모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 시스템 설계 및 구현

Design and Implementation of Scalable ID Federation System in Mobile Computing Environments

유 인 태* 김 배 현** 문 영 준*** 조 영 섭**** 진 승 헌*****
Ryoo, In Tae Kim, Bae Hyun Moon, Young Jun Cho, Yeong Sub Jin, Seung hun

요 약

현재의 네트워크 환경에서는 사용자들이 인터넷상의 여러 서버에 대하여 각각의 독립된 ID(Identity)를 사용하고 있기 때문에 사용자들이 많은 수의 ID와 패스워드를 관리해야하는 불편함이 있다. 이러한 문제를 해결하기위해 ID 관리 시스템을 사용하지만, 앞으로 도래할 유비쿼터스 컴퓨팅 환경에서는 유무선 네트워크상의 수많은 컴퓨터들이 유기적으로 연결되기 때문에 사용자 ID 및 패스워드 관리가 더욱 복잡해지고, 기존의 단일 신뢰영역(COT; Circle of Trust)의 ID 관리 시스템으로는 이러한 어려움을 해결하기에 충분하지 않다. 본 논문에서는 이러한 문제를 해결하기 위해, 다중 신뢰영역 간의 ID 연동(ID Federation)을 유선 컴퓨팅 환경에서뿐만 아니라 모바일 컴퓨팅 환경으로 확장하기 위한 ID 연동 모델을 도출하고 시스템을 구현하였다. 제안한 ID 연동 모델은 ID 확장성 실험을 통해 서로 다른 신뢰 영역에 있는 시스템 간에 ID 연동이 가능함을 검증하였다.

Abstract

Currently, almost of all the Internet users have as many IDs as the number of sites they have subscribed for. The users should memorize and input every independent ID and password whenever they want to login to the system. Although ID management system is used to solve this problem, ID and password management will become more complicated in the forthcoming ubiquitous computing environments because so many computers will be interconnected on various kinds of wired and wireless networks. Furthermore, it is not enough to use the existing single Circle of Trust (COT) ID management system for the forthcoming computing environments. To solve this problem, the paper proposes ID federation models in multiple COT domain and implements an ID federation system that can be scaled to mobile computing environment as well as wired computing environment. The proposed ID federation models has been verified to operate with no problem between the systems in different trust domains by doing the ID scalability test.

☞ Keyword : Mobile Computing, Scalable ID, ID Federation

1. 서 론

본격적인 정보화 시대가 전개되면서 사용자들이 접하게 되는 정보 시스템은 수적인 증가는 물론이고 물리적 환경 또한 유선 컴퓨팅 환경을 뛰어 넘어 모바일 컴퓨팅 환경으로 많이 변화하였다. 일반적으로 사용자는 각 정보 시스템에 접속하기 위하여 ID와 패스워드를 사용하게 되는데, 이런 정보 시스템의 양적 그리고 환경적 변화는 곧 ID와 패스워드의 관리에 많은 어려움을 주고

* 종신회원 : 경희대학교 전자정보대학 부교수
itryoo@khu.ac.kr(제1저자)
** 종신회원 : 한신대학교 정보통신학과 겸임교수
bhyunkim@lycos.co.kr(공동저자)
*** 준 회 원 : 경희대학교 대학원 컴퓨터공학과 박사과정
yjmoon@khu.ac.kr(공동저자)
**** 정 회 원 : 한국전자통신연구원 디지털ID보안연구팀 선임연구원 yscho@etri.re.kr(공동저자)
***** 정 회 원 : 한국전자통신연구원 디지털ID보안연구팀장/선임연구원 jinsh@etri.re.kr(공동저자)
[2005/03/14 투고 - 2005/03/21 심사 - 2005/07/25 심사완료]

있다. 이러한 ID 관리의 복잡성을 해결하기위해 ID 관리 시스템에 대한 연구가 진행되었다. ID 관리는 이기종의 다양한 시스템을 단 한 번의 인증 과정을 거쳐 접근 가능하도록 함으로써 ID와 패스워드 관리의 문제점을 해결할 수 있고 [6,7,8,9], 동시에 시스템 관리자에게는 개별적인 인증시스템 관리의 복잡성을 해결할 수 있게 해 준다.

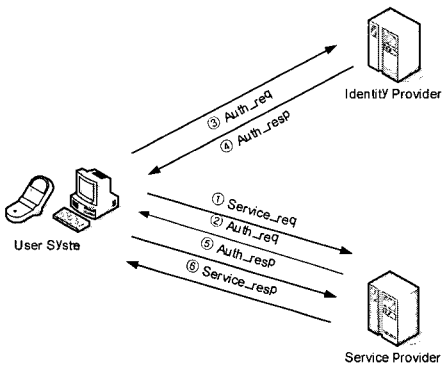
ID 관리 분야는 일반적으로 기업 내 사용자의 ID 관리를 주 대상으로 하는 Enterprise IdM (Identity Management) 분야와 이를 확장하여 일반 인터넷 사용자의 ID 관리 문제를 해결하기 위한 인터넷 ID 관리 서비스 분야가 있다. Enterprise IdM은 단일 신뢰영역에서 조직원이 사용하는 응용 서비스에 따라 많은 수의 ID를 가져가야 했던 문제와 매번 인증을 받아야하는 문제를 해결한다. 그러나 일반적인 인터넷 사용자의 경우 포털, 쇼핑몰 등과 같은 다양한 서비스 영역에서 ID를 등록하고 관리하기 때문에 Enterprise IdM으로는 인터넷 사용자의 중복된 ID 관리, SSO(Single Sign On)등의 문제를 해결하지 못한다. 따라서 인터넷 ID 관리 서비스를 위해서는 단일 신뢰영역이 아닌 다중 신뢰영역 간의 ID 연동을 위한 Federated ID가 제공되어야 한다[1,3,10,11].

인터넷 ID 관리 서비스는 일반적인 인터넷 사용자의 ID 관리 및 개인정보침해 문제를 해결하기 위한 것으로 다음과 같은 서비스를 제공한다[10].

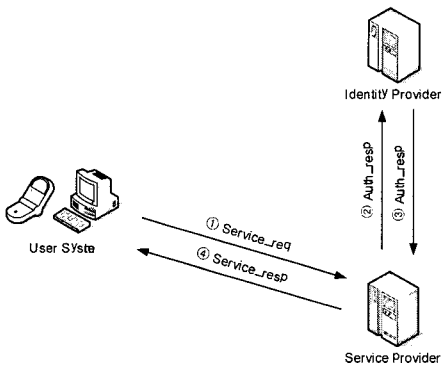
- ID 관리 서비스 : 사용자가 하나의 ID만을 사용하여 자신의 모든 개인정보를 등록, 수정, 관리하는 서비스
- SSO 서비스 : 한 번의 인증 후, 추가적인 인증 없이 여러 사이트를 자유롭게 이용하도록 하는 서비스
- 개인정보 보호 서비스 : 사용자가 등록된 정보를 어떠한 응용 서비스에서 사용하고자 할 때, 사용자의 명시적인 동의를 얻도록 하여 사용자 개인정보의 오남용을 방지하는 서비스
- ID 관리 대행 서비스 : 사용자의 ID 관리 능력이 부재한 사이트에서 사용자 ID 관리를 대행해 주는 서비스
- 인증 대행 서비스 : PKI(Public Key Infrastructure) 인증 등과 같은 부가적인 비용이 발생하는 인증 업무를 대행해 주는 서비스

현재 대표적인 ID 관리 기술로서는 마이크로소프트사의 패스포트, 공개 소스프로젝트인 시볼레, Ping Identity의 SourceID가 있다. 패스포트는 마이크로소프트사에서 제공하는 인터넷 범위의 SSO 서비스이다. 그러나 현재의 패스포트는 ID 연동을 지원하지 않고 있으며 표준화 기구에서 제정하는 표준을 준용하지도 않고 있어 윈도우 플랫폼 외에서는 사용할 수 없고, 마이크로소프트 외에는 이를 수정하여 개발할 수 없다. 향후 커버로스의 지원을 이용하여 영역간의 ID 연동을 지원할 계획을 가지고 있다. 시볼레는 공개 소스 프로젝트로서 internet2로부터 지원을 받고 있으며 대학 연구소간 웹 리소스 공유에 필요한 접근제어를 목적으로 개발된 기술로서 아파치, IIS(Internet Informationl Server)에 추가기능으로 동작할 수 있도록 구현했으며 Federated PKI 기반으로 동작이 가능하도록 하였다. SourceID는 ID 연동을 위한 플랫폼을 제공해주기 위한 공개 소스 프로젝트이다. Ping Identity는 SourceID 플랫폼을 통하여 Federated ID 애플리케이션이나 Federated SSO를 구축할 수 있도록 라이브러리와 샘플을 제공하고 있다.[11] 또한 2001년에, 유무선 환경에서 ID 정보의 공유 및 관리를 목적으로 하는 리버티 연합이 생성되어 Federated ID 관리 지침을 체계적으로 연구하고 있다 [1]. 리버티 연합 프레임워크는 Federated ID 관리에 따른 모바일 데이터 서비스를 위해 생성된 표준으로 이들 내용은 주로 이동 통신 사업자를 주축으로 구체화되었다 [2,3,4,5].

기존의 연구들은 유선환경에서 다중 신뢰영역간의 ID 연동과 관리 서비스를 제공하기위한 연구가 중심을 이루었다. 그러나 현재 인터넷 환경은 유



〈그림 1〉 ID 연동 모델 1



〈그림 2〉 ID 연동 모델 2

선뿐만 아니라, 이동 환경에서의 인터넷 사용이 급속히 증가하고 있다. 따라서 기존의 유선환경에서의 다중 신뢰영역간의 ID 연동과 관리 서비스뿐만 아니라 유무선 연동 환경에서 다중 신뢰영역간의 ID 연동과 관리 서비스가 필요하고 [11], 동시에 유무선 연동에 의한 컴퓨팅 환경의 개방성으로 인해 이동 환경에서의 개인 정보 보호 기술과 보안 문제를 해결하기 위한 기술이 필요하다 [12].

이와 같은 요구 조건을 갖는 ID 연동 기술 개발을 위해 본 논문은 우선 제 2 절에서 모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 모델을 인증 요청 주체와 모바일 장치의 기능에 따라 ID 연동 모델을 제시한다. 제 3 절에서는 제 2 절의 모델을 기반으로 확장 가능한 ID 연동 시스템을 설계하고, 제안한 ID 연동 모델을 파일럿 시스템으로 구현하여 그 성능을 검증한다. 마지막으로 제 4 절에서 본 연구에 대한 결론을 맺는다.

2. 모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 모델

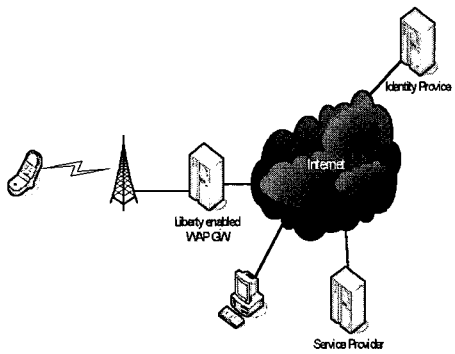
본 장에서는 유무선 연동 환경과 ID 연동을 고려한 모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 모델을 제안한다. 제안된 ID 연동 모델은 인증을 요청하는 주체에 따른 ID 연동 모델과 모바일 장비의 기능에 따른 ID 연동 모델로 구분된다.

2.1 인증 요청 주체에 따른 ID 연동 모델

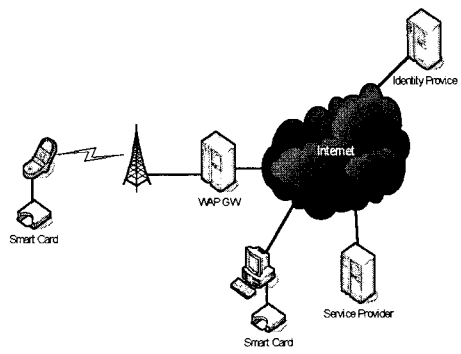
우선 확장 가능한 ID 연동을 위해 모바일 컴퓨팅 환경에서 인증 요청 주체에 따른 모델을 2가지로 구분하였다. ID 연동 모델 1은 그림 1과 같이 사용자 시스템(User System)이 서비스 제공자에게 서비스를 요청하면, 서비스 제공자가 인증을 요청한다. 사용자 시스템은 인증을 받기위해 Identity 제공자에게 인증을 요청하여 인증을 받은 후, 서비스 제공자에게 인증을 넘겨주면, 서비스 제공자는 사용자 시스템에게 서비스를 제공한다. 이 모델은 Ticket 기반 인증과 같은 방법을 생각할 수 있다.

ID 연동 모델 2는 그림 2와 같이 사용자 시스템이 서비스 제공자에게 서비스를 요청하면 서비스 제공자가 직접 Identity 제공자에게 인증을 요청하여 인증을 받은 후 사용자 시스템에게 서비스를 제공하는 것이다. 이 모델에서는 서비스 제공자와 Identity 제공자 사이에 상호 인증과 무결성이 필요하다.

ID 연동 모델 1의 경우, 사용자 시스템이 인증 과정에 참여하고 있기 때문에 사용자 시스템이 인증 과정에서 load가 집중된다. 그러나 서비스 제공자는 인증과정에 직접 참여하지 않기 때문에 두 번째 모델에 비해 load가 적다. ID 연동 모델 2의 경우, ID 연동 모델 1에 비해 사용자 시스템은 인증 과정에 참여하지 않기 때문에 ID 연동



〈그림 3〉 모바일 장치 기능에 따른 ID 연동 모델 1



〈그림 4〉 모바일 장치 기능에 따른 ID 연동 모델 2

모델 1에 비해 load가 적지만 서비스 제공자는 인증 과정에 참여해야 하기 때문에 ID 연동 모델 1에 비해 load가 많아진다.

2.2 모바일 장치 기능에 따른 ID 연동 모델

ID 연동을 모바일 환경으로 확장하기 위해서는 ID 연동 기능을 모바일 환경에 구현해야만 한다. 이것은 ID 연동 기능이 모바일 환경의 사용자 시스템에 구현되어야 한다는 것을 의미한다. ID 연동 기능을 구현하기 위한 사용자 시스템으로 고려할 수 있는 것은 이동전화와 WAP 게이트웨이이다. 이동전화의 경우, 이동전화 단말기에 ID 연동 기능을 직접 구현하거나 스마트카드를 이용하는 방법이 있지만 ID 연동 기능을 사용하기 위해서는 이동전화를 교체해야한다는 문제점이 있다. 따라서 현존하는 WAP 게이트웨이에 연동 ID 관리 기능을 구현한 Federation ID Management Enabled WAP 게이트웨이를 사용하는 것이 더욱 효율적이다. 이에 따라, 연동 ID 관리 기능을 어느 사용자 시스템에 구현하느냐에 따라 그림 3과 그림 4의 두 가지 모델을 제시한다.

〈표 1〉 시나리오 1, 2, 3의 메시지 정의

메시지	파라미터
Service_req	IDuser, PW, PN, IDIdP
Service_req(a)	AuthToken, IDIdP, PN, flag
Service_resp(a)	AuthToken, flag
Service_resp	flag
Auth_req	IDuser, PW, PN, IDIdP, RAND
Auth_req(a)	AuthToken, IDIdP, RAND, flag
Auth_resp	AuthToken, RAND
Auth_resp(s)	RAND, flag
Auth_req_IdP	IDuser, PW, PN, RAND
Auth_req_IdP(a)	AuthToken, RAND, flag
Auth_resp_IdP(s)	RAND, flag
Auth_resp_IdP	AuthToken, RAND

3. 모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 시스템 설계

모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 시스템을 위해 제 2 장에서 제시한 모델 중 ID 연동 모델 2 그림 2에 WAP 게이트웨이가 연동 ID 관리 기능을 수행하는 시스템을 설계하였다. 이 시스템의 설계를 위해 시스템의 구성요소들 간의 동작을 기술하는 12 개의 메시지를 표 1에 정의하였다. 또한 이들 시스템의 운용에서 발생할 수 있는 몇 가지 시나리오에 대한 메시지 시퀀스 차트(Message Sequence Chart: MSC)를 제시한다.

ID 연동은 COT에서 사용자의 개인정보를 저장하고 있는 Identity 제공자에게 한번 인증된 사용자가 허가된 다른 자원으로 접속하는 경우에도 사용자에게 또다시 인증과정을 거치지 않고 빠르게 접속하도록 하는 SSO의 이점뿐만 아니라 다른 COT상의 허가된 다른 자원으로 접속하는 경우에도 사용자에게 또 다른 인증과정을 거치지 않고 접속하도록 한다. 또한 COT는 서비스 제공

자와 Identity 제공자가 갖는 신뢰 관계이다.

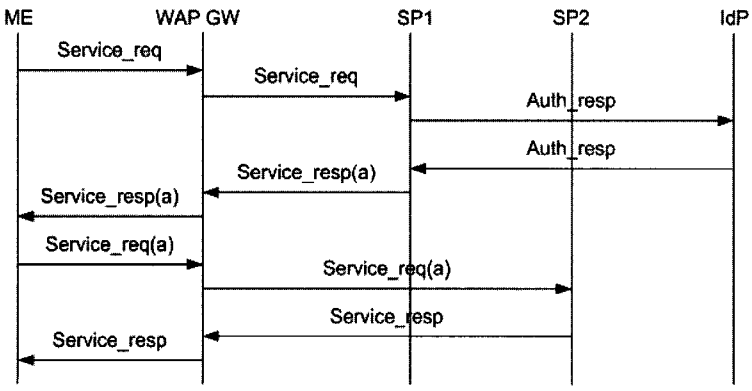
3.1 ID 연동 시나리오 1

시나리오 1은 가입자가 가입한 ID 제공자가 서비스 제공자 SP1과 SP2가 동일한 COT에 속하고 가입자가 서비스 제공자 SP1에서 먼저 인증을 받아 서비스를 받은 후 서비스 제공자 SP2에게 서비스를 받기위한 과정이다. 시나리오 1의 동작 방법은 다음과 같다.

- ME -> WAP GW: Service_req ME는 WAP 게이트웨이에게 Service_req 메시지를 전송한다.
- WAP GW -> SP1: Service_req WAP 게이트웨이는 ME에게 받은 Service_req 메시지를 서비스 제공자 SP1에게 전달한다.
- SP1 -> IdP: Auth_req 서비스 제공자 SP1는 ID 서비스 제공자인 IdP에게 Auth_req 메시지를 전송한다.
- IdP -> SP: Auth_resp ID 서비스 제공자인 IdP는 인증이 성공하면, 서비스 제공자 SP1에게 Auth_resp 메시지를 전송한다.
- SP1 -> WAP GW: Service_resp(a) SP1은 IdP에게 받은Auth_resp에서 AuthToken을 확인하여 인증을 하고, AuthToken과 falg a를 포함하는 Service_resp(a) 메시지를 전송한다.
- WAP GW -> ME: Service_resp(a) WAP GW는 ME에게 SP1으로부터 받은 Service_resp(a) 메시지를 전달한다.
- ME -> WAP GW: Service_req(a) ME는 SP2에게 서비스를 요청하기위해, IdP로부터 AuthToken을 받은 상태이기 때문에 Flag a를 표시하여 Service_req(a) 메시지를 WAP GW에게 전송한다.
- WAP GW -> SP2: Service_req(a) WAP 게이트웨이는 ME로부터 Service_resp(a) 메시지를 서비스 제공자 SP2에게 전송한다.
- SP2 -> WAP GW: Service_resp 서비스 제공자 SP2는 Service_req(a) 메시지에서 AuthToken을 추출하여 동일한 COT에 있는 IdP에서 발생한 AuthToken임을 확인하고, Service_resp 메시지를 WAP 게이트웨이에게 전송한다.
- WAP GW -> ME: Service_resp WAP 게이트웨이는 Service_resp를 ME에게 전달한다.

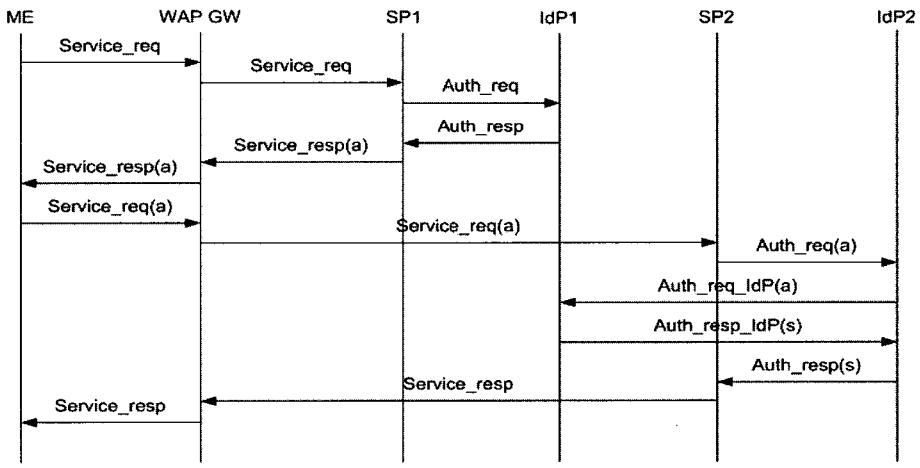
3.2 ID 연동 시나리오 2

시나리오 2는 가입자가 가입한 ID 제공자와 동일한 COT에 존재하는 서비스 제공자 SP1에 서비스를 받기위해 인증을 받은 후, 가입자가 가입하지 않은 ID 제공자의 COT에 존재하는 서비스 제공자 SP2에게 서비스를 받기 원하는 경우이다. 시나리오 2의 동작 방법은 다음과 같다.



〈그림 5〉 시나리오 1

- ME -> WAP GW: Service_req ME는 WAP 게이트웨이에게 Service_req 메시지를 전송한다.
- WAP GW -> SP1: Service_req WAP 게이트웨이는 ME에게 받은 Service_req 메시지를 서비스 제공자 SP1에게 전달한다.
- SP1 -> IdP1: Auth_req 서비스 제공자 SP1은 ID 서비스 제공자인 IdP1에게 Auth_req 메시지를 전송한다.
- IdP -> SP: Auth_resp ID 서비스 제공자인 IdP1은 인증이 성공하면, 서비스 제공자 SP1에게 Auth_resp 메시지를 전송한다.
- SP1 -> WAP GW: Service_resp(a) SP1은 Auth_resp을 받아 AuthToken을 확인하여 인증을 하고, IdP1에게 받은 AuthToken과 falg a를 포함하는 Service_resp(a) 메시지를 전송한다.
- WAP GW -> ME: Service_resp(a) WAP GW는 EM에게 SP1으로부터 받은 Service_resp(a) 메시지를 전달한다.
- ME -> WAP GW: Service_req(a) 다른 COT에 존재하는 SP2에게 서비스를 요청하기위해, ME는 IdP로부터 AuthToken을 받은 상태이기 때문에 Flag a를 표시하여 Service_req(a) 메시지를 WAP GW에게 전송한다.
- WAP GW -> SP2: Service_req(a) WAP 게이트웨이는 서비스 제공자 SP2에게 Service_resp(a) 메시지를 전송한다.
- SP2 -> WAP GW: Service_req(a) 서비스 제공자 SP2는 Service_req(a) 메시지에서 AuthToken을 추출하여 자신의 COT에 있는 IdP2가 발행한 AuthToken이 아니면, 수신한 AuthToken의 인증요청을 위해 Auth_req(a) 메시지를 구성하여 자신의 COT에 있는 IdP2에서 전송한다.
- IdP2 -> IdP1: Auth_req_IdP(a) IdP2는 AuthToken을 발생한 IdP1에게 AuthToken 확인을 요청하기위해 Auth_req_IdP(a) 메시지를 전송한다.
- IdP1 -> IdP2: Auth_resp_IdP(s) IdP1은 AuthToken을 확인하여, 발생한 사실을 IdP2에게 알리기 위해 Auth_resp_IdP 메시지를 전송한다. 만약 IdP1이 발행한 AuthToken이 맞는다면 plag s를 표시한다.
- IdP2 -> SP2: Auth_resp(s) IdP2는 IdP1에게 받은 AuthToken의 확인 결과를 이용하여 SP2에게 인증사실을 알리는 Auth_resp(s) 메시지를 전송한다.
- SP2 -> WAP GW: Service_resp SP2는 WAP 게이트웨이에게 Service_resp 메시지를 전송한다.
- WAP GW -> ME: Service_resp WAP 게이트웨이는 Service_resp를 ME에게 전달한다.

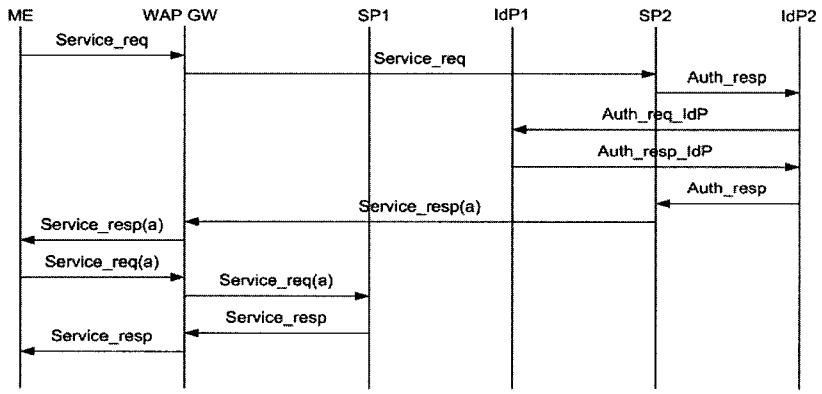


〈그림 6〉 시나리오 2

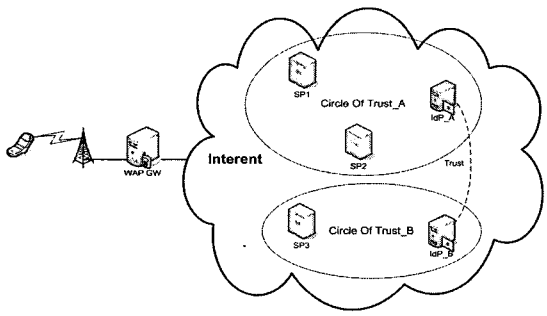
3.3 ID 연동 시나리오 3

시나리오 3은 가입자가 가입하지 않은 ID 제공자의 COT에 존재하는 서비스 제공자 SP2에게 서비스를 받기위해 인증된 후, 가입자가 가입한 ID 제공자와 동일한 COT에 존재하는 서비스 제공자 SP1에 서비스를 받기 원하는 경우이다. 시나리오 3의 동작 방법은 다음과 같다.

- ME -> WAP GW: Service_req ME는 WAP 게이트웨이에게 Service_req 메시지를 전송한다.
- WAP GW -> SP2: Service_req WAP 게이트웨이는 ME에게 받은 Service_req 메시지를 서비스 제공자 SP2에게 전달한다.
- SP2 -> IdP2: Auth_req 서비스 제공자 SP2는 Service_req 메시지에 포함된 ID_{IdP}를 확인하여 SP2가 속한 COT상의 IdP가 아니면, SP2가 속한 COT상의 ID 서비스 제공자인 IdP2에게 Auth_req 메시지를 전송한다.
- IdP2 -> IdP1: Auth_req_IdP IdP2는 IdP1에게 인증을 요청하기위해 Auth_req_IdP 메시지를 전송한다.
- IdP1 -> IdP2: Auth_resp_IdP IdP1은 인증이 되면, AuthToken을 포함한 Auth_resp_IdP 메시지를 전송한다.
- IdP2 -> SP2: Auth_resp IdP2는 IdP1에게 받은 Auth_resp_IdP 메시지에 포함된 AuthToken을 포함하는 Auth_resp 메시지를 SP2에게 전송한다.
- SP2 -> WAP GW: Service_resp(a) SP2는 Auth_resp(a)을 받아 AuthToken을 확인하여 인증을 하고, AuthToken과 falg a를 포함하는 Service_resp(a) 메시지를 WAP 게이트웨이에게 전송한다.
- WAP GW -> ME: Service_resp(a) WAP GW는 EM에게 Service_resp(a) 메시지를 전달한다. ME는 Service_resp(a) 메시지에서 AuthToken을 추출하여 보관한다.
- ME -> WAP GW: Service_req(a) 동일한 COT에 존재하는 SP1에게 서비스를 요청하기위해, ME는 AuthToken을 받은 상태이기 때문에 AuthToken과 Flag a를 포함하는 Service_req(a) 메시지를 WAP GW에게 전송한다.
- WAP GW -> SP1: Service_req_(a) WAP 게이트웨이는 서비스 제공자 SP1에게 Service_req (a) 메시지를 전송한다.
- SP1 -> WAP GW: Service_resp 서비스 제공자 SP1은 Service_req(a) 메시지에서 AuthToken을 추출하여 자신의 COT에 있는 IdP1이 발행한 AuthToken이면, Service_resp메시지를 WAP



〈그림 7〉 시나리오 3



〈그림 8〉 테스트베드

게이트웨이에서 전송한다.

- WAP GW -> ME: Service_resp WAP 게이트웨이는 Service_resp를 ME에게 전달한다.

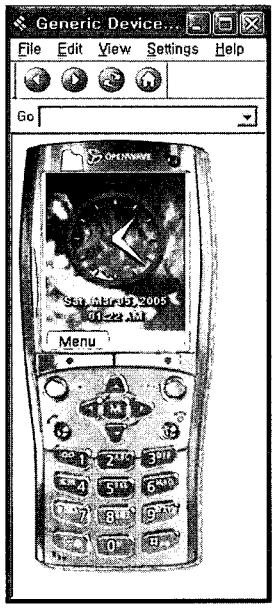
3.4 파일럿 시스템 구현 및 ID 연동 실험 결과

제안한 ID 연동 모델의 ID 연동 실험을 위한 파일럿 시스템을 (그림 8)과 같이 구현하였다.

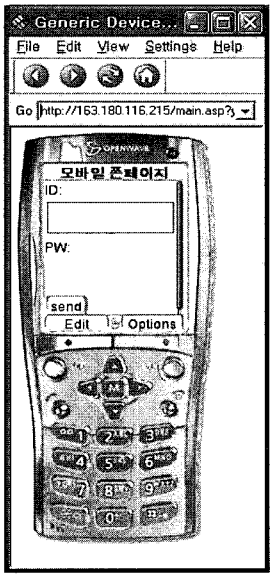
이 파일럿 시스템에는 두 개의 COT가 정의되어있다. COT_A에는 서비스 제공자 SP1 (IP주소: 163.180.116.215)과 SP2 (IP 주소: 163.180.116.214) 그리고 ID 제공자 IdP_A가 존재한다. COT_B에는 서비스 제공자 SP3 (IP 주소: 163.180.116.213)과 ID 제공자 IdP_B가 존재한다. 파일럿 시스템의 서비스 제공자와 ID 제공자 그리고 WAP 게이트웨이는 인터넷에 연결되어 있고 이동전화(ME)는 WAP 시뮬레이터 (Openwave SDK 5.1)를 사용하여 인터넷에 연결되어있다. 한편, ID 연동 실험을 위해 IdP_A와 IdP_B는 서로 신뢰 관계를 맺고 있는 것으로 가정한다.

ID 연동 실험 절차 및 결과를 요약하면 다음과 같다.

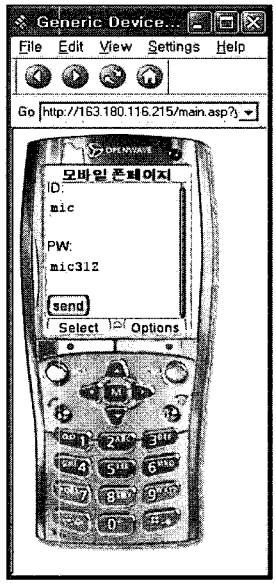
- ME 초기화 그림 9
- ME가 COT_A에 위치한 SP1에 접속 시도
- SP1이 IdP_A에 사용자 인증 요청 -처음으로 로그인을 시도하므로 인증 정보 없음
- IdP_A가 IdP_B에 사용자 인증 요청 -역시 인증 정보 없음
- IdP_A는 SP1에 인증된 사용자가 아님을 통보.
- SP1은 ME에게 ID 및 PW 입력 요청 그림 10



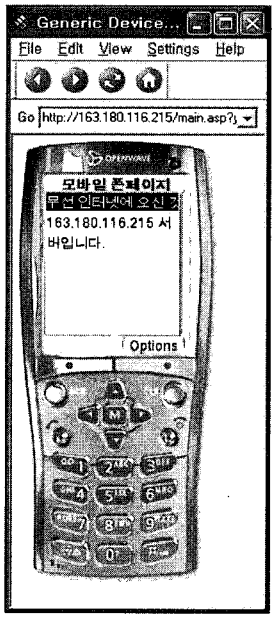
〈그림 9〉 ME 초기 화면



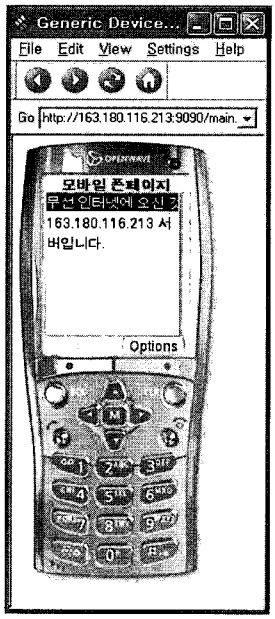
〈그림 10〉 SP1의 ID 및 PW 입력 요청 화면



〈그림 11〉 사용자 ID 및 PW 정보 입력



〈그림 12〉 SP1 접속 성공 화면



〈그림 13〉 SP3 접속 성공 화면

- ME의 사용자 ID 및 PW 입력 그림 11
- SP1이 IdP_A에 사용자 인증 요청
- IdP_A는 SP1에 사용자 인증 결과 통보
- ME의 SP1 접속 성공 그림 12
- 이후 ME는 다른 신뢰 영역 COT_B에 있는 SP3에 접속 시도
- SP3이 IdP_B에 사용자 인증 요청 -IdP_B에는 ME의 인증 정보 없음
- IdP_B가 IdP_A에 사용자 인증 요청
- IdP_A는 IdP_B가 해당 ME가 인증된 사용자임을 통보
- IdP_B는 SP3에게 해당 ME가 인증된 사용자임을 통보
- ME의 SP3 접속 성공 그림 13

그림 14는 ID 연동 실험 절차와 결과를 보여준다.

이상에서와 같이, 제안한 ID 연동 모델은 서로 다른 신뢰 영역에 있는 서비스 제공자가 상호 신

Network Info

File Format

Begin time	Elapsed time	URL	Status	Size
03/05/2005 06:25:23 오후	2 seconds	http://163.180.116.215/	302	1782/440
03/05/2005 06:25:25 오후	0 seconds	http://cnap.khu.ac.kr/aaa.asp?phone_no=0112012599	302	1808/480
03/05/2005 06:25:25 오후	1 seconds	http://mic.khu.ac.kr/aaa_ok.asp?phone=0112012599	302	1807/431
03/05/2005 06:25:26 오후	0 seconds	http://cnap.khu.ac.kr/login_wap.asp?yn=no	302	1855/391
03/05/2005 06:25:26 오후	0 seconds	http://163.180.116.215/main.asp?yn=no	200	1851/627
03/05/2005 06:26:27 오후	0 seconds	http://cnap.khu.ac.kr/login_wap_ok.asp?phone_no=0112012599	302	1966/393
03/05/2005 06:26:27 오후	0 seconds	http://cnap.khu.ac.kr/login_wap_ok.asp?phone_no=0112012599	200	20/508
03/05/2005 06:26:27 오후		http://163.180.116.215/main.asp?yn=yes		1852/?
03/05/2005 06:27:55 오후	0 seconds	http://163.180.116.213:9090/	302	1787/439
03/05/2005 06:27:55 오후	1 seconds	http://mic.khu.ac.kr/aaa.asp?phone_no=0112012599	302	1862/372
03/05/2005 06:27:56 오후	0 seconds	http://cnap.khu.ac.kr/aaa_ok.asp?phone=0112012599	302	1863/399
03/05/2005 06:27:56 오후	0 seconds	http://mic.khu.ac.kr/login_wap.asp?yn=yes	302	1855/366
03/05/2005 06:27:56 오후	0 seconds	http://163.180.116.213:9090/main.asp?yn=yes	200	1857/508

〈그림 14〉 구현 시스템의 동작 절차와 결과

뢰 관계를 가지고 있다면 별도의 독립된 ID 및 패스워드 입력 없이 성공적으로 해당 서비스 제공자에 접속할 수 있음을 확인하였다. 제안한 모델의 상용 망에의 실제 적용에 있어서는, 현재 우리나라의 이동전화는 스마트카드를 적용하고 있는 단말기가 적기 때문에 WAP 게이트웨이에 Federated ID 관리 기능을 구현하고, 이동전화 단말기에는 최소한의 기능을 수행하도록 하는 프로그램을 사용하는 방안을 고려할 수 있다. 단, 이 방안은 사용자 정보 보호 및 보안 기능 지원을 위하여 이동전화 단말기와 WAP 게이트웨이 구간에서 ID와 패스워드를 암호화하여 전송해야 할 필요가 있다. 이동전화 단말기에서 사용자 ID와 패스워드를 암호화하여 전송하는 방식은 애플리케이션과 프로토콜 레벨에서 구현이 가능하다. 애플리케이션 레벨에서의 보안은, 이동전화 단말기 상의 애플리케이션과 Identity 제공자 간의 종단간(end-to-end) 보안을 제공할 수 있으나 프로토콜 레벨에서의 보안은 WAP 게이트웨이의 특성상 보안에 한계가 있다. 따라서 애플리케이션 레벨에서의 보안이 필수적이다. 또한 좀 더 안전한 ID 관리 서비스를 제공하기 위해서는 암호화 알고리즘과 키 그리고 개인 식별자등을 적용한 스마트카드의 사용을 고려해야 한다.

4. 결 론

다수의 정보 시스템을 사용함으로 인해 일반 사용자와 정보 시스템 관리자들은 ID와 패스워드 관리에 많은 어려움을 겪고 있다. 이러한 문제를 해결하기 위한 지금까지의 분산된 ID 관리 기술은 모바일 컴퓨팅 그리고 더 나아가 유비쿼터스 컴퓨팅 등 새로운 컴퓨팅 환경의 등장으로 인한 새로운 서비스와 비즈니스 환경에 적합하지 못하다. 게다가 기존의 ID 연구는 단일 신뢰영역에서 기업 내 사용자의 ID 관리를 주 대상으로 하는 Enterprise IdM 분야에 집중되어 있었다. 따라서 본 연구에서는 Enterprise IdM 분야뿐만 아니라 일반 인터넷 사용자의 ID 관리 문제를 해결하고 분산된 ID 관리 기술의 한계점을 극복할 수 있는 다중 신뢰영역에서의 Federated ID 관리 모델을 연구하였다.

본 연구에서는 모바일 컴퓨팅 환경의 장비로 이동 전화를 고려하여 모바일 환경까지 ID 연동 기능을 확장하기 위한 모델을 제안하고, 제안 모델을 기초로 WAP 게이트웨이가 Federated ID 관리 기능을 수행하는 시스템을 설계하였다. 시스템 설계는 이동 전화와 서비스 제공자, 그리고 ID 제공자 간의 프로토콜 동작을 정의하는 12 개의 메시지를 정의하고 ID 연동 시스템 운용 시 발생할 수 있는 시나리오에 대한 메시지 시퀀스 차트를 제시하였다. 제안한 ID 연동 모델과 시나리오에 따라 파일럿 시스템을 구현하였고, 서로 다른 두 개의 신뢰 영역에 위치한 서비스 제공자에 단 한 번의 사용자 인증만으로 ID 연동이 가능함을 검증하였다. 본 연구 결과는 본 연구에서 구현한 실험 환경뿐만 아니라, 앞으로 도래할 다양한 모바일 컴퓨팅 환경에서의 ID 연동 기술 개발에 응용할 수 있으며, 향후 이와 관련된 연구가 지속되어져야 할 것이다.

참 고 문 헌

[1] LIBERTY ALLIANCE,"Tier 2 Business Guidelines: Mobile Deployments," liberty-bmeg-biz-tier2-mobile-1.1a.doc, http://www.projectliberty.org/.

[2] Nokia,"Mobile Personality," http://www.nokia.com/, 2002.

[3] Nokia,"Liberty Enhances Mobile Identification," http://www.nokia.com/, 2002.

[4] Nokia,"Identity management in mobile services," http://www.nokia.com/, 2003.

[5] Nokia and Sun Microsystems,"Deploying Mobile Web Services using Liberty Alliance's Identity Web Services Framework (ID-WSF)," White

Paper, June 2004.

[6] Andreas Pashalidis and Chris Mitchell,"Using GSM/UMTS for Single Sign-On," 0-7803-7993-4/03, pp.138-145, 2003.

[7] Andrej Volchkov,"Revisiting Single Sign-On, A Pragmatic Approach in a New Context," IT Pro, Jan.-Feb., 2001.

[8] 서대희, 이임영,"Single Sign-on에 적용 가능한 인증모델에 관한 연구," 한국정보보호학회 종합학술발표회 논문집, Vol. 12, No. 1, pp. 311-314.

[9] 두루소프트,"Optimal-Ni Solution for Single Sign On," http://www.thrusoft.co.kr/.

[10] 한국전자통신연구원 정보보호연구단 인증기반연구팀,"인터넷 ID 관리 서비스 기술 백서 ver1.0," 2004.

[11] Linda Elliott, Eric Norlin, Thomas McKenna, and Kevin Werbach,"Scenarios for Identity Federation & Drivers of the Identity Network," White paper, Ping Identity Corporation and Nokia Innovent, 2004.

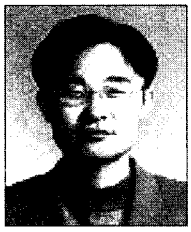
[12] PAMPAS consortium,"Pioneering Advanced Mobile Privacy and Security: Final Roadmap," IST-2001-37763, http://www.pampas.eu.org/.

◐ 저 자 소 개 ◑

유 인 태 (Intae Ryoo)
1987년 연세대학교 전자공학과 졸업
1989년 연세대학교 대학원 전자공학과 공학석사
1994년 연세대학교 대학원 전자공학과 공학박사
1997년 동경대학 전자정보통신전공 Ph. D.
1997년 ~ 1999년 (주)삼성전자 정보통신총괄 선임연구원
1999년 ~ 현재 경희대학교 전자정보대학 부교수
관심분야 : 인터넷, 네트워크 보안, 무선 LAN, IPT
E-mail : itryoo@khu.ac.kr

김 배 현 (Baehyun Kim)
1995년 호원대학교 전자계산학과 졸업
1997년 수원대학교 대학원 전자계산학과 석사
2003년 경희대학교 대학원 컴퓨터공학과 박사과정 수료
2004년 ~ 현재 한신대학교 정보통신학과 겸임교수
관심분야 : Mobile IP, 차세대 네트워크, 네트워크 보안
E-mail : bhyunkim@lycos.co.kr

문 영 준 (Youngjun Moon)
2001년 경희대학교 전자계산공학과 졸업(공학사)
2003년 경희대학교 대학원 컴퓨터공학과 졸업(공학석사)
2003년 ~ 현재 경희대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 인터넷 QoS, 네트워크 보안, 무선 네트워크
E-mail : yjmoon@khu.ac.kr



조 영 섭 (YeongSub Cho)
1993년 인하대학교 전자계산공학과 졸업
1995년 인하대학교 대학원 전자계산공학과 석사
1999년 인하대학교 대학원 전자계산공학과 박사
1998년 12월 ~ 현재 한국전자통신연구원 디지털ID보안연구팀 선임연구원
관심분야 : Identity Management, PKI, 인증인가, Web Service Security, 정보보호
E-mail : yscho@etri.re.kr

진 승 헌 (Seunghun Jin)
1993년 숭실대학교 전자계산학과 학사
1995년 숭실대학교 대학원 전자계산학과 석사
2004년 충남대학교 대학원 컴퓨터과학과 박사
1994년 (주)대우통신 종합연구소 연구원
1996년 (주)삼성전자 통신연구소 전임연구원
1999년 ~ 현재 한국전자통신연구원 디지털ID보안연구팀장/선임연구원
관심분야 : I&AM, PKI, Network Security, EC
E-mail : jinsh@etri.re.kr