[정보보호] 일회용 패스워드(OTP) 통합인증 서비스 프레임워크 표준화 동향

일회용 패스워드(OTP) 통합인증 서비스 소개

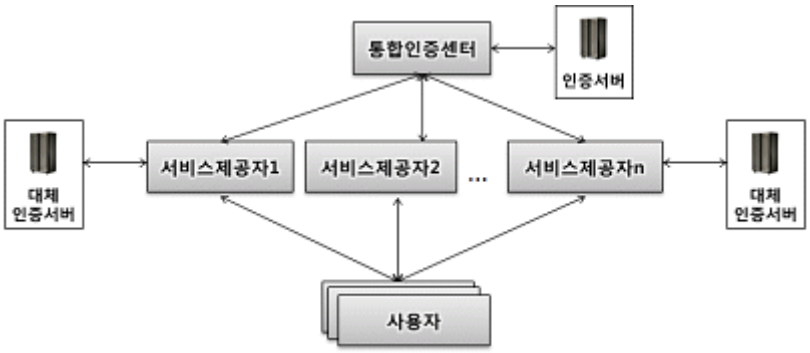
일회용 패스워드(이하 OTP, one time password)는 한번만 사용할 수 있는 비밀번호를 매번 생성하여 인증함으로써 보다 안전한 전자거래가 가능하도록 하는 인증기술이다. OTP는 생성방식에 따라 시간동기화방식, 이벤트동기화방식, 시간-이벤트 혼합방식, 시도-응답방식으로 나뉜다. 국내 인터넷뱅킹에서 흔히 사용되는 OTP는 시간동기화방식으로 보통 30초~1분에 한번씩 OTP를 생성하고 이를 인터넷뱅킹 화면에 입력하여 OTP의 유효성을 인증하는 방식이다. 물론, 한번 사용한 OTP는 다시 사용할 수 없기 때문에 보안성이 우수한 인증기술이라고 할 수 있다. 다만, OTP 서비스를 위해 금융회사는 사용자에게 OTP발생기를 배포하게 되는데, 이때 다수의 금융회사를 이용하는 사용자의 경우 다수의 OTP발생기를 소지해야 하는 불편함이 존재하게 된다.

국내에서는 2007년 OTP 통합인증센터를 개소하고 한 개의 OTP발생기로 다수의 금융회사에서 공동으로 사용할 수 있는 OTP 통합인증 서비스를 세계최초로 도입하였다. 국내를 뒤이어 싱가포르에서도 2011년부터 OTP 통합인증서비스 기반 국가인증프레임워크(NAF)를 구축하고 국가차원에서 전 국민을 대상으로 OTP 서비스를 제공하고 있다.

국내·외 표준화 추진 현황

OTP 통합인증 서비스와 관련된 국내·외 표준은 최초로 OTP 통합인증 서비스를 시작한 국내 주도로 2009년부터 활발히 진행되었다. 먼저 2009년 '일회용 패스워드(OTP) 통합인증 서비스 프레임워크(TTAK.KO-12.0128)'를 TTA 단체표준으로 제정한 것을 시작으로, 같은 해 국내·외 전자금융 환경에 적합하도록 확장된 개념의 OTP 통합인증 서비스 프레임워크를 ITU-T SG17 Q.7(응용서비스보안 분과)에 제안하여 신규아이템으로 채택되었다. 해당 표준안은 2011년 ITU-T X.1153 'Management framework of a one time password-based authentication service' 최종 등록되었다.

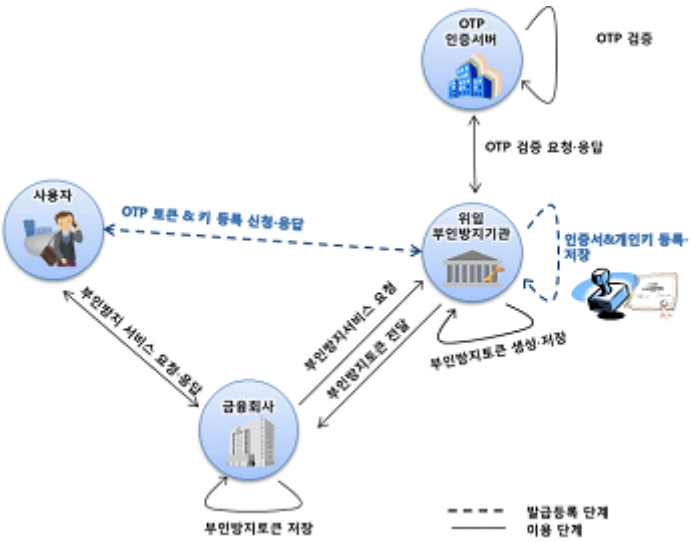
ITU-T X.1153 권고표준은 서비스방식에 따라 통합인증센터 모델, 개선된 통합인증센터 모델, 통합인증센터간 연동 모델의 3가지 서비스모델을 정의하고 있다. 특히 개선된 통합인증센터 모델은 통합인증센터를 통해 중앙집중적으로 OTP 인증업무를 처리하기 때문에 발생할 수 있는 서비스안정성 문제를 개선한 모델로, 현재 국내 전자금융환경에 적용된 모델이다. 개선된 통합인증센터 모델을 구체적으로 살펴보면, <그림 1>과 같이 서비스제공자가 자체적으로 대체인증서버를 구축하여, 통합인증센터 또는 자체 구축한 시스템을 통해 안정적으로 통합인증서비스를 제공할 수 있도록 하는 서비스 모델이다. 예를 들어, 자사에서 발급한 OTP는 대체인증서버를 통해 인증하고, 타행 등록한 OTP는 통합인증센터를 통해 인증하는 방법으로 대체인증서버를 활용한 통합인증서비스가 가능하다.



<그림 1> 개선된 통합인증센터 모델

한편, 거래사실의 부인방지기능은 비대면 전자거래 특성상 서비스 신뢰성 확보를 위해 중요한 기능이다. 이를 위해 2012년 TTA 단체표준으로 제정한 '통합인증기반 부인방지 서비스 프레임워크(TTAK.KO-12.0194)'는 편리하게 부인방지서비스를 제공할 수 있는 통합인증서비스 프레임워크를 정의한다. 이후 해당 표준안은 노르웨이, 스웨덴 등 북유럽에서 이미 널리 사용중인 뱅크아이디(BankID) 서비스 모델을 포함하여 2014년 ITU-T X.1159 국제표준으로 제정되었다. 표준권고안의 주요내용은 제3의 신뢰기관에 사용자의 서명키를 위임하고, 사용자의 명시적인 요청이 있을 때만 신뢰기관이 사용자를 대신하여 부인방지증빙을 생성하는 프레임워크를 정의한다. 대표적인 서비스 예시로는 <그림 2>와 같이 사용자는 공인인증서를 신뢰기관에 미리 등록하고 전자서명이 필요할 때 OTP 인증만 하면 신뢰기관을 통해 거래에 대한

전자서명을 생성하여 인증하는 것이다. 사용자가 별도로 전자서명용 키를 소지·관리하지 않고도 보다 편리하게 부인방지서비스를 제공받을 수 있는 장점이 있다. 추가적으로 생성된 부인방지증빙(예, 전자서명)을 당사자가 직접 관리할 수 있어 분쟁 발생 시 사용자의 적극적인 관여가 가능하도록 하였다. 해당 표준기술은 향후 모바일과 결합한 다양한 형태의 서비스가 가능할 것으로 기대된다.



<그림 2> 위임 부인방지 서비스 예시

결언

최근 국내에서는 핀테크 열풍의 영향으로 사용자가 간편하면서도 쉽게 이용할 수 있는 인증기술의 수요가 증가하고 있는 추세이다. 하지만, 보안이 담보되지 않은 전자금융 서비스는 결국 사상누각(砂上樓閣)으로, 전자금융 서비스의 안전성을 확보하기 위해서는 강력한 인증기술의 도입이 무엇보다 중요하다. 그런 의미에서 OTP 통합인증 서비스는 일회용 패스워드라는 강력한 소지기반 인증기술과 사용자 편의성을 고려한 통합인증기술이 적절히 접목되어 사용자 편의성과 보안성을 동시에 제공할 수 있는 인증기술이라고 할 수 있다. 특히 최근에는 스마트기기와 결합된 다양한 형태의 OTP 기술이 선보이고 있어, 향후 전자금융 분야뿐만 아니라, 전자상거래, 공공, 의료 등 다양한 분야에서 활용도가 높아질 것으로 기대된다.

김근옥 (금융보안연구원 선임, kko@fsa.or.kr)