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

개요

온라인상의 상거래는 현대생활에 없어서는 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 아니다. 상호 교환의 대표적인 프로토콜로 싱글사인온(Single Sign ON)이 있음은 이미 익히 알고 있는 사실이다. 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 있다고 할 때, 이북 상점은 두 개의 아이덴티티 공급자로부터의 속성정보들이 확보되어야 한다. 즉 결재의 주체가 되는 이북 상점에서는 결재 단계에서 20%의 할인을 이용자에게 제공하려면, 신용카드 번호와 학회 멤버십 번호가 확보되어야 하나의 온라인 결재 작업을 진행할 수 있는 것이다.

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

SAML2.0과 같은 연합관리 기술들은 속성을 주장(Assertion)에 내장한다. 그러므로 보편적으로 속성 수집(Attribute aggregation)은 두 개의 해석을 갖는다. 하나는 하나의 주장 안에 모든 속성이 내장되는 경우와 하나의 주장 안에 다른 주장이 내장된 경우를 의미하게 된다.

현재까지 존재하는 속성 수집모델을 분류하기 위하여 두 가지의 기준이 제시된다. 하나는 속성 수집이 어디에서 이루어지는가 하는 것이고 다른 하나는 누가 전반적인 프로세스를 중재하는가이다. 여기서 중재라 함은 수집 메커니즘을 최초 시도하는 것을 의미한다. 어디에서 수집이

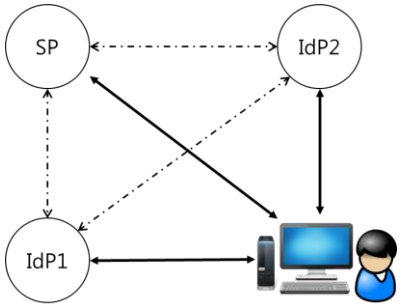
이루어지는가의 기준에 의하면, 수집 메커니즘들은 SP(Service Provider)에서 수집, IdP에서 수집, 클라이언트(이용자 에이전트/브라우저)에서 수집과 같이 3개로 분류된다. 또한 수집이 이루어지는 장소에 더하여 누가 수집을 중재하느냐 하는 기준을 부가하면 SP에서는 SP 중재, IdP 중재, IdP에서는 IdP 중재, 클라이언트는 클라이언트 중재와 같이 분류할 수 있으며, 지난 2014년 46호 ICT Standard Weekly(http://www.tta.or.kr/data/weekly_view.jsp?news_id=4457)에서 분석한 것과 같이 7종의 수집 메커니즘을 분류할 수 있다.

아이덴티티 제공자 중재의 속성수집 모델

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

1. 아이덴티티 링킹 모델

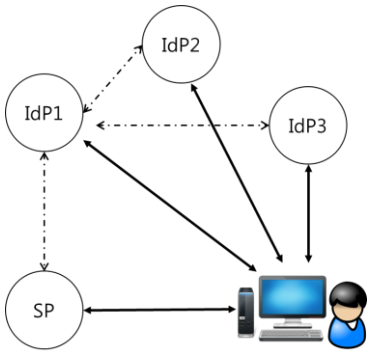
이 모델은 리버티 얼라이언스에서 속성 수집을 위하여 최초로 소개된 모델이다. IdP들은 이용자에게 두 개의 IdP사이에서 상호 링크를 생성할 수 있도록 허용하였다. 링크를 생성하기 위하여, 이용자는 첫 번째의 IdP를 방문하여야 하고 인증 받아야 한다. 첫 번째의 IdP는 이용자에게 다른 IdP와의 연합(Federation)을 할 것인지를 문의하며, 그렇다면 두 번째 IdP로 연합을 요청한다. 이 시점에서 두 개의 IdP 간에 랜덤별명(Random Alias)을 만들기 위하여 상호 연동한다. SP로부터 서비스 접근 동안에는, 하나의 IdP는 속성정보를 포함하는 주장을 그 랜덤별명과 함께 SP에게 제공한다. SP는 다른 IdP로부터 속성정보를 포함하는 주장을 검색하기 위하여 랜덤별명을 사용할 수 있다. 두 개의 IdP로부터의 속성정보를 조합하여, SP는 이용자가 서비스에 접근 가능한지를 결정할 수 있다.



<그림 1> Identity linking model

2. 아이덴티티 프록싱 모델

이 모델에서 SP는 이용자가 상호 신뢰할 수 있는 IdP를 이용하여 다수의 IdP들로부터 속성정보를 수집할 수 있도록 허용한다. 첫째로 이용자는 신뢰하는 IdP로 전달된다. 신뢰 IdP는 이후 이용자를 해당 IdP들에게 전달을 한다. 이용자는 각 IdP들로부터 인증을 받은 후에 속성정보를 포함하는 주장을 신뢰 IdP로 회신한다. 이 시점에서 신뢰 IdP는 각 주장을 검증하고, 속성정보를 검색하여 최종 속성정보를 조합한다. 신뢰 IdP는 자신이 갖고 있는 사용자 속성정보를 더 부가할 수 있으며, 이것을 다시 주장으로 만들어 SP에게 전달한다. 전달된 속성정보를 기반으로 SP는 이용자가 서비스에 접근 가능한지를 결정한다.

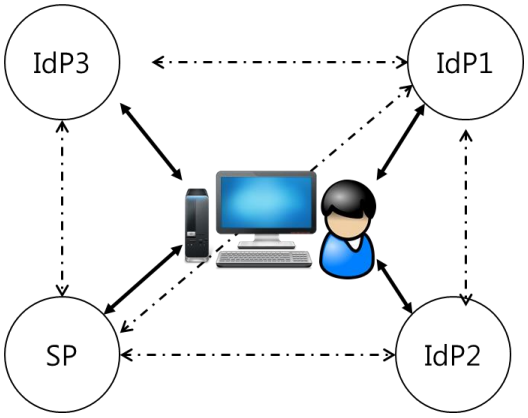


<그림 2> Identity proxying model

3. 아이덴티티 릴레이 모델

본 모델은 프록싱 모델을 일반화된 케이스이다. 프록싱 모델은 SP로 하여금 신뢰 IdP와 강한 신뢰관계를 요구하기 때문에, 프록시 IdP가 전적으로 요구하는 신뢰를 만족시킬 수 없으면 정상적으로 작동할 수 없다. 아이덴티티 릴레이 모델은 신뢰 IdP 대신에 중도적 릴레이(Relay) IdP가 사용된다. 이용자는 처음에 릴레이 IdP에게 전달이 되고, 릴레이 IdP는 이용자를 다수의 IdP들에게 전달을 한다. 이용자는 각 IdP들로부터 개별적으로 인증을 받으며, 이용자 속성정보를 포함하는 주장과 함께 릴레이 IdP로 회신된다. 릴레이 IdP는 모든 주장을 하나의 주장으로

조합하여 SP에게 전달한다. SP는 전달된 주장 안의 각 주장들을 추출하고, 검증 하여 속성정보를 검색한다. 조합된 속성정보를 기반으로 SP는 이용자가 서비스에 접근 가능한지를 결정한다.



<그림 3> Identity relay model

향후 전망

ITU-T SG17 2014년 9월 회의에서 신설된 아이템(X.eaaa: Enhanced Entity Authentication based on Aggregated Attributes)은 여러 가지 모델 중 하나를 주장하여 표준화를 진행하기에는 각국의 이해관계가 얽혀 있다. 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 담겨 지게 되므로, 제공자 관점에서 표준개발이 진행되어야 한다고 판단하고 있다. 그러나 개인정보보호를 위한 사용자 중심의 기술이 이미 유럽을 중심으로 개발되었으며 표준화가 JTC1/SC27 WG5에서 2015년 5월에 신규 연구과제(Study Period on Anonymous Attribute Assurance)가 승인되었고, 연구과제(Study Period on Privacy enhancing identity management schemes using attribute based credentials)가 기간연장 되어 진행되고 있음으로 세 개의 아이템을 같이 고려하여 할 사항이며, 이러한 여건 속에서 한국은 전자지갑이라는 기술을 이미 보유하고 있어 사용자 중심의 속성수집 기술 표준화에 기술적 우위를 확보하고 있다. 향후 사용자 중심의 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)