AutoPassword™

WHITE PAPER

AutoPassword™ 란?

VERSION: 2.0

작성일: 2021년 3월 3일

작성자:
우종현, CEO
+82-10-3386-4017
jhwoo@dualauth.com

목차

DualAuth 간략 소개

저희 회사는 온/오프라인 상호인증 및 출입관리 기술을 개발하였습니다. 이는 사용자가 코드를 제공하기 전에 온/오프라인 서비스 제공자의 진위 여부를 확인할 수 있는 최초의 상호 인증 기술입니다. 상호 인증을 통한 이중 보안과 편리한 사용성 덕분에 단기간에 아래와 같은 결과를 얻었습니다.

1. 주요 기술 업적 Top 5

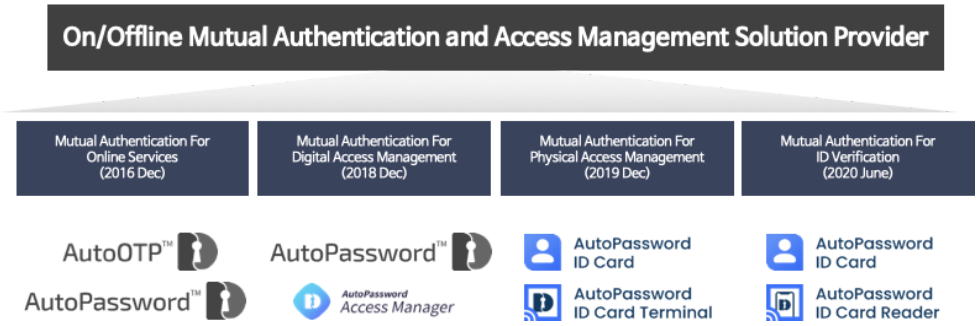
1. IBM 보안 파트너
2. 가트너 주식회사에서 “균형 잡힌 인증 기술”로 지정
3. London Fintech Innovation Awards Top 5 최종우승
4. 대한민국 인터넷 대상수상
5. The international standards body and trade institution for authentication (Oath and FIDO Association) 에서 기술 인증

2. 주요 고객 Top 5

1. 우리은행
2. 청와대
3. Online Privacy Association in Korea
4. 동두천시
5. VP (국내 No.1 온라인 신용카드 결제인증업체)

3. 주요 제품라인

1. AutoOTP
2. AutoPassword
3. AutoPassword Access Manager
4. AutoPassword ID Card & Reader
5. AutoPassword Terminal



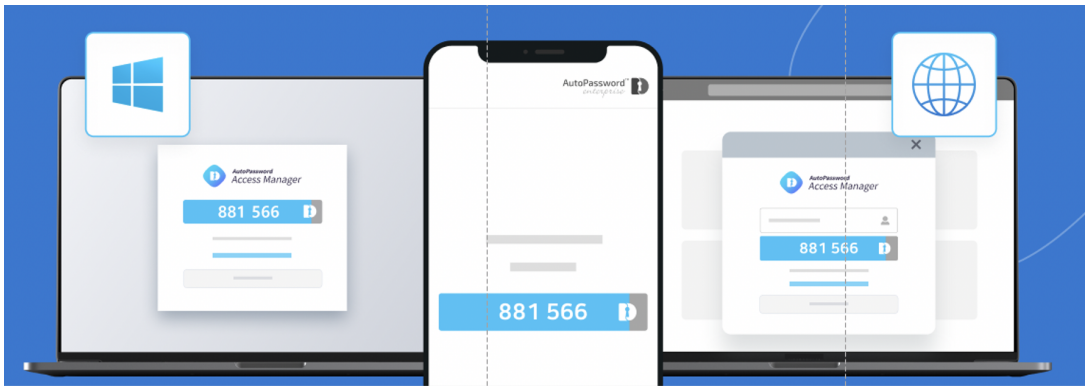
AutoPassword와 AutoPassword ID 카드의 기술 차이점

1. 유저친화적 기술 인증

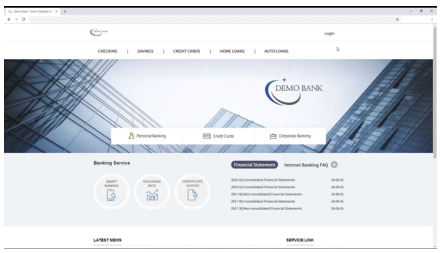
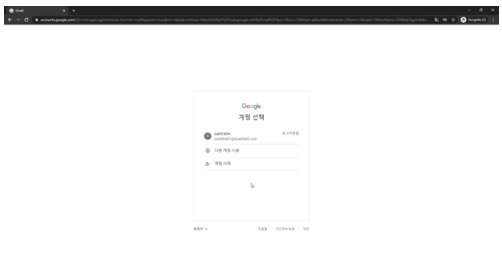
많은 이들은 온라인 서비스에 액세스할 때 사용자 암호를 기억하고 입력하는 것을 싫어하여 사용자 암호를 업데이트하지 않습니다.

사용자들에게 강력한 사용자 암호를 기억하고 관리하도록 요구하는 대신, 저희는 온라인 서비스에서 제공하는 자동 암호를 사용하여 사람들이 암호를 필요하지 않게 되도록 바랍니다.

기존 시스템은 사용자에게 온라인 서비스에 사용자 암호를 제시하도록 요청하고 온라인 서비스는 사용자가 제시한 사용자 암호를 확인합니다. 그러나 AutoPassword를 사용하면 사용자는 온라인 서비스에서 제공하는 자동 암호를 스마트폰의 코드로 확인합니다.



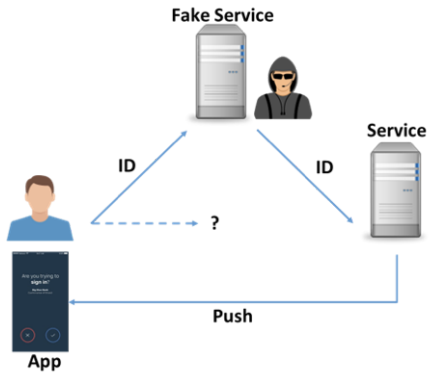
사용자의 역할을 입력에서 확인으로 변경하여 사용자를 비밀번호 부담에서 해방시킵니다. 이것은 컴맹과 기억력이 좋지 않은 사람들에게 반가운 소식입니다.

온라인 서비스 로그인 데모	타 서비스 로그인 데모 (Gmail)
https://youtu.be/zNMKlIyJ4uU	https://youtu.be/l5H1C9gz7tg
	

2. 상호인증 기술

1961년 최초의 컴퓨터가 등장한 이래로 다양한 인증 기술은 사용자의 신원만 확인하는 방식을 사용하고 있습니다.

지난 60년 동안 ICT와 사이버 범죄는 빠르게 성장했습니다. 가장 많이 사용되는 사이버 공격 중 하나는 피싱 및 가짜 사이트입니다. 비밀번호가 도용되었다는 사실을 모르고 같은 유형의 비밀번호를 계속 사용하면 문제에 직면하게 됩니다. 동일한 디자인의 가짜 온라인 서비스를 연결하면, 일반적으로 사용자 자격 증명을 입력합니다. 문제는 전용 인증 기술 때문입니다. 푸시 기반 모바일 인증 기술을 사용해도 문제는 동일합니다. 아래 다이어그램을 참고하세요.

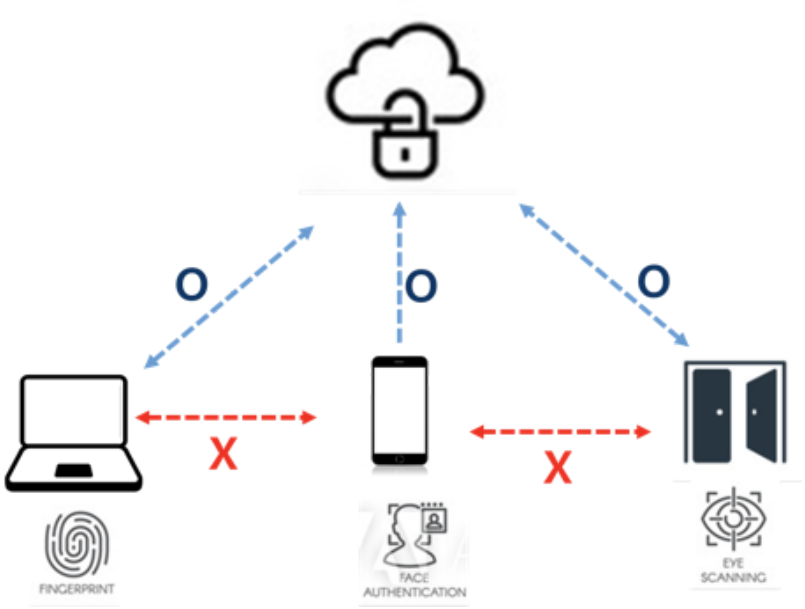


AutoPassword는 사용자가 온라인 서비스의 진위 여부를 눈으로 확인할 수 있는 최초의 기술입니다. 또한 온라인 서비스는 사용자가 두 코드가 일치하는 것을 확인하면 사용자의 진위를 확인합니다.

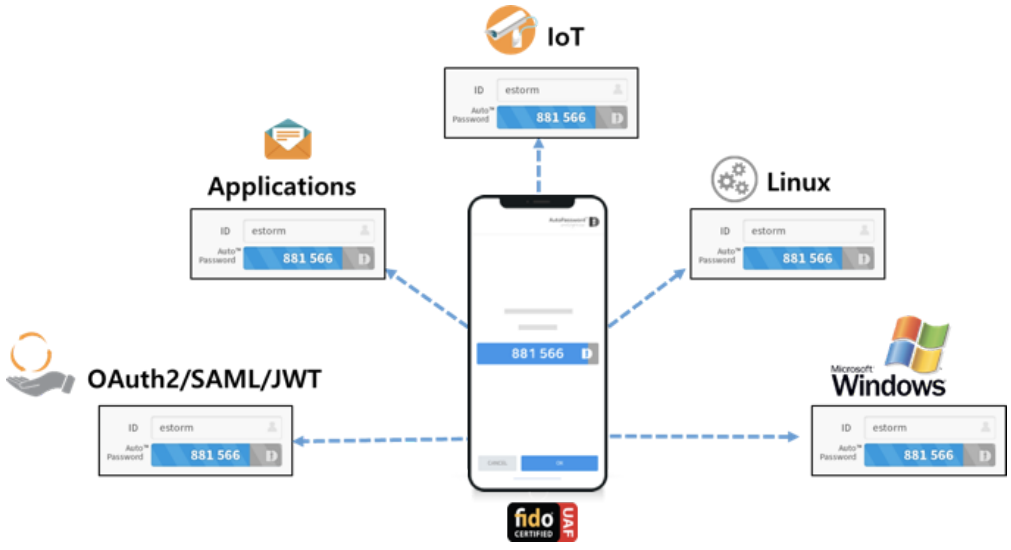
이 시스템은 현재 사용자 인증 기술을 무시하지 않습니다. OTP, PKI, FIDO 생체인식 등 동일한 사용자 인증 기술을 사용하여 서비스의 인증을 확인한 후 합니다.

3. 크로스오버 생체인증 기술

AutoPassword는 FIDO(Fast IDentity Online) Alliance에서 인증한 생체 인식 기술을 사용합니다. 그러나 AutoPassword는 사용자 전용 인증을 위한 기존 생체 인식 기술과 다릅니다.

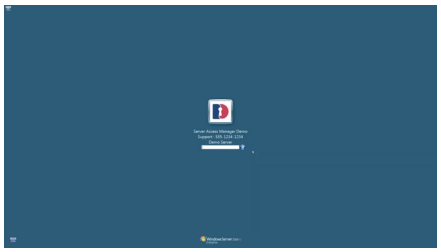


기존 생체 인식 기술은 사용자가 생체 인식을 등록하는 장치에서 실행되는 응용 프로그램에서만 작동합니다. 따라서 스마트폰에 등록된 생체 인식을 PC나 AI 스피커에서 실행되는 애플리케이션에 사용할 수 없습니다. 이 때문에 생체 인식을 인증하려는 모든 장치에 생체 인식을 다시 등록해야 합니다.



AutoPassword를 사용하면 모든 장치에서 생체 인식을 다시 등록할 필요가 없습니다.

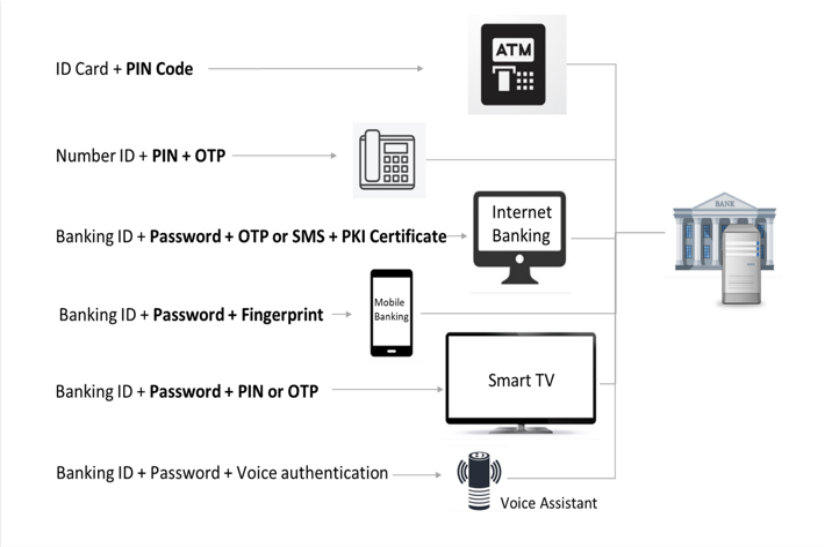
스마트폰에서 자동코드를 제시하면 기기별로 생체인식을 사용할 수 있습니다. AutoPassword는 스마트폰의 생체 인식을 생체 인식을 등록하지 않은 장치에 논리적으로 연결합니다.

윈도우 로그인 데모	리눅스 로그인 데모
https://youtu.be/cjmjBDwgw00	https://youtu.be/FDt0i06otUI
	

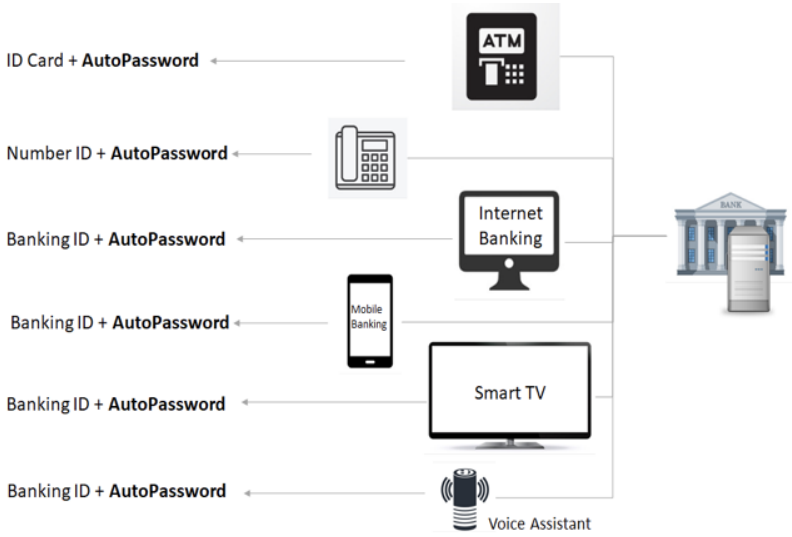
4. 옴니채널 인증기술

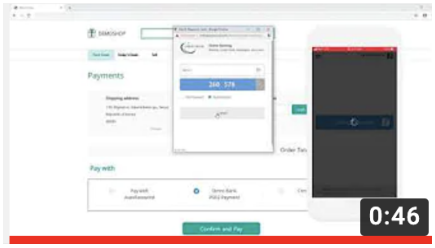
서비스 채널 추가시 더 많은 인증 방법이 필요합니다. 키오스크나 ATM은 카드&핀코드, 모바일은 얼굴인식 또는 지문, 스마트TV는 SMS코드나 핀코드, AI스피커는 음성인증이 필요합니다.

추가 서비스 채널이 추가됨에 따라 장치에 따라 더 많은 인증 방법이 필요합니다. 일을 단순화하려면 틀 밖의 생각을 해야합니다. 사용자 제시 자격 증명을 사용하는 대신 서비스 제시 코드를 사용하여 생활을 단순하게 만들 수 있습니다.



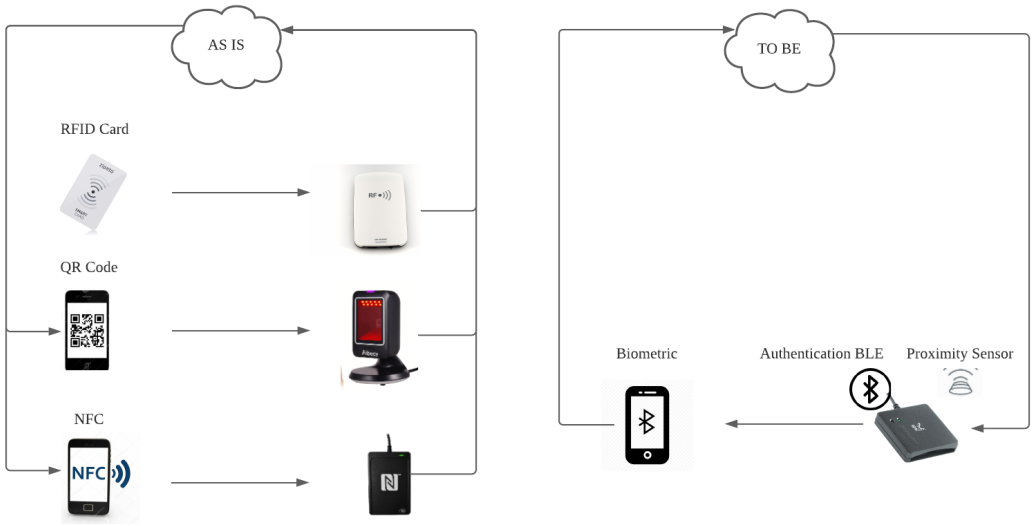
사용하는 서비스 채널이 무엇이든, 서비스에서 제공하는 AutoPassword를 사용하여 서비스에서 제공하는 숫자와 스마트폰에 있는 숫자 사이에 두 숫자가 일치하는지 비교합니다.



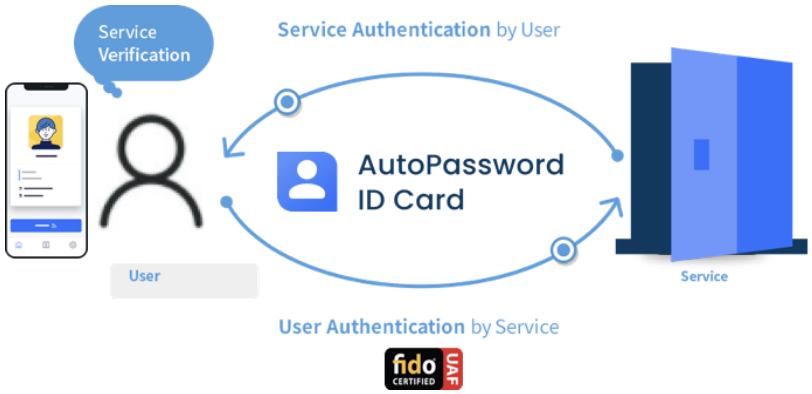
ATM 데모	오픈뱅킹 데모
https://youtu.be/ytJvOE3f-8k	https://youtu.be/C0rQyXE_3VQ
	

5. 온/오프라인 가능 인증기술

온라인 서비스를 위한 서비스 제시 AutoPassword 기술을 개발한 후 오프라인 서비스에도 동일한 개념을 적용했습니다. 마그네틱 스트립, 바코드, QR 코드 및 RFID 칩과 같은 사용자 ID 카드 기술을 제시합니다—이 방법은 모두 사용자의 진위를 확인합니다. 발표자에서 심사위원으로 사용자의 역할을 대체함으로써 우리는 우리의 삶을 더 쉽게 만듭니다. 아래 다이어그램을 확인하십시오. 인증 방향을 AS IS에서 To BE로 변경함으로써 사용자는 인증 방식을 하나의 모바일 앱으로 쉽게 결합할 수 있습니다. 예시: 사용자는 AutoPassword ID 카드 앱으로 자동문 및 조명과 같은 전기 설비를 제어할 수 있습니다.



60초마다 1회 코드가 바뀌는 인증된 블루투스 주파수인 비콘(Beacon)을 사용하기 때문에 사용자는 시설의 진위를 확인할 수 있고 관리자는 사용자가 시설 앞에 있는지 확인할 수 있습니다.



AutoPassword ID 카드는 또한 접촉 및 비접촉 방식을 지원합니다. 따라서 사용자는 비접촉 방식으로 2m, 접촉 방식으로 1cm 떨어진 상태에서 시설을 제어할 수 있습니다. 접촉 방식은 NFC처럼 작동하지만 뒷면뿐만 아니라 사용자가 스마트폰의 양면을 터치면으로 사용할 수 있도록 해줍니다.

접촉 방식 데모	비접촉 방식 데모
https://youtu.be/cqWf8bZtdSk	https://youtu.be/oOIUkjsTlZw