[정보보호] ITU-T SG17 속성수집 모델 표준 - 서비스 제공자 중심

개요

온라인상의 상거래는 현대생활에 없어는 안 되는 부분이 되었으며, 서비스 제공자들을 중심으로 계속적으로 진화를 거듭하고 있다. 이러한 진화의 하나로 인증(Authentication)과 인가(Authorization)의 진화는 서비스의 이용 편리성과 정보의 안전보장이라는 관점에서 계속적으로 진행되고 있는 과제에 속한다. 인증 및 인가에서 속성(Attribute)은 새로운 것이 아니며, 한 아이덴티티 제공자(Identity Provider: IdP)가 관리하는 ID의 속성을 다른 아이덴티티 제공자에게 상호 교환하는 것도 새로운 것이 아니며, 상호 교환의 대표적인 프로토콜로 싱글사인온(Single Sign ON)은 널리 알려진 있는 기술이다. 그러나 서로 다른 아이덴티티 제공자들로부터 획득한 ID(Identity)로부터 속성을 수집하고 추출하여 새로운 ID를 생성하여 인증 및 인가 과정에서 활용하는 것은 수년 동안 해결을 하고자 하는 과제이다. 예를 들면, 이북(eBook) 상점에서 IEEE, ACM 등 우수 학회 멤버에 대하여 20%의 책 세일을 계획하고 있다면, 이러한 경우에 이북 상점은 두 개의 아이덴티티 공급자로부터의 속성정보들이 확보되어야 한다. 즉 결제의 주체가 되는 이북 상점에서는 결제 단계에서 20%의 할인을 이용자에게 제공하려면, 신용카드 번호와, 학회 멤버십 번호가 확보되어야 온라인 결제 작업을 진행할 수 있는 것이다.

연합 아이덴티티 관리에서 속성수집 모델(Attribute aggregation models in federated identity management)

SAML2.0과 같은 연합관리 기술들은 속성을 주장(Assertion)에 저장한다. 현재까지 존재하는 속성 수집모델을 분류하기 위하여 두 가지의 기준이 제시된다. 하나는 속성 수집이 어디에서 이루어지는가 하는 것이고 다른 하나는 누가 전반적인 프로세스를 중재하는 가이다. 여기서 중재라 함은 수집 메커니즘을 최초 시도하는 것을 의미한다. 어디에서 수집이 이루어지는가의 기준에 의하면, 수집 메커니즘들은 SP(Service Provider)에서 수집, IdP에서 수집, 클라이언트(이용자 에이전트/브라우저)에서 수집과 같이 3개로 분류된다. 또한 수집이 이루어지는

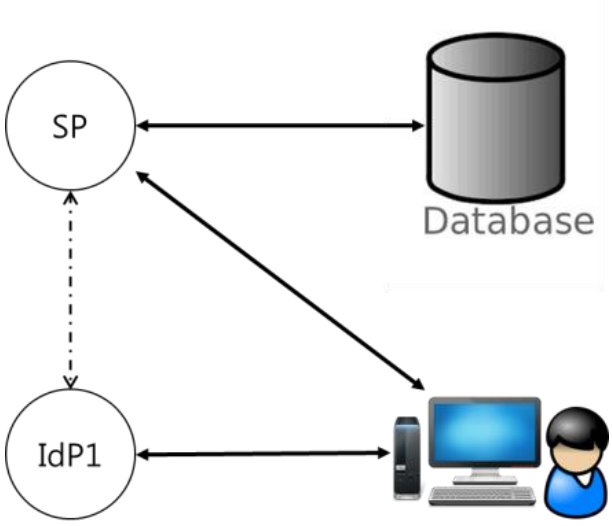
장소에 더하여 누가 수집을 중재하느냐 하는 기준을 부가하면 SP에서는 SP 중재, IdP 중재, IdP에서는 IdP 중재, 클라이언트는 클라이언트 중재와 같이 분류할 수 있으며, 지난 2014년 46호 ICT Standard Weekly(http://www.tta.or.kr/data/weekly_view.jsp?news_id=4457)에서 분류한 것과 같이 7종의 수집 메커니즘을 분류할 수 있다.

서비스 제공자(SP: Service provider) 중재의 속성수집 모델

본고에서는 7종의 속성수집 모델에서 서비스 제공자 중재의 3가지 모델을 분석하고 그 특성을 알아본다.

1. 응용 DB

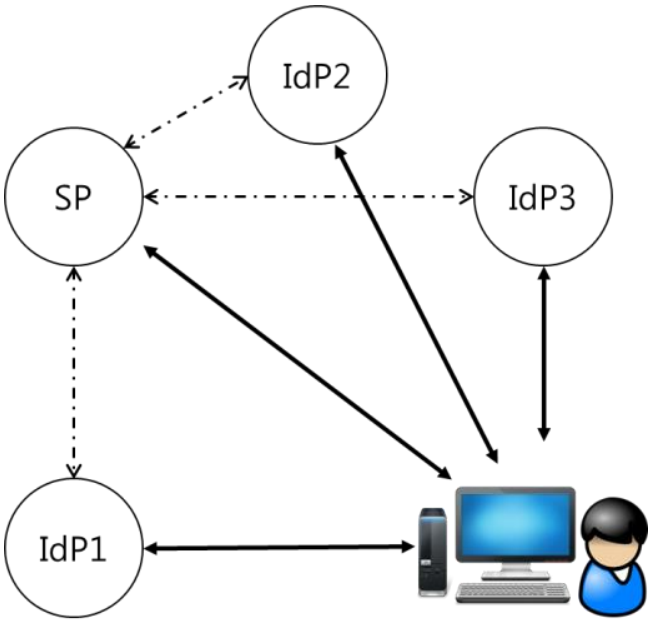
이 모델은 가장 간단한 속성 수집모델이다(<그림 1> 참조). 서비스 제공자는 IdP로부터 제공되는 속성에다가 로컬 식별자나, 특정 서비스를 위한 사용자 선호도, 그룹 멤버십과 같은 사용자 속성을 추가적으로 저장할 수 있다. 그리고 서비스 제공자는 이러한 추가적인 속성을 로컬 저장소에 저장하는 ID 제공자의 식별자와 연관된 SP-식별자와의 매핑을 만든다. 이러한 로컬 속성들은 후에 매핑을 통하여 참조될 수 있으며, 서비스 제공자는 최종 사용자가 서비스에 접근이 가능한지를 결정한다.



<그림 1> 응용DB 모델

2. 서비스 제공자 중재

서비스 제공자 중재 모델은 <그림 2>에서와 같이 사용자가 하나의 세션에서 다수의 ID 제공자들로부터 속성을 수집하도록 제공한다. 사용자는 필요한 속성을 보유한 ID 제공자에게 각각 인증을 수행하고 각 ID 제공자가 보유하고 있는 속성정보를 서비스 제공자에게 전달을 한다. 서비스 제공자는 속성들의 집합들을 최종적으로 합치고 사용자가 서비스에 접근할 수 있는지에 대하여 결정을 한다.

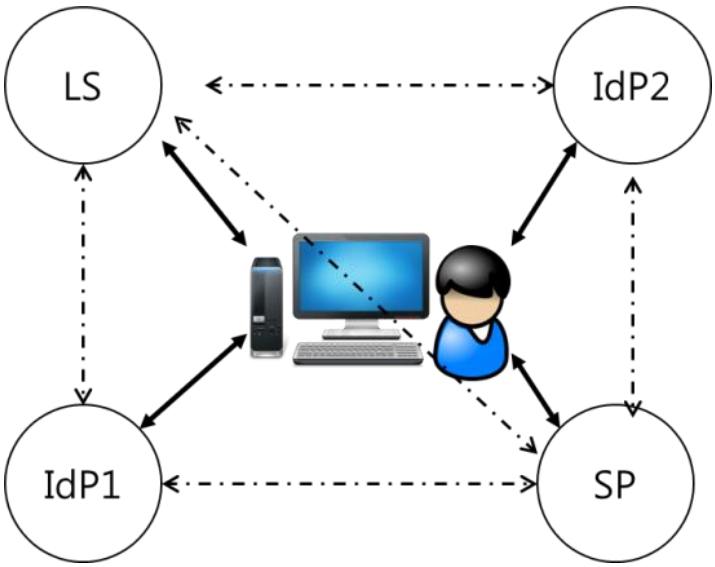


<그림 2> SP 중재 모델

3. 연결 서비스

연결 서비스 모델은 ID연결 모델과 ID 릴레이 모델의 조합이다. 이것은 연결 서비스(LS: Linking Service)라고 지칭하는 서비스 제공자가 존재하며 사용자는 LS가 제공하는 식별자를 이용한다. 이 식별자는 ID 제공자가 제시하는 연결 테이블의 LS의 식별자를 다른 ID 제공자들이 연결할 경우에 이용된다. 즉, 서비스에 접근하려고 하면, 사용자는 해당 서비스 제공자를 방문하여야 하며, 이후 첫 번째 ID 제공자에게(<그림 3>의 IdP1) 전달된다. 사용자는 IdP1에서 인증을 수행하고 사용자 속성을 포함하는 주장(Assertion)과 LS에 대한 식별자와 주소가 서비스 제공자에게 전달된다. 서비스 제공자는 속성들을 수집하기 위하여 LS로 식별자를 전달한다. 이후

두 개의 선택이 있는데, 하나는 LS가 식별자에 연결되어 있는 ID 제공자들 목록을 참조하여 LS에 저장되어 있는 속성들을 찾아서 서비스 제공자에게 전달하는 것과, 또 다른 하나는 LS가 연결되어 있는 ID 제공자들의 목록을 서비스 제공자에게 전달하고 이후 서비스 제공자가 각 ID 제공자로부터 속성정보를 찾는 방법이다. 수집된 속성들을 기반으로 서비스 제공자는 사용자가 서비스에 접근할 수 있는지에 대하여 결정을 한다.



<그림 3> 서비스 (Linking Service) 모델

향후 전망

ITU-T SG17 2014년 9월 회의에서 신설된 아이템은 여러 가지 모델 중 하나를 주장하여 표준화를 진행하기에는 각국의 이해관계가 얽혀있다. 즉, ITU-T SG17의 아이덴티티 관리 연구과제는 SAML2.0, XACML3.0의 연장선 상에서 본 제안서를 검토하고 있으며, 특히 개인정보보호에 있어서 사용자가 제어를 하는 것이라 할 지라도, 사용자의 정보는 네트워크에 담겨지게 되므로, 제공자 관점에서 표준개발이 진행되어야 한다고 판단하고 있다. 그러나 개인정보보호를 위한 사용자 중심의 기술이 이미 유럽을 중심으로 개발되었으며 표준화가 JTC1/SC27 WG5에서 논의가 진행 중이며, 한국은 전자지갑이라는 기술을 이미 보유하고 있어 사용자 중심의 속성수집 기술 표준화에 기술적 우위를 확보하고 있다. 향후 사용자중심의 표준은

연령검증과 같은 영역에 확대 적용이 가능한 메커니즘으로 사이버공간에서 이루어지는 전자상거래에 대한 신뢰성 제고에 필수적인 표준이라 사료되며 이에 전략적 대응이 필요하다.

나재훈 (한국전자통신연구원 사이버보안연구본부 전문위원, jhnah@etri.re.kr)