[정보보호] 스마트 그리드 등 신규 스마트 IT 서비스에 적용 가능한 디지털 인증서 기술 표준

스마트 그리드, M2M, IoT 등은 최신 스마트 IT 산업 분야의 중심이라 할 수 있다. 또한, 해당 산업의 경우 언제, 어디서나, 누구라도 접속이 가능하고 서비스 제공자의 인지 없이도 바로 서비스 제공이 가능해야 하기 때문에 무엇보다 해당 기기 및 이용자의 식별과 인증이 무엇보다 중요하다. 특히, 생활에 없어서는 안될 전력망, 통신망 등을 다루는 서비스이기 때문에 전 국가적 나아가 전세계적으로 보안에 많은 관심과 노력을 기울이고 있다. 이를 위한 표준은 미국의 NIST를 중심으로 많은 연구가 개발이 되고 있으며, IEEE 역시 스마트 그리드 분야에 표준을 개발하고 있다. 특히 NIST의 경우 스마트 그리드 보안전략을 위한 도메인 구성 방식, 보안 위협요소 정의, 시스템별 보안 요구사항 및 상호운용성 등에 대한 보안 기능들을 정의하고 있다. 또한, IEEE에서는 스마트 그리드 산업의 실현을 위한 전문지식 확보를 위해 표준 개발을 포함한 다양한 활동을 진행 중에 있다. 이외에도 ISO/IEC JTC1, IEC TC57 등에서도 스마트 그리드 보안 관련 표준을 개발 중에 있으며, ITU-T에서는 JCA-SG&HN에서 관련 표준을 개발하고 있고, SG17에서는 스마트 그리드 보안 관련 표준을 개발 중에 있다. 현재 SG17에서 개발 중인 스마트 그리드 보안 표준은 스마트 그리드 서비스 등에 적용 가능한 디지털 인증서 관련 표준으로 지난 9월 정기회의를 통해 표준으로 채택되었으며, 2013년 4월 스위스 제네바에서 개최되는 SG17 정기회의부터 본격적으로 관련 표준안의 개발이 추진될 예정이다. 지난 회의에 채택된 표준안은 '스마트 그리드에 적용 가능한 디지털 인증서 프로파일(Smart Grid Profile)'과 '디지털 인증서 발급 및 관리(Establishment and maintenance for Smart Grid)' 등 총 2건이다. 본 표준화 보고서는 지난 2012년 8월 29일부터 9월 7일까지 스위스 제네바에서 개최된 ITU-T SG17 정기회의에서 채택된 스마트 그리드 서비스 등에 적용 가능한 디지털 인증서 관련 표준화 동향을 소개하고자 한다.

스마트 그리드 등에 적용 가능한 디지털 인증서 표준 기술의 필요성 및 유사 기술과의 비교

위에서 언급한 대로 NIST, IEEE, IEC 등에서는 주로 스마트 그리드 시스템 및 도메인 등 주로 서비스 제공을 위한 전반적인 시스템 보안, 네트워크 보안 그리고 물리적인 보안 위주의 표준들이 개발되고 있으며, 실제 기기간 식별 및 인증을 위한 직접적인 기술에 대한 표준은 아직까지 개발하지 않고 있다. 물론 기존 시스템/네트워크/물리적 보안 등이 매우 중요하며 우선적으로 개발이 되어야 하겠지만 실 서비스 시 가장 민감하고 트랜잭션이 많은 단말기단에서의 인증 및 데이터 보안이 무엇보다 중요하다. 사용자 단말에서의 인증에 문제가 발생할 경우 이용자에게 직접적인 금전적 피해뿐 아니라 주요한 개인정보에 대한 유출도 가능할 수 있기 때문에 각 가정에 위치한 단말 등에 적용될 수 있는 인증 표준 기술 개발이 매우 중요하다 할 수 있다.

현재, PC환경뿐만 아니라 모바일 기기에서 사용자 인증을 위해 가장 널리 사용되고 있는 것이 디지털 인증서이다. 현재 디지털 인증서는 인터넷뱅킹, 증권, 전자거래 등 다양한 분야 및 다양한 단말에서 광범위하게 사용되고 있으며, 생활필수품으로까지 불려지고 있다. 하지만, 현재 사용되고 있는 디지털 인증서 기술은 스마트 그리드, IoT 등 주로 연산력이 떨어지고 저장공간이 현저히 부족한 단말, 센서 등을 사용하고 있는 산업분야에서 적용이 어려운 것이 사실이다. 그렇다고 이러한 스마트 IT산업에서 정당한 사용자 및 기기를 인증하는 보안 기술이 배제될 수도 없기 때문에 해당 서비스에 적합한 디지털 인증서 기술 표준은 반드시 필요하다. 특히, 스마트 그리드, IoT 서비스에 적용되기 위해서는 연산요구를 최소화시킬 수 있도록 경량화된 인증서 프로파일 및 검증 프로세스가 적용되어야 하며, 기존과는 비교가 안될 만큼 많은 기기들에 적용되고 또한 사람의 간섭 없이 기기간 인증이 이루어져야 하기 때문에 이에 적합한 기술들이 적용되어야 한다. 이에 따라, 본 표준에서는 이를 만족하기 위해 경량화된 인증서 프로파일을 개발할 예정이며, 최소화된 PKI 구조, 프로토콜 교환 그리고 PDU 크기 역시 최소화하는 표준을 개발할 예정이다.

스마트 그리드 등에 적용 가능한 디지털 인증서 기술 표준화 진행 상황 및 표준화 회의 결정사항

디지털 인증서 기술 관련 표준은 ITU-T와 IETF에서 주로 개발하고 있다. 우리가 현재 사용하고 있는 디지털 인증서는 ITU-T에서 개발한 X.509 인증서이다. 본 인증서는 1988년 6월 X.500 표준안의 일환으로 시작되었으며, 1993년 인증기관 고유 식별자와 주체고유 식별자가 추가된 v2가 발표되었고 1996년에 확장(Extension) 기능을 이용해 데이터를 추가할 수 있는 v3가 발표되어 현재 전세계적으로 널리 쓰이고 있다. X.509 인증서 발급을 위해서는 최상위인증기관, 인증기관(CA) 등이 필요하며 X.500 규약에 따라 공개키를 포함하는 인증서를 발행한다. IETF는 ITU-T의 X.509 표준을 기반으로 실제 PKI 시스템을 구축/운영할 수 있는 다양한 실증표준들을 개발하고 있다.

하지만, 현재 사용하고 있는 X.509 기반의 인증서 외에 별도 연산력이 부족한 단말들을 위한 디지털 인증서 기술 표준은 개발되지 않고 있었으나, 금번 ITU-T SG17 회의를 통해 신규 아이템으로 스마트 그리드 등에 적용 가능한 디지털 인증서 기술 표준이 제안되었으며 SG17 Plenary 회의를 통해 신규아이템으로 채택되었다. 본 신규 표준안은 그간 X.500 시리즈 표준을 개발한 Q11이 주개발 Question이 되었으며, Q10과 공동으로 개발하기로 결정되었다. 이에 따라, 2013년부터 시작되는 차기 연구회기(2013-2016) 동안에 국제표준 초안이 개발될 예정이며, 2015년 하반기에 완성을 목표로 개발될 예정이다.

표준안 관련 시장 전망 및 국내 표준화 활동에의 제언

본 표준안은 2012년 9월 회의에 신규아이템으로 제안된 것으로 아직은 표준화 완료 시까지 많은 시간이 필요할 것으로 보인다. 하지만, 명확한 목적과 수요가 있는 표준안이기 때문에

국내에서도 주목해 볼 만하다. 이미 수년 전부터 신규 스마트 IT산업에 많은 투자를 하고 있는 국내 상황을 고려해볼 때 표준완료 이전이나 완료 시점에 바로 서비스에 적용하게 될지도 모르기 때문이다. 현재에도 공인인증서는 다양한 분야에서 널리 각광받고 있는 보안 서비스 중에 하나로 어느 정도는 안전성이나 인지도 측면에서는 공인된 부분이고, 신규 스마트 IT 서비스 사업자 및 이용자가 보안의 중요성을 익히 인지하고 있기 때문에 해당 표준안이 시장에 미치는 영향은 의외로 클 수도 있다. 그렇기 때문에 국내 관련 기관 및 업체에서는 해당 표준의 개발 진행상황을 지켜보면서 필요 시 적극적인 대응을 하는 것도 필요하다. 현재, ITU-T SG17에는 국내 표준전문가들이 부의장, 라포처 등을 수행하고 있기 때문에 사전에 국가차원의 논의를 통해 국내 의견을 적극 반영시키는 것이 가능하다. 또한, 디지털 인증서 이외에 스마트 IT 보안과 관련한 표준 아이템이 있다면 적극 발굴하고, 현재 한국이 가지고 있는 국제 표준화 인프라를 활용한다면 해당 분야의 다양한 국제 표준 개발이 가능할 것으로 보인다. 이를 통해, ITU-T 내에서 한국의 위상과 국내 기술의 우수성을 확고히 다지는 발판을 마련할 수 있을 것으로 기대된다.

백종현 (ITU-T SG17 Q6 라포처, jhbaek@kisa.or.kr)