모바일 서비스를 위한 ID 공유 게이트웨이 기술

Digital Identity Interchange Gateway Technology for Mobile Services

조상래 (S.R. Cho) 인증기술연구팀 선임연구원
진승헌 (S.H. Jin) 인증기술연구팀 팀장

목 차

* 본 연구는 지식경제부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행하였음.[2007-S-601-03, 자기통제 강화형 전자 ID 지갑 시스템 개발]

본 고에서는 사용자가 모바일 환경에서 자신의 ID 정보를 효율적으로 공유하기 위한 ID 공유 게이트웨이 기술에 대해 기술하고 있다. ID 공유 게이트웨이는 모바일 환경에서 ID 정보 공유시 문제가 될 수 있는 프로토콜 변환 및 메시지 보안 기능을 전담하여 처리하는 것이 목적이다. 이러한 게이트웨이 기술은 향후 ID 공유 기술을 이용한 다양한 융복합 서비스를 모바일 웹 응용서비스에서도 가능하게 한다는 의미를 가지고 있다.

Ⅰ. 서론

현재의 인터넷 환경은 사이트마다 각기 다른 인증 방법과 개인정보 입력방법으로 인해 피싱(phishing) 공격 등에 의한 개인정보 유출이 심각하여 편의성과 보안성 측면에서 취약함을 보인다[1]. 그리고 서비스 제공을 위해 필요 이상의 개인정보를 요구하고 사이트 가입 시에 포괄적인 약관동의만으로 개인정보 통제에 대한 모든 권리가 사이트로 이양되어 개인정보에 대한 사용자의 자기 통제권이 부재하게 된다는 문제점이 있다. 따라서 직관적이고 일관성 있는 인증 방법을 제공하고 개인정보에 대한 자기통제권을 강화하여 개인정보의 오남용으로 인한 개인정보 침해를 줄일 수 있는 대책이 요구된다.

정보의 공유 및 사용자의 참여 그리고 개방을 통한 고부가가치 서비스를 제공하는 웹 2.0은 2007년 말까지 대기업의 30% 이상이 웹 2.0 관련 사업을 시작할 것이고 콘텐트 및 기술을 하나로 컨버전스하는 매시업 서비스가 빠른 성장을 보일 것으로 예상되나, 개인정보의 사용과 관련된 프라이버시 침해와 기존 웹 환경의 보안 취약점이 여전히 문제로 남아 있다. 그리고 개인정보 공유가 늘어나면서 프라이버시 침해에 대한 우려 또한 여전히 존재하고 있다. 따라서 인터넷에 계속적으로 축적된 개인정보들을 보호하고 프라이버시에 대한 보호대책이 요구된다.

위에서 언급된 문제를 해결하기 위하여 기존의 Identity 관리 기술을 적용하기에는 사용자 입장에서 다음과 같은 한계가 있다[2]-[4]. 사용자들은 여전히 여러 사이트에서 발급된 많은 크리덴셜들을 관리해야 하는 불편을 겪어야만 한다. 또한 각 사이트마다 프라이버시 정책(policy)이 상이하고 사용자가 그러한 정책을 이해하고 인식하기 어려우며, 사용자 자신이 자기정보가 어떻게 유통되고 이용되는지에 대한 통제권을 보장받지 못한다. 사업자 입장에서는 다음과 같은 한계가 있다. 각 도메인마다 보안 및 프라이버시 정책이 서로 상이하여 이미 구축된 시스템 및 서비스들을 통합하는 데 많은 시간과 비용이 소요되고 공유하려는 도메인이 많은 경우 그 복잡성이 기하급수적으로 증가하여 사업자의 의도대로 Identity 정보를 공유하기 어려운 문제가 발생할 수 있다. 또한 사업자들마다 존재하는 서비스들을 연계하기 위해서는 공통의 Identity 식별과 표현양식이 필요하나, 이러한 필요성을 충족시켜 줄만한 장치가 아직 마련되어 있지 않다. 그리고 무엇보다도 사업자들간의 이해관계가 서로 상충하여 연합을 통한 서비스를 제공하기가 쉽지 않다는 문제가 있다[5],[6].

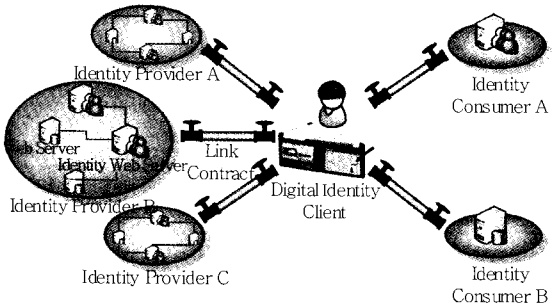
또한 점점 더 모바일 컴퓨팅 환경이 널리 사용됨에 따라 기존의 PC 환경보다 사용자는 웹 서비스를 이용하기 위해 더욱 열악한 환경에 놓여지게 된다. 모바일 디바이스의 작은 디스플레이는 사용자에게 보여지는 정보의 양을 제한하고 입력의 불편함은 로그인시 필요한 인증을 하기가 쉽지 않다. 이 경우 간편하고 편리한 크리덴셜 관리와 인증 기능은 모바일 환경의 활성화에는 필수 불가결하다.

모바일 환경에서 사용되는 사용자의 모바일 디바이스는 GPS, 사진, 일정 등과 같은 사용자의 아이덴티티 정보를 생성하는 다양한 응용 프로그램이 존재한다. 하지만 현재의 모바일 환경은 이러한 정보들이 서비스 제공자와 자유롭게 공유될 수 있는 환경을 제공하고 있지는 못하다. 이러한 사용자 생성 아이덴티티 정보가 다양한 웹 응용 사이트에 공유될 수 있으면 좀 더 편리하고 유용한 서비스를 사용자에게 제공할 수 있다.

본 고의 구성은 다음과 같다. Ⅱ장에서 디지털 ID 공유 모델에 대하여 기술한다. Ⅲ장은 디지털 ID 공유 프레임워크를 정의하며, Ⅳ장에서는 프레임워크를 기반으로 개발된 디지털 ID 공유 시스템을 설명하고 있다. Ⅴ장에서는 모바일 환경에서 ID 공유 서비스를 제공하기 위한 ID 공유 게이트웨이 기술에 대하여 설명한다. 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 디지털 ID 공유 모델

(그림 1)은 사용자의 디지털 ID 정보를 공유하기 위해 필요한 엔티티들을 도식화한 개념적인 모델이다.



(그림 1) 디지털 ID 공유 개념 모델

1. Identity Web Server

Identity Web Server(IDWS)는 엔티티에게 사용자의 ID 정보를 제공하는 주 서버이다. IDWS가 주로 ID 정보를 제공하는 역할을 하면 Identity Provider(IdP)이고 그렇지 않으면 Identity Consumer (IdC)가 된다. 웹서버는 사용자에게 서비스를 제공하기 위해 필요한 ID 정보를 IDWS에게 요청한다.

2. Digital Identity Client

Digital Identity Client(DIC) 또는 전자 ID 지갑은 사용자에게 인증 및 크리덴셜 관리, ID 공유, 프라이버시 보호 기능을 제공하는 프로그램이다. DIC가 IdP 또는 IdC와 ID 정보를 공유할 경우에는 각 도메인에 있는 IDWS와 링크를 설정한다. (그림 1)에 이 링크는 파이프로 표현되어 있다. 링크가 설정되면 DIC는 ID 정보 공유시 프라이버시 보호 서비스를 제공하기 위해 IDWS와 디지털 계약을 맺는다. 이렇게 되면 사용자의 ID 정보는 공유시 항상 DIC를 통하여 이루어지고 이러한 흐름은 사용자에게 자신의 정보를 언제나 통제할 수 있는 권한을 행사할 수 있다. 모바일 환경에서는 기존의 전자 ID 지갑 기능에 모바일에 특화된 서비스를 제공하기 위한 모바일 전자 ID 지갑을 제공할 수 있다.

3. Identity Provider

Identity Provider(IdP)는 사용자의 ID 정보를 관리하고 DIC가 요청할 때 제공하는 엔티티이다. 엔티티의 역할은 사용자의 ID 정보를 제공하느냐 또는 소비하느냐에 따라 제공자 또는 소비자가 될 수 있다. 하지만 경우에 따라서는 두 가지 역할을 함께 수행할 수도 있다.

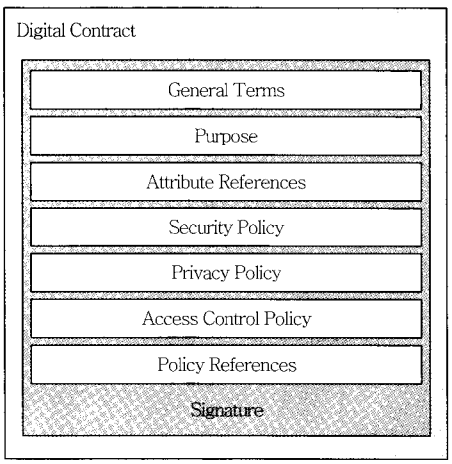
4. Identity Consumer

Identity Consumer(IdC)는 서비스 제공에 필요한 사용자의 ID 정보를 DIC에 요청하는 엔티티를 의미한다. IdC는 사용자가 제공하는 ID 정보를 이용하여 다양한 부가서비스를 사용자에게 제공하는 서비스 제공자를 의미한다.

5. 디지털 계약

IdP와 IdC 사이의 ID 정보의 공유는 반드시 DIC를 거쳐가야 한다. 이러한 흐름은 사용자에게 자신의 ID 정보를 제어할 수 있는 자기정보 통제권에 대한 기회를 제공한다. 디지털 계약(digital contract)은 중요한 핵심 요소 기술로 ID 정보 공유에 있어 사용자에게 아주 세밀한 제어를 제공할 수 있다. (그림 2)는 이러한 디지털 계약의 구조를 보여주고 있다.

디지털 계약에서 정의할 수 있는 제어의 종류에는 ID 공유 관계를 중재할 수 있는 다양한 정책들을 포함하고 있다. 이러한 디지털 계약은 법 또는 정책에 따라 요구가 될 수도 있고 경우에 따라서는 필요



(그림 2) 디지털 계약의 구조

가 없을 수도 있다. 디지털 계약은 공유되는 ID의 흐름 또는 보유를 제어하기 위해서만 필요하다. 디지털 계약은 실세계의 계약서와 같이 융통성 및 확장성을 보유하고 있다.

(1) General Terms: 버전, 계약서 동의 날짜, 계약서 유효기간, 그리고 사용자 알림 등을 포함하고 있음(필수 사항)
(2) Purpose: 사용자 ID 정보의 사용 목적(필수 사항)
(3) Attribute References: 사용자의 ID 중 어느 속성을 참조하는지를 설정(필수 사항)
(4) Security Policy: 상호 인증 및 보안에 대한 정책을 설정(필수 사항)
(5) Privacy Policy: ID 정보의 보존 기간을 포함하는 프라이버시 관련 정책을 설정(선택 사항)
(6) Access Control Policy: 현재 사용하고 있는 다양한 접근제어 정책을 설정(선택 사항)
(7) Policy References: 다른 곳에 정의된 정책(예, 인증서 정책)을 참조할 때 사용(선택 사항)
(8) Signature: 위 항목들에 대한 서명. 서명은 계약서에 동의하는 최대 두 엔티티가 하며 계약서의 서명은 유효성과 무결성을 보장(필수 사항)

Ⅲ. 디지털 ID 공유 프레임워크

1. 디자인 원칙

프레임워크는 다양한 컴퓨터 환경에서 효율적인 사용자 개인정보 공유를 위하여 다음과 같은 디자인 원칙을 가지고 있다.

• Independent

프레임워크는 특정 응용 또는 네트워크에 종속되어 운영되지 않는다. 프레임워크는 다양한 환경에 적용되어 운영될 수 있게 디자인 되어야 한다.

• Pluggable

모바일 또는 유비쿼터스 컴퓨팅 환경에서 사용자는 다양한 디바이스를 소유하고 사용하게 된다. 이러한 경우 사용자가 필요한 것은 특정 디바이스에서 사용자를 식별하고 사용자의 ID를 공유할 수 있는 정보가 필요한데 이러한 정보는 어느 디바이스에도 적용될 수 있는 안전하고 정형화된 구조로 디자인 되어야 한다.

• Flexible

프레임워크 자체는 소형 모바일 디바이스에서부터 대형 워크스테이션에 이르기까지 다양한 환경에 적용할 수 있게 디자인 되어야 한다. 이것은 프레임워크가 어떤 환경에도 적용될 수 있게 형상화가 잘 되어야 한다는 것을 의미한다.

• Scalable

프레임워크는 소형 도메인에서부터 도메인들간의 개인정보 공유에도 사용될 수 있게 새로운 통신 또는 컴퓨팅 부담을 주지 않고 확장성을 보장해야 한다.

• Interoperable

프레임워크는 기존에 존재하는 ID 관리 시스템들과 상호운영성을 제공할 수 있는 기능을 제공해야 한다.

2. 프레임워크 구성요소

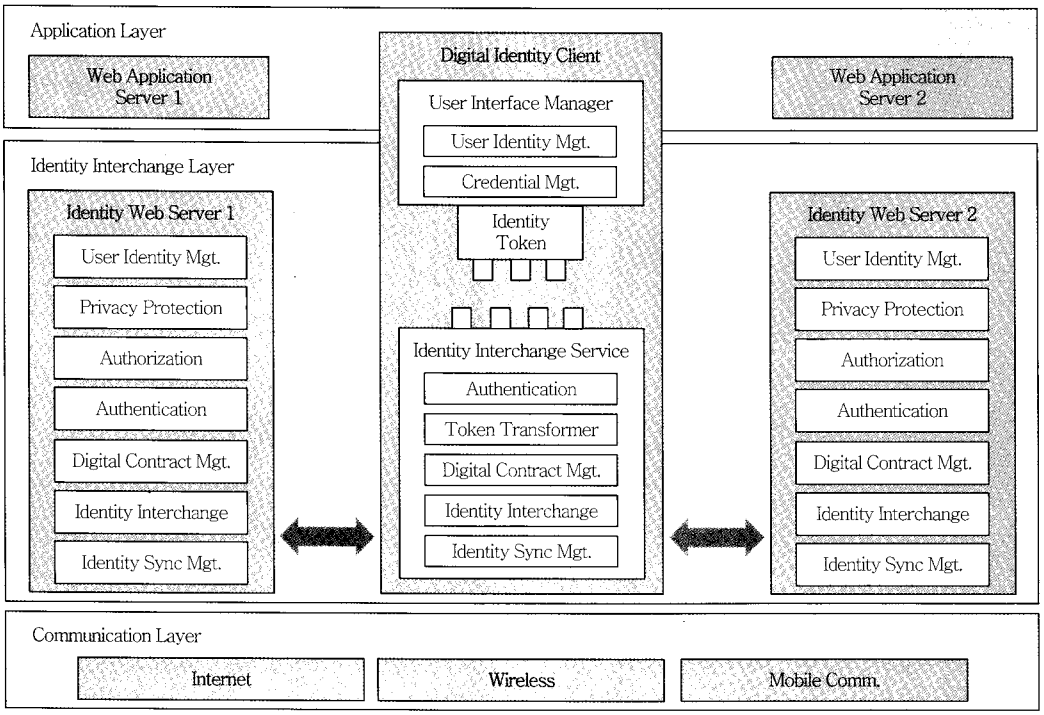
(그림 3)은 이러한 디자인 원칙을 만족하는 ID 공유 프레임워크의 기능적인 구성요소를 나타내고 있다.

DIC는 본 프레임워크에서 가장 핵심 컴포넌트이다. DIC는 모든 사용자의 IdP와 IdC를 연결하여 ID 공유를 가능하게 하는 열쇠이다. 사용자는 사전에 연결되어 있는 링크를 이용하여 언제든지 자신의 ID 정보를 추출하고 갱신할 수 있다.

DIC는 세 개의 파트로 구성이 되어 있다: User Interface Manager, Identity Interchange Service and Identity Token.

• User Interface Manager

User Interface Manager는 사용자의 ID와 크리덴셜 정보를 표현하는 화면 정보로 구성된다. 이 컴포넌트는 다양한 서비스에서 사용자의 ID를 공유하



(그림 3) 디지털 ID 공유 프레임워크

거나 웹응용 서버에 로그인할 때 사용된다. 본 프레임워크에서는 사용자의 ID와 인증 크리덴셜과 관련하여 어떤 정보를 관리해야 하는지만 기술한다.

• Identity Interchange Service

Identity Interchange Service는 ID 공유와 동기화를 책임지는 서비스 부분이다. 통신 네트워크의 환경과 상관없이 이 서비스는 응용 환경에 맞게 수정되어 사용될 수가 있어야 한다. 예를 들면, 이 서비스의 모듈이 핸드폰에 개발될 때와 사용자의 개인 컴퓨터에 운영될 때는 개발 사양이 많이 다를 것이다.

• Identity Token

Identity Token은 디지털 ID의 데이터 모델이다. 본 토큰은 DIC에 끼워지면 User Interface Manager를 Identity Interchange Service와 연결하여 DIC가 기능을 수행할 준비가 된다. 토큰의 그래픽 표현은 User Interface Manager가 연결되면 제공된다. 만약 사용자의 컴퓨팅 환경이 개인 컴퓨터에서 모바일 폰으로 변경되면 사용자는 단지 Identity Token만을 가지고 모바일 폰에 장착하면 된다. Identity Token은 스마트 카드, USB 토큰과 별도의 하드웨어를 이용하여 이동할 수 있다.

• 사용자 ID 관리(User Identity Management)

사용자 ID는 프로파일과 공유 ID로 구분한다. 프로파일은 일반적으로 사이트에 가입할 때 제공되는 사용자의 정보이고, 공유 ID는 사용자와 사이트간에 생성된 정보를 공유하기 위한 규약, 데이터 등을 의미한다.

클라이언트의 경우에는 사용자가 자신의 정보를 입력하여 프로파일을 생성하고 카드 형태로 관리된다. 사용자는 사이트에 가입할 때 자신의 정보를 직접 입력하지 않고 전자 ID 지갑의 프로파일 카드를 이용하여 정보를 제공할 수 있다. 사용자 프로파일은 전자 ID 지갑에서 수정이 가능하다. 사용자가 사이트를 이용하며 생성한 ID가 공유를 필요로 하게 되면 전자 ID 지갑에서는 이 정보를 공유 ID로 관리한다. 공유 ID는 공유되는 ID의 항목 그리고 공유시 준수해야 할 계약 사항을 나타내는 공유 정책 등을 포함한다.

• 통합 크리덴셜 관리(Credential Management)

통합 크리덴셜 관리는 인증 크리덴셜 관리를 의미한다. 인증 크리덴셜은 패스워드, PKI, 생체로 구분되고, 이와 관련된 기능은 인증 크리덴셜 조회, 수정, 삭제, 생성 등이 있다.

인증 크리덴셜은 사용자가 전자 ID 지갑을 이용하여 사이트에 인증시 제출되는 패스워드, PKI, 생체 정보 등을 말한다. 전자 ID 지갑에서는 사이트 카드 형태로 이 정보들을 관리한다. 패스워드, PKI, 생체로 카테고리를 구분하고, 사이트 가입시 제공된 크리덴셜을 기록하여 인증 크리덴셜 카드와 사이트 카드를 연결하여 둔다. 사이트에 로그인할 때, 사용자는 전자 ID 지갑을 통하여 인증 크리덴셜 카드를 선택함으로써 인증 작업을 수행할 수 있다.

• 프라이버시 보호(Privacy Protection)

사용자의 ID 공유시 발생할 수 있는 프라이버시 관련 문제를 해결하는 기능을 제공한다. IdP는 사용자가 동의하는 모든 내용을 프라이버시 보호 기능을 사용하여 관리하고 필요할 때 사용한다. 또한 link contract와 연계하여 다양한 프라이버시 보호 정책을 실행하는 서비스를 제공할 수도 있다.

• 인가(Authorization)

인가 서비스는 사용자의 권한을 확인하여 인가 결정을 내리고 그 결정에 따라 사용자의 시스템에 대한 접근을 제어하는 것을 의미한다. 이 서비스는 선택적으로 적용될 수 있으며 현재 제공되는 다양한 접근제어 메커니즘을 사용할 수 있다.

• 범용 인증(Authentication)

범용 인증 기능은 사이트가 제공하는 여러 인증 방식을 지원하기 위한 전자 ID 지갑의 인증 기능이다. 범용 인증은 여러 인증 메커니즘을 지원한다. 사용자가 전자 ID 지갑을 이용하여 사이트에 가입을 할 때, 향후 사용될 인증 메커니즘을 협상한다. 사이트가 수용할 수 있는 인증 메커니즘 목록을 전자 ID 지갑으로 전송하고, 사용자는 전자 ID 지갑을 통하여 원하는 메커니즘을 선택한다. 범용 인증은 사이트 로그인 또는 사용자가 사이트를 이용하며 높은 수준의 보안을 요구하는 서비스를 이용하는 경우에 사용될 수 있다. 또한 사이트에 따라 two-factor 인증을 지원할 수 있다. 서버의 경우, 인증은 공유시각 객체를 인증하는 공유 인증을 의미한다.

• 토큰 변환기(Token Transformer)

이 컴포넌트는 다른 ID 관리 시스템과의 상호운용성을 제공한다. 기본적으로 대부분의 ID 관리 시스템들은 보안정보나 사용자의 ID를 교환하기 위해 토큰을 사용하는데 토큰 변환기는 중간에서 전자 ID 지갑으로 들어오고 나가는 모든 토큰들을 전자 ID 지갑이 이해할 수 있는 포맷으로 변화하는 서비스를 제공한다.

• ID 공유(Identity Interchange)

가장 핵심적인 컴포넌트로 ID 공유 기능은 전자 ID 지갑과 사이트 간에 Identity 정보를 공유하는 메커니즘을 제공한다. ID 공유는 전자 ID 지갑과 ID 정보를 제공하는 사이트인 IdP 간에 또는 전자 ID 지갑과 ID 정보를 사용하는 사이트인 IdC 간에 이루어진다. ID 정보는 전자 ID 지갑에서 공유 ID 형태로 관리된다.

• Digital Contract 관리(Digital Contract Manager)

IdP 또는 IdC와 전자 ID 지갑 간에 사용자 ID 정보에 대한 공유가 설정되며, 공유되는 정보에 대한 인증, 접근 제어, 프라이버시 보호 등에 대한 규약을 담은 link contract를 생성하고 전자서명하며, link contract의 생명주기를 관리하는 기능을 제공한다. 사용자의 ID 정보를 공유할 때 항상 link contract를 조회하여 사용자가 미리 설정해 놓은 정책에 부합하는지를 판단할 수 있다. 따라서 전자 ID 지갑에서는 link contract를 이용하여 개인정보의 흐름을 제어할 수 있다.

• 동기화 관리(Identity Synchronization Manager)

ID 동기화 기능은 사용자에 의해 변경된 사용자 ID 정보가 전자 ID 지갑을 통하여 IdP 또는 IdC에 반영되도록 하는 기능이다. 세부적인 기능으로 ID 동기화 설정, 실행 및 해지 기능 등이 있다.

Ⅳ. 디지털 ID 공유 시스템

(그림 4)는 디지털 ID 공유 프레임워크 개념을 기반으로 개발한 디지털 ID 공유 시스템이다.

디지털 ID 공유 시스템은 전자 ID 지갑과 ID 공유서버로 구성되어 있는 Client-Server 형태의 시스템이다. 그림에서 웹 응용 서버는 사용자에게 다양한 동적인 웹 서비스를 제공하기 위해 사용되는데 ID 공유 서버는 웹 응용 서버가 필요로 하는 사용자의 아이덴티티 정보를 제공하기 위해 사용된다. 전자 ID 지갑은 웹 응용 서버와 ID 공유 서버 간의 상호 작용을 통하여 사용자의 아이덴티티 정보를 주고받는다. 이러한 구성은 ID 공유 레이어를 별도로 두어 위로는 응용시스템과 아래로는 통신 네트워크에 독립적으로 운영이 가능하기 때문에 보다 융통성이 있고 확장 가능하며 상호호환성을 보장해주는 시스템 구성이 가능하다.

1. 전자 ID 지갑

전자 ID 지갑은 독립적으로 운영이 가능하지만 대부분의 경우 웹 브라우저의 플러그인 형태로 작동한다. 사용자가 특정 웹 사이트에 가입, 인증하거나 자신의 아이덴티티 정보를 제공할 때 웹 브라우저를 통하여 전자 ID 지갑 플러그인을 호출한다. 전자 ID 지갑의 기능은 크게 웹 사이트 가입 지원 기능과 가입 후 사이트 방문시 필요한 인증을 지원하는 기능이 하나이고 다른 하나는 분산된 자신의 아이덴티티 정보를 IdP로부터 가져와 IdC에 제공하는 ID 공유 지원 기능이다.

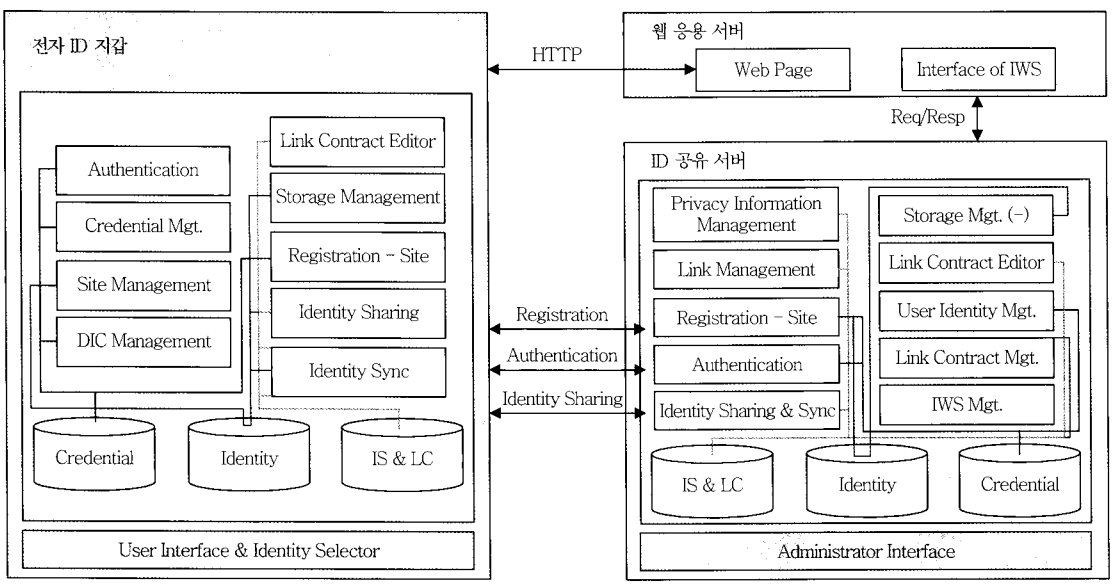
2. ID 공유 서버

ID 공유 서버는 전자 ID 지갑과 웹 응용 서버에 사용자의 아이덴티티 정보를 제공하는 것을 목적으로 하고 있다. ID 공유 서버의 개발은 웹 응용 프로그램 형태로 개발되어 필요할 경우 웹 응용 서버와 하나 또는 독립적으로 운영이 가능하다.

ID 공유 서버는 link 및 link contract를 관리하고 필요시 사용자의 아이덴티티 정보를 요청 또는 제공하는 공유 기능을 수행한다. 또한 필요한 정보의 동기화 기능도 제공한다.

3. 웹 응용 서버

웹 응용 서버는 사용자에게 웹 서비스를 제공한



(그림 4) ID 공유 시스템 구조

다. 웹 서비스 제공시 사용자의 아이덴티티 정보가 필요하면 ID 공유 서버에게 요청한다. 현재 개발된 시스템은 기존의 웹 응용 서버에 추가 개발을 가능한 적게 필요하도록 설계되어 다양한 웹 응용 서버에 간편하게 적용될 수 있다.

V. ID 공유 게이트웨이

1. 필요성

기존의 ID 공유 서버를 모바일 환경에서 그대로 사용하기에는 다음과 같은 문제점이 있다.

- 프로토콜 경량화 - 현재 사용하는 공유 프로토콜은 다양하고 복잡한 경우를 고려하여 설계되어 모바일에서 사용하기에는 통신량을 과도하게 사용
- 보안 모듈 경량화 - 보안 모듈도 모바일 디바이스의 컴퓨팅 파워 사용과 처리 지연속도가 높은 문제

위 두 가지 문제를 해결하기 위해서는 공유 서버를 다시 개발해야 하는데 동일한 기능을 하는 두 가지 버전의 서버를 개발하는 것 보다는 탈 부착할 수 있는 ID 공유 게이트웨이 모듈을 개발하는 것이 타당하다고 판단된다.

2. 구조

ID 공유 게이트웨이의 구조는 (그림 5)와 같다. 기존의 ID 공유 서버 위에 ID 공유 게이트웨이 모듈을 탑재하여 모바일용 전자 ID 지갑에서 오는 모든 요청을 처리하게 구성된다.

게이트웨이의 구조는 하나의 ID 공유 서버가 ID 공유 게이트웨이 모듈을 장착하면 모바일용으로 사용할 수 있고 제거하면 바로 PC용 서버로 사용이 가능하게 디자인 된다.

전자 ID 지갑의 경우 모바일용은 모바일 디바이스에 맞추어 새로 개발이 필요하기 때문에 이때 ID 공유 게이트웨이 모듈을 탑재하면 된다.

3. 프로토콜 변환 기능

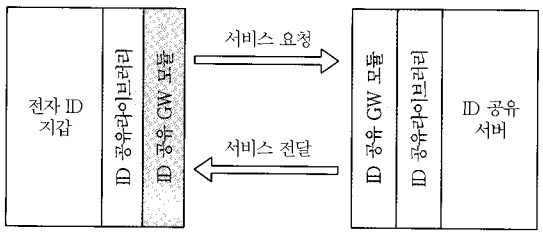
기존의 ID 공유 프로토콜은 모바일 환경을 지원하기 위해 변경이 불가피하다. 본 기능은 모바일 전자 ID 지갑에서 사용하는 수정된 ID 공유 프로토콜과 기존의 ID 공유 프로토콜간의 상호 호환성을 제공하기 위하여 변환 기능을 제공한다.

요청 프로토콜 변환 기능은 모바일 전자 ID 지갑에서 요청하는 모든 프로토콜을 기존의 ID 공유 프로토콜이 이해하고 IDWS가 처리할 수 있는 형태로 변환하는 기능을 제공한다.

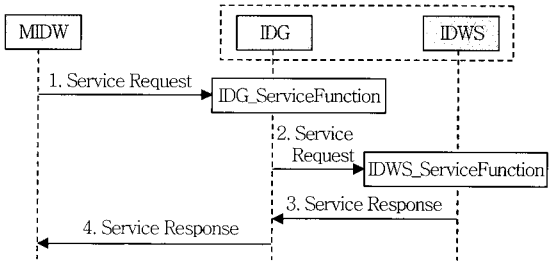
응답 프로토콜 변환 기능은 IDWS에서 응답하는 모든 기존의 ID 공유 프로토콜을 모바일 전자 ID 지갑이 이해하는 프로토콜 형태로 변환하는 기능을 제공한다.

요청 및 응답 프로토콜의 기능 흐름은 (그림 6)과 같다. 모바일 전자 ID 지갑은 ID 공유 게이트웨이에 서비스를 호출하여 서비스를 요청하면 서비스는 link 관리, link contract 관리 기능과 같은 서비스를 호출한다.

ID 공유 게이트웨이는 IDWS가 원하는 프로토콜 형태로 요청메시지를 변환한 후 IDWS의 서비스를



(그림 5) ID 공유 게이트웨이 구조



(그림 6) 요청 및 응답 기능 처리 흐름

호출한다. IDWS는 요청을 처리 후 결과를 응답메시지에 담아 ID 공유 게이트웨이에 반환한다.

ID 공유 게이트웨이는 IDWS에서 온 응답메시지를 검토한 후 모바일 전자 ID 지갑에 서비스 요청에 대한 결과를 반환한다.

4. Artifact 관리 기능

Artifact는 모바일 전자 ID 지갑이 IDWS에 제공한 사용자 Identity 정보에 대한 참조번호(reference number)이다. 모바일 응용 프로그램에서 artifact를 응용 서버에 제출하면, 응용 서버는 artifact를 이용하여 ID 공유 게이트웨이에서 사용자의 Identity 정보를 조회할 수 있다.

Artifact 생성 기능은 ID 공유 게이트웨이가 모바일 전자 ID 지갑에서 사용자의 특정 Identity 정보를 받으면 응답 시에 artifact를 생성하여 모바일 전자 ID 지갑에 반환하는 기능이다. ID 공유 게이트웨이는 생성한 artifact를 응용서버가 조회할 때까지 보관한다.

Artifact는 공유 및 동기화 시에만 생성되어 모바일 전자 ID 지갑에 전달된다. Artifact는 사용자의 공유된 Identity 정보를 응용서버에서 나중에 조회할 수 있는 기능을 제공한다.

(그림 7)에서 IDWS가 3번 흐름에서 공유 요청을 처리한 후 4번에서 응답 메시지를 ID 공유 게이트웨이에 전달하면 ID 공유 게이트웨이는 artifact를 생성한다. 생성된 artifact는 기본 응답메시지에 담겨 모바일 전자 ID 지갑에 전달한다.

Artifact 조회 기능은 ID 공유 게이트웨이에서 발급한 artifact에 대한 데이터를 요청하면 응답하는 기능이다. 응용서버에서는 모바일 응용 프로그램에서 제출한 artifact를 ID 공유 게이트웨이에 제출하면, ID 공유 게이트웨이는 참조하는 ID 정보를 조회하여 응용서버에 반환하고 저장소에서 artifact를 삭제한다.

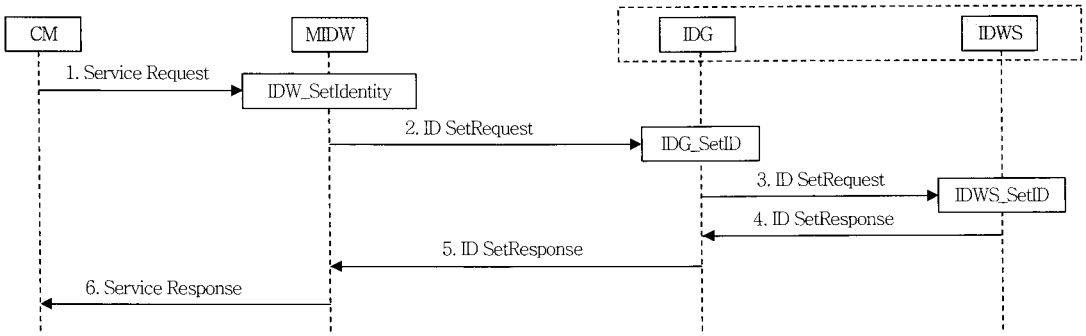
5. 메시지 보안 기능

메시지 보안 기능은 모바일 전자 ID 지갑에서 사용할 수 있는 전자서명 및 암호화 기능을 의미한다. ID 공유 게이트웨이에서는 그것을 처리하는 하는 기능을 제공한다.

전자서명 기능은 link contract 또는 프로토콜 메시지의 무결성을 보장하기 위해 사용되며 모바일 전자 ID 지갑 또는 IDWS에서 서명하면 다른 한쪽에서 서명을 검증하는 기능을 제공한다.

모바일 전자 ID 지갑은 자신의 비밀키로 프로토콜 요청 메시지에 서명하고 ID 공유 게이트웨이의 서비스를 호출한다. ID 공유 게이트웨이는 사용자가 보내온 요청 메시지에서 서명을 검증하고 문제가 없으면 보내온 요청 메시지에서 서명을 제거한 후에 IDWS로 보낸다. IDWS는 요청을 처리 후 결과를 응답메시지에 담아 ID 공유 게이트웨이에 반환한다.

ID 공유 게이트웨이는 IDWS에서 온 응답메시지를 검토한 후 서버의 비밀키로 서명을 한 후에 모바일 전자 ID 지갑에 서비스 요청에 대한 결과를 반환한다.



(그림 7) Artifact 관리 기능 흐름

암호화 기능은 모바일 전자 ID 지갑과 IDWS 간에 사용되는 기능으로 두 개체간 주고 받는 메시지의 기밀성을 보장하기 위해 암호화와 복호화 기능을 제공한다. 암호화 기능을 사용하기 위해서는 모바일 전자 ID 지갑은 사전에 암복호에 필요한 키를 ID 공유 게이트웨이와 공유하고 있어야 한다.

모바일 전자 ID 지갑은 ID 공유 게이트웨이와 공유하고 있는 암호화키로 프로토콜 요청 메시지를 암호화하여 ID 공유 게이트웨이에 전달한다.

ID 공유 게이트웨이는 사용자가 보내온 암호화 메시지를 공유하고 있는 암호화키로 복호화하여 변환한 후에 IDWS에 전달한다. IDWS는 요청을 처리 후 결과를 응답메시지에 담아 ID 공유 게이트웨이에 반환한다. ID 공유 게이트웨이는 IDWS에서 온 응답 메시지를 검토한 후 자신의 암호화키로 암호화한 후에 모바일 전자 ID 지갑에 서비스 요청에 대한 결과를 반환한다.

Ⅵ. 결론

본 고에서는 사용자가 모바일 환경에서 자신의 ID 정보를 효율적으로 공유하기 위한 ID 공유 프레임워크상의 ID 공유 게이트웨이 기술에 대하여 기술하고 있다. PC 환경보다 여러 가지 면에서 제약이 많은 모바일 환경에서 기존의 ID 공유 서버가 제공하는 기능을 제공하기 위해서는 ID 공유 게이트웨이가 가장 현실적인 대안이라고 생각한다.

이러한 ID 공유 게이트웨이에서 제공하는 기능들은 프로토콜 변환, 메시지 보안 및 artifact 관리 기능들이 있다. 이 기능들의 실제 처리 흐름을 보여주기 위해 본 고에서는 일반화된 세부 흐름도를 제시하여 각각의 기능들의 특징을 설명하였다. 처리 흐름에서도 나타나듯이 ID 공유 게이트웨이를 이용하면 실제 동작하는 ID 공유 서버와 독립적으로 모바일 ID 공유서비스의 구축이 가능하여 향후 다양한 모바일 응용서비스에 접목이 용이하고 기존의 웹 서비스와의 연계 시에도 호환성을 높일 수 있는 가능성을 제시하고 있다.

● 용 어 해 설 ●

Digital Identity Client: 사용자에게 인증 및 크리덴셜 관리, ID 공유 및 프라이버시 보호 서비스를 제공하는 클라이언트 프로그램

Identity Web Server: 클라이언트에 사용자의 크리덴셜 및 ID 공유 정보를 제공하는 서버

Digital Contract: ID 공유에 필요한 조건에 동의하는 두 엔티티가 서명한 디지털 형태로 이루어진 계약서

사용자: 최종사용자를 의미. 사용자는 클라이언트를 사용하는 사람 또는 가입자

약어 정리

CoT	Circle of Trust
DIC	Digital Identity Client
DIIF	Digital Identity Interchange Framework
IdC	Identity Consumer
IDG	Identity Gateway
IdM	Identity Management
IdP	Identity Provider
IDWS	Identity Web Server
SP	Service Provider
XML	eXtensible Markup Language

참 고 문 헌

[1] IDC, Worldwide Identity Theft Black Market 2006-2010 Forecast, 2006.
[2] Liberty Alliance Project, http://www.project-liberty.org/
[3] Microsoft, Introducing Windows CardSpace, http://msdn.microsoft.com/
[4] OpenID, http://openid.net/
[5] Security Assertion Markup Language(SAML) OASIS Standard Specification, Version 2.0, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
[6] Higgins Project, http://www.eclipse.org/higgins/