情報保護學會論文誌
第18卷 第4號, 2008. 8

인터넷 ID관리를 위한 서비스 모델 제안*

송 정 환[1†], 강 연 정[2], 장 환 석[1‡]
[1]한양대학교, [2]한국정보보호진흥원

Proposal for Service Model for Internet Identity Management*

Junghwan Song[1†], Yeonjung Kang[2], Hwanseok Jang[1‡]
[1]Hanyang University, [2]Korea Information Security Agency(KISA)

요 약

인터넷 상에서 개인 식별을 가능하게 함으로써 개인의 안녕과 이해관계에 영향을 미치는 정보로서 각종 ID와 개인정보를 포함하도록 인터넷 ID를 정의한다면, 이를 안전하게 이용할 수 있도록 보호하고 관리하는 인터넷 ID 관리(Internet Identity Management) 기술이 필요하다는 것은 자명한 일이다. 현재의 인터넷 ID 관리 기술은 서비스의 수가 많아질수록 기억하고 관리해야 하는 ID와 인증정보의 수가 늘어나고, 심지어는 자신이 어떤 서비스에 어떤 ID와 인증정보를 등록하였는지 기억하지 못하는 경우도 발생하게 된다. 이런 이유로 유사하거나 동일한 ID와 인증정보의 사용, 개인정보의 수정의 어려움 등 여러 가지 문제점들이 발생하게 되었고, ID 관리와 관련된 개인정보 침해 사고도 빈번해졌다. 본 논문에서는 현재의 인터넷 환경에서 ID 관리 문제점을 해결하기 위한 대안으로서 인터넷 ID 관리 서비스 모델을 제시한다.

ABSTRACT

The incredible progress of information and communication technology has allowed various information and communication services to emerge in the Web environment. Such a service is initiated when the user provides his/her personal information to the service provider and is then given an identifier and authentication data. A series of the processes is inconvenient as it requires authentication by the service provider each time that the user requests the service. Furthermore, as the user subscribes to more services, the volume of ID and authentication information increases. This compels the users to use an ID that is easy to remember or to register the same ID over and over, increasing the risk of ID hacking. It is clear that such threats will become more serious as our lives become more dependent upon the Internet and as the Internet service environment advances. With the introduction of different services, the need to efficiently manage ID has been raised. In this paper, a Internet Identity Management Service that enables the control of the flow of the user's personal information, which is used and stored for the Internet service, is proposed from the user's perspective.

Keywords : Identity Management, service model

접수일 : 2007년 11월 28일; 수정일 : 2008년 2월 17일;
채택일 : 2008년 5월 7일
* 본 연구는 한국정보보호진흥원 위탁연구과제 결과로 수행되었음. (KISA-WP-2007-0044).
† 주저자, camp123@hanyang.ac.kr
‡ 교신저자, jhs1003@hanyang.ac.kr

Ⅰ. 서 론

1990년대 초에 WWW(World Wide Web, 웹)의 등장으로 대중들에게 알려지기 시작한 인터넷은 현재 우리 생활 깊숙이 차지하고 있는 기반구조가 되었다. 이로

인해, 인터넷을 통한 전자 금융거래, 전자정부 서비스, 사이버 교육 등 그 수를 헤아릴 수 없을 정도의 인터넷을 이용한 서비스들이 급격한 증가 추세에 있으며, 오프라인에서 이루어지던 주변의 생활 형태들이 자연스럽게 온라인상으로 옮겨가게 되었다. 향후에는 유비쿼터스(ubiquitous) 환경과 같은 고도의 발전된 형태의 인터넷 환경이 도래함에 따라 더욱 인터넷 이용 서비스가 확대 적용될 것으로 예상된다[1,3,4].

인터넷을 이용한 서비스를 이용하기 위해서는 서비스 제공자로부터 사용자 신원확인을 받아야 한다. 이를 위해 사용자들은 자신의 개인정보를 사전에 등록하고, 서비스 제공자로부터 식별자(ID; Identifier)와 인증정보(예; 패스워드)를 설정하여, 서비스 이용을 원할 경우에 등록된 식별자와 인증정보로 사용자 신원확인을 수행하게 된다. 이것은 사용자가 이용하려는 서비스의 수가 많아질수록 기억하고 관리해야 하는 식별자와 그에 따른 인증정보의 수가 늘어나는 불편함을 초래한다. 심지어는 자신이 어떤 서비스에 어떤 식별자와 인증정보를 등록하였는지 기억하지 못하는 경우도 발생하게 된다. 이런 이유로, 일반적인 대부분의 사용자는 기억하기 쉬운 형태 혹은 자신과 관련된 정보들을 이용해 식별자를 등록하거나 또는 동일한 식별자를 여러 서비스 제공자에게 등록하기 때문에 식별자에 대한 해킹의 위험이 커지게 된다. 또한, 해당 서비스 가입절차를 거칠 때, 거의 비슷한 개인정보를 반복적으로 입력하라는 요구를 받게 되고, 만약 개인정보의 수정 사항이 생겼을 경우 가입된 서비스를 일일이 찾아가 자신의 정보를 직접 수정해야 하는 불편함도 있으며, 어떤 웹사이트에서 자신의 변경된 개인정보를 수정해야 되는지 조차도 파악하기 어렵다.

요즘 큰 사회적 문제로 대두되고 있는 개인 정보 침해의 문제도 위와 같은 ID 관리 문제에 기인한다. 최근 이슈가 된 온라인 게임 명의도용사건, 공공기관 홈페이지를 통한 개인정보 누출, 타인의 주민번호 도용으로 특정 사이트에 가입한 여러 사건 등은 ID 관리 문제에 의한 것이며, 인터넷 규모의 ID 관리 필요성을 말해 주고 있는 현실에서의 예이다. 이러한 예들은 우리의 생활에서 인터넷 의존도가 점점 높아지고, 인터넷 서비스 환경이 고도화되면 더욱 심각하게 나타날 것이라는 예상을 더욱 분명하게 만든다. 국내외적으로 ID 관리 문제를 해결하기 위한 노력이 법적인 방안과 여러 프로젝트들로 행해지고 있다. 대표적인 예로, Microsoft 사의 'Laws of Identity'[5]에 기반한 ID Metasystem 개념을 Infocard 프로젝트로 구현한 Cardspase[7]와 ETRI의 e-IDMS ETRI-Identity Management System)[6] 등이 있다. e-DMS의 경우는 IDSP(Identity Service Provider)의 역할 비중이 크다. 이 시스템의 경우는 사용자의 개인정보 및 인증정보들을 IDSP에 등록하여, 특정 SP(Service Provider)를 이용하는 경우는 IDSP의 인증을 거친 후 IDSP로부터 SP에게 사용자의 인증확인 정보가 전달되게 된다. 또한 IDSP는 등록된 사용자의 개인정보를 SP에게 제공할 수 있도록 되어 있는 시스템이다. 따라서 IDSP는 사용자의 개인정보 및 인증정보들을 수집해야 되고, 이를 데이터베이스로 구성하여 유지, 관리해야 된다. 이런 시스템은 웹서비스 기반의 ID 관리 서비스로 사용상의 편리함을 제공해 주고, 전달되는 개인정보가 사용자에 의해 통제 된다 하더라도 사용자들의 모든 개인정보들이 IDSP로 수집되고, 집중화되는 문제점을 지닌다고 볼 수 있다. 이로부터 IDSP는 개별 사용자의 웹서비스 사용현황 등과 같은 분석된 사용자의 개인정보를 자연스럽게 수집할 수 있는 문제점 등도 발생할 수 있다. 또한 개인정보의 집중화를 방지하기 위해 서비스를 위한 개인정보를 IDSP와 SP가 분산 수용한다 하더라도, 사용자의 개인정보는 일정부분 IDSP에 저장될 수밖에 없으므로 정보의 집중화는 피할 수 없는 문제이다. 또한 연산상의 부하가 IDSP에 집중될 수 있다는 문제점도 지니고 있다. IDSP는 SP에서 요구하는 사용자의 인증 프로세스를 수행해야 한다. 따라서 많은 SP와 사용자를 보유한 IDSP의 경우, 높은 수준의 연산을 할 수밖에 없다. CardSpace의 경우, CardSpace에 의해 이미 공유된 개인정보는 사용자가 IDSP에서 수정하더라도, SP에 영향을 주지 않는다. 즉 동기화가 되지 않기 때문에 사용자는 항상 최신의 개인정보가 어느 카드에 저장되어 있는지 숙지하고 있어야 하는 불편을 초래할 수 있다.

본 논문에서는 사용자의 인증 정보를 제공하는 IDSP의 역할이 축소되고, SP가 인증 주체가 되어 자체 발급한 인증정보를 가지고 사용자를 인증하며, 동기화 기능 등을 통해 최신의 정보를 제공하는 개선된 인터넷 ID 관리를 위한 서비스 모델을 제안하고자 한다. 이를 위해 인터넷 ID 관리 서비스 제공 주체를 식별하고, 각 주체에 대한 요구사항을 도출하며, 인터넷 ID 관리 서비스에서의 개인정보보호정책의 적용 적합성을 살펴본다.

Ⅱ. 인터넷 ID 관리 서비스의 구성

인터넷 환경은 다양한 인증 체계와 그 수단에 있어서 사용자의 ID 및 인증정보의 보관, 관리, 유지에 대한 불편함과 유사한 ID, 인증정보의 중복등록 등과 같은 취약점이 있고, 최근 이를 이용한 공격 기술들이 등장하여 사회적인 문제점으로 대두되었다. 이를 해결하기 위한 대안으로 제시하는 것이 인터넷 ID 관리 서비스이다. 이것은 최근 사회 인식 및 흐름을 반영하는 사용자 중심(User-controlled)의 ID 관리 서비스이며, 사용자 중심의 ID 관리 서비스는 자신의 개인정보와 인증정보를 안전하게 관리하고 있다가 언제, 어디서나 자신을 인증하고 개인정보를 자신의 통제 하에 선택하여 이용할 수 있는 시스템을 말한다. 본 논문에서 제시하는 인터넷 ID 관리 서비스가 갖추어야 할 기본적인 사항을 다음과 같이 설정하였다.

- 안전하고 편리한 사용
- 사용자에 의한 정보 제어
- 최소한의 개인정보 수집 및 수집 목적의 명확성
- 개인정보, 인증정보 등 정보의 안전한 전송 및 관리

이는 기존 인터넷 환경에서 부족한 측면들을 보완하며, 사용자 중심의 ID 관리 및 최근 개인정보보호와 관련된 정책 동향을 바탕으로 설정한 것이다.

2.1 용어 정의

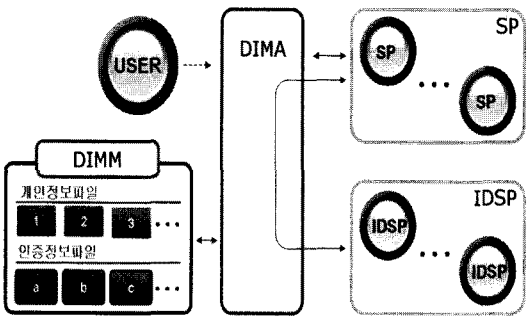
인터넷 ID 관리 서비스 모델을 제안하는데 사용되는 용어를 [표 1]에 정의한다.

2.2 서비스 모델의 구성객체

인터넷 ID 관리 서비스는 ID 관리 서비스를 제공하는 IDSP와 이를 이용하는 User, 인터넷 서비스를 제공하는 SP들로 구성한다. 여기서, SP는 상황에 따라 IDSP가 될 수도 있다. 즉, User가 과거에 SP의 서비스를 이용하면서 생성한 특정 사용자생성정보를 다른 SP의 서비스를 받는 과정에서 필요로 할 경우에 과거의 SP는 IDSP 역할을 하게 된다. [그림 1]은 인터넷 ID 관리 서비스의 기본 구성객체와 이들의 관계를 도식화한 것이다.

〔표 1〕 용어 정의

기본 구성 객체	사용자(User)	인터넷 ID 관리 서비스를 이용하여 인터넷 서비스를 이용하는 주체로, 전자 ID 관리 모듈을 제어함
	서비스 제공자 (SP)	인터넷 서비스를 필요로 하는 User에게 제공하는 주체이며, IDSP와 사용자생성정보를 공유하여 서비스를 제공함
	ID 관리 서비스 제공자(IDSP)	인터넷 서비스 제공뿐만 아니라 인증정보 및 서비스에 필요한 사용자생성정보를 제공 또는 공유하는 주체
전자 ID 관리 모듈 (DIMM)		User의 신원확인 수단이 있으며, 인터넷 ID 관리 서비스에 관한 User의 개인정보파일, 인증정보파일 등 User의 전자적 기록을 안전하게 보관하고 관리하는 이동 가능한 모듈
디지털 ID 관리 지원 어플리케이션 (DIMA)		DIMM을 이용하여 User가 인터넷 ID 관리 서비스를 이용할 수 있도록 지원하는 어플리케이션. 인가된 사용자의 접근에 대해서만 DIMM 내의 개인정보파일, 인증정보파일 등 User의 전자적 기록을 이용하여 인터넷 ID 관리 서비스를 제공함
인터넷 ID 관리 서비스 지원기관		DIMA와 DIMM을 제공하는 기관
개인정보파일		인터넷 ID 관리 서비스를 이용하여 특정 서비스에 가입할 경우에 필요한 User의 기본적인 개인정보만을 담고 있는 정보파일. 최소한의 개인정보만을 담고 있어야 하며, 서비스 제공자가 가입 시에 요구하는 개인정보의 항목에 따라 여러 종류가 존재할 수 있음
인증정보파일		인터넷 ID 관리 서비스를 이용하여 특정 서비스에 가입한 이후에 로그인(log-in)을 위한 ID, 인증정보 및 사용자생성정보, 서비스 관련 항목 등을 담고 있는 정보파일. 가입한 SP에 의해 발급되며, ID와 인증정보는 각각 안전한 길이의 난수열을 사용함.
사용자생성정보		User가 특정 서비스를 제공받기 위해 직접 입력하거나, 입력된 정보의 처리와 가공을 통해 얻어진 개인정보 이외의 정보들을 말함. IDSP가 제공하여 공유되는 사용자생성정보를 공유사용자생성정보라 함.



〔그림 1〕 인터넷 ID 관리 서비스 모델 기본 구성

2.2.1 User, DIMA 및 DIMM

User는 인터넷 ID 관리 서비스를 이용하여 인터넷 서비스를 이용하는 주체로서, DIMA를 이용해 자신의 DIMM을 제어하여 인터넷 ID 관리 서비스를 이용할 수 있다. 이를 위해 인터넷 ID 관리 서비스 지원기관을 통해 DIMA와 DIMM을 설치해야 한다. 또한 User는 세부적인 기술을 인지할 필요는 없지만, 인터넷 ID 관리 서비스를 사용하기 위한 기본적인 절차 및 사용법을 숙지하고 있어야 하며, 인터넷 ID 관리 서비스에서 처리, 전송되는 개인정보, 인증정보, 사용자생성정보 등에 대한 DIMA의 명시적인 확인 절차에 대해 응해야 한다.

DIMM은 인터넷 ID 관리 서비스의 핵심 요소로 DIMA을 통해 로드(load)되며, User는 정상적인 접근제어 절차를 통과 했을 경우에만 인터넷 ID 관리 서비스를 이용할 수 있다. 즉, DIMA는 DIMM의 접근제어 기능을 이용하여 User의 신원확인을 수행하고, User로부터 인가된 접근제어를 통해 DIMM에 수록된 정보를 이용하게 된다. 이런 방식을 통해 DIMA는 다수의 User가 사용할 수 있으며, User는 자신의 DIMM을 원하는 저장소에 저장하여 DIMA가 설치된 장소에서 인터넷 ID 관리 서비스를 이용할 수 있게 된다.

DIMM은 개인정보의 빈번한 노출을 막기 위해서 인터넷 서비스 가입 시 필요한 User의 개인정보를 담고 있는 '개인정보파일'과 가입 후 발급되는 로그인에 필요한 인증정보, 서비스 이용정보, 사용자생성정보 등을 담고 있는 '인증정보파일'로 구분하여 User의 정보를 포함하며, 이를 안전하게 보관한다. 개인정보파일은 DIMA을 통해 User 또는 공인된 기관에 의해 생성될 수 있으며, User의 실명인증에 필요한 내용이 반드시 하나 이상 포함되어야 한다.

2.2.2 IDSP와 SP

SP는 인터넷 서비스를 User에게 제공하는 주체로서 인터넷 ID 관리 서비스에서 IDSP부터 제공되는 개인정보 및 서비스관련 정보들을 이용하여 서비스 편의를 도모한다. SP는 User가 신규 가입하거나 전환 가입에 필요한 인터페이스 및 로그인 기능을 제공해야 하며, User가 인터넷 ID 관리 서비스를 사용하기 위한 기본적인 절차 및 사용법을 숙지하도록 유도해야 한다. 또한, 가입에 필요한 개인 정보 항목을 제공 서비스에 준해 설정해야 하며, 각 개인정보 항목에 대한 정당한 수집 이유를 반드시 명시해야 한다. 정보항목 공유 및 동기화를 위한 사용자생성정보의 항목에 대한 정책을 수립하고, 인터넷 ID 관리 지원 어플리케이션이 요청할 경우 사용자생성정보를 제공해야 한다. SP는 User에게 서비스를 제공하는 과정에서 User의 입력이 필요한 정보 항목이 있다면, DIMA과의 프로토콜을 통해 해당 항목의 내용을 제공해 줄 수 있는 다른 SP 즉, IDSP가 있는지를 확인할 수 있고, 이를 User에게 확인 후 IDSP에게 그 항목의 내용을 요청할 수 있다. 이 때, IDSP는 User의 동의를 얻은 요청에는 반드시 응해야 한다. 그리고 SP는 전반적인 시스템의 흐름 및 기술적인 전문지식을 보유하고 있어야 하며, 문제 발생 시 이에 대응할 수 있어야 한다.

2.3 필요 기능 정의

편리하고 안전한 인터넷 ID 관리 서비스를 제공하기 위해 구성객체들이 기본적으로 포함하고 있어야 되는 기능은 [표 2]와 같다.

Ⅲ. 인터넷 ID 관리 서비스 모델

인터넷 ID 관리 서비스의 가입 모델은 User가 이용하고자 하는 인터넷 서비스에 가입신청을 하면서 이루어진다. 가입모델에는 신규가입, 기존 가입자 처리 등이 있다.

3.1 서비스 가입 모델

3.1.1 신규 가입

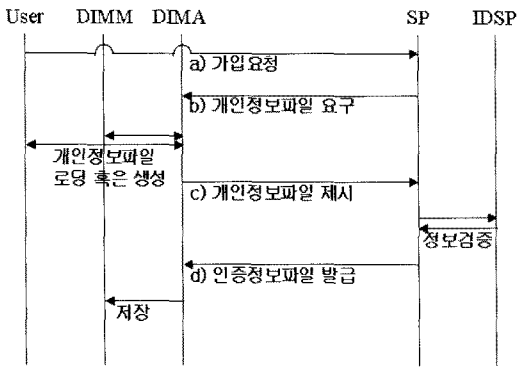
User가 SP의 웹사이트에 가입요청을 하면 SP는 필요한 User의 개인정보를 요구한다. 개인정보파일을 제

〔표 2〕 필요 기능 정의

기능 정의	내용
접근제어 기능	User의 식별, DIMM 내의 정보에 대한 외부 접근 금지, DIMM 내의 중요 정보에 대한 별도의 접근 제어 기능, 인증정보파일을 이용한 로그인 등의 기능을 말한다.
DIMA의 기본 관리 기능	개인정보 항목에 대한 조회, 수정, 변경이 가능해야 하며, 가입된 SP 사이트 목록 조회 및 해당 사이트에서 생성한 사용자생성정보에 대한 조회가 가능해야 하며, 생성정보들 간의 연관성를 표시하는 기능을 포함한다.
안전한 통신 채널 구성 기능	DIMA와 SP 혹은 DIMA과 IDSP 사이에서 정보 교환을 위해 안전한 채널을 구성하거나 해지하는 기능을 말한다.
정보 공유 기능	안전한 통신 채널을 구성하여, 사용자생성정보를 SP에서 필요로 하는 정보 항목들을 IDSP에서 공유하는 기능을 말한다.
정보 동기화 기능	안전한 통신 채널과 정보 공유 기능을 이용하여, 변경되거나 수정된 개인정보 또는 사용자생성정보의 동기화 기능을 말한다.
유지관리 기능	SP시스템 환경의 개선 작업이나 성능 향상을 안전하게 할 수 있으며, 수집된 User 개인정보들이 안전하게 보존, 유지 될 수 있는 기능을 말한다. SP는 전반적인 시스템의 흐름 및 기술적인 전문지식을 보유하고 있어야 하며, 문제 발생 시 이에 대응할 수 있어야 한다.

시하여, 가입 절차를 완료하면 SP로부터 인증정보파일을 발급받는다. 일반적으로 User는 DIMM에 저장해 놓은 개인정보파일을 이용하여 인증정보파일을 발급받을 수 있지만, 개인정보파일을 이용해 또 다른 개인정보파일을 생성할 수도 있다. 이는 i-PIN[2,13] 계정을 획득하기 위한 경우가 해당될 수 있다. User는 i-PIN 계정을 획득하기 위해 자신의 개인정보파일을 i-PIN 발급기관에 제시하고, 발급된 i-PIN 계정을 이용해 새로운 개인정보파일을 생성한다. User가 개인정보파일을 통해 제시한 기본적인 개인정보 이외에도 SP 측에서 원활한 서비스 제공을 위해 필요한 가입 정보가 있다면, 필요한 부분에 대해서는 직접 입력하도록 할 수 있다. 다음에 기술된 가입 절차의 흐름도는 [그림 2]와 같다.

a) User는 SP의 웹페이지에서 인터넷 ID 관리 서비스를 이용한 가입을 선택한다.



〔그림 2〕 신규 가입 모델의 흐름도

b) SP는 User의 DIMA를 호출, 개인정보파일을 요청한다.

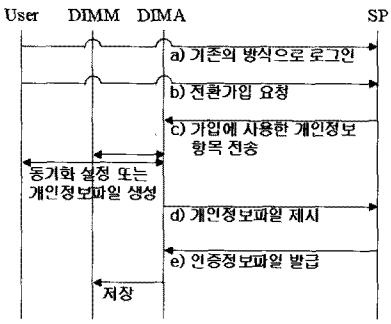
c) DIMA는 SP가 요청한 내용과 일치하는 DIMM의 개인정보파일을 User의 동의를 얻어, 안전한 채널을 통해 SP에게 제공한다. 만약, 일치하는 개인정보파일이 없다면 User가 이를 생성하도록 유도한다.

d) ID 및 인증정보를 생성하고, 서비스에 필요한 다른 정보를 User가 입력하면, 이를 포함하는 인증정보파일을 생성하여 안전한 채널을 통해 DIMA에게 제공, DIMM에 저장한 후 가입 단계를 완료한다.

- 개인정보파일에 포함된 항목 중 추가 검증이 필요한 경우에는 검증에 필요한 절차를 수행한다.

3.1.2 전환 가입

이미 SP에게 가입이 되어있는 User의 경우, 요청에 의해 인터넷 ID 관리 서비스를 이용할 수 있다. 이런 경우, User가 소유하고 있는 개인정보파일들 중 SP가 원하는 개인정보를 포함하고 있는 개인정보파일이 존재한다면, 이를 이용하여 SP와 User의 DIMA간의 동기화 목록을 설정할 수 있다. 만약 SP가 요구하는 개인정보를 포함하는 개인정보파일이 없을 경우, DIMA을 이용해 DIMM에 개인정보파일을 추가 생성할 수도 있다. 이후 서비스 제공자는 로그인 시 필요한 ID와 인증정보, 서비스 제공자가 보유하고 있던 사용자생성정보 등



〔그림 3〕 전환 가입 모델의 흐름도

을 포함하여 인증정보파일을 생성하고, 이를 User에게 제공한다.

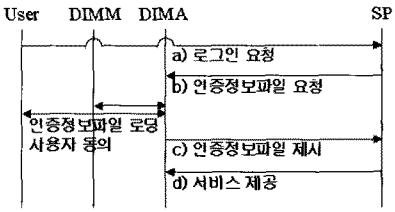
a) User는 기존의 방식으로 로그인 한다.
b) 로그인 한 상태에서 전환 가입 신청을 선택한다.
c) SP는 보유한 User의 개인정보들 중 인터넷 ID 관리 서비스 가입 정책에 준하는 항목들을 이용하여 전환 가입을 실시한다.
d) SP는 User의 DIMA를 호출하여, 안전한 채널을 통해 DIMM이 보유하고 있는 개인정보파일과 전환 가입 시 사용할 개인정보 목록을 비교하여, 동기화 목록을 설정한다. 만약, 일치하는 개인정보파일이 없다면 User가 이를 생성하도록 유도한다.
e) ID 및 인증정보를 생성하고, 이것과 사용자생성정보 등을 포함하는 인증정보파일을 생성하여 안전한 채널을 통해 User의 DIMA에게 제공, DIMM에 저장한 후 가입 단계를 완료한다.

User가 인터넷 ID 관리 서비스를 요청할 경우, SP는 개인정보파일에 포함되지 않으면서 동시에 서비스 제공자가 제공하는 서비스와 무관한 User의 개인정보들의 처리에 관한 정책이 있어야 하며, 이는 반드시 User에게 통보, 확인 과정을 거쳐야 한다. 또한, 인터넷 ID 관리 서비스를 사용 중인 User의 중복 가입에 대해서 SP는 중복 가입 여부를 정책적으로 결정할 수 있다. 다음 [그림 3]은 전환 가입의 흐름도를 나타낸 것이다.

3.2 서비스 이용 모델

3.2.1 기본 서비스 이용

User는 인터넷 ID 관리 서비스를 통해 이미 가입한



〔그림 4〕 기본 서비스 이용 모델의 흐름도

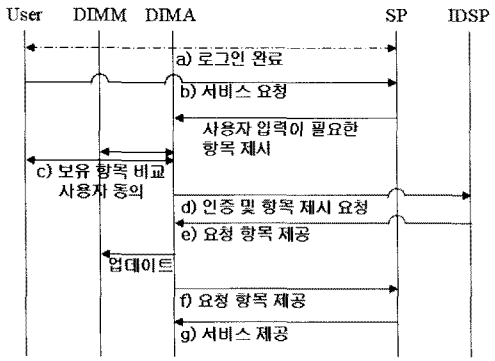
SP의 서비스를 이용하기 위해 인증정보파일을 제시하는 간단한 로그인 과정을 통하면 된다. SP의 웹페이지에는 기존의 로그인 인터페이스와 함께 인터넷 ID 관리 서비스의 인증정보파일을 업로드 할 수 있는 로그인 인터페이스를 제공해야 한다. DIMA는 User가 보유하고 있는 인증정보파일을 쉽게 이용할 수 있도록, SP와의 프로토콜을 통해 해당 인증정보파일만을 활성화하는 기능을 제공해야 한다. 인증정보파일을 이용한 로그인과 서비스 이용절차는 다음 [그림 4]와 같다.

a) User는 SP의 웹페이지에 접속하여 로그인 요청을 한다.
b) SP는 User의 신원확인을 위해, DIMA를 호출하고 인증정보파일을 요청한다.
c) DIMA는 해당 인증정보파일을 User의 화면에 나타내고, User 동의를 얻어 안전한 채널을 통해 SP에게 제공한다.
d) SP는 제공된 인증정보파일의 인증정보를 이용하여 User 신원확인을 하고, 로그인 과정을 완료하여 안전한 채널을 통해 서비스를 제공한다.

User가 서비스를 제공받으면서 생성한 사용자생성정보는 DIMA가 수집하여 DIMM의 인증정보파일에 저장할 수 있다. 이를 위해 SP는 수집 가능한 항목을 결정해야 하며, 수집된 항목에 대해서만 동기화 또는 공유를 할 수 있다.

3.2.2 사용자생성정보 공유

User가 가입을 완료한 두 개 혹은 그 이상의 SP는 생성된 사용자생성정보를 User 편의를 위해 공유할 수 있다. DIMA는 정보를 공유하고자하는 SP들 사이에서 정보의 흐름을 제어하며, 이는 User의 동의하에 이루어져야 한다. 사용자생성정보 공유에서 두 SP는 각각 역할에 따라, 정보를 제공하는 SP는 IDSP의 역할이며, 정보



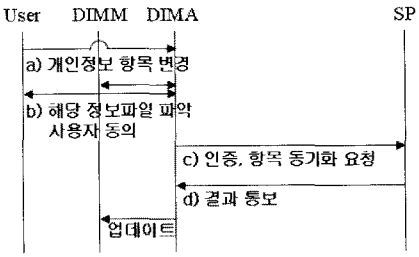
〔그림 5〕 사용자생성정보 공유 모델의 흐름도

를 제공받는 SP는 SP의 역할이다. 사용자생성정보의 공유 절차는 다음 [그림 5]와 같다.

a) User는 '기본 서비스 이용' 절차에 따라 로그인 한다.
b) User는 특정 서비스를 요청하고, SP는 IDMA를 호출하여 필요한 사용자생성정보 항목을 요청한다.
c) DIMA는 DIMM을 통해 보유한 사용자생성정보 항목과 비교하여, 이를 보유하고 있는 IDSP와 보유 정보의 목록을 User에게 제시한다. 중복되는 항목의 경우는 User가 선택하도록 한다.
d) User의 동의하에 해당 항목을 보유하고 있는 SP에게 안전한 채널을 통해 제공 요청을 한다.
   - DIMA의 요청 시, IDSP에서 DIMA를 인증하기 위해서는 인증정보파일을 이용한다.
e) DIMA의 정보 요청에 IDSP는 자신이 보유한 정보를 안전한 채널을 통해 DIMA에게 제공한다. 이때, DIMA는 해당 항목의 연관성(항목 제공처(IDSP), 항목 사용처(SP), 제공 시간 등)을 기록하여 공유사용자생성정보로서 DIMM의 인증정보파일에 보관한다.
f) User의 동의를 얻어 SP에게 보유한 생성정보를 제공한다. 추가적인 서비스 항목에 대해서는 User가 직접 입력한다.
g) SP는 입력 내용을 기반으로 User에게 서비스를 제공한다.

3.2.3 개인정보 동기화

User는 DIMA를 통해 자신의 개인정보파일에 포함된 개인정보를 변경하고 동기화 할 수 있다. User가 개인정보 항목을 변경하게 되면, DIMA는 변경 사항을 개



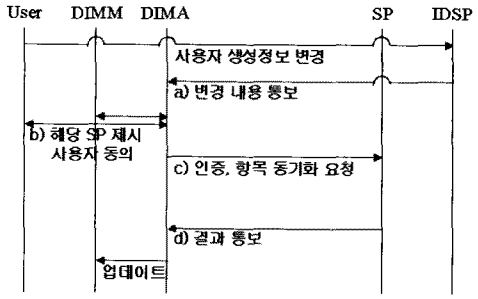
〔그림 6〕 개인정보 동기화 모델의 흐름도

인정보파일들에 반영한다. DIMA는 이 개인정보파일들을 사용하여 가입했던 SP의 개인정보 항목을 동기화한다. 이를 위해 DIMA는 해당 SP의 목록을 User에게 제시해야 하고, User는 이 목록에서 선택적으로 동기화 여부를 결정할 수 있다. DIMA는 동기화가 결정된 SP들의 개인정보 항목을 동기화하고, 관련된 내용을 해당 SP의 인증정보파일에 저장, 관리해야 한다. 다음의 개인정보 변경에 따른 동기화 모델을 기술한 것의 흐름도는 [그림 6]과 같다.

a) User는 DIMA를 호출하고 신원확인을 거쳐, 변경된 자신의 개인정보항목을 수정, 변경한다.
b) DIMA는 변경된 항목을 포함하고 있는 개인정보파일을 가입 시 사용한 SP에게 안전한 채널을 통해 동기화 요청을 한다. 이때, DIMA는 SP의 목록을 User에서 제시하고, User가 동기화시키기를 원하지 않는 SP가 있으면 이를 제외하도록 유도한다.
   - DIMA의 요청 시, IDSP에서 DIMA을 인증하기 위해서는 인증정보파일을 이용한다.
c) DIMA의 동기화 요청에 대해, SP는 해당 개인정보 항목을 동기화 한 후, 그 결과를 안전한 채널을 통해 DIMA에게 통보한다.

3.2.4 공유사용자생성정보 동기화

User에 의해 공유사용자생성정보가 변경된다면, 해당 공유사용자생성정보를 제공받은 SP의 정보도 동기화될 수 있어야 한다. 이를 위해, IDSP는 User에 의한 사용자생성정보 변경 시 변경된 항목을 DIMA에게 통보해야 하며, DIMA은 관련 항목을 제공받은 모든 SP들의 목록을 User에게 제시해야 한다. User는 이 목록에서 선택적으로 동기화 여부를 결정할 수 있다. DIMA는 동기화가 결정된 SP들의 공유사용자생성정보 항목을 동기화하고, 관련된 내용을 해당 SP의 인증정보파일



〔그림 7〕 공유사용자생성정보 동기화 모델의 흐름도

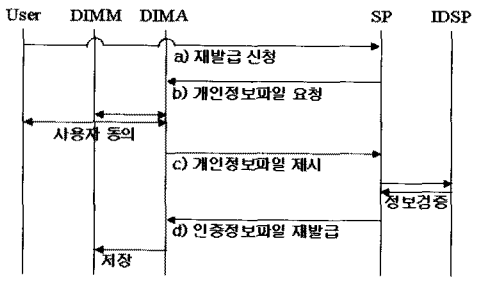
에 저장, 관리해야 한다. 다음은 공유사용자생성정보 변경에 따른 동기화 모델을 기술한 것이다.

a) User에 의해 변경된 사용자생성정보에 대해 IDSP는 DIMA를 호출하여 변경된 내용을 통보한다.
b) DIMA는 변경된 정보의 항목을 제공받은 SP의 목록을 User에게 통보하여 동의를 구한다.
c) User가 동의한 SP에 한해서 동기화 요청을 한다.
   - DIMA의 요청 시, IDSP에서 DIMA을 인증하기 위해서는 인증정보파일을 이용한다.
d) 정당한 동기화 요청에 대해, SP는 이를 반영하고 결과를 DIMA에게 통보한다.

3.2.5 인증정보파일 재발급

보유 인증정보파일을 분실하거나 User의 실수로 인한 삭제 등으로 인해 인증정보파일의 재발급 및 갱신이 필요할 경우, 인증정보파일은 재발급 및 갱신발급 신청을 통해 발급받을 수 있다. 이에 대한 절차는 다음 [그림 8]과 같다.

a) User는 SP의 웹페이지에 접속하여 인증정보파일 재발급신청을 한다.
b) SP는 User의 DIMA를 호출하고, 개인정보파일을 요청한다.
c) DIMA는 SP가 요청한 내용과 일치하는 개인정보파일을 User의 동의를 얻어, 안전한 채널을 통해 SP에게 제공한다.
d) SP가 보유하고 있는 기존의 인증정보를 삭제하고, 새로운 인증정보를 생성한다. ID와 인증정보, 사용자생성정보 등을 포함하는 인증정보파일을 생성하여 안전한 채널을 통해 DIMA에게 제공하고, DIMA는 DIMM에 저장하는 것으로 재발급 절차를 완료한다.
   - 개인정보파일에 포함된 항목 중 추가 검증이 필요한 경우에는 에 필요한 절차를 수행한다.



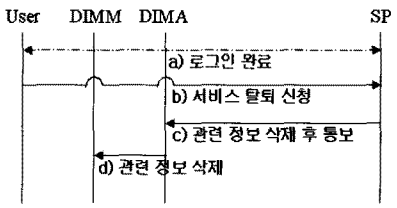
〔그림 8〕. 인증정보파일 재발급 모델의 흐름도

3.3 서비스 탈퇴 모델

가입된 SP에 대해서 User가 탈퇴하기를 원하는 경우, User는 해당 인증정보파일을 통해 SP에게 로그인한 후, 정해진 절차에 의해 탈퇴할 수 있다. 이 경우, SP는 보유하고 있던 모든 User 관련 정보를 삭제해야 하며, DIMA도 관리하고 있는 정보들을 삭제해야 한다. User의 SP에 대한 탈퇴절차는 다음 [그림 9]와 같다.

a) User는 '기본 서비스 이용' 절차에 따라 로그인 한다.
b) 서비스 탈퇴 신청을 한다.
c) SP는 보유한 User의 개인정보, 사용자생성정보, ID 및 인증정보 등을 삭제하고 결과를 User에게 통보한다.
d) DIMA는 해당 SP가 발급한 인증정보파일과 관련 관리 목록들을 삭제한다.

IDSP의 역할을 수행했던 SP에 대한 탈퇴의 경우, DIMA는 User에게 IDSP가 공유사용자생성정보를 제공한 SP의 목록을 알려주어야 하며, IDSP의 서비스에서 User가 탈퇴함으로 인해서 생길 수 있는 문제점을 경고해야 한다. 또한 User가 원할 경우 해당 항목에 대



〔그림 9〕 서비스 탈퇴 모델의 흐름도

한 적절한 조치(가장 최근의 내용을 유지 혹은 항목의 내용을 초기화 등)를 취할 수 있도록 해야 한다.

Ⅳ. 개인정보보호정책의 적용 적합성

3장에서 제시한 서비스 모델을 기반으로 개인정보보호 정책의 적용 적합성을 파악한다. 이를 위해 OECD 8대 원칙[8]을 기준으로 분석하였다. 아래의 [표 3]은 OECD 8대 원칙을 요약하고, 제안한 인터넷 ID 관리 서비스를 이용할 경우의 원칙 반영 여부를 분석한 것이다.

제안한 서비스 모델은 개인정보파일과 인증정보파일을 사용함으로서, 가입시 필요한 개인정보의 항목을 규정하여 사용하고, SP가 제공하는 서비스에 따라 수집하는 개인정보 항목을 제안하도록 하여 수집 제한의 원칙, 수집 목적의 명확화 원칙에 부합한다. 또한 처리, 전송되는 모든 정보에 대해 User의 동의를 필요로 하고, 정보 동기화 기능들을 통해 최신의 정보를 유지시킬 수 있으므로 개인 참여의 원칙과 사용 제한의 원칙, 정보 정확성 원칙을 만족시킬 수 있다. 안전성 확보 및 공개의 원칙, 책임 소재의 원칙 등은 구체적인 구현 모델에서 기술적, 정책적으로 충분히 해결될 수 있을 것이라 보여 진다. 본 논문에서 제안하는 서비스 모델은 실제 구현모델의 초기 개념적 단계이며, 기존 구현모델을 개선한 측면이 강하므로 개인정보보호 정책을 충분히 반영할 수 있을 것이라 사료된다. 또한, 국내에 제정되어 있는 개인정보보호와 관련된 여러 법안과 지침들도[9-, 12] OECD 8대 원칙을 크게 벗어나지 않는다는 점을 감안하면, 국내의 인터넷 환경에서도 적합하다고 보여 진다.

Ⅴ. 결 론

본 논문은 사회문제로 대두되고 있는 인터넷 ID 관리상의 문제와 이로 인한 파생되는 개인정보 침해 문제 등을 해결하기 위해 User 중심의 인터넷 ID 관리 서비스 모델을 제안하였다. 이 모델은 User의 인증 정보를 제공하는 IDSP의 역할이 축소되고, SP가 인증 주체가 되어 자체 발급한 인증정보를 가지고 User를 인증하며, 동기화 기능 등을 통해 최신의 정보를 제공하는 보다 개선된 인터넷 ID 관리를 위한 서비스 모델이다. 제안된 모델은 User가 자신과 관련된 모든 정보의 흐름을 소유하고 제어함에 따라 안전하게 정보를 관리할 수 있고, SP가 수집하는 개인정보의 목적과 사용처를 분명히 하고, User에 의해 수정, 변경 등의 관리가 손쉽고 안전하게 함으로서 문제를 해결할 것이라 보여 진다. 제안된 서비스 모델을 기반으로 향후 다양한 서비스 개발에 대한 수요 조사와 실제 구현 모델의 개발이 필요하다고 사료된다.

참고문헌

[1] 윤재석, 민경식, 김정희, "인터넷 디지털 ID 추진 현황 및 전망", available at http://kidbs.itfind.or.kr/WZIN/jugidong/1311/131101.pdf

[2] '개인정보보호와 i-PIN', 한국정보보호진흥원., available at http://help.mic.go.kr/eBook/iPIN/iPIN/default1.html

[3] 조영섭, 진승헌, "Digital Identity 관리 기술 현황 및 전망", 전자통신동향분석, 제 22권 제1호,

[표 3] OECD 8대 원칙과 제안한 서비스 모델의 적용 여부

OECD 8원칙	주요 내용	제안한 서비스 모델의 적용 여부
수집 제한의 원칙	합법적이고 공정한 방법을 통한 개인정보의 수집	개인정보파일의 사용, SP의 가입 정책
정보 정확성의 원칙	개인정보의 정확성, 안전성 유지	개인정보 동기화 기능
수집목적의 명확화의 원칙	수집 시에 개인정보수집 목적 명시, 명시된 목적에 적합한 개인정보 사용	개인정보 항목의 수집 목적 명시
사용 제한의 원칙	정보주체 동의 및 법규정이 없는 경우 목적 외 이용 및 공개 금지	처리/전송 정보의 User 제어
안전성 확보의 원칙	개인정보 침해 방지를 위한 물리적, 조직적, 기술적 안전조치 확보	DIMM 접근제어, 안전한 통신 채널 구성
공개(고시)의 원칙	개인정보 처리 및 보호를 위한 정책 공개, 개인정보관리자의 신원, 연락처, 이용목적 등 공개	SP의 정책에서 반영 가능
개인참여의 원칙	정보주체의 개인정보 열람/정정/삭제 청구권 보장, 열람거절 등에 대해 불복이 있는 경우 이의제기	처리/전송 정보의 User 제어, 개인정보 변경, 동기화 기능
책임소재의 원칙	개인정보 관리자에게 원칙준수 의무 및 책임부과	SP의 정책에서 반영 가능

2007년 2월

[4] Johannes Ernst. "The Identity Landscape of 2006", available at http://netmesh.info/jernst/Digital_Identity/ three-standards.html

[5] Kim Cameron, "THE LAWS OF IDENTITY", *Kim Cameron's Identity Weblog*, available at http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[6] 조영섭, 진승헌, 문필주, 정교일, "ID 연계 기반의 인터넷 ID Management System: e-IDMS", *전자공학회논문지*, 제43권, 2006년.

[7] Windows CardSpace (formerly "InfoCard"), available at http://msdn2.microsoft.com/ko-kr/winfx/Aa663320.aspx

[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at http://www.oecd.org/document/18/0,3343, en_2649_201185_1815186_1_1_1_1,00.html

[9] '공공기관의개인정보보호에관한법률'

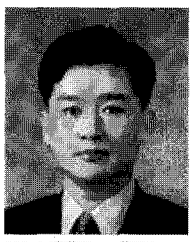
[10] '정보통신이용촉진및정보보호등에관한법률'

[11] '법률 개정에 따른 개인정보보호를 위한 기본지침', 정보통신부, 한국정보보호진흥원, 2007.2.

[12] '공공기관의 개인정보보호를 위한 기본지침', 행정자치부, 2006.2.

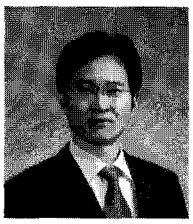
[13] 'i-PIN 서비스 프레임워크', 한국정보통신기술협회, 2007.

〈著者紹介〉



송 정 환 (Junghwan Song)
1984년 2월 : 한양대학교 수학과 졸업
1989년 5월 : Syracuse University 수학과 석사
1993년 5월 : Rensselaer Polytechnic Institute 수학과 박사
1999년 3월~현재 : 한양대학교 수학과 부교수
<관심분야> 암호학, 정보보호, 수리계획법

강 연 정 (Yeonjung Kang) 정회원
2003년 2월 : 한양대학교 전자전기공학부 졸업
2006년 8월 : 한양대학교 수학과 석사
2006년 6월~현재 : 한국정보보호진흥원 연구원
<관심분야> 암호학, 정보보호



장 환 석 (Hwanseok Jang) 학생회원
2002년 2월 : 한양대학교 수학과 졸업
2004년 2월 : 한양대학교 수학과 석사
2004년 3월~현재 : 한양대학교 수학과 박사과정
<관심분야> 암호학