

일회용 패스워드(OTP) 통합인증 서비스 프레임워크



김근옥 금융보안연구원 인증서비스본부 선임연구원

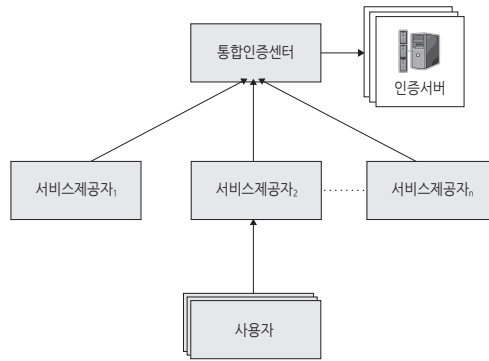
1. 머리말

일회용비밀번호(이하 OTP, one time password)는 거래 시마다 한 번만 사용할 수 있는 비밀번호를 매번 생성하여 인증함으로써 보다 안전한 전자거래가 가능하도록 하는 인증기술로 흔히 은행에서 발급받는 OTP 토큰을 통한 인증이 이에 속한다. OTP 토큰은 종류에 따라 토큰형과 카드형으로 구분할 수 있으며, OTP를 생성하는 방식에 따라 시도-응답방식, 시간동기화방식, 이벤트동기화방식, 시간-이벤트 혼합방식으로 나뉜다. 국내 인터넷뱅킹에서 흔히 사용되는 OTP는 시간동기화방식으로 보통 30초~1분에 한 번씩 OTP를 생성하고 이를 인터넷뱅킹 화면에 입력한 후 금융회사 또는 OTP 통합인증센터를 통하여 OTP의 유효성을 인증하는 방식이다. 물론 한번 사용한 OTP는 재사용이 불가하다.

2007년 OTP 통합인증센터는 OTP 통합인증 서비스를 개시하여 금융권역에 보다 안전한 인증

수단인 OTP의 도입을 촉진하고 전자금융거래의 보안성과 편의성을 향상하고자 하였다. OTP는 보안성이 매우 뛰어난 기술이기는 하나 실제 전자금융이용자가 사용하기 위해서는 인증수단의 배포·소지 등의 사용자 편의성 측면의 개선이 필요하다. 특히 여러 금융회사에서 거래하는 전자금융이용자의 경우 여러 개의 OTP 토큰을 소지·관리해야 하는 불편함이 따른다. 이를 개선하기 위하여 OTP 통합인증센터는 전자금융이용자가 하나의 OTP 토큰으로 여러 금융회사에서 OTP 인증서비스를 받을 수 있도록 OTP 통합인증서비스를 제공한다.

OTP 통합인증센터는 2009년부터 서비스를 통해 축적한 경험을 기반으로 전자거래환경의 보안성을 확보하기에 적합한 OTP 통합인증서비스 프레임워크와 관련된 국내의 표준화를 추진하였다. 같은 해 국내 표준안은 제정을 완료하였으며, 2011년 ITU-T



[그림 1] 통합인증센터 모델

X.1153 ‘Management framework of a one time password-based authentication service’가 국제 표준으로 등록되면서, 명실공히 국내·외에서 인정 받는 표준으로 자리매김하였다.

OTP 통합인증서비스 프레임워크는 OTP 통합 인증서비스를 위한 서비스 모델, 기능, 보안 고려 사항 등을 정의한다. OTP 통합인증서비스 모델은 사용자가 다수의 서비스 제공자로부터 서비스를 받을 수 있는 서비스를 기반으로 구성되기 때문에 반드시 통합인증센터가 필요한 모델이다. 서비스를 구성하는 방식에 따라서 3가지의 서비스 모델을 제시하고 각각의 기능 및 보안 고려사항을 정의 하기 때문에 적용환경에 따라 적합한 모델의 선택 적용이 용이하다.

2. OTP 통합인증서비스 모델

OTP 통합인증서비스 모델은 사용자가 다수의 서비스 제공자로부터 서비스를 받을 수 있는 모델로 서비스를 제공받는 사용자, 전자거래 서비스를 제공하는 서비스제공자 그리고 OTP 통합인증서비스를 제공하는 통합인증센터로 구성된다. OTP를 인증 하기 위해서는 별도의 인증서버가 필요한데, 인증

서버의 위치와 인증방법에 따라 OTP 통합인증서비스 모델을 다음의 3가지로 구분할 수 있다.

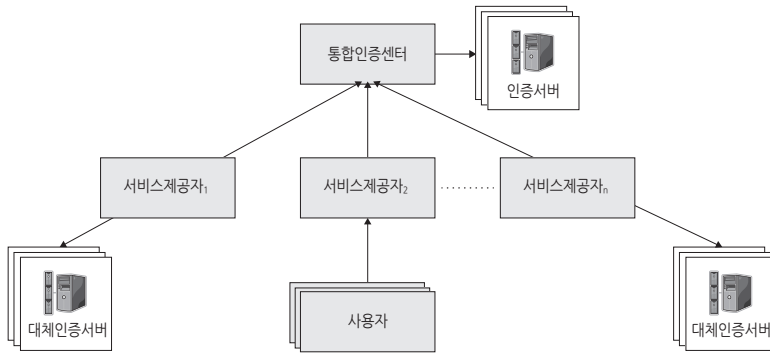
- 통합인증센터 모델
- 개선된 통합인증센터 모델
- 통합인증센터 간 연동 모델

국내 표준안에서는 통합인증센터 모델과 개선된 통합인증센터 모델을 센터 모델로, 통합인증센터 간 연동 모델을 센터 간 연동 모델로 정의하고 있다. 본 고에서는 ITU-T X.1153에서 정의한 것과 같이 센터 모델을 세분화하여 각각 3개의 서비스 모델로 설명한다.

2.1 통합인증센터 모델

통합인증센터 모델은 [그림 1]과 같이 통합인증센터를 중심으로 각각의 서비스제공자를 연결하고 OTP 인증은 통합인증센터를 통해서 이루어지도록 하는 가장 기본적인 모델이다.

서비스제공자는 사용자로부터 OTP 인증을 요청 받으면 해당 인증정보를 통합인증센터로 전달하고, 통합인증센터는 서비스제공자를 대신하여 OTP를 인증하는 역할을 수행한다. 그렇기 때문에 서비스



[그림 2] 개선된 통합인증센터 모델

제공자는 별도로 인증서버를 구축하지 않아도 OTP 서비스를 제공가능하며, 사용자는 하나의 OTP 토큰을 여러 서비스제공자에게 이용 등록하여 여러 서비스제공자로부터 OTP 인증서비스를 제공받을 수 있다.

통합인증센터는 서비스제공자가 선택한 다양한 종류의 OTP 토큰을 지원하기 위해 센터 내 수용 가능한 OTP 인증기술을 통합하여 인증서버를 구축해야 한다. 통합인증센터는 모든 인증 요청을 중앙 집중적으로 관리하므로 신뢰된 자에 의해 운영되어야 하며, 서비스제공자가 서로 경쟁하는 경우가 많기 때문에 가입된 서비스제공자와 이해관계가 없는 제3자에 의해 관리되어야 한다. 또한, 통합 인증센터의 보안 취약점으로 피해가 발생된 경우, 피해의 파급이 전체 서비스제공자에게 영향을 미치므로 안정적인 보안운영은 필수적이다. 또한, 일단 구축된 통합 인증 센터는 서비스제공자의 요구 사항에 따라 업무나 제공되는 서비스 변경이 어려우므로 표준화된 기술에 의해서만 서비스가 가능하도록 구성하여야 한다.

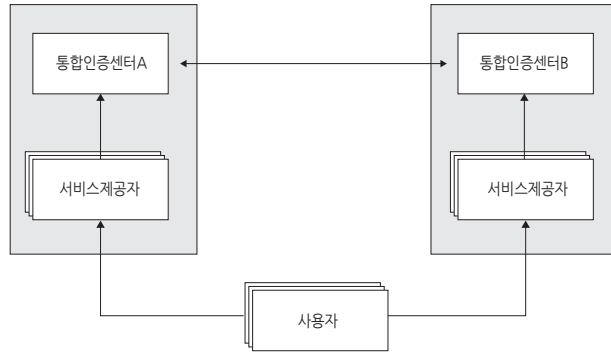
통합인증모델의 장점은 서비스제공자가 인증 서버를 구축하지 않아도 OTP 인증을 제공할 수 있다는 것으로 서비스제공자는 구축비용을 절감할 수

있으며, 통합 인증 센터가 지원하는 다양한 종류의 OTP 기기를 모두 사용할 수 있다. 사용자의 입장에서는 다수의 서비스제공자에 가입되어 있는 경우, 1개의 OTP 기기로 여러 서비스 제공자의 서비스들을 공통으로 사용할 수 있어 편의성 측면이 우수하다.

2.2 개선된 통합인증센터 모델

통합인증센터 모델은 모든 서비스제공자가 OTP 인증요청 및 상태확인을 통합인증센터에 중앙집중적으로 요청해야 하기 때문에 통합인증센터에 장애가 발생하는 경우 연결된 모든 서비스제공자에게 영향을 주어 서비스 장애가 발생할 수 있는 단점이 있다. 따라서 이러한 문제점을 보완하고 서비스의 안정성을 향상시키기 위해, 서비스 중단이 치명적인 서비스제공자의 경우 대체인증서버를 서비스제공자 내부에 선택적으로 구축 가능한 모델이 [그림 2]의 개선된 통합인증센터 모델이다.

통합인증센터에 위치한 인증서버와 동일한 인증업무를 수행하는 대체인증서버는 서비스제공자가 발급한 OTP 토큰에 대해서는 자체적으로 인증업무를 제공할 수 있지만, 타 서비스제공자가 발급한 OTP 토큰을 등록하여 사용하는 경우에는 통합인증센터 내의 인증서버를 통해 인증해야 한다.



[그림 3] 통합인증센터 간 연동 모델

또한, 대체인증서버가 구축되어 있는 경우, 사용자는 서비스제공자 내부의 대체인증서버를 통해 OTP 인증 요청을 할 수 있고, 통합인증센터의 인증서버를 통해서도 OTP 인증 요청을 할 수 있기 때문에, 2개의 인증서버에서 각각 OTP 인증 요청이 성공한다면 동일한 OTP가 각각의 서버에서 인증 성공으로 될 수 있는 문제점이 있다. 따라서 이를 방지하기 위해서 서비스제공자는 대체인증서버를 구축할 경우, 통합인증센터의 인증서버와 대체인증서버 간의 인증정보를 실시간으로 동기화하도록 시스템을 구축해야 하며 내부적으로 OTP 인증 요청에 대한 감사정보를 기록하여야 한다. 실시간 동기화 문제는 시스템 구성을 복잡하게 하기 때문에, 대체인증서버를 구축할 때 장·단점을 비교할 필요가 있다.

2.3 통합인증센터 간 연동 모델

서로 다른 도메인에 존재하는 OTP 통합인증센터 간의 연동은 기존 시스템의 변경 없이 가능하다. 즉, [그림 3]에서 A 도메인에 있는 통합인증센터 A는 B 도메인의 서비스 요구 사항 및 보안정책 등을 분석하여 OTP 토큰을 B센터에서도 사용할 수 있도록 허용할 경우에, 센터 등록 기능을 통해 OTP 통합인증센터B와 연동 절차를 수행하면 된다. 만약 도메인

간의 OTP를 발급하기 위한 서비스 요구 사항(예: 신원 확인 방식 등)이 다르다면 서비스 연동은 제한적으로 이루어져야 한다. 즉, 보안 강도가 높은 도메인에서 보안 강도가 낮은 도메인으로의 연동은 가능하지만, 그 반대의 경우는 연동하지 않는 등의 정책적 판단이 중요하다.

사용자가 한 도메인에서 발급한 OTP 토큰을 다른 도메인의 서비스제공자에서 사용하고자 할 때에는 OTP 등록 과정에서 OTP 토큰을 발급했던 도메인을 통합인증센터에 알리고 통합인증센터는 서비스 요구 사항에 따라 미리 등록된 도메인일 경우 등록을 허용하는 방식으로 서비스 제공이 가능하다.

3. OTP 통합인증서비스 기능

OTP 통합인증서비스의 기능은 <표1>과 같이 기본적으로 인증, 발급, 재발급/갱신, OTP 상태 관리, 보정, 오류 건수 초기화, 조회, 기기 등록, 타 기관 이용 등록, 타 기관 이용 등록 해지 등의 기능이 요구되며, 개선된 통합인증 모델은 동기화, 통지, 기기 이관 기능이 통합인증센터간 연동 모델은 센터등록 기능이 추가적으로 필요하다.

<표 1> OTP 통합인증서비스 기능

모델		기능	설명
센터간연동모델	개선된 통합인증센터 모델	인증	사용자가 OTP 검증을 요청할 경우 검증서버를 통하여 OTP의 유효성을 검증하는 기능
		발급	OTP 사용자가 OTP 토큰을 발급받는 기능으로, 서비스제공자를 방문하여 신원확인 후 OTP 토큰을 발급받음
		재발급	OTP 토큰이 유효기간 이내에 분실 또는 파손 등의 사유로 신규로 발급받기 위한 기능으로, 발급과 마찬가지로 서비스제공자를 방문하여 신원확인 후 OTP 토큰을 재발급받음
		갱신	OTP 토큰의 유효기간이 만료되어 갱신하기 위한 기능으로, 발급과 마찬가지로 서비스제공자를 방문하여 신원확인 후 기존 OTP 토큰을 반납하고 신규 OTP 토큰을 교체 발급받음
		상태관리	사용자가 OTP 상태변경을 요청할 때 서비스제공자가 이를 반영하는 기능을 의미하며, OTP 사고 신고 및 사고회복, 하드웨어 PIN을 사용하는 OTP 토큰의 경우 H/W PIN 번호 잠금 해제, 폐기 등이 이에 속함
		보정	사용자의 OTP 토큰과 인증 서버 간에 동기화 정보(예, 시간, 이벤트 카운트 정보 등)를 보정하는 기능
		오류건수 초기화	OTP의 누적 오류가 일정횟수(예, 10회) 이상 초과로 OTP 토큰의 사용이 금지된 경우 오류 건수를 초기화 하는 기능
		조회	OTP 관련 정보를 조회하는 기능으로 사용자별 OTP 리스트 조회, OTP 토큰별 이력 및 상태조회(발급, 사고신고, 폐기 등), OTP 토큰 오류횟수 조회, OTP 토큰 상세조회 등이 포함됨
		기기등록	OTP 토큰을 신규로 발급하기 전에 미리 일괄 등록하는 기능
		타 기관 이용등록	OTP 토큰의 발급기관이 아닌, 타 기관의 서비스제공자를 통해 동일한 OTP 토큰으로 서비스를 제공받고자 하는 경우 타 기관이용을 등록하는 기능
		타 기관 이용등록 해지	타 기관 등록하여 사용하던 OTP 토큰의 이용을 해지하기 위한 기능
		동기화	대체인증서버가 구축된 서비스제공자와 통합인증센터의 인증서버 간의 OTP 운영 관련 정보를 동기화하는 기능
		통지	타 기관 등록하여 사용하는 OTP 토큰의 경우 다른 기관을 통하여 OTP를 인증하거나 상태 변경 등의 업무를 처리한 경우 발급기관(OTP를 발급한 서비스제공자)에게 통지하는 기능
		기기기관	OTP 인증서버를 자체 운영하던 서비스제공자가 통합인증센터를 통한 통합인증서비스를 받고자 한 경우 기발급한 OTP 토큰을 등록하는 기능
		센터 등록	서로 다른 도메인에 있는 OTP 센터 간의 연동을 제공하기 위해 필요한 기능으로, 사전에 서비스 제공 범위 및 보안정책 등을 서로 합의한 후에 통합인증센터목록 등에 OTP 센터코드 등록

<표 2> 보안 고려사항

구분	설명
안전한 통신망	OTP를 전송하기 위해 사용되는 통신망은 상호 인증과 기밀성, 무결성을 제공하는 안전한 통신망을 이용해야 함
키 등록 및 발급 절차	OTP 서비스제공자는 OTP 등록, 발급, 갱신, 폐기 절차를 위한 동일한 수준의 보강정책을 수립하고 공통적으로 운영해야 함
OTP 동기화 절차	내부적으로 대체인증 서버를 구축해 운영하는 OTP 서비스제공자는 통합인증센터의 인증서버와 실시간으로 OTP 인증정보를 동기화하도록 시스템을 구축해야 함
통합인증 프레임워크 간 상호 합의된 보안정책	서로 다른 도메인간에 OTP 통합인증 서비스를 제공하기 위해서는 사전에 서로 합의된 보안정책과 OTP 인증 절차에 따라 동등한 수준의 보안을 유지하면서 서비스를 운영해야 함
보정 정책	OTP 토큰의 진동자, 배터리 잔량 정도 사용자 조작 등에 의해서 인증서버와 사용자가 가지고 있는 OTP 토큰 간의 동기화 인증정보 차이가 발생할 수 있어, 적절한 보정 정책을 유지해야 함

4. 보안고려사항


OTP 통합인증서비스의 구축 및 운영 시 서비스의 안전성 향상을 위하여 <표 2>와 같이 안전한 통신망, 키 등록 및 발급 절차, OTP 동기화 절차, 통합인증 프레임워크 간 상호 합의된 보안 정책, 보정 정책 등의 보안고려사항을 참고할 수 있다.

5. 맺음말

전자거래환경의 보안 위협이 날로 증가하고, 해킹 기술이 고도화되면서 전자거래의 안전성 확보를 위한 다양한 인증기술에 대한 연구가 활발히 진행되고 있다. 안전한 인증기술은 전자거래의 매우 중요

한 요소이지만, 그만큼 중요한 것이 인증기술을 안전하게 운영·관리하는 것이다.

OTP 통합인증서비스 프레임워크는 현재 국내 전 금융권역에 적용되어 서비스되고 있는 OTP 통합인증센터 모델을 표준화한 것으로, OTP 인증기술뿐만 아니라 인증서비스를 운영·관리하면서 습득한 노하우를 바탕으로 개발되어 국제적으로 인정받은 실용표준이라는 점에서 그 의미가 있다고 하겠다.

국내에서는 금융권 이외에도 공공·의료 등 타 권역에서도 보다 안전한 OTP 인증서비스를 위하여 해당 표준안을 활용 가능할 것으로 기대되며, 더 나아가 국내·외 전자거래의 안전성 확보와 사용자 편의성 증대를 위한 다양한 서비스에 활용이 가능할 것으로 기대된다. 

정보통신 용어해설

사이버레이션 Cyberlation [관리운용]

사이버 공간에서의 만남과 관계.

'사이버'(cyber)와 관계를 뜻하는 '레이션' (relation)의 합성어로 카페와 미니홈피, 블로그, 소셜네트워크서비스(SNS)와 같이 우리 삶 속에 깊숙이 들어온 인터넷이 사람과 사람 사이의 관계에 중요한 역할을 하고 있는 현상을 의미한다. 비대면적인 사이버 공간에서의 폭넓고 다양한 색다른 인간관계를 체험할 수 있으나 상호 믿음에 바탕을 둔 깊이 있는 만남을 하기에는 한계가 따른다.

