[정보보호] 일회용 패스워드 인증 프레임워크의 표준화 동향

일회용 패스워드(One-Time Password)는 매번 로그인 할 때마다 그 세션에서 사용 가능한 1회용 비밀번호를 생성하는 보안 매체로서, 현재 사용하는 비밀번호로부터 다음에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성을 가진다. 따라서 OTP를 이용한 인증 방식은 기존의 ID/패스워드 인증방식에서 문제가 되었던 패스워드 재사용 공격, 키로거(Keylogger) 프로그램을 이용한 패스워드 탈취 공격 등의 여러 공격들로부터 안전성을 제공하기 때문에, 금융권 전자금융거래, 기업체 사내시스템 접근통제, 인터넷포털 사이트의 사용자 인증 등 민감한 자원을 다루는 분야에서 활발하게 사용되고 있다. 이와 관련하여 IETF 등에서는 OTP 알고리즘 및 보안 프로토콜을 중심으로 표준화를 진행하고 있는 상태이며, 많은 벤더들로부터 여러 제품들이 출시되어 다양한 산업영역에 도입되어 서비스 되고 있는 중이다.

OTP를 사용하기 위해서 사용자는 패스워드를 생성하는 디바이스를 소지해야 하며, 해당 디바이스가 등록된 인증시스템으로 해당 OTP에 대한 인증 확인을 받아야 한다. OTP 인증 방식이 사용자가 기억하고 있는 패스워드와 함께 OTP 디바이스를 소지해야만 한다는 측면에서 멀티팩터 인증방식으로 잘 알려져 있다. 그러나, 최근 OTP 기반의 인증과 관련하여, 사용자 편의성을 고려하지 않을 경우 여러 응용서비스들을 사용하는 사용자는 하나 이상의 OTP 디바이스를 소지해야 하는 문제가 제기되고 있다. 따라서 좀더 단순화되거나 사용자 편의성을 고려하는 처리 모델이 요구되고, 이를 위해서 통합 프레임워크 내지 인증 시스템 간 연동 프레임워크의 개발 필요성이 제기되었었다.

이러한 요구사항으로부터 ITU-T에서는 2008년 9월 회의에서 국내 금융보안연구원의 주도로 OTP 인증 프레임워크에 대한 신규 표준화 아이템 제안이 SG17의 Q7(Secure Application Services)로 기고 및 채택(x.sap-3)되었으며, 2009년 6월 ITU-T 임시회의에서 2번째 개정된 표준 초안이 발표되었다. 또한 이상에서 언급된 마지막 ITU-T 회의에서 일회용패스워드 프레임워크의 표준화 추진현황에 대하여 Liberty Alliance의 계승그룹인 Kantara Initiative, OASIS, ITU-T Q.16/SG13으로 알리고 관련 표준 그룹의 의견을 수렴하기 위해 연락문서(Liaison Statement)를 발송하였다.

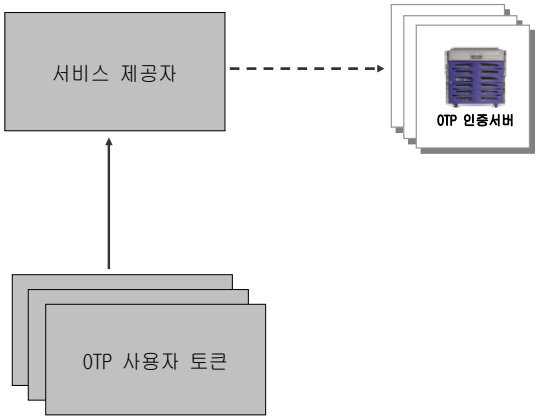
OTP 인증 프레임워크

서비스 프로바이더는 OTP 인증 서비스를 제공하기 위해서 해당 서비스 도메인의 요구사항과 응용특성에 따라 기본 모델과 상호 운용 관리 모델을 구현할 수 있으며, 후자는 다시 중앙집중형 모델, 확장된 중앙집중형 모델 그리고 크로스 도메인 모델로 구분된다.

- 기본 관리 프레임워크-기본 모델

OTP 인증 기본 프레임워크는 <그림 1>과 같이 사용자와 단일 서비스 제공자 간의 인증모델로서 단순하지만 가장 많이 사용되고 있는 모델이다. 기본 관리 프레임워크는 OTP 인증

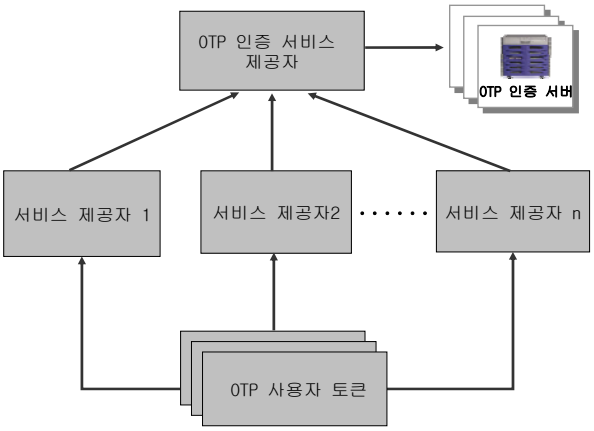
서비스가 제공되기 위해 필수적으로 제공되어야 하는 구성요소만을 지니고 있다.
사용자는 OTP 인증 서비스를 제공받기 위해 특정 서비스 제공자로부터 OTP 기기를 발급받으며, 서비스 제공자는 자체적으로 OTP 인증서버를 구축하고 사용자로부터의 OTP 인증 요청 검증 기능을 제공한다. 서비스 제공자의 결정에 따라 1개의 OTP 인증서버를 통해 단일 벤더(예, OTP 기기제조사) OTP 기기만을 지원하거나, 2 종류 이상의 벤더가 제공하는 OTP 기기를 지원하기 위해 여러 개의 OTP 인증서버를 구축할 수 있다.



<그림 1> OTP 인증 기본 프레임워크(FW)

• 상호 운용 관리 프레임워크-중앙집중형 모델

OTP 중앙집중형 프레임워크는 <그림 2>와 같이 다수개의 기본 프레임워크가 혼합된 형태이다. 즉, 개인 사용자가 다수의 서비스 제공자들을 이용하는 시나리오를 의미한다. 중앙집중형 프레임워크는 기본 프레임워크와 달리 중앙에 단일화된 OTP 인증 시스템이 구축되며, 다수의 서비스 제공자들에게 OTP 인증을 대행하는 기능을 수행한다.
특정 사용자는 OTP 인증 서비스를 제공받기 위해 특정 서비스 제공자로부터 최초 OTP 기기를 발급받게 된다. 이 사용자가 다른 서비스 제공자에서도 OTP 인증을 사용하기 위해서, 새로운 OTP 기기를 발급 받지 않고, 이미 발급받은 OTP 기기를 이용·등록하여 사용할 수 있다. 서비스 제공자는 사용자로부터 요청되는 OTP 인증을 중앙집중화된 해당 인증서버에 전달하여 처리한다. 따라서, 서비스 제공자는 자체적으로 OTP 인증 서버를 구축하지 않아도 강한 인증 서비스를 제공할 수 있게 된다.

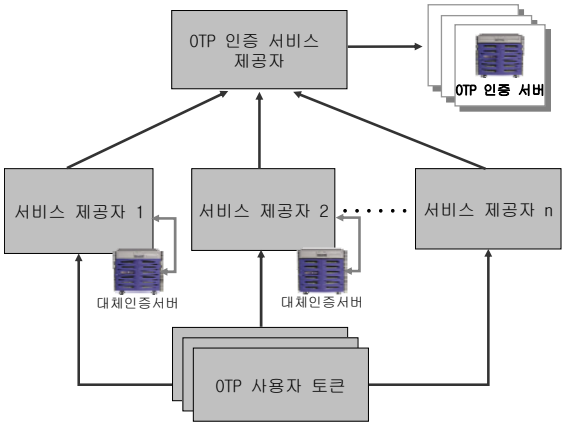


<그림 2> 상호운용관리 FW-중앙집중형 모델

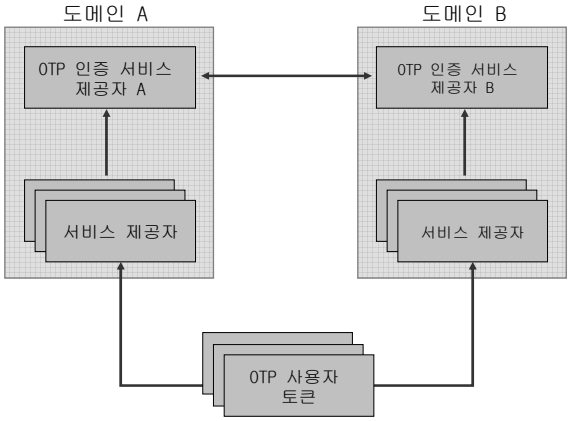
• 상호 운용 관리 프레임워크-확장된 중앙집중형 모델

OTP 중앙집중형 모델은 OTP 인증 서비스 제공자의 인증시스템 장애에 의존적인 영향을 받는다는 점이 가장 큰 문제점이다. 안정성 보장을 위해 OTP 인증 서비스 제공자의 모든 시설을 이중화 할 수 있지만, 그럼에도 불구하고 통신구간의 오류나 복구 불가능한 파손이 있는 경우 서비스 제공자는 서비스 중단이 될 수 밖에 없다. 따라서, 서비스 중단이 치명적인 손실을 주는 전자금융이나 전자결재 등의 특정 분야에서는 서비스의 안정적인 운영을 위해 대체방안을 <그림 3>의 확장형 중앙집중형 모델과 같이 확장할 수 있다.

확장된 중앙집중형 모델은 개별 서비스 제공자가 자체적으로 별도의 OTP 인증 시스템(대체인증서버)을 가지는 점만 제외하고는 OTP 통합인증 프레임워크와 동일한 구조를 가지고 있다. 별도의 OTP 인증 시스템은 서비스 제공자 자체에서 발급한 OTP 기기에 대해서 자체적으로 인증업무를 제공할 수 있다. 물론, 타 서비스 제공자가 발급한 OTP 기기를 등록하여 사용하는 경우에는 OTP 인증서비스 제공자의 인증서버를 통해 인증을 수행한다. 따라서, 개별 서비스 제공자의 별도 OTP 인증서버는 서비스 중단이 치명적인 응용분야 등에서 선택적으로 운용될 수 있다.



<그림 3> 상호운용관리 FW-확장된 중앙집중형 모델



<그림 4> 상호운용관리 FW-센터 간 통합인증 모델

• 상호 운용 관리 프레임워크-크로스 도메인 모델

크로스 도메인 모델은 다수개의 중앙집중형 모델 간에 연동을 지원할 수 있다. 여기서 각 도메인은 금융도메인, 전자정부도메인, 타국가의 특정 도메인 등의 예를 들 수 있다. <그림 4>와 같이 다수개의 중앙집중형 OTP 프레임워크에 가입된 사용자는 1개의 OTP 토큰을 가지고 모든 서비스 제공자에게 인증 서비스를 받을 수 있다.

크로스 도메인 프레임워크는 해당 도메인을 담당하는 OTP 인증서비스 제공자 간의 인증시스템 연동만으로 기존 시스템의 변경 없이 도메인 간 확장이 가능하다. 특히 해당 도메인 간의 서비스 요구사항 분석을 통해 상이한 보안 정책 및 수준이 존재할 경우는 사전에 도메인 간 보안 정책 협상과정을 필요로 한다.

이상에서 언급된 OTP 인증 모델을 통해서 서비스 프로바이더의 응용 특성, 서비스 모델, 사용자 요구사항에 따라 다양한 서비스 시나리오를 구현할 수 있다.

향후 전망

차기 회의는 9월에 개최될 예정이며, 이번 회의 결과를 통해 Q7/SG17로 OTP 인증서비스 관리 프레임워크(X.sap-3)로 최종 초안을 제출하고, 관련 표준화 기구들로 송부된 Liaison Statement로부터 의견을 수렴할 예정이다. 현재 진행 중인 표준화 아이템은 사용자 인증을 더 엄격하게 수행할 수 있도록 제공 및 관리하는 OTP 기반의 멀티팩터 인증 관리 프레임워크이다. 따라서 기존에 정의되어 있던 일반 인증 프레임워크와의 연동 관리 방안이 고려될 필요가 있으며, 관련 분야로서 아이덴티티 관리 프레임워크 및 생체인증 등의 멀티팩터 인증 프레임워크들의 표준 추진 현황도 주의 깊게 검토할 필요가 있다. 이는 강한 인증서비스(strong authentication)를 제공하기 위해서 신뢰성 있는 인증 서비스의 체계적인 관리 프레임워크 정의라는 측면에서 상관성에 대한 분석이 요구된다. 이와 관련하여 일본측에서는 차기 9월 회의에서 본 표준에 관련하여 범용 인증 관리 프레임워크(X.sap-4)에 대해 신규 아이템을 제안할 예정이며, OTP, 바이오인증, 및 PKI 인증 프레임워크와 아이덴티티 프레임워

크 간의 상호연동 및 관리 프레임워크 정의를 포함하고자 하는 목적을 가진다.

임형진 (금융보안연구원 OTP통합인증센터 선임연구원, hjlim@fsa.or.kr)