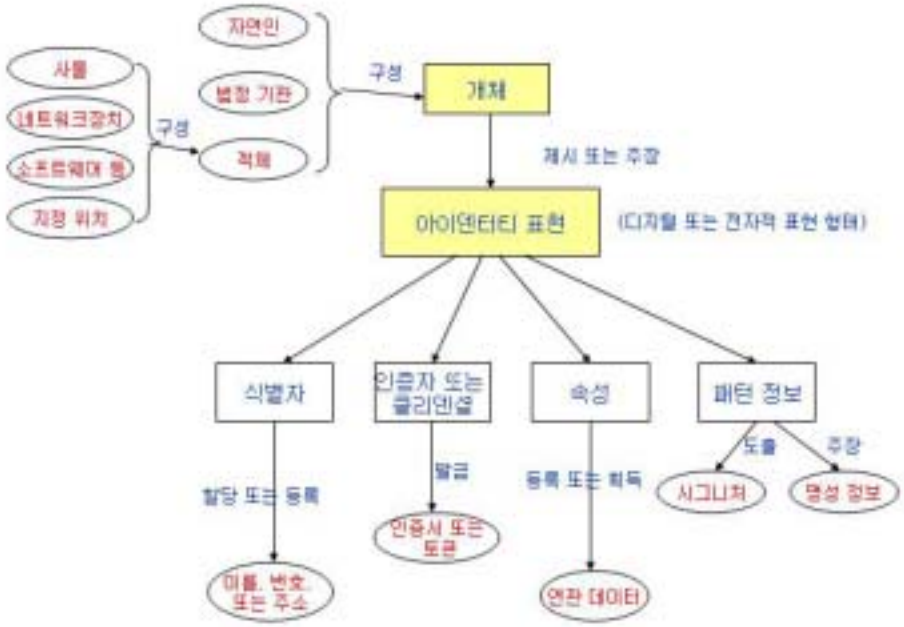
[정보보호] 글로벌 아이덴터티 관리 프레임워크 권고안은 ITU-T에서 최종 승인될 수 있을까?

ITU-T에서 정보보호 선도 연구그룹인 SG17 회의가 지난 2008년 4월 초에 스위스 제네바에서 열렸다. 이번 회의에서 가장 중요한 결과 중 하나는 "글로벌 아이덴터티 관리 신뢰 및 상호운영을 위한 요구사항" 표준초안이 일차 승인(determination)된 것이며, 이 결과로 국가별 의견수렴 과정에 들어가게 되었고 이르면 2008년 9월 SG17 회의에서 최종 승인(approval)이 이루어지게 되었다는 것이다. 이 표준초안은 글로벌 아이덴터티 관리를 위한 기반 문서로 활용될 수 있으며, 이 표준초안에 근거하여 향후 추가적인 국제표준이 계속 개발될 수 있다는 점에서 많은 주목을 받고 있다. 본 고에서는 국제표준 개발에 있어 현재까지의 추진 현황 및 주요 이슈들에 대해 정리해 보고, 이에 대한 국내 대응 방안에 대해 논한다.

아이덴터티 정의



<그림 1> 아이덴터티 관계 및 특성
(출처: "ITU-T Q.6/17 아이덴터티 용어 정의 특별위원회 보고서")

아이덴터티는 개체(entity)를 "특정 환경에서 하나 이상의 식별자, 클리덴셜, 그리고 속성 등의 형태로 표현한 데이터 구조"로 정의하고 있다. <그림 1>에서 알 수 있듯이 개체는 자연

인, 법정기관, 그리고 객체로 구성되며, 객체는 다시 사물, 네트워크 장치, 그리고 소프트웨어 또는 콘텐츠 등으로 구성된다. 아이덴터티는 물리적 표현 또는 디지털(전자적) 표현을 갖게 되며. 아이덴터티는 식별자, 클리덴셜, 속성, 그리고 패턴 정보로 구성된다. 식별자는 스스로 자신이 부여하는 식별자와 다른 개체에 의해 피동적으로 할당되는 식별자로 구성되며, 주로 이름, 숫자, 또는 주소 등이 대표적인 예이다.
우리나라에서 주민등록번호는 아이덴터티의 일부인 숫자로 표현되는 식별자임을 알 수 있다. 또한 어떤 자연인의 이름은 스스로 부여한 고유 식별자임을 알 수 있다. 크리덴셜의 대표적인 예는 공인 인증서와 이와 연관되는 개인키 등이며, 인증서는 사람의 이름과 속성과 개체의 공개키를 각각 바인딩한 것으로, 속성과 바인딩 되는 경우 속성 인증서로, 이름과 연관되는 경우 공개키 인증서가 된다. 우리가 금융거래 시에 사용하는 공인 인증서는 자연인의 이름과 공개키를 바인딩한 공개키 인증서임을 알 수 있다. 속성은 주소나 우편번호와 같이 개체와 연관되는 부가 정보를 의미한다. 마지막으로 패턴 정보는 사용자의 반복 행위를 표현한 특징 정보(signature)와 특정 개체에 대해 증언하는 명성 정보(reputation)로 구성된다. 아이덴터티 관리(생명주기)는 여러 다양한 시스템을 통해 아이덴터티의 규칙적인 생성, 표현, 획득, 저장, 유지, 사용, 파괴 등으로 정의되고 있다.

아이덴터티 표준초안의 주요 내용

현재 개발되고 있는 아이덴터티 관리 관련 표준초안들은 기본 요구사항을 정의하고 있는 "글로벌 아이덴터티 신뢰 및 상호연동을 위한 요구사항(X.idmreq)", "공통 아이덴터티 데이터 구조(X.idmdm)", 그리고 "사용자 제어 강화 디지털 데이터의 상호 교환 프레임워크(X.idmif)"들을 개발하고 있다. 첫 번째 표준초안인 요구사항에 관한 문서는 최근 ITU-T SG17 회의(2008.4)를 통해 일차 승인을 획득했으며, 나머지 두 개의 표준초안은 2008년 9월 일차 승인을 목표로 개발되고 있다. X.idmreq는 다음과 같이 9가지 영역에서 정의된 87개의 요구사항들로 구성되어 있다.

- 공통 아이덴터티 관리 모델: "삼자간 아이덴터티 관리 모델을 지원해야 한다" 등의 5가지 요구사항
- 상호연동 가능한 아이덴터티 관리를 위한 기본 기능: "통신망은 상호 연동 가능한 아이덴터티 관리를 실현하기 위한 여러 기능 집합을 구현해야 한다"는 등의 2가지 요구사항
- 식별자, 속성, 클리덴셜, 그리고 패턴 정보 아이덴터티 서비스: "아이덴터티 제공기관은 다양한 아이덴터티를 제공할 수 있어야 한다" 등의 37가지 요구사항
- 아이덴터티 발견 서비스: "다른 공인 아이덴터티 제공기관을 찾을 수 있어야 한다" 등의 3가지 요구사항
- 상호 연계와 브리징: "인증 도메인을 확립할 수 있어야 한다" 등의 8가지 요구사항
- 거래 데이터에 대한 무결성, 부인방지 등을 제공하는 보안과 정책: "거래 데이터에 대한 부인방지 기능을 제공해야 한다" 등의 25가지 요구사항

- 감사 기능: "감사 기능을 제공해야 한다" 등의 3가지 요구사항
- 성능, 가용성, 신뢰성 특성: "신뢰성과 가용성을 보장 해야 한다" 등의 3가지 요구사항
- 언어(Language): 다양한 언어 제공이 가능한 국제화 관련 한가지 요구사항

X.idmreq 일차 승인 과정에서 각국 입장 및 논쟁

일차 승인을 위한 SG17 폐막 총회에서 찬반은 북미/아시아권 회원국과 유럽 회원국으로 분명히 갈렸다. 독일이 자국의 규제 문제와 아이덴터티 용어 정의를 수용할 수 없다는 이유로 본 표준초안의 일차 승인을 반대했다. 이어 프랑스도 일차 승인의 연기를 주장했고, 스페인도 이에 가세했다. 이에 반해, 미국은 완성도가 높고, 의도적인 승인 지연은 의미가 없으며, 산업체가 해당 표준초안 승인을 기다리고 있으며, 아이덴터티 관리 표준 개발의 주도권을 ITU-T SG17이 유지해야 하며, 반대 사유에 대해서는 최종 승인 단계 전까지 해결 가능하다는 이유로 이번 회의에서 일차 승인이 되어야 한다고 주장하였다.

한국도 완성도와 아이덴터티 용어 특별 위원회의 합의 결과를 수용해야 한다는 이유로 승인에 찬성했다. 이어 아랍, 시리아, 중국, 러시아 등이 찬성했다. 영국은 중립적 입장을 표명했다. 이에 잠시 정회를 통해, 프랑스의 입장이 국가별 의견 수렵 기간 동안 독일이 제기한 문제가 해결되지 않을 경우, 다음 9월 회의에서 최종 승인하지 말고, 2009년 2월에 승인을 연기하자는 절충안이 나왔다. 독일은 국가별 의견 수렴기간 동안 합의안을 마련할 시간이 부족하다는 이유와 최종 입장을 결정하는데 시간이 필요하다고 주장하면서 일차 승인에 여전히 동의하지 않았다. 이때 스페인이 프랑스의 조정안을 지지하게 되었고, SG17 의장은 일차 승인을 선언하였고, 프랑스와 독일의 의견을 SG17 총회 보고서에 각각 기록하는 조건으로 일차 승인되었다.

회의 성과 및 향후 대응 방안

현재의 표준초안은 한국형 아이덴터티 관리 기법인 아이핀(i-PIN)과 동일한 모델로 이루어져 있고, 아이핀이 갖는 고유 요구사항이 현재 표준초안에 반영되었으므로 우리나라는 본 표준초안 승인에 찬성해야 한다고 생각하며, 국가별 의견 수렴이 종료된 후, 9월 SG17 회의에서 최종 국제표준으로 승인될 때까지 본 표준초안에 대한 심각한 문제가 발견되지 않는다면 최종 승인에 찬성해야 할 것으로 생각한다. 국내 아이핀 기술과 본 표준초안의 비교분석한 결과, 아이덴터티 제공 서비스와 속성 제공 서비스를 결합한 아이덴터티 서비스를 제공하고 있으며, 두 가지 영역의 강제 요구사항을 모두 만족하는 것으로 분석되었다. 따라서 한국형 아이덴터티 관리 기법인 아이핀은 ITU-T 국제 표준초안과 호환되고 있다고 판단된다. 국내 정보보호 산업체는 아이덴터티 관리 시스템을 개발 시, 일차 승인이 완료된 국제 표준초안을 참조해야 할 것으로 판단된다.

염흥열 (ITU-T SG17 Q.9 Rapporteur, 순천향대 교수, hyyoum@sch.ac.kr)