가로막고 개인정보의 도용이나 프라이버시 침해같은 심각한 문제를 야기할 수 있다. 이러한 상황은 본질적으로 인터넷 상에서 개인들의 아이덴티티가 적절하게 관리되고 보호받지 못해서 발생한 것이다. 아이덴티티란 개인을 식별하는 id를 비롯해 신상정보와 같은 개인정보를 포괄한 개념이다. 본 논문에서는 이를 ID로 표기한다. 현재는 사용자 자신이 자신의 ID를 주로 기억에 의존해 관리하고 있으며, 이를 효과적으로 관리할 어떤 수단을 갖고 있지 못하다. 또한 ID는 적절히 보호 받지 못하고 있고, 사용자가 이를 지키기 위해 취할 수 있는 수단도 거의 없는 상황이다.

본 논문에서는 인터넷 상의 ID를 적절히 관리하고 보호하기 위한 방법으로 인터넷 ID 관리 서비스를 소개한다. 인터넷 ID 관리 서비스는 사용자 ID 정보를 관리하며 이를 통해 단일 인증, 개인 정보 보호를 제공하는 서비스이다[1]. 본 논문은 다음과 같이 구성되어 있다. II장에서는 인터넷 ID 관리 서비스의 개념과 서비스 내용, 기반 기술 및 서비스 도입에 따른 기대 이익을 설명한다. III장에서는 현재 세계적으로 시도되고 있는 인터넷 ID 관리 서비스들과 관련 기술 및 표준화 동향, 적용 사례들을 소개한다. IV장에서는 ETRI에서 개발하고 있는 인

* 한국전자통신연구원 정보보호연구단 인증기반팀({sunchoi, sangrae, ayo, jinshl}@etri.re.kr)
** 한국전자통신연구원 정보보호연구단 정보보호기반연구그룹(kyoil@etri.re.kr)

터넷 ID 관리 서비스 시스템의 기능과 구조에 대해 기술하고 V장에서 결론을 맺는다.

II. 인터넷 ID 관리 서비스

1. 개 념

인터넷 ID 관리 서비스는 인터넷 ID 관리 서비스 제공자(IDSP, ID Service Provider)를 두고 일반 사용자는 여기에 가입해 id와 개인 정보를 등록한 후, 이 id를 이용해 인터넷을 이용하도록 하는 서비스이다. 서비스 제공자(SP, Service Provider)는 인터넷 ID 관리 서비스에 가맹하여 IDSP에 가입한 사용자들에게 서비스를 제공한다.

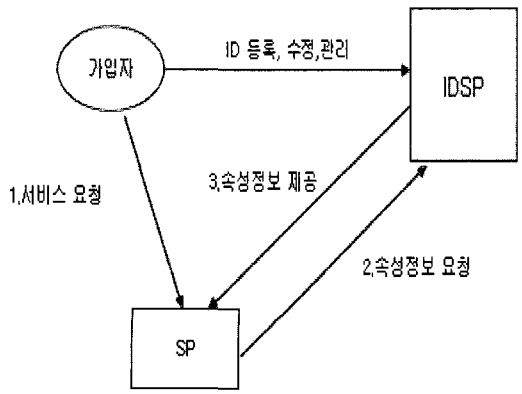
2. 서비스 내용

2.1 가입 및 ID 정보 관리

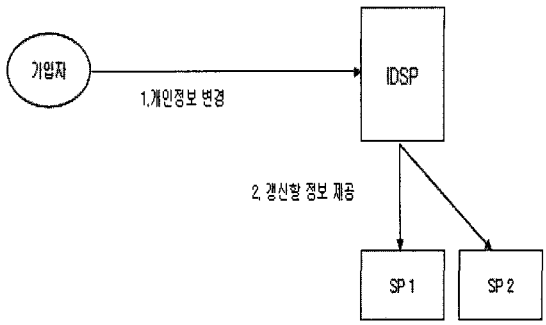
가입자가 IDSP에 하나의 id를 이용해서 가입한다. 그리고 해당 IDSP에서 자신의 모든 개인 정보를 등록, 수정, 관리한다. SP는 IDSP로부터 개인정보를 포함한 속성 정보를 제공받기 때문에 별도로 사용자 정보를 등록받지 않아도 가입자에게 서비스를 제공할 수 있다. 그림 1에서 이러한 흐름을 보여준다.

IDSP 서비스가 시행되기 전에 가입자가 특정 SP에 가입하여 SP의 id를 보유하고 있는 경우에는 해당 SP의 id와 IDSP의 id를 연계하면 된다.

SP는 제공받은 정보를 별도로 저장하는 방식을 택할 수도 있고, 자체적으로 저장하지 않고 필요할 때마다 IDSP에서 열람하는 방식을 택할 수도 있다. SP가 자체적으로 사용자 정보를 저장하는 경우, 가입자가 IDSP에



〔그림 1〕 ID 정보 관리

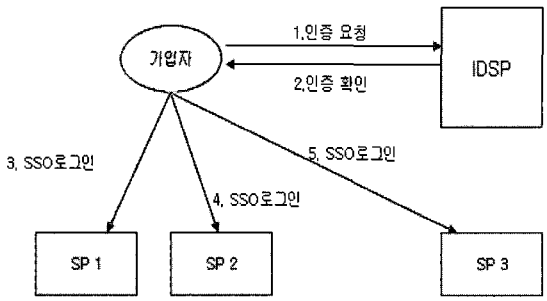


〔그림 2〕 ID 정보 변경 통보

서 자신의 개인정보를 변경할 때, 양쪽에 저장된 정보가 불일치하는 경우가 발생할 있다. 이 경우 그림 2에 나타난 것처럼 IDSP는 변경 내역을 SP에 통보하여 SP가 자동으로 가입자 정보를 최신으로 유지할 수 있도록 한다.

2.2 SSO

IDSP에서 한번 로그인한 후에 SP를 이용할 때는 추가적으로 로그인없이 서비스를 이용하는 SSO를 제공한다. 가입자는 SP마다 다른 id를 기억할 필요없이 IDSP id와 패스워드만 기억하면 된다. 이용 상의 편리함과 id, 패스워드 분실을 처리하기 위한 복잡한 절차와 비용을 최소화할 수 있다. 그림 3에서 SSO 흐름을 보여준다.

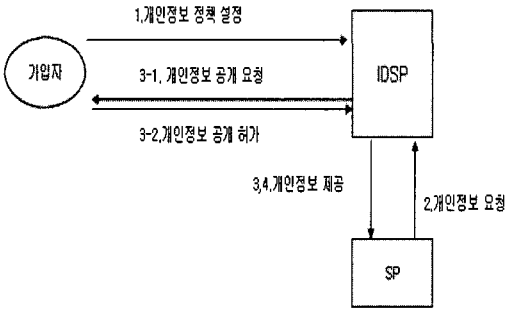


〔그림 3〕 SSO

2.3 개인정보 보호

기존의 사용자들은 웹사이트에 등록한 개인 정보를 관리하고 보호하기 위한 어떠한 수단도 갖고 있지 못했다. 인터넷 ID 관리 서비스에서는 IDSP에 등록한 자신의 정보에 대해 가입자의 자기 통제권을 행사할 수 있다. IDSP에서 SP에 제공하는 정보의 종류와 정보가 제공되는 대상에 대한 분명한 통제를 행사할 수 있고, 개인정보 제공 내역 로그도 조회할 수 있다. 그림 4는 개인정보 보

호 흐름을 보여준다. 개인 정보에 대한 통제 방식은 다음과 같이 이루어 질 수 있다. 가입자가 미리 개인정보 공개 정책을 설정한 경우(1단계), SP가 가입자의 개인정보를 요청하게 되면(2단계), IDSP는 가입자의 개인정보를 제공하기 전에 가입자가 사전에 동의한 정보만을 SP에 제공할 수 있게 된다(3단계). SP가 요구하는 개인정보가 가입자의 정책에 위배되지만 서비스를 제공하기 위해서 반드시 필요한 경우, IDSP는 가입자에게 해당 정보의 공개 여부를 질의할 수 있다. IDSP는 가입자에게 요청(3-1단계)을 하게 되고, 가입자가 이를 허가(3-2단계)하면 SP는 개인정보를 받아서(4단계) 서비스를 제공하게 된다.



〔그림 4〕 개인정보 보호

3. 인터넷 ID 관리 서비스 기반 기술

3.1 SSO

SSO 기술은 인증을 담당하는 인증서버와 인증서버에 인증확인을 요청하는 서비스 사이트들 간에 연동을 위한 프로토콜을 핵심으로 한다. 프로토콜 자체의 안전성과 인증서버의 오버헤드를 최소화하는 것이 중요하며 여러 인증 서버를 연계해 여러 도메인으로 SSO의 범위를 넓히는 것이 핵심 기술이다.

3.2 ID Federation

SSO와 ID 정보관리 서비스를 수행하는 방식에는 크게 두가지가 있다. 하나는 통합 ID 방식이고 하나는 ID 연계(Federation)방식이다. 통합 ID 방식은 모든 가입자 정보가 중앙 집중되어 있고, 기존에 사용하던 id들을 모두 폐지하고 IDSP가 제공하는 하나의 id만을 사용하는 것이다. 이 방식은 단일 조직 내의 SSO와 ID 관리에는 효과적이지만, 개별 시스템의 자치권이 사라지고 확장성이 부족한 문제가 있기 때문에, 여러 조직에서 개별적으로 운영하는 사이트들에 대해 SSO와 ID 관리를 제공해야 하는 인터넷 ID 관리 서비스에는 적합하지 않다.

ID 연계 방식은 SP가 기존에 보유하고 있던 id를 그대로 유지하면서 IDSP의 id와 연계를 통해 SSO와 ID 관리를 달성하는 방식이다. SP들의 정보 자치권이 그대로 유지되므로, 이용자들이 SP에서는 기존 id를 통해 로그인할 수도 있다. 또한 IDSP 간에도 id 연계방식을 적용해서, 가입하지 않은 IDSP의 가맹 SP에서도 똑같은 SSO와 ID 정보관리 기능을 이용할 수 있게 된다.

3.3 Permission based attribute sharing

SP의 개인정보 열람과 이에 대한 통제를 위해서는 개인정보 통제 정책 수립과 이를 통한 개인 정보 접근 제어 기술이 필요하다. 또한 가입자에게 개인정보 열람 허가 여부를 필요시 대화형으로 질의할 수 있는 기술도 필요하다.

개인 정보 통제 정책은 가장 중요한 요소이다. 얼마나 정교하게 개인정보의 열람을 통제할 수 있는가 만큼, 얼마나 쉽고 간단하게 자신의 정책을 설정할 수 있는가 하는 것이 중요하다. 아무리 정교한 정책도 설정과 관리가 불편하면, 누구도 이를 사용하지 않을 것이다.

개인 정보에 대한 접근제어는 개인 정보 열람 프로토콜과 함께 고려되어야 한다. 개인 정보 열람 프로토콜의 안전성과 함께, 설정된 정책에 대한 정확한 접근 제어가 필수적이다.

대화형 질의는 여러 가지 방식으로 이루어 질 수 있다. 사용자가 SP의 서비스를 이용할 때 발생하는 개인정보 열람은 SP의 인터페이스를 통해 질의될 수 있다. 그러나 사용자가 SP를 이용하고 있지 않을 때 SP가 사용자 정보 열람을 시도한다면, 이메일, SMS, 메신저 등 다른 방법으로 사용자와의 상호작용을 시도할 수 있게 된다.

4. Business Benefits

인터넷 ID 관리 서비스는 인터넷 환경을 편리하고 안전하게 사용할 수 있도록 해주는 서비스이다. 하지만 기존의 인터넷 환경에서 인터넷 ID 서비스를 도입하기 위해서는 어느 정도 변화가 요구된다. ID 관리 부분을 인터넷 ID 서비스로 변환하는 기술적인 측면뿐만 아니라, 기관 간에 신뢰 협정을 맺는 기술 외적인 측면도 고려되어야 한다.

이러한 변화를 시도하기 위해서는 기술적인 측면뿐만 아니라 인터넷 ID 관리 서비스를 도입하면서 얻을 수 있는 이점을 사용자, 서비스 제공자와 ID 서비스 제공자가 충분히 공감할 수 있어야 한다.

4.1 가입자의 이점

자주 사용하고, 믿음이 가는 계정을 통하여 다른 모든 사이트를 편리하게 이용

인터넷 ID 관리 서비스의 핵심 기술은 가입자가 사용하는 사이트들의 ID 정보를 하나로 연동하는 것이다. 그 중에 한 ID에 대한 인증이 확인되면, 가입자는 추가적인 확인 과정 없이도 다른 사이트의 서비스를 제공받을 수 있는 것이다. 따라서 가입자는 자신이 가입한 사이트의 ID를 모두 기억할 필요 없이, 자주 사용하는 사이트의 ID를 사용함으로써 인터넷을 쉽게 이용하게 된다.

개인정보의 적극적 관리

기존에는 사이트에서 미리 설정한 개인정보 보호 정책에 의해서만 가입자의 개인정보를 보호받을 수 있었다. 하지만 인터넷 ID 관리 서비스는 가입자가 설정한 정책에 따라서 정보를 제공하고 관리할 수 있는 기능이 제공되기 때문에, 가입자가 자신의 개인정보를 보호할 수 있게 된다. 또한 중요한 정보의 경우에는, 해당 정보를 사용하기에 앞서 사이트에서 가입자에게 동의를 구한 뒤에 사용을 결정하게 된다. 인터넷 ID 관리 서비스를 통해 가입자는 자신의 정보가 어떤 목적으로 사용되는지 알 수 있고, 자신이 직접 개인정보의 공유를 제어할 수 있기 때문에 신뢰성이 보장된다.

간편한 ID 정보 관리

가입자의 ID 정보가 변경되는 경우, 이 정보를 모든 사이트에 반영하는 것은 현실적으로 어렵다. 인터넷 ID 관리 서비스는 가입자가 ID 관리를 쉽게 할 수 있도록 도와준다. 한 사이트의 ID 정보만 수정하면 변경된 정보를 나머지 사이트의 ID 정보에 자동으로 반영하거나 참조할 수 있기 때문에, 개인 정보를 최신의 상태로 유지할 수 있게 된다.

사용자에 특화된 프리미엄 서비스 이용

인터넷 ID 관리 서비스는 사용자의 ID 정보를 공유하여, 서비스 제공자들이 사용자가 원하는 정보를 쉽게 제공할 수 있도록 한다. 따라서 사용자는 자신의 정보를 이용하여 더 나은 서비스를 제공받을 수 있으며, 관심 있는 정보만 선별하여 가치 있는 정보를 인터넷에서 찾을 수 있게 된다.

4.2 서비스 제공자의 이점

개인 정보의 관리 비용 감소

개인 정보 보호에 대한 인식이 강화되고 법제화나 인증 레벨을 통한 고도의 보안 수준을 요구하는 현실에서, 사용자의 개인 정보를 보유하고 있다는 것은 적절한 보안 수준의 구축을 위한 비용뿐만 아니라 심각한 관리 부담을 초래한다. 따라서 서비스 제공자는 개인 정보의 유지 부담을 줄이는 방향을 선택할 것이며, 인터넷 ID 관리 서비스를 이용하는 것이 최선의 대안이 될 것이다.

사용자에게 특화된 서비스 제공

사용자의 행동 패턴을 한 사이트에서 수집하기에는 자료의 신뢰성이 부족하다. 인터넷 환경에서의 사용자 구매 패턴이나 관심 자료들이 전체적으로 유지 관리되고 있다면, 이러한 데이타는 서비스 제공자들이 활용하고자 하는 중요한 정보가 된다. 인터넷 ID 관리 서비스는 이러한 정보를 서비스 제공자에게 제공하여 가입자의 성향에 따른 적절하고 효과적인 서비스를 제공하여 사용자의 구매를 촉진하는 것이 가능하다.

가입자 확보가 용이

서비스 제공자는 가입자를 확보하여 유무상의 서비스를 제공하거나 상품을 판매하는 것을 목적으로 하므로 가능한 많은 가입자를 확보하려고 한다. 인터넷 ID 관리 서비스를 도입하면 ID 서비스 제공자가 보유하고 있는 방대한 사용자를 그대로 자신의 가입자로 확보할 수 있다. 이들을 대상으로 다양한 마케팅을 실시할 수 있는데, 특히 개인 취향 등의 정보를 획득할 수 있으므로 맞춤 마케팅이 가능하다.

보안 비용 절감

사용자의 정보를 등록, 저장하고 사용자를 인증하는 부분은 서비스 제공을 위해 필수적인 부분이다. 이를 안전하게 하기 위해서는 별도의 시스템을 구축 해야 하는 경우가 많다. 중소 규모 사이트들은 이러한 시스템을 구축하고 유지하는데 필요한 비용을 지불할 여력이 없고, 이는 보안성이 취약한 상태로 남아 있는 것을 의미한다. 인터넷 ID 관리 서비스에 가맹하면 이 모든 것을 인터넷 ID 관리 서비스에서 제공해 주며 가맹자는 약간의 수수료만을 납부하면 된다.

4.3 ID 서비스 제공자의 이점

기존 고객 정보를 이용한 새로운 서비스 창출

인터넷 ID 관리 서비스는 기존에 많은 고객 ID를 보유한 포털이나 금융, 정부, 통신 서비스 제공자 들에 의해 제공될 가능성이 높다. 이러한 사이트들은 기존의 고객 DB를 이용하여 인터넷 ID 관리 서비스라는 새로운

서비스를 시작하고 가맹 사이트를 모집하여 새로운 수익원을 창출할 수 있다.

고객의 접속 증가

가입자가 자신의 ID를 인증 받기 위해 ID 서비스 제공자에게 접근할 기회가 더욱 빈번해진다. 가입자는 ID 서비스 제공자의 사이트에서 이동할 수 있는 사이트를 좀 더 안전하다고 판단할 것이고, 쉽게 다른 사이트로 이동할 수 있기 때문에 선호도가 상승할 것이다. 가령 포털 사이트인 경우에는 가입자가 필요로 하는 모든 정보를 제공하는 동시에, 인터넷 환경에서의 사용자 ID를 증명하여 다른 사이트에게 제공하는 방법이 가능하다. 편리함과 신뢰감을 제공하는 인터넷 ID 관리 서비스를 통하여, 가입자들은 포털 사이트를 더욱 많이 이용할 것이다.

고객의 만족도 향상

인터넷 ID 관리 서비스에서 가입자의 ID정보를 다른 사이트와 공유함으로써 가입자 중심의 서비스를 제공해 줄 수 있게 된다. 또한 ID와 관련된 번거로운 작업을 가입자에게 강요하지 않기 때문에 고객의 편리함과 서비스 만족도가 향상된다. 인터넷 ID 관리 서비스를 안전하게 제공하는 것으로, ID 서비스 제공자뿐만 아니라 ID 서비스 제공자의 서비스를 받는 하부 사이트들 전체에 대해 서비스의 신뢰성 및 안전성을 보장할 수 있게 된다.

Ⅲ. 관련 기술 동향

1. ID 관리 서비스 현황

1.1 패스포트

패스포트[2]는 Microsoft 사에서 개발한 단일 로그인 서비스로서, 현재 웹 상에서 가장 큰 인증 서비스라고 할 수 있다. 패스포트의 가장 큰 특징은 중앙집중적으로 관리되는 사용자 계정이다. 사용자는 Microsoft가 관리하는 중앙의 패스포트 서버를 통하여 서비스에 가입하고, 자신의 신원을 제시하여 인증받게 된다. 패스포트는 SSO 서비스를 통해서 사용자가 한 번 로그인 만으로 가맹 사이트를 추가 인증없이 자유롭게 이동할 수 있도록 하였다. 가맹 사이트는 패스포트의 인증 시스템을 통해서 사용자를 인증하기 때문에 독자적인 인증 시스템을 구축할 필요가 없어진다.

중앙 집중적 사용자 계정관리 때문에 지적되었던 사생활 보호 정책을 강화하여, 사용자가 동의하지 않은 정보 수집과 이용을 배제하고 사용자 중심의 관리 정책을 지원하고 있다. 또한 사용자가 로그인 할 때 같은 정보를 중복해서 입력해야 하는 번거로움을 피하기 위하여 패스포트가 가지고 있는 정보로 채워주는 템플릿 기능 등을 제공하고 있다.

패스포트는 현재의 중앙 집중적 구조를 분산되고 연방적인 모델로 변경하려고 하고 있다. Microsoft는 다음 버전의 패스포트에서 커버로스(Kerberos)[3]를 지원하겠다고 공표하였는데 커버로스의 지원은 두가지 중요한 의의를 가진다. 첫 번째는 커버로스가 표준이라는 점이고, 두 번째는 커버로스가 다중 인증 도메인에서 동작할 수 있기 때문이다. 연방화된 버전의 패스포트는 커버로스를 이용하여 도메인간의 연동이 가능할 것이다.

1.2 Ping ID network 서비스

PingID 네트워크[4]는 최초의 회원제 ID 네트워크 서비스로, 비즈니스 환경에서 법률적인 요소를 중점으로 하여 개인적인 ID와 공개적인 ID 간의 상호 동작이 가능하도록 설계되었다. PingID 네트워크는 보안성과 확장성, 그리고 수준 있는 ID 연동을 보장하는 것을 목적으로 한다. ID 정보를 공유하기 위해서는 다음 요구 사항을 충족시키고자 하였다.

- ID의 분산화 보강 및 지원
- 기존 기술에 중립을 유지하면서 공개 표준 지원
- 기술과 비즈니스 도입에서의 상호운용성 지원
- 개인의 프라이버시를 상시 보호
- ID 도용의 위협에서 멤버 보호

PingID 네트워크는 연방화된 ID 관리를 선택했다[5]. 연방화된 관리에서는 인증 기법마다 다른 정도의 보안을 제공하기 때문에, 자신이 원하는 인증 레벨을 맞추는 작업이 선행되어 한다.

PingID 네트워크는 비용이 많이 들어가는 양방향 협상이나 협약을 맺을 필요 없이, 기관들 간에 ID 정보를 공유할 수 있도록 해준다. 그러는 도중에도 변함없이 최종 사용자의 프라이버시 정책은 유지하고 있다. PingID 네트워크의 회원 제도는 기업들이 독자적으로 협약을 맺지 않아도 되며, 각각의 파트너가 나름대로 연방화된 Identity 전략을 수행하기 용이하다[6][7].

1.3 국내 SSO 서비스

국내에서도 SSO 서비스가 시도되고 있다. SK 계열 몇 개의 웹 사이트를 묶은 SK 원클릭, 롯데 계열 사이트를 묶은 롯데 패밀리 등의 서비스가 있다. 그런데 이 서

비스들은 관련 사이트 몇 개 만을 묶은 것으로 포괄적인 인터넷 ID 관리 서비스라고 보기 어려운 점이 있다. 이 서비스들은 독자적인 프로토콜을 사용하고 있어 상호 연동성 측면에서도 가능성이 봉쇄되어 있는 상황이다.

2. 관련 기술 및 표준화 동향

인터넷 ID 서비스 기술 개발은 여러 진영에서 이루어지고 있는데 이들은 기술 개발과 동시에 표준화를 추진하고 있다.

2.1 OASIS SAML

SAML(Security Assertion Markup Language)[8]은 XML 관련 표준을 주관하는 OASIS[9]에서 추진하는 인증/인가 정보 전달 방식의 표준화를 위해 고안된 언어이다. 인증/인가의 상호연동성을 중심으로 하는 인터넷 ID 관리 서비스에 사용되는 핵심 기술이다.

SAML 1.0

SAML은 도메인 간에 사용자 정보를 안전하게 교환하기 위해 만들어진 확장 언어로, SOAP 프로토콜을 통하여 제공된다. SAML은 보안 토큰의 형식을 정의하고, 프로파일에서는 이들 assertion을 사용하여 웹 SSO를 제공할 수 있는 방법을 정의하였다. SAML은 3 가지 종류의 assertion을 정의하였는데, 바로 인증, 속성 정보, 인가 정보에 관한 것이다.

SAML 1.1

SAML 1.0 스펙의 피드백과 수정 사항을 주로 반영하였다. 1.0과 마찬가지로 도메인간의 표준화된 양방향 SSO를 정의하였다. 또한 디지털 인증서를 이용한 SAML assertion 서명 방법에 대한 가이드라인, 기업간의 상호 호환성 문제, assertion 과 서버 측의 기능 요소들, 구현 프로파일, 요청/응답 메시지 프로토콜 등이 정의되어 있다. SAML 1.0에 대해 assertion 레벨의 하향 호환성을 제공하지 않는다.

SAML 2.0

SAML 2.0은 주로 개발자들의 요구 사항을 반영하고, 리버티 ID-FF 1.2에서 나온 SAML의 기능상 미미한 점들을 보완하는 측면으로 개발되기 시작했는데 현재는 리버티 ID-FF를 모두 대체할 수 있도록 id federation 기능을 포함하는 범위까지 확대되었다.

2.2 리버티

리버티[10]는 연방화된 네트워크 ID 관리와 ID 기반의 서비스를 위한 공개 표준을 개발할 목적으로 2001 년 9 월에 결성되었고, 2004 년 현재 157 개의 멤버를 가진 조직으로 성장하였다.

리버티 1 단계(ID-FF 1.0)

ID-FF라고 불리는 리버티 표준 스펙의 1 단계는, 연방화된 네트워크 ID 관리를 시작하기 위한 작업을 담당한다. 여러 기능 중에서, 신뢰 관계를 맺은 CoT(Circle of Trust) 내의 서비스 제공자들이 보유하고 있는 ID들을 연결해주고 SSO를 지원한다. 추가로 ID 연동, ID 제공자 알림 서비스, 익명 ID 매핑과 글로벌 로그 아웃 서비스도 지원한다. 리버티 1 단계는 SAML 1.0을 확장한 SAML assertion을 사용하며, 연방 조직 내부의 멤버들을 ID제공자와 서비스 제공자라는 역할로 구분하여 정의하였다.

리버티 1 단계(ID-FF 1.1)

ID-FF 1.0 스펙에서 나온 피드백과 문제점을 보완하였다.

리버티 2 단계 (ID-FF 1.2)

리버티 1 단계에서 ID-FF가 지원하는 옵트-인 방식의 계정 연결과 SSO 서비스에 추가하여 익명성 서비스와 가맹 관계 설정 기능 등을 추가하였다. 익명성 서비스는 사용자의 id를 보여주지 않고 일부 상태 정보만을 요구할 때 사용하는 기능으로, 리버티 2 단계에서는 일회용 identity assertion을 이용하여 익명성을 제공한다. 가맹 관계 설정 기능은 사용자가 직접 가맹 사이트들을 선택하여 ID를 연동하는 프로토콜이다. 리버티 2 단계는 SAML assertion 을 이용하여 직원과 고객에 관한 정보를 사이트 간에 주고 받을 수 있는 메커니즘을 제공한다.

리버티 2 단계(ID-WSF 1.0: IDentity-Web Services Framework)

기존의 리버티 프레임워크에 웹 서비스를 통한 디스커버리 기능과 ID와 관련된 서비스를 제공하도록 확장하였다. 사용자가 공유하기로 결정한 정보만을 선택적으로 제공해주는 허가-기반의 속성 정보 공유 서비스(Permissions-Based Attribute Sharing), 사용자의 Identity 서비스 위치를 자동으로 찾아주는 Identity 디스커버리 서비스, 사용자가 제공해야 하는 개인 정보를

대신 제공해주는 서비스, 프라이버시와 보안에 관련된 요구 사항을 명시하는 보안 프로파일 서비스, 사용자가 모바일 환경에서 웹 서비스를 쉽게 이용할 수 있는 확장 클라이언트 지원 서비스 등을 ID-WSF가 지원하게 된다. 리버티 2 단계는 SAML 1.1 에서 정의한 메시지와 프로토콜 바인딩을 채용하고, WS-Security의 안전한 SOAP 메시지를 통하여 보안을 제공한다.

리버티 3 단계(ID-SIS: IDentity Services Interface Specifications)

리버티 3 단계는 기업들에게 표준화된 방법을 제공하여, Identity를 기반으로 하는 서비스를 구축할 수 있도록 도와준다. 이들 서비스는 리버티 2 단계에서 나온 ID-WSF 위에서 제공된다. 초기에 나온 서비스는 기본 프로파일 정보를 제공해주는 ID-Personal/Employee 프로파일 서비스로, 사용자의 등록 과정에 사용된다. 이름, 주소, 회사 주소, E-Mail 같은 정보를 보유하고 있으면서, 필요할 때 해당 정보를 알려주고, 다른 서비스와 상호 동작할 수 있다. 이 표준안 들은 1.0 버전의 스펙이 나온 상태로, ID-WSF를 이용하여 속성 정보를 교환하는 서비스를 추가할 예정이다. 예를 들어 전자 지갑이나 일정/주소록 서비스 같은 기능들이 이전에 완성된 프레임워크 위에서 동작하게 될 것이다.

2.3 WS-*

WS-*[11]는 Web Service 연동을 위해 제정된 일련의 규격들을 의미한다. 그 중 보안과 ID 관리에 연관된 몇가지 규격들을 소개한다.

WS-Security

WS-Security 스펙[4]은 보안 토큰을 이용한 무결성과 신뢰성을 웹 서비스 메시지(SOAP)에 반영하기 위한 메커니즘을 정의한다. 메시지의 무결성, 신뢰성, 인증을 포함하는 메시지 보호 수준(Quality of Protection)을 제공하기 위한 SOAP 메시지의 활용 방안이 기술되어 있다. 바이너리 보안 토큰들을 인코딩하는 방법을 설명하는 부분에서, X.509 인증서나 커버로스(Kerberos) 티켓 등을 사용하는 방식과 인증서의 특성들을 설명하는 확장 메커니즘이 추가되어 있다. WS-Security는 보안 토큰에 사용할 수 있는 여러 범용 기술을 제공하기 때문에, 다양한 종류의 보안 모델과 암호화 기술에 적용될 수 있다는 특징을 가진다. WS-Security는 정해진 보안 토큰 뿐만 아니라, 여러 형식을 사용하여 확장할 수 있도록 설계되어 있다.

WS-Security Extensions

웹 서비스 중심의 메커니즘을 기반으로 보안 도메인에서 사용할 인증, 인가, 정책에 대한 스펙을 제공한다.

WS-Trust는 신뢰 관계를 맺는 방법을 정의하는데, 직접 맺는 방법과 신뢰할 수 있는 중간 계층을 통해서 맺는 방법을 소개하고 있다. 신뢰 관계를 맺은 기관들은 WS-Security를 사용하여, 보안 토큰을 안전하게 전달하기 위한 발급 서비스를 제공하게 된다. 추가적으로 WS-Trust는 기존의 신뢰 메커니즘을 활용하는 방안과 권한 위임, 대행에 대한 서비스를 명시할 계획이다.

WS-Policy는 수신자와 송신자가 자신들의 요구 사항과 지원 가능한 정도를 명시하는 방법을 제공한다. 요구 사항과 지원 정도를 명시하는 방식에는 제한이 없지만, 이 스펙에서는 프라이버시 정보, 인코딩 형식, 보안 토큰 요구 사항, 지원되는 알고리즘 같은 몇 가지 기본 서비스를 위주로 설명하고 있다. WS-Policy는 단순한 보안 정책 이상을 지원하는 SOAP 형식을 정의하고, SOAP 메시지에 정책을 포함시키는 메커니즘을 정의할 예정이다.

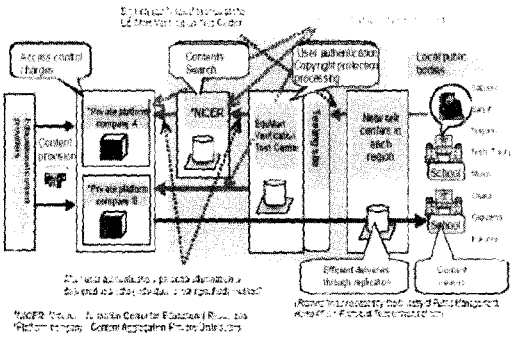
WS-Federation은 연방화된 신뢰 시나리오를 구축하는 방법을 정의하고, 커버로스와 PKI 기반 구조를 연동하는 방법 등을 표현한다. WS-Security, WS-Policy, WSTrust, WS-Secure Conversation 스펙에 기반하고, 신뢰 정책을 사용해 자신이 요구하는 신뢰 형식을 전달·제한·확인하는 절차를 정한다. WS-Federation은 신뢰 관계를 관리하는 메커니즘에 대한 정의도 추가할 것이다.

3. 적용 사례

3.1 EduMart

일본의 국가적 전략 산업인 'e-Japan 전략' 에서는 네트워크를 통해 모든 초/중/고등학교에 교육 콘텐츠를 공급할 계획을 갖고 있다. 이 사업은 여러 콘텐츠 사업자가 참여 할 수 있도록 상호운용성을 가져야 하고, 콘텐츠에 대한 적절한 보호와 관리가 가능하며, 사용자 인증을 위해 SSO가 가능하고, 기술에 종속적이지 않은 공개 기술 스펙이어야 한다는 요구 사항을 도출하였다. 결국, 교육용 콘텐츠를 분배하는 이 시스템이 'e-Japan 우선 정책 프로그램'에서의 요구 사항에 부합되는지 개념적으로 검증하려는 시도를 하게 되었다. 이 파일럿은 일본의 'EduMart(Education과 Market의 합성어) 검증 테스트'로 명명되어서 수행하게 되었다[12].

분석을 통하여 리버티의 1단계 스펙이 EduMart 검증 테스트로 선택되었다. 이것은 리버티 프로토콜이 공개



(그림 5) EduMart 아키텍처

스펙에 기반하고 있고 여러 업체로부터 지원을 받고 있기 때문이었다. 호환성을 제공하기 위해 리버티 스펙을 선택하고 난 뒤, EduMart 검증 테스트 시스템은 수 개월 만에 성공적으로 완성되었으며 리버티 스펙으로 만들어진 세계 최초의 e-Learning 시스템을 개발하게 되었다. 일본 전역에 있는 98개 공립 학교에 설치된 3500 여 개의 터미널로 언제나 콘텐츠를 사용할 수 있도록 개발되었다.

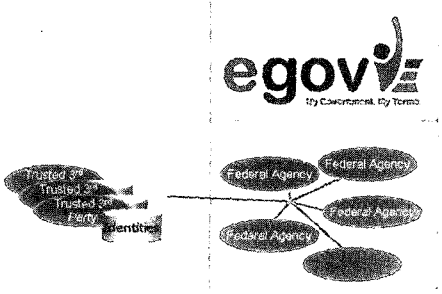
3.2 E-Authentication

미국의 E-Authentication[13] 계획은 신뢰할 수 있고 안전한 표준 인증 아키텍처를 만들어서, 24개의 E-Government 기관들에게 제공하는 것을 목표로 추진되고 있다. 이 프로젝트는 네트워크 ID를 형성하기 위한 단일화된 절차를 제공하고, 기관이 ID나 전자 서명을 확인하기 위한 솔루션에 중복 투자하지 않도록 한다.

E-Authentication 전략은 국가적인 통합 id를 사용하지 않고, 개인정보를 중앙에서 관리하지 않으며, 거래의 종류에 따라 필요한 인증레벨을 다양하게 두는 등의 기본적인 요구사항에 근거하여 시작되었다.

E-Authentication이 성공적으로 구축되면 시민과 정부에게 수많은 이점을 제공할 것이다. 시민과 비즈니스는 안전하고, 쉽고, 안정성 있는 방법을 통해 identity를 증명할 수 있고, 등록할 때 같은 정보를 매번 입력해야 하는 부담을 덜게 될 것이다. 정부 기관은 인증 시스템을 중복으로 개발할 필요가 없어져, 인증 시스템 개발을 위한 자원과 비용을 다른 업무에 투자할 수 있게 될 것이다.

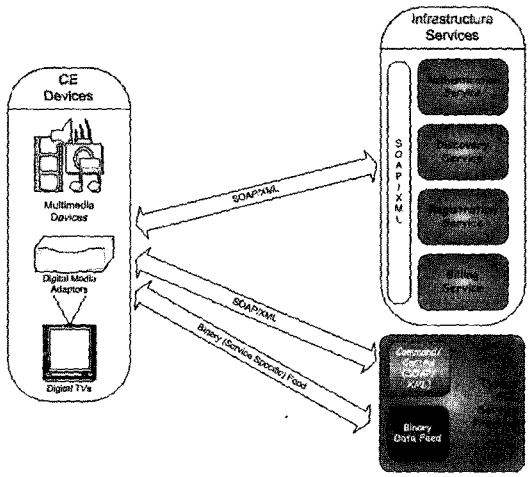
현재는 개념 정립 단계로 SAML 1.0 artifact 프로파일을 활용하는 방향으로 모델을 수립하고 있다. 또한 기존에 표준화 된 리버티 얼라이언스와 WS-*와의 호환도 고려하고 있다. 특히 GSA와 DoD는 2003년 중반에 리버티에 가입하여 활동 중에 있다.



(그림 6) E-Authentication 아키텍처

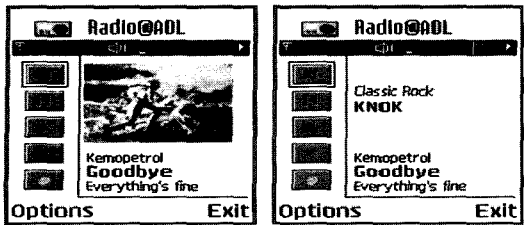
3.3 AOL

AOL은 휴대폰과 같은 모바일 디바이스에서 디지털 라디오, 디지털 사진 등의 컨텐츠를 제공하는 서비스를 만들었다[14]. 서비스는 웹서비스 방식을 사용하고 모바일 디바이스가 직접 웹서비스 클라이언트로 동작한다. 컨텐츠 서비스는 써드파티 서비스 제공자들이 제공하고 인증, 서비스 검색, 등록, 과금과 같은 인프라 서비스는 AOL에서 제공한다. AOL은 이러한 웹서비스의 인프라 서비스를 위해 Liberty의 ID-WSF 규격을 채택하였다. 그림 7은 이러한 AOL 서비스 구조를 보여 준다. 클라이언트는 SOAL기반으로 동작하는 ID-WSF의 Authentication 서비스를 이용해 로그인하고 Discovery Service를 이용해 컨텐츠 서비스에 대한 접근 주소를 찾는다.



(그림 7) AOL Service 아키텍처

현재 제공되는 서비스는 D-Link사에서 제공하는 디지털 라디오 서비스인 Radio@AOL가 있다. 현재 웹 서비스 클라이언트가 탑재된 Nokia의 휴대폰을 통해 이러한 서비스를 이용할 수 있다. 그림 8은 Radio@AOL의 서비스 화면을 보여준다.



(그림 8) Radio@AOL Service

IV. ETRI 인터넷 ID 관리 서비스 기술

한국전자통신연구원(ETRI)에서는 인터넷 ID 관리 서비스를 제공할 수 있는 시스템을 개발 중에 있다. 이 시스템은 Liberty ID-FF 1.2 규격을 준용하여, id federation 방식을 사용하여 높은 확장성과 상호 운영성을 달성할 수 있고, 복합인증, SSO, 단일로그아웃, ID 정보열람, 대화형 질의, 개인정보보호 등의 기능을 제공한다.

1. 특 징

다양한 인증 메커니즘 지원

기업의 자원 또는 서비스는 필요에 따라서 서로 다른 사용자 인증 강도를 요구한다. 본 시스템은 다양한 종류의 인증 메커니즘을 지원하도록 설계되어 있다. 현재 지원하는 인증 메커니즘으로는 패스워드와 X.509 인증서를 지원하고 있으며 향후 생체인식 기술에 대해 지원할 것이다.

SSO와 개인화 서비스

SSO 서비스는 사용자가 한번만 인증하면 관련되는 모든 웹사이트의 정보 또는 서비스를 이용할 수 있게 해주는 서비스로 사용자의 편의성을 대폭 향상시켜주고 웹사이트 간에 사용자 정보를 공유하여 보다 개인화된 서비스를 제공할 수 있다는 장점이 있다.

중앙 집중적인 정책 관리·지원

전반적인 ID 관리 시스템은 IDSP가 주도적으로 정책을 설정하고 사용자를 인증하는 구조로 설계되어 일관된 정책의 설정과 실행을 수행할 수 있다. 본 시스템은 관리자가 보다 편리하게 정책을 설정하도록 도와주고 한번 설정된 정책이 일관성 있게 실행될 수 있도록 여러 가지 기능을 지원한다.

가입자 중심의 개인정보 보호 서비스

가입자가 직접 본인의 정보 제공여부를 결정하여 정책으로 지정할 수 있는 기능을 제공하여 개개인의 개인정보 요구사항을 유연하게 충족시켜 주는 서비스이다. 또한 특정 정보의 경우에는 실시간으로 가입자의 동의를 얻어야 가입자 개인 정보를 유통할 수 있도록 하는 기능을 제공하여 개인정보에 대한 가입자의 통제권을 확대하는 기능을 제공한다.

강화된 보안 서비스

인터넷 ID 관리 시스템은 기본적으로 보안을 처음 디자인 단계부터 고려하여 설계에 반영한다. 따라서 보안 취약성이 예상되는 곳에 미리 적합한 보안 메커니즘을 적용하여 기밀성, 무결성, 가용성 등과 같은 다양한 보안 요구사항을 만족시킨다.

표준화

타 ID 관리 시스템과의 상호 연동성과 보안성 입증을 위해 다양한 국제 표준을 준용하였다. Federation과 SSO를 위한 표준으로 리버티 ID-FF 1.2를 채택하였고, 인증 assertion은 OASIS의 SAML 1.1, XML의 보안을 위해 W3C의 xmlenc와 xmldsig를 사용하였다.

2. 서비스 모델

인터넷 ID 관리 서비스는 IDSP와 서비스에 가입한 가입자, 서비스에 가맹한 SP로 구성된다. 가입자는 자신의 개인정보를 등록하고 id와 패스워드를 등록하여 가입하게 된다. 인터넷 ID 관리 서비스 제공자는 기존에 가입자를 많이 확보하고 있는 포털 등이 될 가능성이 높은데 이 경우 가입자가 새로 등록할 필요 없이 기존에 등록된 개인정보와 id를 사용하면 된다. 가맹 웹 사이트는 서비스 제공자와 사전에 비즈니스 관계를 갖고 있을 가능성이 있으며 가맹 수수료는 이러한 비즈니스 관계에 따라 처리된다.

인터넷 ID 관리 서비스 가입자가 SP를 이용하는 경우에는 IDSP의 인증을 거치게 된다. SP에는 인증 확인 정보가 전달되며, 한번 인증을 거친 후에는 다른 SP를 이용하는 경우에도 IDSP가 SP에 인증 확인 정보를 전달하기만 하면 되기 때문에 추가적인 인증 없이 이용할 수 있다. IDSP는 등록된 개인 정보를 SP에 전달할 수 있다. SP에 가입이 필요한 경우, IDSP가 개인정보를 제공해 주기 때문에 가입자는 자신의 개인정보를 추가로 등록할 필요가 없게 된다. 개인정보가 변경된 경우에도 IDSP에 등록된 정보만 변경해 주면 IDSP가 이를 SP에

전달하여 항상 최신 정보를 유지할 수 있다. 인터넷 ID 관리 서비스에서는 SP가 자신의 사용자 DB를 유지하지 않고 IDSP가 제공하는 개인정보를 이용해서 서비스할 수도 있다. 이러한 개인정보의 전달 과정은 가입자의 통제 하에 이루어진다. 어떤 SP에게 어떤 정보를 제공해도 되는지 여부를 가입자가 결정하는 것이다.

인터넷 ID 관리 서비스에서는 하나의 IDSP와 해당 서비스 가입자, 해당 서비스 SP 들의 집합을 하나의 서비스 도메인으로 정의한다. 가입자가 도메인을 넘어 다른 도메인에 가맹된 SP를 이용하는 경우를 로밍이라고 한다. 가입자가 로밍 서비스를 요구할 때에는 IDSP 간에 사전에 제휴가 되어 있어 인증 확인 정보를 상호 교환하는 방식으로 동작한다. SP는 자신이 가맹한 IDSP로부터 인증 확인 정보를 제공받는다. IDSP는 사용자가 가입되어 있는 도메인의 IDSP로부터 인증 확인 정보를 제공받게 된다.

3. 시스템 구조

인터넷 ID 관리 시스템은 그림 9와 같이 구성되어 있으며 각각의 구성 요소가 제공하는 기능은 다음과 같다.

인터넷 ID Server

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

인터넷 ID Server Admin

인터넷 ID Server를 운영하기 위한 관리 도구로서 인터넷 ID 관리 서비스의 다양한 정책과 시스템 운영을 관리하기 위한 기능을 제공한다.

웹 응용 Server Agent

가맹 웹 사이트의 웹 서버에서 실행되며 웹 응용 프로그램과 연동하여 인터넷 ID 관리 서비스를 제공하기 위한 Agent 모듈이다. 인증 요청, 개인정보 열람 기능을 수행한다.

가입자 웹 브라우저

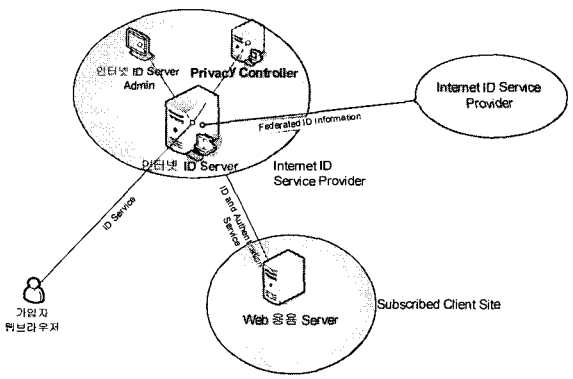
인터넷 ID 관리 서비스는 기본 브라우저 만으로 실행된다. 가입자는 브라우저를 통해, 가입, 개인정보 관리, 개인정보 보호 정책 관리 등의 기능을 수행하게 된다.

4. 주요 기능

시스템 기능은 크게 가입자에게 다양한 인증 메커니즘을 지원하는 복합인증 기능, 한번 인증에 모든 사이트 접근을 지원하는 인터넷 SSO 기능, 가입자 ID 정보 생명주기를 관리하는 ID 관리 기능 및 개인정보의 오남용 방지를 지원하는 개인정보 보호 기능을 제공하고 가맹사이트에는 가입자의 ID 정보에 대한 열람 기능을 제공하는 ID 정보 열람 기능으로 구분된다.

복합 인증 기능

가입자가 처음에 시스템에 접근하면 시스템은 인증서 또는 패스워드 방식의 인증 메커니즘 중에 하나를 선택적으로 이용하여 가입자에게 credential을 제출할 것을 요구한다. 가입자가 credential을 제출하면 시스템은 검증하여 가입자를 인증한다. 시스템을 사용하기 위해 반드시



〔그림 9〕 ETRI 인터넷 ID 관리 시스템 아키텍쳐

거쳐야 하는 기본 기능으로 제공된다.

인터넷 SSO 기능

가입자가 가맹사이트에 접근하면 가맹사이트는 가입자에게 인증을 요청한다. 가입자가 인증이 필요하면 앞에서 설명한 복합 인증 기능을 이용하여 인증하고 가입자가 이미 한번 인증을 받은 경우에는 추가적인 인증 없이 가맹사이트를 이용할 수 있도록 한다. 가입자가 이미 인증을 받았지만 가맹사이트가 다른 인증 메커니즘으로 사용자를 인증할 것을 요구할 때는 가입자 재인증 요구 기능을 지원한다. IDSP들 간의 SSO도 본 기능을 이용한다.

개인정보 보호 기능

가입자가 자신이 IDSP에 등록한 개인정보 중에 가맹사이트에 제공할 것을 허용하는 정보에 대하여 정책을 설정할 수 있도록 하는 기능이다. 또한 개인정보 중 필요에 따라 사용자에게 직접 정보의 사용 허가 유무를 질의할 수 있도록 하는 대화형 질의 기능을 제공한다. 가입자는 또한 자신의 정보 통제 설정 기능을 조회할 수 있도록 하는 기능을 제공한다.

ID 관리 기능

가입자는 시스템에 가입할 때 가입자 id와 개인정보를 제공한다. 가입 후에는 id 생명주기 관리 기능을 이용하여 가입자 id를 제외한 개인정보를 변경 및 삭제할 수 있다. 인증서와 같은 가입자의 credential은 credential 위탁 기능을 이용하여 시스템의 저장소에 위탁 보관할 수 있고 필요 시에 인출하여 사용할 수 있다. 가입자가 가맹사이트와 IDSP 간의 ID를 연동하려고 할 때는 ID Federation 설정 기능을 이용한다. 이렇게 설정된 정보들은 가입자가 필요 시 조회 할 수 있고 해제도 가능하다.

ID 정보 열람 기능

가입자의 ID 정보 열람은 크게 시스템에서 가맹사이트로 가입자 정보를 자동 갱신 해주는 기능과 가맹사이트에서 시스템에 정보를 조회하는 기능으로 나누어진다. 가입자 정보 자동 갱신 기능을 사용하기 위해서는 가맹사이트에서 시스템에 등록 신청을 한다. 등록이 완료되면 가맹사이트에서는 가입자의 개인정보가 변경될 때마다 자동으로 정보를 받아 볼 수 있다. 가입자의 ID 정보 조회는 가맹사이트 또는 다른 IDSP에서 필요 시 조회한다. 이때 조회하는 정보가 가입자의 동의를 얻을 필요가 있으면 시스템은 대화형 질의 기능을 이용하여 가입자에게 동의 여부를 물어본다.

V. 결 론

인터넷 상의 산재한 id와 개인정보를 효과적으로 관리하고 편리하게 이용할 수 있도록 해주는 인터넷 ID 관리 서비스에 대해, 이제는 필요성에 대한 논의를 넘어 이것을 어떻게 도입하고 적용하는가에 대해 세계적인 IT메이저들이 치열하게 기술 경쟁을 벌이고 있는 실정이다. 이미 선진국에서는 전자 정부, e-learning, 모바일 서비스 등에 이를 적용하고 있으며 앞으로 그 범위는 더욱 확대될 것이다. 이러한 흐름에 뒤떨어지지 않기 위해서 국내에서도 인터넷 ID 관리 서비스를 위한 기술 개발과 도입이 시급한 실정이다. 이미 IT 강국으로 인정받고 있는 훌륭한 인프라와 전국민이 얼리어답터인 우리의 조건은 인터넷 ID 관리 서비스의 도입과 활용에 있어서도 짧은 기간에 세계 최고 수준으로 도약할 수 있을 것이다. 이를 위해 ETRI에서는 인터넷 ID 관리 서비스 시스템 개발에 박차를 가하고 있으며 2004년 11월 첫번째 버전을 내놓을 예정이다.

참 고 문 헌

[1] 전길수, 권현조, 정재호, "아이덴티티 위협에 대처하는 아이덴티티 매니지먼트 기술," 정보보호 뉴스, KISA, 2004

[2] Geiger, ".Net My Services and .Net Passport User Authentication Overview", Microsoft white paper, 2001

[3] Kerberos, http://web.mit.edu/kerberos/www/

[4] PingID 네트워크, http://www.pingid.com

[5] Federation Standards Overview, Ping Identity, 2003

[6] Ping Identity, http://www.pingidentity.com

[7] SourceID, http://sourceid.org

[8] Open SAML, http://www.opensaml.org

[9] OASIS Web Services Security TC http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[10] Liberty, http://www.projectliberty.org

[11] WS-Security, http://www-106.ibm.com/developerworks/webservices/library/ws-secure

[12] Edumart 실증실험보고서, 일본총무성, 2003

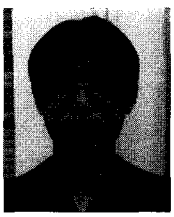
[13] e-authentication, http://www.whitehouse.gov/omb/egov/ea.htm

[14] Identity Management Market Consolidation: Not the End of Innovation, Mark McClain, Digital ID World March/April p.66-67, 2004
[15] 한국전자통신연구원, "인터넷 ID 관리 서비스 기술 백서 v1.0", June 2004

〈著 者 紹 介〉

최 대 선 (Dae-Seon Choi)
정회원

1995년 : 동국대학교 전자계산학과 학사
1997년 : 포항공과대학교 전자계산학과 석사
2003년~현재 : 한국과학기술원 전산학과 박사과정
1997년~1999년 : 현대전자/현대정보기술 정보시스템연구소
1999년~현재 : 한국전자통신연구원 정보보호연구단 인증기반연구팀 선임연구원
관심분야 : ID 관리, 신뢰관리, P2P/MANET 보안



조 상 래 (Sangrae Cho)
정회원

1996년 : Imperial College of Science, Technology and Medicine, 전산과 (학사)
1997년 : Royal Holloway, University of London, 정보보호 (석사)
1997년~1999년 LG 종합기술원 연구원
1999년~한국전자통신연구원 정보보호연구단 인증기반연구팀 선임연구원
관심분야 : PKI, 접근제어(RBAC), 프라이버시 보호 기술

김 승 현(Seung-Hyun Kim)
정회원

2002년 : 금오공과대학교 컴퓨터공학과 학사
2004년 : 포항공과대학교 컴퓨터공학과 석사
2004년 1월~ 현재 : 한국전자통신연구원 정보보호연구단 인증기반연구팀 연구원
관심분야 : 정보보호, 소프트웨어 프로세스

진 승 헌 (Seung-hun Jin)
정회원

1993년 2월 : 숭실대학교 전자계산 공학과 공학사
1995년 2월 : 숭실대학교 전자계산공학과 공학석사
2004년 2월 : 충남대학교 컴퓨터과학과 공학박사
1994년 12월~1996년 4월 : 대우통신 종합연구소
1996년 5월~1999년 5월 : 삼성전자 통신연구소
1999년 6월~현재 : 한국전자통신연구원 정보보호연구단 인증기반연구팀장/선임연구원
관심분야 : 컴퓨터/네트워크 보안, 정보보호(PKI)

정 교 일 (Kyo-il Chung)
정회원

1981년 : 한양대학교 전자공학과(공학사)
1983년 : 한양대학교 산업대학원 전자계산학과 (공학석사)
1997년 : 한양대학교 대학원 전자공학과 (공학박사)
1982년~현재 : 한국전자통신연구원 정보보호연구단 정보보호기반연구그룹장/책임연구원
관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리