[정보보호] ITU-T SG17 속성수집 모델 표준 - 사용자 중심

개요

다수의 속성 제공자들로부터 속성을 수집하는 초기 작업은 각 엔티티는 글로벌한 유일한 식별자(Identifier)를 가지고 있다는 전제를 기반으로 한다. 그러나 현실에서는 각 엔티티는 글로벌 식별자를 갖고 있지 않으며, 다수의 아이덴티티 제공자(Identity Provider: IdP)로부터 할당된 각각의 식별자와 속성정보를 갖고 있다. Liberty Alliance는 -현재는 Kantara Initiative가 후속으로 표준을 담당- 연합ID환경에서 이러한 문제를 해결하는 첫 번째 그룹이었다. 그러나 이러한 문제 중의 하나는 서비스 제공자가(Service Provider: SP) 접근제어에 대한 결정을 내리기 위한 표준화된 방안이 없다는 것이다. 이렇듯 관심을 끌고 있는 속성수집 모델은 다음과 같은 실생활의 유스케이스들을 갖는다. E-커머스 서비스 환경에서 사용자의 연령대를 구분하여야 할 필요가 있는 서비스 판매, 즉 온라인 상에서 청소년 보호를 위해 유해성이 우려되는 서비스에 대한 접근에 대하여 제삼의 공인기관으로부터 사용자의 연령대 정보수집, 그리고 이북(eBook) 상점에서 IEEE, ACM 등 우수 학회 멤버에 대하여 20%의 책 세일을 계획하고 있다. 이러한 경우에 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 온라인 결재와 또 전세계적으로 가상협업 환경에서 자원의 이용과 허용을 위한 그룹관리 및 차등적인 접근관리를 위한 가상협업 관련 속성정보의 수집이 선결되어야 안전하게 자원(물적·인적) 접근제어를 관리하는 기술과 표준이 마련될 수 있다.

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

SAML2.0을 기반으로 하는 연합관리 기술들은 속성을 주장(Assertion)에 내장한다. 현재까지 존재하는 속성 수집모델을 분류하기 위하여 두 가지의 기준이 제시된다. 하나는 속성 수집이 어디에서 이루어지는가 하는 것이고 다른 하나는 누가 전반적인 프로세스를 중재하는 가이다.

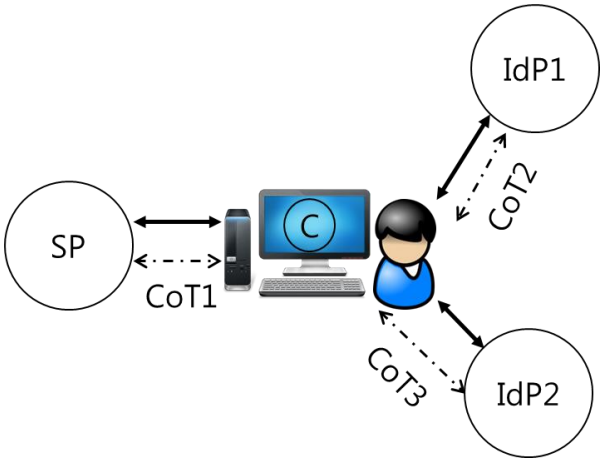
여기서 중재라 함은 수집 메커니즘을 최초 시도하는 것을 의미한다. 어디에서 수집이 이루어지는가의 기준에 의하면, 수집 메커니즘들은 SP(Service Provider)에서 수집, IdP에서 수집, 클라이언트(이용자 에이전트/브라우저)에서 수집과 같이 3개로 분류된다. 또한 수집이 이루어지는 장소에 더하여 누가 수집을 중재하느냐 하는 기준을 부가하면 SP에서는 SP 중재, IdP 중재, IdP에서는 IdP 중재, 클라이언트는 클라이언트 중재와 같이 분류할 수 있으며, 지난 2014년 46호 ICT Standard Weekly에서 분석한 것과 같이 7종의 수집 메커니즘을 분류할 수 있다.

엔티티 중재의 속성수집 모델

본고에서는 7종의 속성수집 모델에서 엔티티 중재의 한가지 모델인 클라이언트 모델의 특성을 알아보고, 이전에 소개되었던 모델들(2014년 46호, 2015년 48호)과 합하여 총 7가지 모델의 장단점을 비교한다.

클라이언트 모델

이 모델은 다른 아이덴티티 공급자로부터 속성수집을 할 수 있는 능력을 갖는 클라이언트(엔티티-에이언트 또는 응용)를 이용한다. 서비스 제공자는 신뢰하는 아이덴티티 제공자들에 대한 목록을 클라이언트에게 공지한다. 그러면 클라이언트는 목록에 있는 아이덴티티 제공자들에게 차례로 엔티티를 리다이렉트(Redirect)한다. 이후 각 아이덴티티 제공자에게 인증을 수행하고, 클라이언트는 각 아이덴티티 제공자로부터 속성정보를 포함하는 주장을 획득하고, 서비스 제공자에게 합쳐진 주장을 전달한다. 최종 서비스 제공자(SP)는 이용자가 서비스에 접근 가능한지를 결정할 수 있다.



<그림 1> Client model

엔티티 중재의 속성수집 모델

이전까지 언급되었던 7가지 모델들은 전통적인 연합ID 관리 시스템의 새로운 접근 방안이 된다. 각 모델들은 추가적인 요소와 상호작용을 갖고 있다. 이러한 요소를 가지고 어떤 것을 선택하여야 할 것인지에 대하여 7가지 모델을 비교한다. 즉 설계자나 개발자들은 누가 속성수집을 중재하고, 수행하고, 검증하는가 하는 사항과 구현의 난이도, 그리고 추가적이거나 새로운 요소와 같은 점에 대하여 생각하여야 할 것이다.

7가지 모델은 속성수집을 위하여 SAML 2.0을 기반으로 제안하였으며, 이러한 모델들은 SAML 주장 안에 속성정보를 적절히 표현함으로 상호운용 문제를 해결할 수 있다고 생각된다. 아래 표는 속성수집 중재자, 수행자, 그리고 추가적 요소와 같은 관점에서 속성수집 모델을 분석한 것이다.

표의 'O' 표시는 세로의 속성수집 모델이 가로의 능력을 가지고 있다는 것을 표시한 것이며, 표시된 능력은 각 모델에서 제공이 되어야 하는 것으로 권고한다.

<표 1> 수집모델 비교표

수행능력 / 수집모델	IdP 중재	SP 중재	Client 중재	IdP 수집	SP 수집	Client 수집	추가적 요소
Identity linking	O				O		
Identity proxying	O			O			
Identity relay	O			O			
Application database		O			O		DB
Service provider		O			O		
Linking service		O			O		LS
Client			O			O	Client

아이덴티티 링킹 모델의 관점에서 속성수집은 아이덴티티 제공자가 중재(시작)를 하고, 서비스 제공자에서 수행된다. 이것은 속성수집 프로토콜이 아이덴티티 제공자와 서비스 제공자들에게 공히 구현되어야 한다는 것을 의미한다. 다른 모델의 경우에 있어서는 중재자와 수행자가 동일 제공자에서 구현될 수 있다는 것은 아이덴티티 링킹 모델보다는 쉽게 또는 효율적으로 구현되고 운영될 수 있다는 것을 알 수 있다. 추가적인 요소(속성수집 서비스 구조관점에서 추가적인 기능 요소)에 관하여는, 응용DB 모델은 자체의 DB가 필요하고, 링킹서비스 모델은 LS(Linking Service), 엔티티 모델은 에이전트로서 클아이언트가 필요하다. 이러한 결과들을 비교 분석할 때에 아이덴티티 프록싱 이나 아이덴티티 릴레이 모델이 아이덴티티 중재모델에서는 추천되고, 서비스 제공자 모델에서는 SP-중재 모델이 추전된다.

향후 전망

ITU-T SG17 2014년 9월 회의에서 신설된 아이템은 여러 가지 모델 중 하나를 표준화 진행하기에는 각국의 이해관계가 얽혀 있는 관계로, ITU-T SG17의 아이덴티티 관리 연구과제는 SAML2.0, XACML3.0의 연장선 상에서 표준화를 추진하였다. 개인정보보호를 중시하여 마이크로소프트사는 CardSpace와 같은 기술을 강하게 산업에 적용하는 것을 추진하였으나, 엔티티의 간섭과 처리가 많아진다는 단점으로 보급이 소강상태에 빠졌다는 점을 간과해서는 안 된다. 본고와 관련한 국제표준은 ITU-T SG17에서 표준화 완료단계에 있다. 그리고 후속과제로는 일곱 가지의 모델 중에 개인정보보호를 보장하고, 이종 도메인간의 정보보호 수준 보증(Level of Assurance)과 같은 주제를 보강한 실질적인 메커니즘을 표준화가 필요하다고 사료된다. ITU-T

SG17과는 협력 및 경쟁 관계에 있는 JTC1/SC27 WG5에서는 유럽을 중심으로 개발되었으며 사용자 기반의 기술 표준화가 2016년 4월에 NP가 제안되어 투표가 진행되고 있다. 한국은 본 주제와 관련하여 전자지갑이라는 기술을 이미 보유하고 있어 사용자 중심의 속성수집 기술 표준화에 기술적 우위를 확보하고 있으며, 향후 연령검증과 같은 영역에 확대 적용이 가능한 메커니즘으로 사이버공간에서 이루어지는 전자상거래에 대한 신뢰성 제고에 필수적인 표준이라 사료되며 이에 전략적 대응이 필요하다.

나재훈 (한국전자통신연구원 정보보호연구본부 전문위원, ITU-T SG17 라포처, jhnah@etri.re.kr)