情報保護學會論文誌
第17卷 第6號, 2007. 12

모바일 환경에서 사용자 중심의 전자ID지갑 운용 메커니즘*

송 동 호[1†], 임 선 희[1], 이 옥 연[2‡], 임 종 인[1]
[1]고려대학교 정보경영공학전문대학원, [2]국민대학교 자연과학대학 수학과

A Digital ID Wallet User-oriented Mechanism in a Mobile Environment

Dongho Song[1†], Sun-Hee Lim[1], Okyeon Yi[2‡], Jongin Lim[1]
[1]Graduate School of Information Management and Security, Korea University,
[2]Department of Mathematics, Kookmin University

요 약

유비쿼터스 환경이 도래함에 따라 모바일 단말을 이용한 무선 인터넷의 이용이 증가하고 있다. 그 결과 사용자가 관리해야 하는 Digital Identity 정보가 기하 급수적으로 증가하고 있다. 또한 사용자가 가입 시 SP(Service Provider)에게 등록한 개인정보는 기초적인 신상정보부터 금융정보에 이르기까지 다양한 정보들을 포함하고 있다. 따라서 개인 정보를 사용자 스스로가 통제가 가능하며 전자ID지갑에 단순한 인증정보뿐만 아니라 금융, 결제 등 다양한 정보를 포함한 Ticket을 전자ID지갑에서 간단하게 선택해 자신의 정보를 안전하게 관리할 수 있어야 한다. 이를 위하여 사용자 스스로가 개인정보의 활용을 통제할 수 있는 모바일 환경에서의 사용자 중심의 Digital Identity 운용 메커니즘을 제안한다.

ABSTRACT

As a ubiquitous environment approaches and the use of the wireless Internet using the mobile terminals is on the increase. Therefore, the users have to undergo the inconvenience of repeatedly input the same information for the user registration and the ID certification. The information the users have to put in to register in on-line services range from the basic personal information to the more other private information such as financial information. Accordingly the user can be in control of users personal information and safely manage the information by conveniently selecting from the Digital ID Wallet the Ticket that holds various information including the basic, financial or payment certification-related information. Consequently, we propose a digital identity management mechanism to control one's personal information in a mobile environment.

Keywords : Mobile Digital Id Wallet, 4G, GBA Based On Artifact Mechanism, USIM Multi Application

Ⅰ. 서 론

모바일 환경에서 사용자가 언제 어디서나 모바일 단말을 이용한 무선 인터넷 서비스 사용이 빠르게 증가하면서 사용자는 서비스마다 자신의 개인정보를 등록하고 서비스를 이용하기 전에 인증 받는 과정을 수행해야만 한다.[1] 사용자가 가입 시 SP에게 등록한 개인정보는 기초적인 신상정보부터 사용자와 긴밀하게 관련되는 다양한 정보들을 포함하고 있지만, 이러한 개인정보가 SP마다 중복적으로 존재하고 어떠한 방식으로 관리, 사용, 폐기되는지 확인이 불가능하므로 보안측면에서 위험

접수일: 2007년 8월 9일; 채택일: 2007년 9월 21일
* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2007-(C1090-0701-0025))
† 주저자, a95rd038@nate.com
‡ 교신저자, oyyi@kookmin.ac.kr

하다.

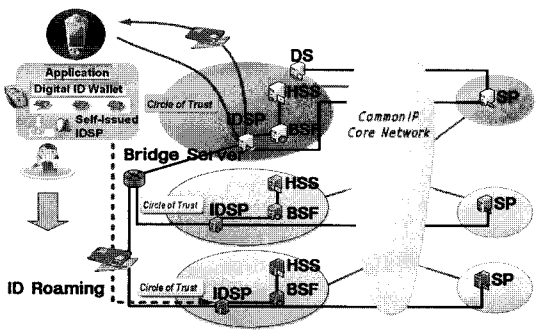
최근에 3GPP에 Liberty Alliance를 바탕으로 인증과 키 일치를 위한 AKA(Authentication and Key Agreement)을 통해 IDSP(Internet ID Service Provider)가 발급한 인증서를 이용하여 간편한 인증과 접근 제어 보안 메커니즘이 제안되었다.[8] 이 메커니즘은 사업자 중심의 ID관리 메커니즘으로 단순히 SSO 서비스만을 제공한다.

따라서 본 고에서는 Liberty Alliance를 적용한 사용자가 본인의 개인정보의 제공여부를 직접 관리할 수 있는 사용자 중심의 모바일 환경에서의 전자ID지갑 서비스를 제안한다.

Ⅱ. 모바일 전자ID지갑의 필요성

앞으로 다가올 4G 이동통신 환경에서는 유선환경의 서비스보다 사용자가 무선환경을 통한 서비스 이용이 빠르게 증가할 것으로 예상된다.[3] 따라서 사용자는 수많은 사이트에 개인정보를 등록하고 인증을 위해 같은 ID 정보를 반복적으로 입력해야 하는 불편을 겪고 있으며, 불법적인 개인정보의 노출과 악용의 위험에 직면해 있다.[2]

따라서 [그림 1]과 같이 단말의 USIM에 전자ID지갑을 탑재함으로써 전자인증에 필요한 개인정보 및 인증정보를 단말의 USIM에 저장한 후 사용자가 응용서비스를 이용 시 기존에 발급 받은 Ticket의 정보를 이용하여 사용자 스스로 Ticket의 발급함으로써 시간과 장소에 제약 없이 개인정보를 전송할 수 있다. 또한 사용자가 속한 단일 신뢰 영역에서 멀티미디어 서비스를 제공받



〔그림 1〕 A Digital ID Wallet Mechanism using USIM

는 중 그 영역을 벗어나게 되면 기존에 발급한 Ticket를 다른 신뢰 영역의 IDSP에 제공함으로써 사용자는 단절 없이 서비스를 계속 제공 받을 수 있다. 즉 기존에 유선환경에서 이루어지는 사업자 중심의 ID 관리 시스템 위주가 아니라 언제 어디서나 전자ID지갑이 탑재된 휴대폰을 통해 개인정보를 저장하여 간단하게 선택하여 서비스를 이용함으로써 사용자 스스로가 자신의 개인정보에 대한 흐름을 제어할 수 있는 사용자 중심의 모바일 전자ID지갑 메커니즘이다.

Ⅲ. 표준화 동향 및 GBA(Generic Bootstrapping Architecture) 기반의 Artifact 메커니즘 분석

3.1. Liberty [1]

ID-FF는 서로 다른 사이트에 존재하는 동일 사용자의 ID를 연계하는 Federation과 SSO를 제공하기 위한 규격이며 ID제공자 알림 서비스, 익명 ID매핑과 글로벌 로그아웃 서비스를 정의하였다.

ID-WSF는 개인정보를 선택적으로 제공해주는 허가-기반의 속성정보 공유 서비스를 지원한다.

ID-SIS는 기본 프로파일 정보를 제공해주는 ID 프로파일 서비스로 사용자의 등록 과정에서 사용되며 다른 서비스와 상호 동작이 가능하다

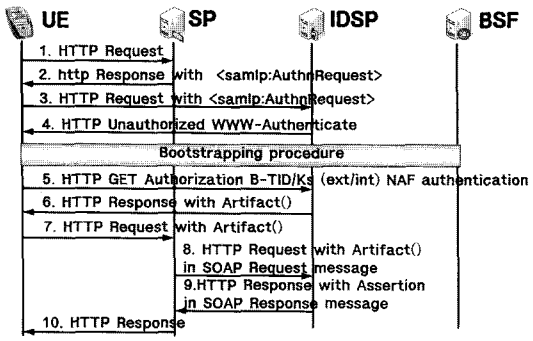
3.2. WS-* [6]

WS-Security는 보안 토큰을 이용한 무결성과 신뢰성을 웹 서비스 메시지(SOAP)에 반영하기 위한 메커니즘과 메시지 보호 수준을 제공하기 위한 활용을 지원하며 WS-Trust는 신뢰 관계를 직접 맺는 방법과 신뢰할 수 있는 중간 계층을 통해서 맺는 방법을 정의한다. WS-Policy는 송수신자가 자신들의 요구사항과 지원 가능한 정도를 명시하는 방법을 제공한다. 또한 WS-Federation은 커버로스와 PKI 기반 구조를 연동하는 방법 등이 기술 되어 있다.

3.3. GBA 기반의 Artifact 메커니즘 분석

3.3.1. GBA 기반의 시스템 구조

GBA는 인증과 접근 제어가 필요한 특정 응용에서



〔그림 2〕 Message flow for SSO with Artifact and usage of GBA

사용 될 수 있는 보안 메커니즘으로 UE(User Equipment), BSF(Bootstrapping Server Function), NAF (Network Application Function), HSS(Home Subscriber Server)로 구성되며 BSF와 HSS 사이에 가입자의 정보와 세션키를 갱신을 통해 상호 인증을 하는 구조이다. [7]

GAA(Generic Authentication Architecture)는 간편한 인증과 세션키 관리를 제공하며 AKA를 기반으로 하며 GAA에서 인증 모델은 인증서를 이용하는 방법으로 사용되는 보안 메커니즘이 GBA이다. [9]

GBA 기반의 Artifact 메커니즘에서 SAML을 이용한 서비스 중에 가장 핵심적인 내용은 인증확인서 역할을 하는 Assertion이다. 반면 Artifact는 SSO에 사용되는 Ticket과 같은 역할을 한다. [8]

3.3.2. GBA 기반의 Artifact를 이용한 서비스 제공 Flow

Artifact를 이용하여 [그림 2]와 같이 사용자가 특정 서비스를 요청할 경우 GBA의 AKA 과정과 Bootstrapping과정을 통해 세션키를 공유한다. 사용자는 IDSP로부터 전송 받은 Artifact를 SP에게 전송하고 SP는 IDSP에게 Assertion을 요청하여 검증 후 사용자는 SP의 특정 서비스를 이용하는 구조이다.

GBA 기반의 Artifact를 이용한 서비스 제공과정은 다음과 같다.

① UE->SP : GBA 기반의 인증 사항을 포함한 HTTP Request를 전송한다.

② SP->UE : SP는 IDSP의 URL을 전송한다.

③ UE->IDSP : UE는 IDSP의 URL을 통해 IDSP에 접속한다.

④ IDSP->UE : IDSP는 UE에 대한 비인증 상태의 HTTP 응답을 전송한다.

⑤ UE->IDSP : B-TID와 패스워드로 Ks_(ext/int)_NAF 및 LAP와 관련된 사용자 data를 전송한다.

⑥ IDSP->UE : IDSP는 Artifact와 SP로 메시지를 Redirection 시키기 위한 SP의 URL을 전송한다.

⑦ UE->SP : UE는 Artifact를 SP에게 전송한다.

⑧ SP->IDSP : SP는 UE로부터 Artifact를 추출하여 IDSP/NAF에게 전송하고 Assertion을 요청한다.

⑨ IDSP->SP : IDSP는 SP로부터 전송 받은 Artifact를 확인한 후 SP에게 Assertion을 전송한다.

⑩ SP->UE : SP는 Assertion을 검증하고 UE에게 메시지를 전송한다.

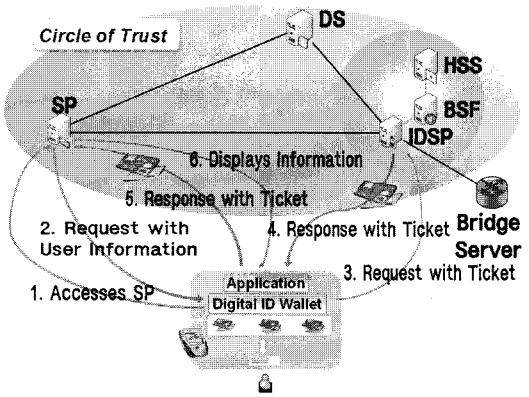
Ⅳ. USIM Muti-Application Platform

전자ID지갑 시스템에서는 USIM에 전자ID지갑 애플리케이션을 탑재하는 구조이다. USIM은 기본적으로 가입자 정보를 탑재한 SIM카드와 다양한 애플리케이션을 담을 수 있는 UICC가 결합된 형태로 이동통신 가입자 인증 기능과 개인정보 관리 서비스를 제공한다. 메모리와 CPU의 향상으로 인하여 다양한 애플리케이션의 탑재가 가능하며 애플리케이션 간에 정보를 공유할 수 있다. 따라서 무선 네트워크상에서 단말기에 애플리케이션 관련 정보를 USIM에 저장하는 것이 가능하기 때문에 전자ID지갑에 이용할 수 있다.

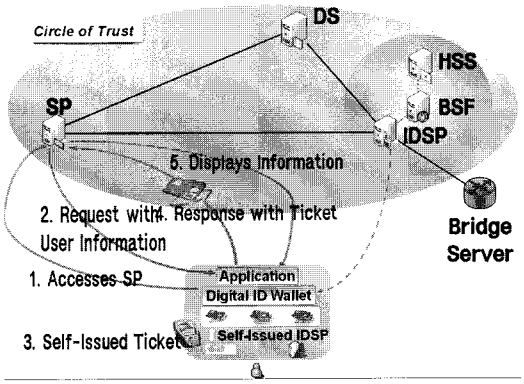
Ⅴ. 모바일 환경에서의 전자ID지갑 메커니즘

기존의 GBA기반의 Artifact를 이용한 메커니즘은 GBA 인증 과정을 통해 세션키를 공유하고 IDSP에서 발급한 Artifact를 이용하여 단순히 SSO 서비스를 제공받는 구조이다.

본 장에서 제안하는 모바일 환경에서의 전자ID지갑 메커니즘은 사용자가 이동 중에 무선 인터넷을 이용할 때 사용자가 서비스를 요청 시 AKA을 통한 Bootstrapping 인증과정 후 사용자가 SP가 제공받을 수 있는 속성을 선택하여 Ticket을 발급받아 저장 후 사용하며 기존에 발급 받은 Ticket의 정보를 이용하여 사용자 스스로 Ticket을 발급함으로써 개인정보를 사용자가



〔그림 3〕 Message flow Tickets issued by Identity Provider



〔그림 4〕 Message flow for Self-Issued Tickets

스스로 통제가 가능하다. 이 메커니즘은 GBA와 Liberty Alliance에서 제공하는 ID 정보의 요청/제공, 검색, 인증에 대한 규격, 사용자 질의에 대한 규격, ID 정보의 종류와 타입을 기반으로 한다.

5.1. 전자ID지갑 Ticket 발급 메커니즘

5.1.1. Tickets Issued by Identity Provider

[그림 3]과 같이 SP가 요구하는 정보를 포함하는 Ticket이 사용자에게 없을 경우 IDSP에서 새로운 Ticket을 발급받아 SP의 인터넷 서비스를 이용하는 경우는 다음과 같다.

① UE->SP : UE는 SP에게 서비스 요청한다.
② SP->UE : SP는 UE가 서비스를 제공받기 위해 필요한 정보를 전송한다.
③ UE->IDSP : IDSP에 SP가 요구하는 정보를 포함하는 Ticket을 요청한다.
④ IDSP->UE : IDSP는 Ticket을 발급 후 전송한다.
⑤ UE->SP : UE는 IDSP가 발급한 Ticket을 저장한 후 SP에게 전송한다.
⑥ SP->UE : SP는 Ticket을 검증하고 UE에게 메시지를 전송한다.

5.1.2. Self-Issued Tickets

[그림 4]와 같이 사용자 스스로가 기존의 Ticket을 기반으로 SP가 요구하는 정보를 포함하는 Ticket을 생성하여 인터넷 서비스를 이용한다.

① UE->SP : UE는 SP에게 서비스 요청한다.
② SP->UE : SP는 UE가 서비스를 제공받기 위해 필요한 정보를 전송한다.
③ UE : 기존에 Tickets의 정보를 이용하여 SP가 요구하는 정보를 포함하는 Ticket을 생성한다.
④ UE->SP : 생성한 Ticket을 SP에게 전송한다.
⑤ SP->UE : SP는 Ticket을 검증하고 UE에게 메시지를 전송한다.

5.2. 인증과 키 일치 과정을 통한 Bootstrapping 인증

5.2.1. Bootstrapping

Bootstrapping과정은 GBA 인증과 접근 제어가 필요한 특정 서비스에서 사용되는 보안 메커니즘이다. AKA 과정은 USIM과 AuC만 이용할 수 있는 분배된 비밀키 K의 정보를 이용하여 사용자와 네트워크의 상호 인증 및 키 일치 과정이다. AKA를 통해 사용된 CK, IK를 가지고 Bootstrapping 인증과정과 Bootstrapping 사용과정 즉 키 일치 과정을 통해 세션키(Ks)를 생성하여 사용자와 인증서버 간에 세션키를 동의하는 과정이다. [8]

5.2.2. Bootstrapping Authentication

Bootstrapping Authentication 과정은 사용자가 HN(Home Network)에 인증 과정과 키를 전송하는 과정으로 이루어진다.

① UE가 BSF에 사용자 이름을 보내서 요청한다.
② BSF는 RES와 XRES(Expected Response)를 비교하여 인증하고 HSS로부터 사용자 이름에 대응하는 GUSS(GBA User Security Setting)/USS(User Security Setting), 인증벡터를 가져온다.
③ 이 단계에서 상호 인증이 완료된다.
④ BSF는 RAND값과 BSF 이름을 이용하여 B-TID를 생성한다.
⑤ UE와 BSF는 CK와 IK를 이용하여 새로운 Ks를 생성하게 된다.

5.2.3. Bootstrapping Usage Procedure

Bootstrapping 사용과정은 키 일치 과정이다.
① UE는 NAF에 B-TID를 가지고 응용 요청 메시지를 전송한다.
② NAF는 BSF에 B-TID에 대응키를 전송받기 위해 B-TID, NAF-ID를 포함한 인증 메시지를 전송한다.
③ BSF는 주어진 호스트 이름을 사용하여 NAF가 권한 여부를 확인 후 B-TID가 가진 키를 찾는다.
④ BSF는 Bootstrapping 시간을 가진 Ks_NAF와 NAF의 유효 시간을 보낸 후 Ks_NAF에 NAF는 BSF에 특정정보를 요청한다. 하지만 B-TID에 대응키가 없으면 BSF는 NAF에게 UE와 Bootstrapping 과정을 요청한다.

5.3. 전자ID지갑 인증 메커니즘의 안정성 분석

5.3.1. 수동적인 공격 및 적극적인 공격자의 반송 공격

공격자는 메시지를 도청하여 UE_{Send}와 BSF_{Send}를 획득하거나 중간에서 되돌려 보내어 잘못된 세션키를 유도하려 할 수 있다. 그러나 UE는 $AK=f5_K(RAND)$, $SQN_{HE}=(SQN_{HE}\oplus AK)\oplus AK$, $XMAC=f1_K(SQN_{HE} \| RAND \| AMF)$를 계산 후 $XMAC \doteq MAC$, $SQN_{MS} \doteq SQN_{HE}$를 확인하여 인증하므로 공격자가 이 값들을 획득한다 하더라도 nonce와 사용자와 HSS 사이에 미리 공유된 K를 알 수 없으므로 UE_{Rcv}와 BSF_{Rcv}를 계산할 수 없다.

5.3.2. 적극적인 공격자의 수정 공격 및 재전송 공격

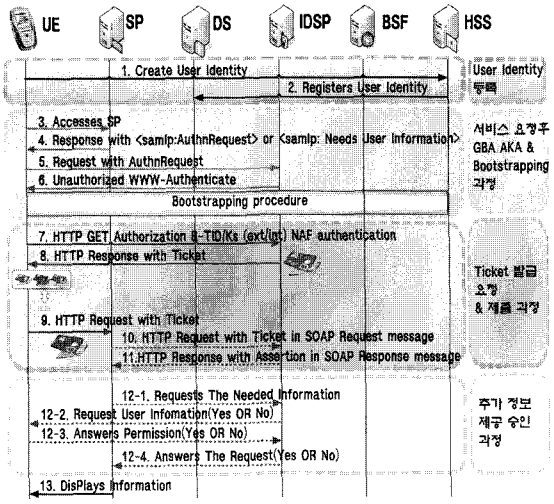
공격자가 UE와 BSF 중간에서 수정하여 상대에게 전송한다면, 이 위조된 값들은 UE 와 BSF에 의해 UE_{Rcv}와 BSF_{Rcv}를 생성하는데 각각 사용되게 되며 재전송 공격은 이전 세션의 전송 메시지들을 저장해 두었다가 이후 세션들에 이용하는 공격이다. 그러나 UE와 BSF는 매 세션 마다 새로운 임의의 난수를 생성하여 사용하여 UE_{Rcv}, BSF_{Rcv}를 계산하기 때문에 검증 단계에서 확인 가능하다.

5.3.3. 합법적인 참여자로 위장 및 메시지 재전송 공격

공격자가 합법적인 참여자로 위장하여 정상적인 방법으로 다른 합법적인 참여자와 세션키를 공유하려고 할 수 있다. 그러나 공격자는 미리 공유된 K를 계산할 수 없으며 NAF로부터 전송받은 UE_{Send}=Ks_NAF ‖ Bootstrap time ‖ Key lifetime을 공격자가 메시지를 재전송해도 Bootstrap time로 인해 freshness를 보장하게 되므로 공격은 성공할 수 없다.

5.4. 모바일 환경에서의 전자ID지갑 메커니즘 Flow

모바일 환경에서의 전자ID지갑 메커니즘은 [그림 5]와 같이 User Identity 등록과정, GBA의 AKA과정 후 Bootstrapping과정, Ticket 발급요청 및 제출과정, 추가정보의 제공 승인과정으로 나누어진다.



[그림 5] Message flow Digital ID Wallet usage of GBA

5.4.1. User Identity 등록

GBA사용자가 특정 서비스를 요청하기 전에 사용자가 통신 사업자의 AS에 영구적인 가입자 데이터를 등록한 후 IDSP에 사용자가 Ticket의 발급을 요청 시 필요한 정보를 보관하게 된다. 그 후 사용자 데이터가 보관된 IDSP의 주소를 DS(Discovery Service)에게 등록함으로써 사용자가 다른 신뢰영역에 위치한 SP의 인터넷 서비스를 요청 시 DS를 통해 사용자의 데이터가 저장된 IDSP를 찾을 수 있다.

5.4.2. GBA의 AKA과정과 Bootstrapping과정

사용자가 특정 서비스를 요청할 경우 사용자와 인증서버 간에 세션키를 동의하는 과정이다.

만약 UE와 BSF사이에서 Bootstrap절차가 실행되었다면 [그림 5]의 ⑤번 과정과 ⑥번 과정은 실행되지 않는다. UE가 IDSP에 의해서 인증되지 않았다면 인증과정을 거쳐야 하며 IDSP는 UE에 유효한 Key가 없거나 Key의 freshness가 만족하지 않으면 BSF와 Bootstrapping을 통해 세션키를 생성한다.

5.4.3. Ticket 발급요청 및 제출과정

SP가 요청한 사용자 정보 속성이 USIM에 없는 경우는 SP가 요청한 사용자 정보 속성을 IDSP에게 전송하여 Ticket의 발급을 요청하고 IDSP는 UE가 전송한 정보에 관한 인증정보가 없다면 BSF에게 인증정보를 BSF에게 요청하고 인증정보가 포함되어 있으면 Ticket를 발행한다. UE는 발급 받은 Ticket을 저장한 후 SP에게 전송하면 SP가 IDSP에게 Assertion을 요청한다. IDSP는 SP로부터 전송 받은 Ticket이 자신에 의해서 발행 여부를 확인 후 SP에게 Assertion을 전송하면 사용자는 해당서비스를 이용한다. 이 때 전송 받은 Ticket의 정보 속성은 USIM에 저장된다.

SP가 요청한 사용자 정보 속성의 일부가 기존에 발급 받은 Ticket에 있는 경우는 일부 정보 속성을 IDSP에게 요청하여 전달받아 기존의 Ticket에 저장하여 사용자가 새로운 Ticket을 발급한다.

SP가 요청한 사용자 정보 속성이 USIM에 있는 경우는 그 정보를 이용하여 사용자가 Ticket을 발행한다. 이 경우는 [그림 5]의 ⑦번 과정과 ⑧번 과정을 생략하고 Ticket을 생성 후 ⑨번 과정에서 전송한다. 만약 SP와 IDSP가 단일 신뢰 영역 안에 존재하는 경우는 ⑩번과정과 ⑪번 과정은 생략된다.

5.4.4. 추가 정보의 제공 승인과정

사용자가 Ticket을 전송하여 서비스 이용 중에 SP가 추가 정보의 제공을 요청할 경우 새로운 Ticket을 사용하지 않고 사용자와 IDSP간의 질의를 통해 사용자가 해당 정보의 사용을 정보의 제공 여부를 사용자가 선택하여 승인하면 IDSP가 SP에 해당 정보를 제공하여 서비스를 이용하는 과정이다.

모바일 환경에서의 전자ID지갑 메커니즘 Flow는 [그림 5]와 같다.

① UE->HSS : 사용자는 HSS에 영구적인 가입자 데이터를 등록한다.

② HSS->DS : HSS는 IDSP에 등록 후 DS에 사용자의 정보를 가진 IDSP의 주소를 등록한다.

③ UE->SP : GBA 기반의 인증 사항을 포함한 HTTP Request를 전송하여 접속한다.

④ SP->UE : SP는 IDSP의 URL과 사용자 정보 속성을 전송하고 UE는 IDSP의 주소를 획득한다.

⑤ UE->IDSP : SP로부터 전송 받은 IDSP의 URL을 통해 IDSP에 접속한다. UE는 SP에게 IDSP로부터 인증 확인 Token을 생성하기 위해서 전송한다.

⑥ IDSP->UE : UE가 IDSP에 의해서 인증되지 않았다면 인증 과정을 거치며 IDSP는 UE에 NAF에 Key가 유효하지 않거나 freshness가 만족하지 않으면 BSF와 Bootstrapping을 통해 세션키를 생성한다.

⑦ UE->IDSP : B-TID와 패스워드로 Ks_(ext/int)_NAF 및 LAP와 관련된 사용자 data와 함께 UE가 요청한 서비스에 필요한 사용자 정보 속성을 IDSP에게 전송하고 Ticket을 요청한다. 메시지를 전송 받은 IDSP는 UE가 전송한 정보에 관한 인증정보가 없다면 BSF에게 인증정보를 BSF에게 요청한다.

⑧ IDSP->UE : IDSP는 UE에게 Ticket과 SP로 Redirection 시키기 위한 SP의 URL을 전송한다.

⑨ UE->SP : UE는 메시지 Redirection을 위한 SP의 주소와 Ticket을 사용하여 SP에게 전송한다.

⑩ SP->IDSP : SP는 UE로부터 전송받은 Ticket을 IDSP/NAF에게 전송하고 Assertion을 요청한다.

⑪ IDSP->SP : IDSP는 SP로부터 전송 받은 Ticket을 IDSP/NAF에 의해서 발행 여부를 확인 후 상태코드나 요청된 <saml:Assertion>를 SOAP 응답 메시지와 <samlp:Response>를 SP에게 전송한다.

⑫-1 SP->IDSP : 서비스 이용 시 SP가 추가 정보가 필요할 때 사용자의 정보를 요청한다.

⑫-3 IDSP->UE : IDSP는 UE에게 SP가 요청한 정보를 제공할 것인지 질의한다.

⑫-3 UE->IDSP : UE는 정보 제공 여부를 전송한다.

⑫-4 IDSP->SP : 사용자가 정보 제공을 승인하면 SP에게 정보를 제공한다.

⑬ SP->UE : SP는 Assertion의 IDSP/NAF의 서명을 검증하고 UE에게 메시지를 전송한다.

Ⅵ. 결 론

앞으로 다가올 4G 환경에서는 모바일 단말 사용의 증가로 인해 모바일 환경에서의 서비스 이용이 급격하게 증가할 것이다. 따라서 4G 환경에서 ID 연동 모델의 확장하기 위한 메커니즘으로 USIM에 전자ID지갑 애플리케이션을 탑재하여 GBA의 AKA과정을 통한 Bootstrapping과정 후 세션키를 공유해서 사용자가 SP가 요구한 속성을 IDSP에 전송하여 Ticket의 발급을 요청한다. 또한 IDSP로부터 발급 받은 Ticket 정보를 USIM에 저장하여 사용자 스스로가 IDSP가 되어 Ticket을 전자ID지갑에 저장하고 관리하는 전자ID지갑 메커니즘을 살펴보았다.

따라서 기존에 유선환경에서 이루어지는 사업자 중심의 ID 관리 시스템 위주가 아니라 모바일 환경에서 사용자가 이동 중에서도 언제 어디서나 사용자가 필요한 시점에 무선 인터넷 서비스를 이용하고자 할 때 전자ID지갑에서 USIM카드에 다양한 저장된 다양한 정보를 이용하여 사용자가 Tickets를 발급하여 서비스를 제공받음으로써 언제 어디서나 사용자가 개인정보의 흐름을 통제할 수 있다.

향후 연구계획으로는 앞으로 다가올 4G 환경에서 USIM의 저장용량의 확대 및 다양한 서비스를 제공할 수 있는 전자ID지갑의 설계가 필요하며, 4G 환경의 유무선 통합 환경에서 유무선 공통으로 사용할 수 있는 Java기반의 전자ID지갑 모듈의 연구와 개발이 필요할 것이다.

참고문헌

[1] "Liberty Alliance Project : Introducion to the Liberty Alliance Identity Architecture," 2003

[2] ISO/IEC JTC1/SC27 WG5 N4721, A Framework for Identity Management, 2005.

[3] WWRF, http://www.wireless-worldresearch.org

[4] 3GPP TR 33.920 v.7.2.0. SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature, Release 7, June 2007.

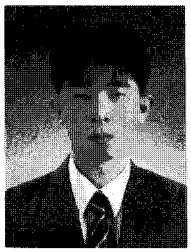
[5] J. Bigun, "Multi-modal Person Authentication," Face recognition, Sringer-Verlag, pp. 26-50, 1997.

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

[7] 3GPP TR 33.919 v.7.2.0. 3G Security; Generic Authentication Architecture (GAA); System description, Release 7, March 2007.

[8] 3GPP TR 33.980 v.7.5.0. Liberty Alliance and 3GPP security interworking; Interworking of ID-FF, ID-WSF and GAA, Release 7, June 2007.

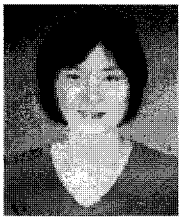
〈著者紹介〉



송 동 호 (Dongho Song) 정회원

2006년 3월~현재 : 고려대학교 정보경영보호대학원 석사과정

<관심분야> 정보보호, Digital ID, 무선통신



임 선 희 (Sun Hee Lim) 정회원

1999년 2월 : 고려대학교 컴퓨터 학과 졸업

2005년 2월 : 고려대학교 정보보호대학원 석사

2005년 3월~현재 : 고려대학교 정보보호대학원 박사과정

<관심분야> 무선통신, 정보보호

이 옥 연 (Okyeon Yi) 정회원

1988년 2월 : 고려대학교 수학과 졸업

1990년 2월 : 고려대학교 이학석사

1996년 8월 : Univ. of Kentucky Ph.D.

1999년~2001년 : ETRI 선임연구원

2001~현재 : 국민대학교 수학과 조교수

<관심분야> 이동통신 정보보호, 컴퓨터 보안

임 종 인 (Okyeon Yi) 정회원

1980년 2월 : 고려대학교 수학과 졸업

1982년 2월 : 고려대학교 수학과 석사

1986년 8월 : 고려대학교 수학과 박사

1986년~1999년 : 고려대학교 수학과 교수

2000년~현재 : 고려대학교 정보보호 대학원 원장

<관심분야> 정보보호, 암호이론, 프로토콜, 정보이론