情報保護學會論文誌
第15卷 第6號, 2005. 12

모바일 환경으로 확장 가능한 federated ID 연동 방안에 관한 연구

김 배 현,[1†] 유 인 태[2‡]

[1]한신대학교 정보통신학과, [2]경희대학교 전자정보대학

A Study on Scalable Federated ID Interoperability Method in Mobile Network Environments

Baehyun Kim,[1†] Intae Ryoo[2‡]

[1]Dept. Information Science and Telecommunication, Hanshin University,

[2]College of Electronics & Information, Kyunghee University

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 federated ID 연동을 유선 컴퓨팅 환경에서뿐만 아니라 모바일 컴퓨팅 환경으로 확장하기 위한 federated ID 연동 모델을 제안하고 평가하였다.

ABSTRACT

While the current world wide network offers an incredibly rich base of information, it causes network management problem because users should have many independent IDs and passwords for accessing different servers located in many places. In order to solve this problem users have employed single circle of trust(COT) ID management system, but it is still not sufficient for clearing the problem because the coming ubiquitous network computing environment will be integrated and complex networks combined with wired and wireless network devices.

The purpose of this paper is to describe the employment and evaluation of federated ID interoperability method for solving the problem. The use of the proposed model can be a solution for solving network management problem in the age of mobile computing environment as well as wired network computing environment.

Keywords : *Mobile Computing, Scalable ID, ID Federation*

접수일 : 2005년 7월 15일 ; 채택일 : 2005년 11월 2일

† 주저자 : bhyunki@hs.ac.kr

‡ 교신저자 : bhyunkim@hs.ac.kr

Ⅰ. 서 론

본격적인 정보화 시대가 전개되면서 사용자들이 접하게 되는 정보 시스템은 수적인 증가뿐만 아니라 물리적 환경 또한 유선 컴퓨팅과 모바일 컴퓨팅이 연동하는 환경으로 변화하였다. 일반적으로 사용자는 각 정보 시스템에 접속하기 위하여 ID와 패스워드를 사용하게 되는데, 이런 정보 시스템의 양적 증가와 환경적 변화는 ID와 패스워드의 관리에 많은 어려움을 주고 있다. 이러한 ID 관리의 복잡성을 해결하기위해 ID 관리 시스템에 대한 연구가 진행되었다. ID 관리는 이기종의 다양한 시스템을 단 한 번의 인증과정을 거쳐 접근 가능하도록 함으로써 ID와 패스워드 관리의 문제점을 해결할 수 있고[1,2,9,10,] 동시에 시스템 관리자에게는 개별적인 인증시스템 관리의 복잡성을 해결할 수 있게 해준다. ID 관리 분야는 일반적으로 기업 내 사용자의 ID 관리를 주 대상으로 하는 Enterprise IdM(Enterprise Identity Management) 분야와 이를 더욱 확장하여 일반 인터넷 사용자의 ID 관리 문제를 해결하기 위한 인터넷 ID 관리 서비스 분야가 있다. Enterprise IdM은 기업 내 사용자 관리를 주 대상으로 하는 것으로 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. federated ID는 사용자가 하나의 신뢰영역에 등록한 하나의 ID를 이용하여 자신의 신뢰영역 뿐만 아니라 다른 신뢰영역에서도 인증을 받는 것이다. 따라서 인터넷 ID 관리 서비스를 위해서는 단일 신뢰영역이 아닌 다중 신뢰영역간의 ID 연동(ID federation)을 위한 federated ID가 제공해야한다[3,4,6,11]. 또한 모바일 환경에서도 인터넷을 사용하려는 요구가 증가하고 있고, 향후 도래할 유비쿼터스 환경에서는 유무선 네트워크상의 수많은 컴퓨터가 유기적으로 연결되기 때문에 ID관리 서비스를 모바일 환경으로 확장하여야한다.

따라서 본 논문은 인터넷 ID관리 서비스를 제공하기위한 federated ID를 유선 컴퓨팅 환경에서 모바일 컴퓨팅 환경으로 확장하기위한 federated ID 연동 모델을 제안하고 이를 평가하기위해, 2장에서는 인터넷 ID 관리와 기술동향에 대해 살펴보고, 3장에서는 모바일 컴퓨팅 환경으로 확장 가능한 federated ID 연동 모델과 3가지 시나리오를 제시한다. 4장에서는 제안 모델을 평가하였으며 5장에서는 결론을 내린다.

Ⅱ. ID 관리 기술 동향 및 적용사례

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 연동(ID federation)을 지원하지 않고 있으며 표준화 기구에서 제정하는 표준을 준용하지도 않고 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 연동(ID federation)을 위한 플랫폼을 제공해주기 위한 공개 소스 프로젝트이다. Ping Identity는 SourceID 플랫폼을 통하여 federated ID 어플리케이션이나 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[4]. 리버티 연합 프레임워크는 federated ID 관리에 따른 모바일 데이터 서비스를 위해 생성된 표준으로 이들 내용은 주로 이동 통신 사업자를 주축으로 구체화되었다 [5,6,7,8].

Ⅲ. 모바일 컴퓨팅 환경에서 확장 가능한 federated ID 연동 모델

3장에서는 지금까지 알아본 유무선 환경에서의 federated ID 관리 방법에서 SSO 구현에 초점을 맞추어 모바일 환경에서 확장 가능한 federated ID 연동 모델 4가지와 가능한 3가지의 시나리오를 제시하고 모델 별로 3가지의 시나리오를 적용한다. 본 논문에서는 모바일 환경에서의 장치들

중에서 이동전화를 대상으로 모바일 컴퓨팅 환경으로 확장 가능한 federated ID 연동 방안을 제안한다.

1. 모바일 컴퓨팅 환경의 ID 인증 요청 모델

우선 모바일 컴퓨팅 환경에서 인증 요청 모델을 2가지로 구분하였다.

사용자 시스템 인증 요청 모델은 그림 1과 같이 사용자 시스템(User System)이 서비스 제공자(Service Provider)에게 서비스를 요청하면, 서비스 제공자는 사용자 시스템에게 인증을 요청한다. 사용자 시스템은 인증을 받기위해 Identity 제공자(Identity Provider)에게 인증을 요청하여 인증을 받은 후, 서비스 제공자에게 인증 사실을 넘겨주면, 서비스 제공자는 사용자 시스템에게 서비스를 제공한다. 이 모델은 Ticket 기반 인증과 같은 방법을 생각할 수 있다. 사용자 시스템 인증 요청 모델의 개념은 리버티연합의 SSO 모델과 유사하며, 리버티 연합에서는 사용자 시스템이 아닌 사용자 에이전트 개념을 사용한다[6,7,13].

서비스 제공자 인증 요청 모델은 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.

사용자 시스템 인증 요청 모델의 경우, 사용자 시스템이 인증과정에 참여하고 있기 때문에 사용자 시스템이 인증 과정에서 load가 집중된다. 그러나 서비스 제공자는 인증과정에 직접 참여하지 않기 때문에 서비스 제공자 인증 요청 모델에 비해 load가 적다. 서비스 제공자 인증 요청 모델은 사용자 시스템 인증 요청 모델에 비해 사용자 시스템이 인증 과정에 참여하지 않기 때문에 load가 적지만, 서비스 제공자가 인증과정에 참여해야 하기 때문에 load가 많아진다.

2. federated ID 기능 구현 장치에 따른 모델

federated ID를 모바일 환경으로 확장하기 위해서는 federated ID 기능을 모바일 환경에 구현해야만 한다. 이것은 federated ID 기능이 모바일 환경의 사용자 시스템에 구현되어야 한다는 것을 의미한다. federated ID 기능을 구현하기 위한 사용자 시스템으로 고려할 수 있는 것은 이동전화와 WAP 게이트웨이이다. 이동전화의 경우, 스마트카드가 적용된 이동전화를 사용할 경우에는 현재의 WAP 게이트웨이를 그대로 사용하고 스마트카드를 이용하여 federated ID 관리 기능을 이동전화기에 구현이 가능하다. 그러나 현재 GSM 방식을 사용하는 국가들이나 CDMA 방식을 사용하는 국가들 모두에서 스마트카드가 일부 사용되고 있지만 아직은 널리 보급 되지 못했다. 따라서 스마트카

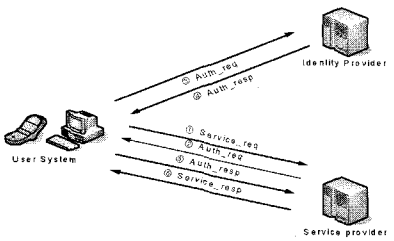


그림 1. 사용자 시스템 인증 요청 모델

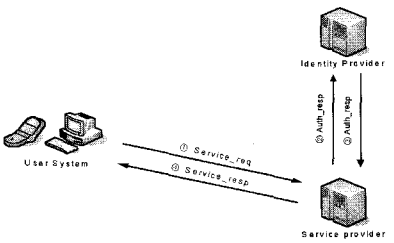


그림 2. 서비스 제공자 인증 요청 모델

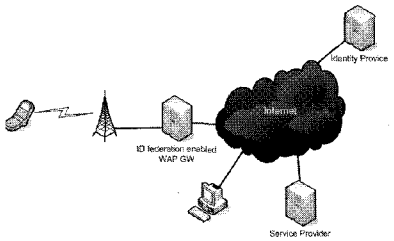


그림 3. ID federation enabled WAP/GW 모델

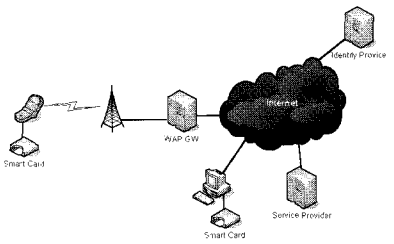


그림 4. ID federation Mobile Phone 모델

드가 사용되지 않는 이동전화의 경우, federated ID 관리 기능을 적용하는 것이 곤란하다. 그렇기 때문에 현존하는 WAP 게이트웨이에 federated ID 관리 기능을 구현한 ID federation enabled WAP 게이트웨이가 필요하다[6,7].

이에 따라, federated ID 관리 기능을 어느 사용자 시스템에 구현하느냐에 따라 그림 3과 그림 4와 같이 2가지 모델로 구분 할 수 있다.

3. 제안 모델

3장의 1, 2 절에서 살펴본 모델을 기반으로 본 논문에서는 모바일 환경으로 확장 가능한 federated ID 연동 모델 4가지를 제시한다.

제안 모델 1은 사용자 시스템 인증 요청 모델(그림1)에 ID federation enabled WAP/GW 모델(그림 3)을 적용한 모델이며, 이 모델은 [7]과 유사하다. 제안 모델 2는 사용자 시스템 인증 요청 모델(그림1)에 ID federation enabled Mobile Phone 모델(그림 4)을 적용한 모델이다.

제안 모델 3은 서비스 제공자 인증 요청 모델 2 (그림 2)에 ID federation enabled WAP/GW 모델(그림 3)을 적용한 모델이고, 제안 모델 4는 서비스 제공자 인증 요청 모델(그림2)에 ID federation enabled Mobile Phone 모델(그림 4)을 적용한 모델이다.

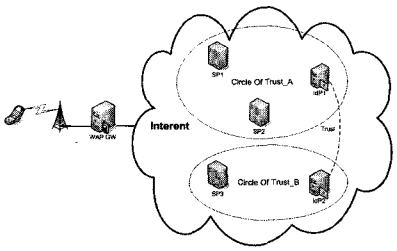


그림 9. federated ID 연동 시나리오

4. 제안 모델의 federated ID 연동 시나리오

논 본문에서 제안한 federated ID 연동 모델을 평가하기위해 적용 가능한 3가지 시나리오를 제시한다. 그림 9는 본 논문에서 제시한 시나리오의 환경을 나타낸다. 그림 9는 두 개의 신뢰영역 COT_A와 COT_B가 있다. COT_A상에는 Identity 제공자 IdP1과 서비스 제공자 SP1, SP2가 있고 COT_B 상에는 Identity 제공자 IdP2와 서비스 제공자 SP3이 있다. 또한 IdP1과 IdP2는 신뢰관계라고 가정한다.

시나리오 1은 가입자가 가입한 Identity 제공자 IdP1과 서비스 제공자 SP1과 SP2가 동일한 신뢰 영역에 속하고 가입자가 서비스 제공자 SP1에서 먼저 인증을 받아 서비스를 받은 후 서비스 제공자 SP2에게 서비스를 받기위한 경우이다. 시나리오 2는 가입자가 가입한 Identity 제공자 IdP1

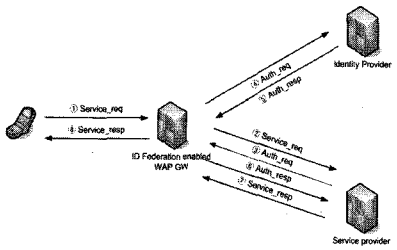


그림 5. 제안 모델 1

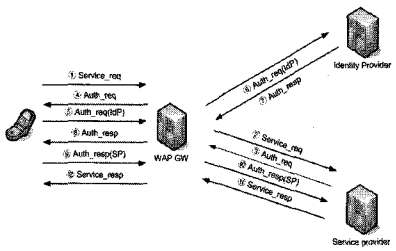


그림 6. 제안 모델 2

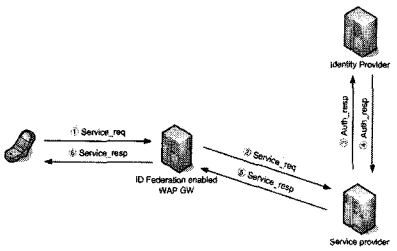


그림 7. 제안 모델 3

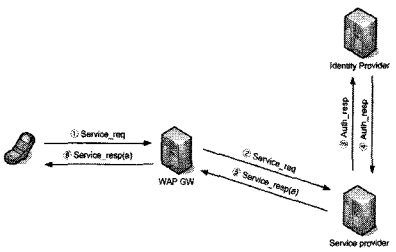


그림 8. 제안 모델 4

과 동일한 신뢰영역에 존재하는 서비스 제공자 SP1에 서비스를 받기위해 인증을 받은 후, 가입자가 가입하지 않은 Identity 제공자 IdP2의 신뢰영역에 존재하는 서비스 제공자 SP3에게 서비스를 받기 원하는 경우이다. 시나리오 3은 가입자가 가입하지 않은 Identity 제공자 IdP2의 신뢰영역에 존재하는 서비스 제공자 SP3에게 서비스를 받기위해 인증된 후, 가입자가 가입한 Identity 제공자 IdP1과 동일한 신뢰영역에 존재하는 서비스 제공자 SP1에 서비스를 받기 원하는 경우이다.

이제, 제안 모델 4종류에 3가지 시나리오를 각각 적용하여 federated ID 연동 방안에 대한 시나리오를 제시한다.

4.1 제안 모델 1에 대한 3가지 시나리오

제안 모델 1에 3가지의 시나리오를 적용한 시나리오(그림 10~그림 12)를 제시한다.

표 1. 제안 모델 1에서 시나리오 1, 2, 3의 메시지 정의

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

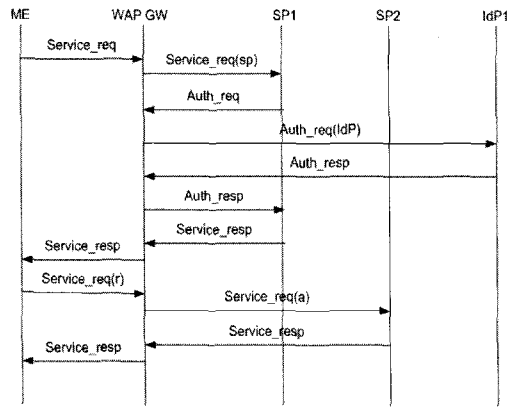


그림 10. 제안 모델 1의 시나리오 1

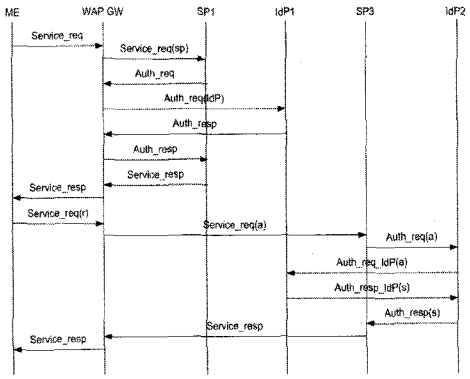


그림 11. 제안 모델 1의 시나리오 2

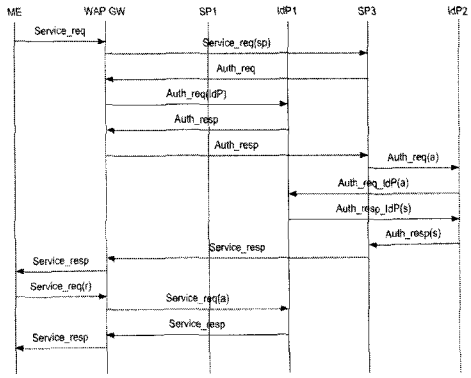


그림 12. 제안 모델 1에서 시나리오 3

4.2 제안 모델 2에 대한 3가지 시나리오

제안 모델 2에 3가지의 시나리오를 적용한 시나리오(그림 13~그림 15)를 제시한다.

표 2. 제안 모델 2에서 시나리오 1, 2, 3의 메시지 정의

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

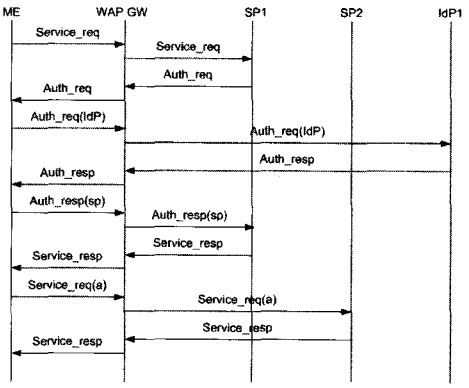


그림 13. 제안 모델 2에서 시나리오 1

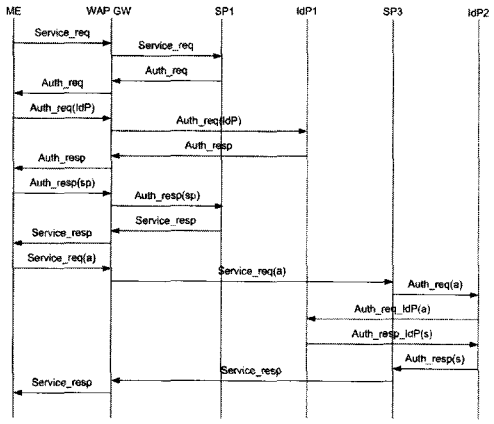


그림 14. 제안 모델 2에서 시나리오 2

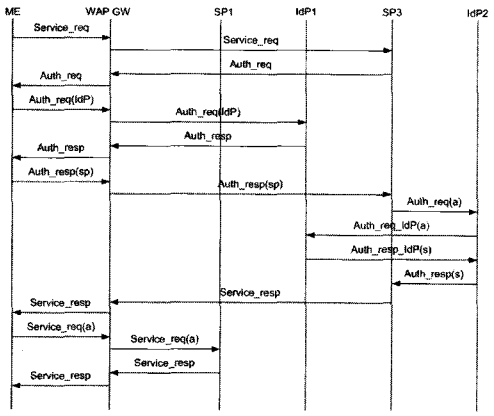


그림 15. 제안 모델 2에서 시나리오 3

4.3 제안 모델 3에 대한 3가지 시나리오

제안 모델 3에 3가지의 시나리오를 적용한 시나리오(그림 16~그림 18)를 제시한다.

표 3. 제안 모델 3에서 시나리오 1, 2, 3의 메시지 정의

메시지	파라미터
Service_req	IDuser, PW, PN, IDIdP, IDSP
Service_req(r)	PN, IDIdP, IDSP, flag
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, IDIdP, RAND
Auth_req_IdP_(a)	AuthToken, RAND, flag
Auth_resp_IdP(s)	RAND, flag
Auth_resp_IdP(a)	AuthToken, RAND, flag

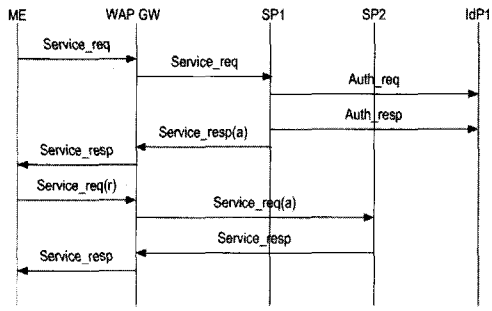


그림 16. 제안 모델 3에서 시나리오 1

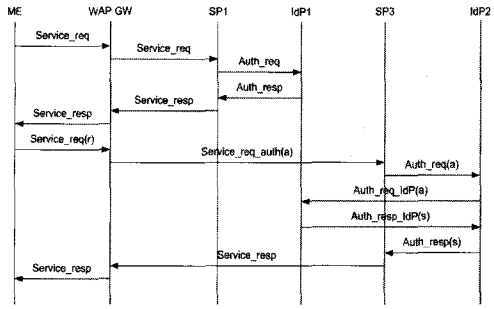


그림 17. 제안 모델 3에서 시나리오 2

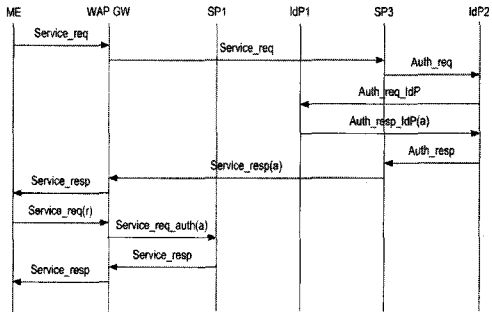


그림 18. 제안 모델 3에서 시나리오 3

4.4 제안 모델 4에 대한 3가지 시나리오

제안 모델 4에서 3가지의 시나리오를 적용한 시나리오(그림 19~그림 21)를 제시한다.

표4. 제안 모델 4에서 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

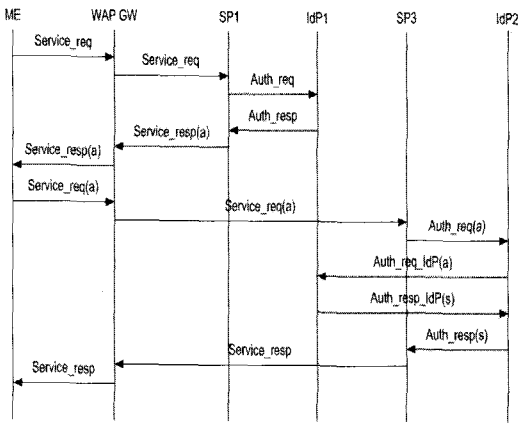


그림 19. 제안 모델 4에서 시나리오 2

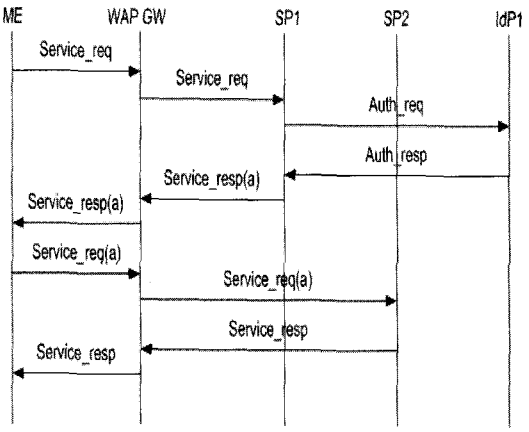


그림 20. 제안모델 4에서 시나리오 1

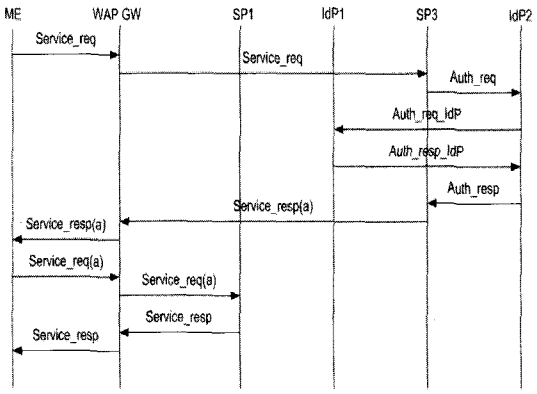


그림 21. 제안모델 4에서 시나리오 3

Ⅳ. 분석 및 평가

본 논문에서 제안한 4가지 모델에 3가지 시나리오를 적용하여 발생하는 메시지의 수와 각 주체별로 메시지 처리횟수를 표 5에서 비교 분석하였다. 표5에서는 각 시나리오별 발생하는 메시지의 수는 모델 2가 가장 많고 모델1 그리고 모델 3과 4의 순으로 적어짐을 보여준다. 또한 WAP 게이트웨이가 처리하는 메시지의 수도 모델2, 모델1, 그리고 모델 3과 4의 순으로 적어진다는 것을 보여준다. 이것 이외에도 전체적으로 기존의 [6], [7]에서 사용하는 모델 1이 모델 2 보다는 효율적이지만 본 논문에서 제안한 모델 3과 4가 발생하는 메시지의 수와 주체별 메시지 처리횟수가 적다는 것을 알 수 있다. 따라서 federated ID 연동을 위해서는 서비스 제공자가 Identity 제공자에게 직접 사용자의 인증요청을 처리하는 모델이 더 효율적이다. 또한 서비스 제공자가 Identity 제공자에게 직접 사용자의 인증요청을 처리하는 모델인 경우 federated ID 연동기능을 WAP 게이트웨이에 구현하거나 이동장치인 이동전화에 구현하더라도 발생되는 메시지의 수나 각 주체별 메시지 처리횟수에는 차이가 없다. 그러나 제안한 모델을 상용망에의 실제 적용하는데 있어서, 현재 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 있

표 5. 제안된 모델별 시나리오에 따른 메시지 수와 메시지 처리 횟수

			Model 1	Model 2	Model 3	Model 4
시나리오 1	주체별 메시지 처리 횟수	ME	4	8	4	4
		WAP G/W	12	16	8	8
		SP1	4	4	4	4
		SP2	2	2	2	2
		IdP1	2	2	2	2
	총 메시지 수		12	16	10	10
시나리오 2	주체별 메시지 처리 횟수	ME	4	8	4	4
		WAP G/W	12	16	8	8
		SP1	4	4	4	4
		SP3	4	4	4	4
		IdP1	4	4	4	4
		IdP2	4	4	4	4
	총 메시지 수		16	20	14	14
시나리오 3	주체별 메시지 처리 횟수	ME	4	8	4	4
		WAP G/W	12	16	8	8
		SP1	2	2	2	2
		SP3	6	6	4	4
		IdP1	4	4	2	2
		IdP2	4	4	4	4
	총 메시지 수		16	20	12	12

다. 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 식별자 등을 적용한 스마트카드의 사용을 고려해야 한다.

V. 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 관리 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 논문에서는 모바일 컴퓨팅 환경의 장비로 이동 전화를 고려하여 모바일 환경까지 federated ID 연동 기능을 확장하기 위한 4가지 모델과 3가지 시나리오를 제안하고 제안 모델에 3가지 시나리오를 적용하여 제안 모델들을 평가 분석하였을 뿐만 아니라, 현재 모바일 컴퓨팅 환경에 적합한 federated ID 연동 방안을 제시하였다. 본 논문의 연구결과는 향후 도래할 유선 컴퓨팅과 모바일 컴퓨팅이 연동하는 다양한 환경에서 federated ID 연동 기술 개발에 적용가능하다.

참 고 문 헌

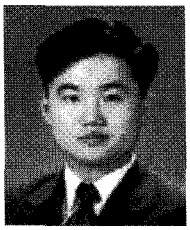
[1] 서대희, 이임영,"Single Sign-on에 적용 가능한 인증모델에 관한 연구," 한국정보보호학회 종합학술발표회 논문집, Vol. 12, No. 1, pp.311-314.

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

[3] 한국전자통신연구원 정보보호연구단 인증기반연구팀,"*인터넷 ID 관리 서비스 기술 백서*

ver1.0," 2004.
[4] LIBERTY ALLIANCE,"*Tier 2 Business Guidelines: Mobile Deployments*," liberty-bmeg-biz-tier2-mobile-1.1a.doc, http://www.projectliberty.org/.
[5] Nokia,"*Mobile Personality*," http://www.nokia.com/, 2002.
[6] Nokia,"*Liberty Enhances Mobile Identification*," http://www.nokia.com/,2002.
[7] Nokia,"*Identity management in mobile services*," http://www.nokia.com/, 2003.
[8] Nokia and Sun Microsystems,"*Deploying Mobile Web Services using Liberty Alliance's Identity Web Services Framework (ID-WSF)*," White Paper, June 2004.
[9] Andreas Pashalidis and Chris Mitchell,"*Using GSM/UMTS for Single Sign-On*," 0-7803-7993-4/03, pp.138-145, 2003.
[10] Andrej Volchkov,"*Revisiting Single Sign-On, A Pragmatic Approach in a New Context*," IT Pro, Jan.-Feb., 2001.
[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/.
[13] LIBERTY ALLIANCE, "*Identity Federation and Web services - technical use cases for mobile operators*," nokia_sun_a4_2812.pdf, http://www.projectliberty.org

〈著紹介〉



김 배 현 (Baehyun Kim) 정회원
1995년 2월: 호원대학교 전자계산학과 졸업
1997년 2월: 수원대학교 전자계산학과 석사
2003년 2월: 경희대학교 컴퓨터공학과 박사수료
2004년 9월~현재: 한신대학교 정보통신학과 겸임교수
〈관심분야〉 Mobile IP, 차세대 인터넷, WLAN, 네트워크 보안

유 인 태 (Intea Ryoo) 정회원
1987년 2월: 연세대학교 전자공학과 졸업
1989년 2월: 연세대학교 전자공학과 석사
1994년 2월: 연세대학교 전자공학과 박사
1997년 9월: 동경대학 전자정보통신전공 Ph.D
1997년 10월~1999년 3월: 삼성전자 정보통신총괄 선임연구원
1999년 3월~현재: 경희대학교 전자정보대학 부교수
〈관심분야〉 인터넷, 네트워크 보안, 무선 LAN, IPT