DualAuth

제로트러스트를 위한 패스워드리스 기술

AutoPassword 제품소개서

DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

04

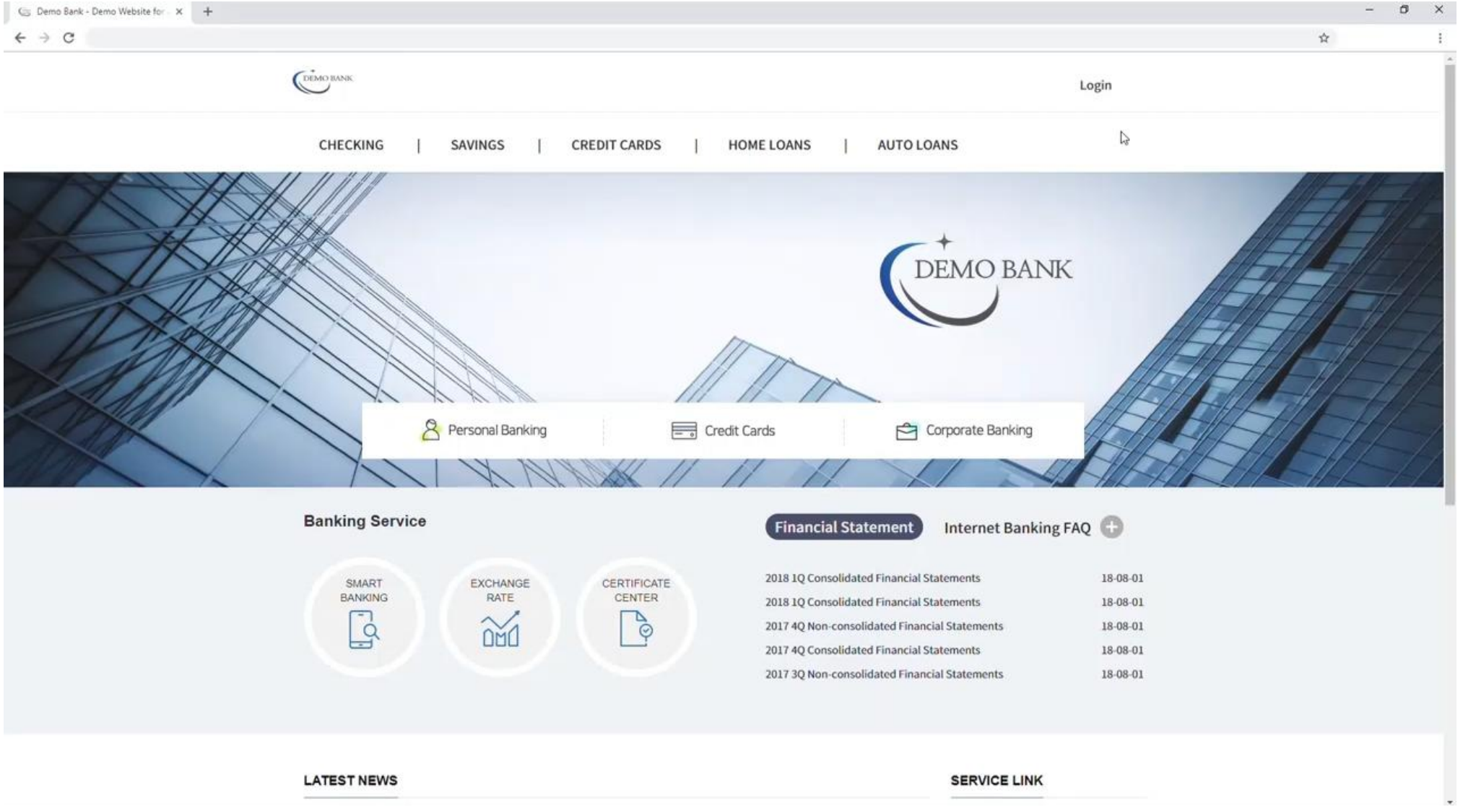
회사소개

Passwordless 인증기술

AutoPassword

패스워드리스 솔루션인 AutoPassword는 사용자가 패스워드를 입력하는게 아니라 온라인 시스템이 사용자에게 자동패스워드를 제시하고 사용자는 스마트폰으로 온라인 시스템이 제출한 자동패스워드를 확인하는 상호 인증 기술입니다. (국제표준 X.1280)

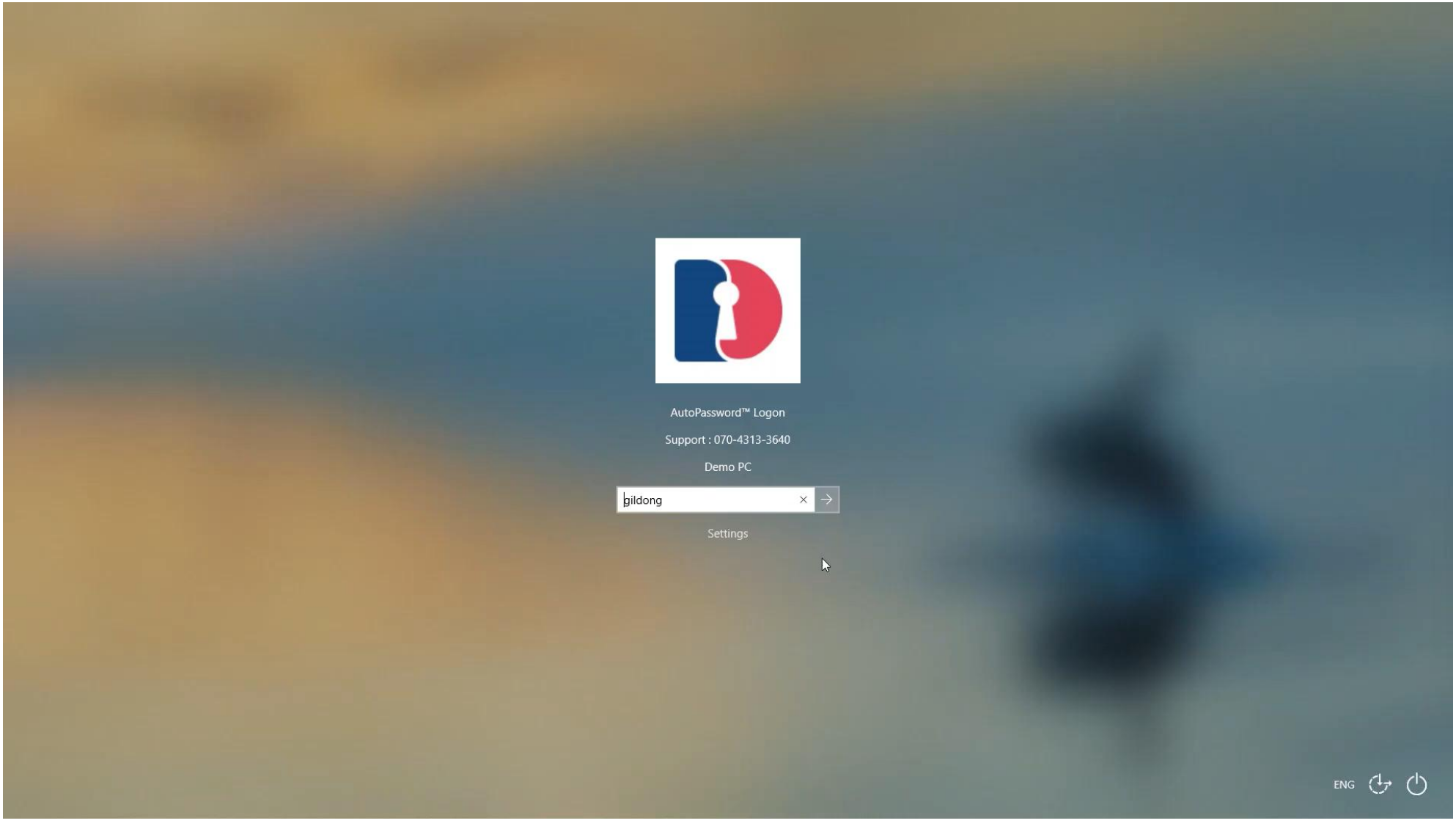
01 제품 개요



https://youtu.be/ejT8qU36OMw

https://youtu.be/ebN2kTGZIRE

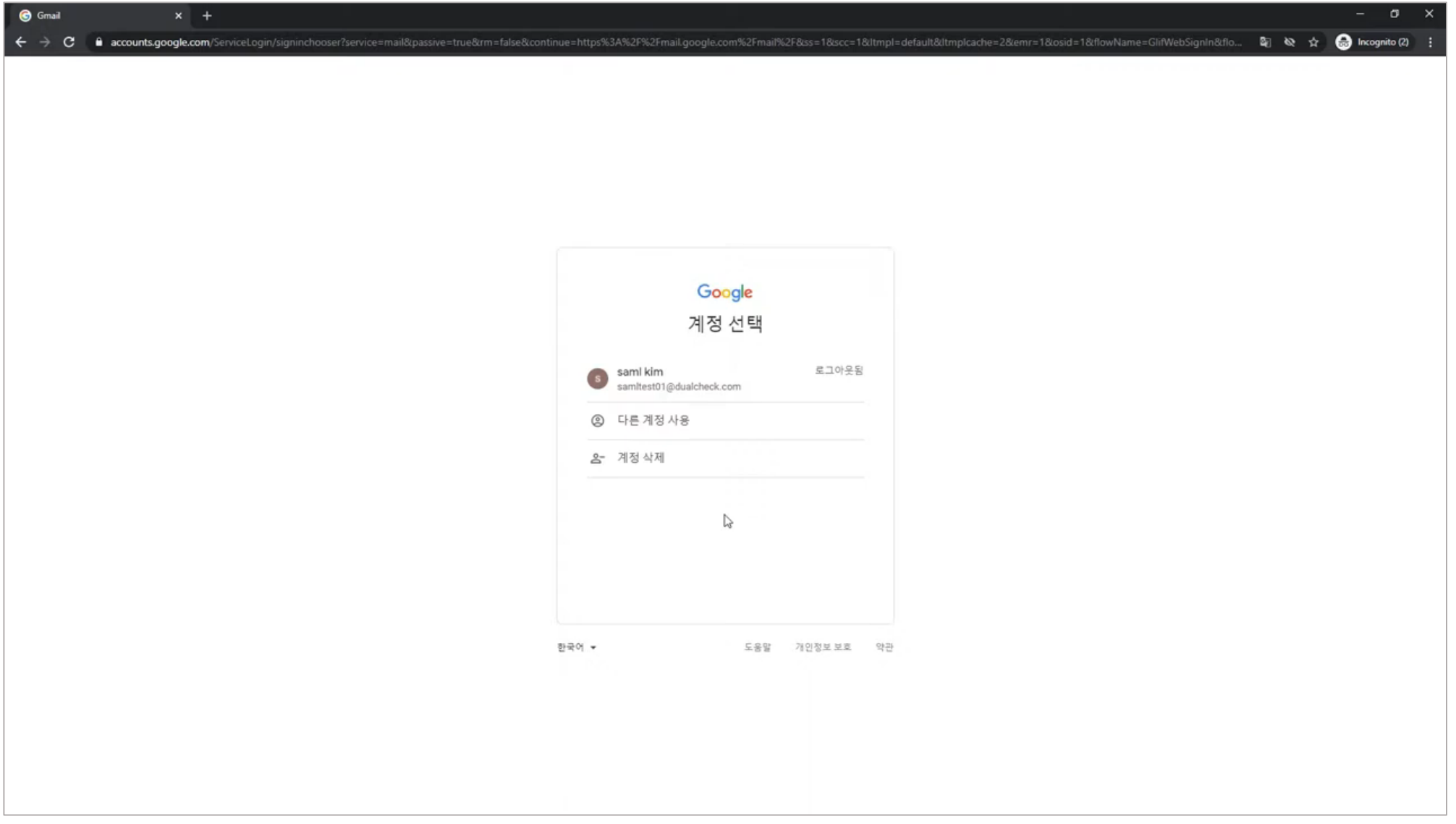
01 제품 개요



https://youtu.be/cjmjBDwgw00

https://youtu.be/FDt0i06otUI

01 제품 개요

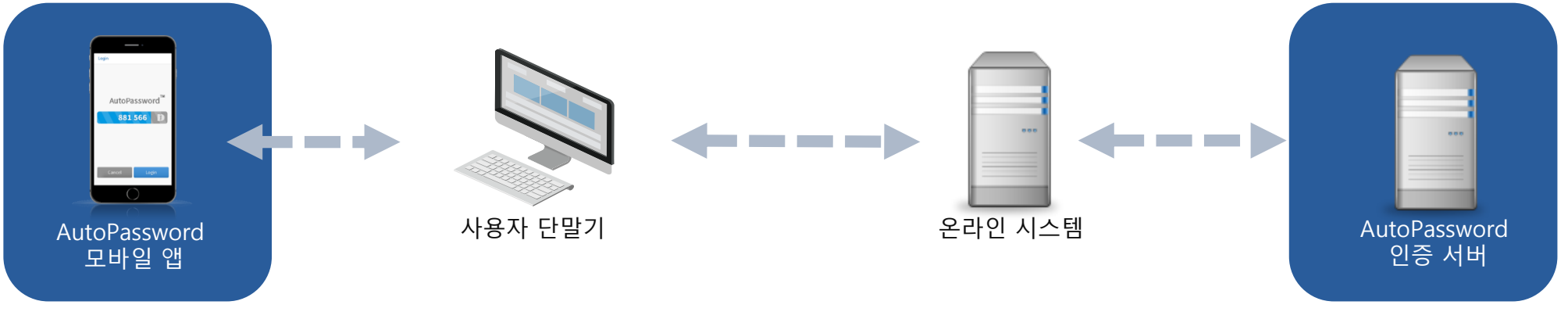


https://youtu.be/l5H1C9gz7tg

AutoPassword 아키텍처

AutoPassword로 전환하기 위해서는 기존 온라인 시스템에 AutoPassword 인증서버와 AutoPassword 모바일 앱을 추가하면 됩니다. 기존 서비스 구조를 크게 변경하지 않으면서도 안전하고 편리한 인증 환경을 구축할 수 있습니다. 관리자는 먼저 AutoPassword 인증서버를 설치한 후, 온라인 시스템과 인증서버 간의 통신을 가능하게 하도록 AutoPassword API를 연동합니다. API 연동은 서비스에서 자동패스워드가 표시되도록 하는 설정입니다.

사용자는 앱스토어에서 AutoPassword 모바일 앱을 설치해야 합니다. 앱 설치 후에는 본인확인 절차를 거쳐 해당 사용자의 계정과 모바일 앱을 연결합니다. 이 과정에서 사용자의 ID와 앱이 인증서버에 등록되며, 이후 해당 사용자는 등록된 스마트폰에서 자동패스워드 확인 및 대역외 생체인증을 통해 안전하게 온라인 시스템에 접속할 수 있습니다.



DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

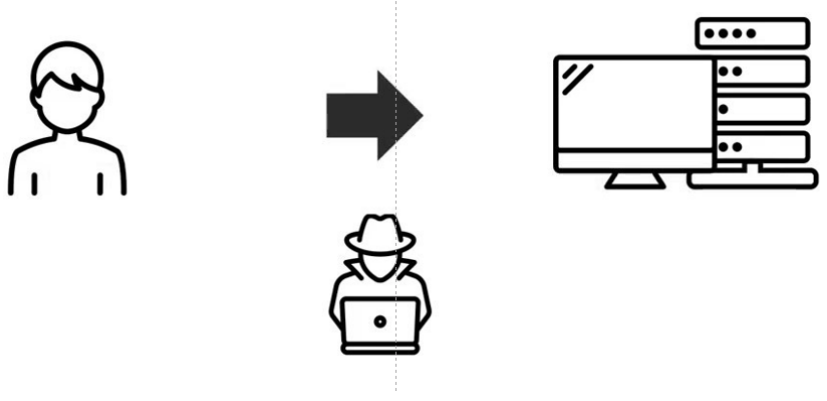
04

회사소개

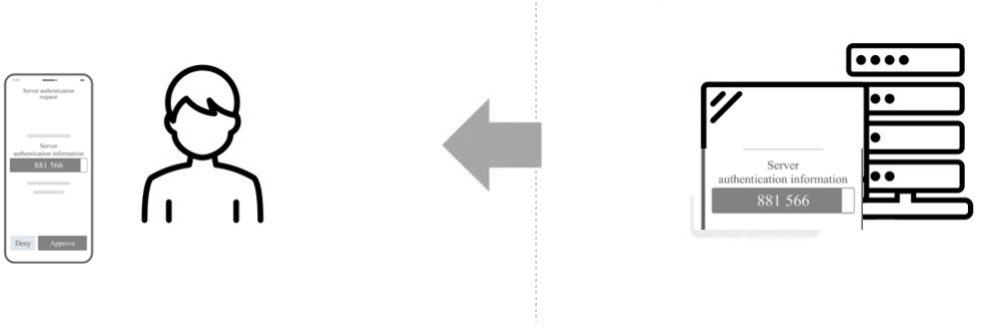
특징 1 – 피싱, 파밍, 중간자 공격에도 안전한 인증 기술

AutoPassword는 사용자가 직접 패스워드를 입력하는 방식이 아니라, 온라인 시스템이 자동패스워드를 생성·출력하고 사용자가 이를 검증한 뒤, 스마트폰 통신을 통해 사용자 인증값을 온라인 시스템에 전달하는 방식입니다.
이러한 구조 덕분에 인증 과정에서 사용자의 단말기에 패스워드나 인증값이 입력·저장되지 않으며, 그 결과 피싱, 파밍, 중간자 공격 등 기존 방식에서 발생하던 인증정보 탈취 시도가 원천적으로 무력화됩니다.

탈취나 도용 가능한 입력기반의 인증기술



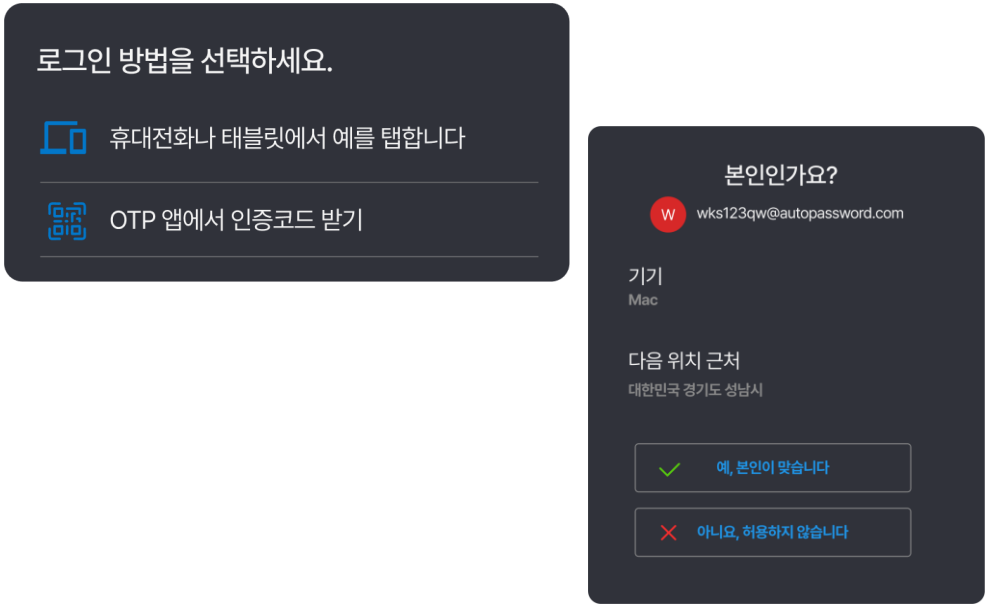
탈취나 도용이 불가능한 출력기반의 인증기술



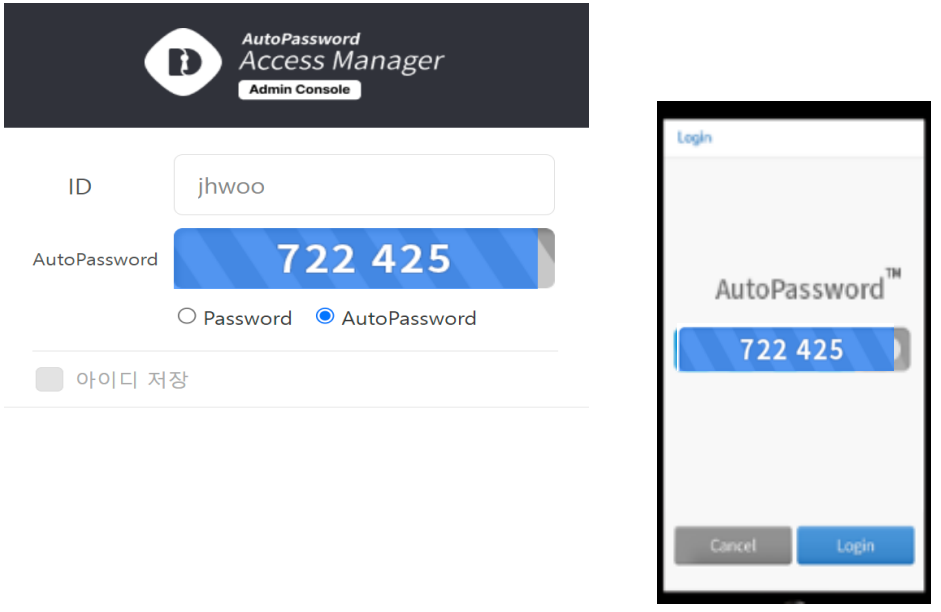
특징 2 – 모바일 상호인증 기술

기존의 모바일 인증 기술은 사용자를 확인하는 인증기술로, 푸시 알림이나 문자 메시지를 사용자의 스마트폰으로 전송하고, 사용자가 이를 확인·승인하는 방식입니다. 모바일 사용자 인증 방식은 사용자가 '정당한 모바일 인증기'를 소지하고 있는지만 확인할 뿐, 사용자가 접속한 서비스가 실제 정상 시스템인지 여부를 검증하지 않습니다. 그 결과, 사용자가 접속한 대상이 피싱 사이트나 위장된 시스템인 경우에 무심코 인증 요청을 승인하게 되어 인증이 도용될 수 있습니다. 그에 반해 AutoPassword는 모바일을 이용하지만 접속한 시스템을 먼저 확인할 수 있는 상호인증 기술입니다.

사용자만 인증하는 모바일 인증기술



온라인 시스템과 사용자를 동시에 인증하는 모바일 상호인증 기술

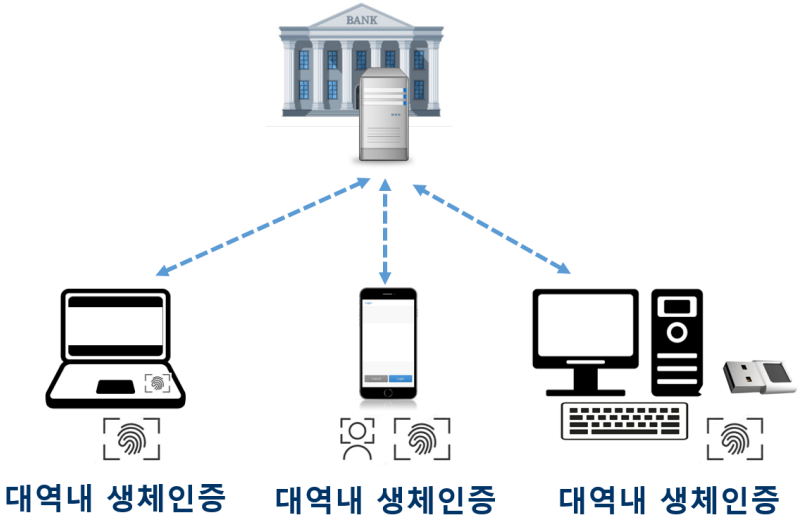


특징 3 – 가장 경제적인 생체인증 기술

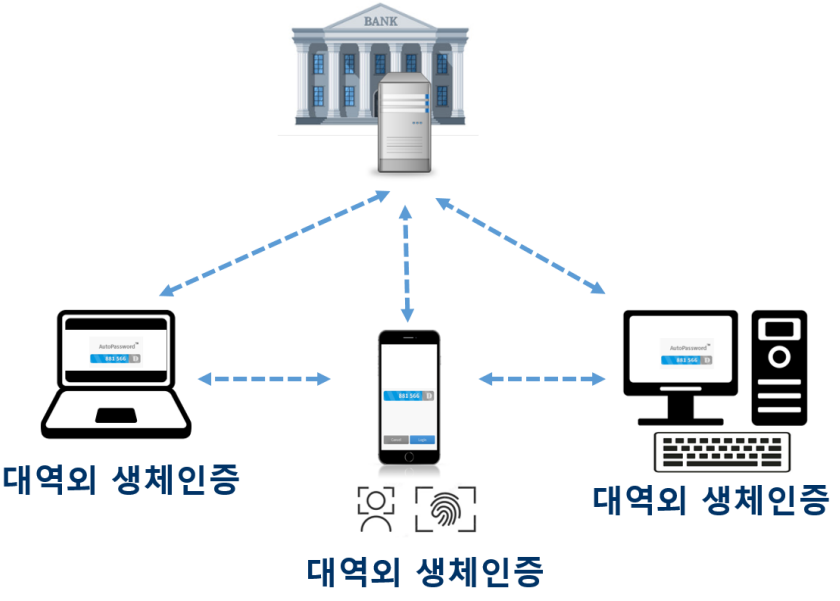
기존 FIDO나 Passkey와 같은 생체인증 기술은 '대역내(in-band) 생체인증' 기술로, 인증을 수행하는 각 사용자 단말기에 반드시 생체인증 센서가 장착되어 있어야 합니다. 스마트폰에는 기본적으로 지문·얼굴 인식 센서가 있지만, 데스크톱이나 일부 랩톱에는 이러한 센서가 없기 때문에, PC 환경에서 생체인증을 사용하려면 별도의 하드웨어 센서를 구매·설치해야 합니다.

이에 반해 AutoPassword는 '대역외(out-of-band) 생체인증' 방식을 채택하여, 사용자가 이미 보유한 스마트폰의 생체인증 센서를 활용해 데스크톱, 랩톱 등 다양한 기기에서 대역외 생체 인증을 수행할 수 있습니다. 대역외 생체인증 방식은 PC나 랩톱에 별도의 생체인증 센서를 추가할 필요가 없어, 장치 도입 비용을 획기적으로 절감합니다.

단말기 마다 생체인증 센서가 필요한 대역내 생체인증



단말기 마다 생체인증 센서가 필요 없는 대역외 생체인증

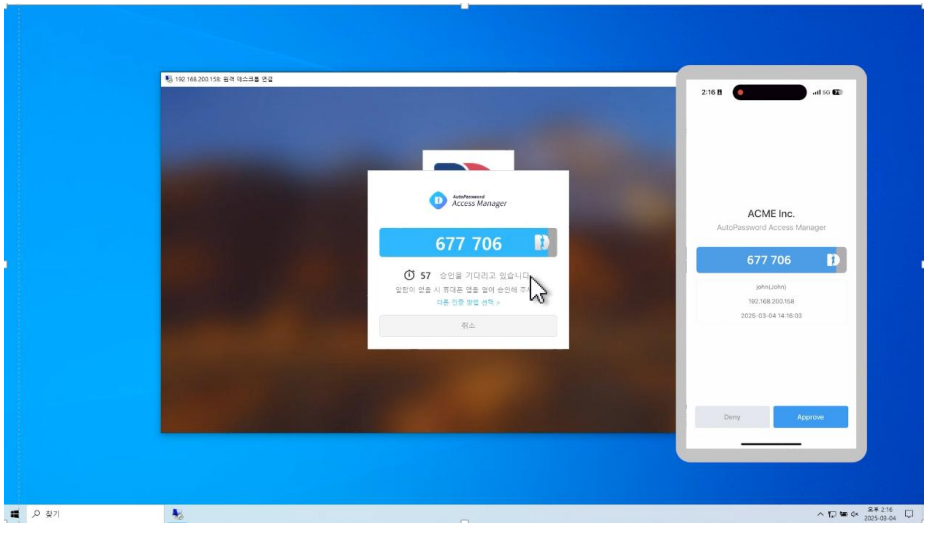


특징 4 – 센서를 추가할 수 없는 클라우드와 IoT기기까지 지원하는 생체인증 기술

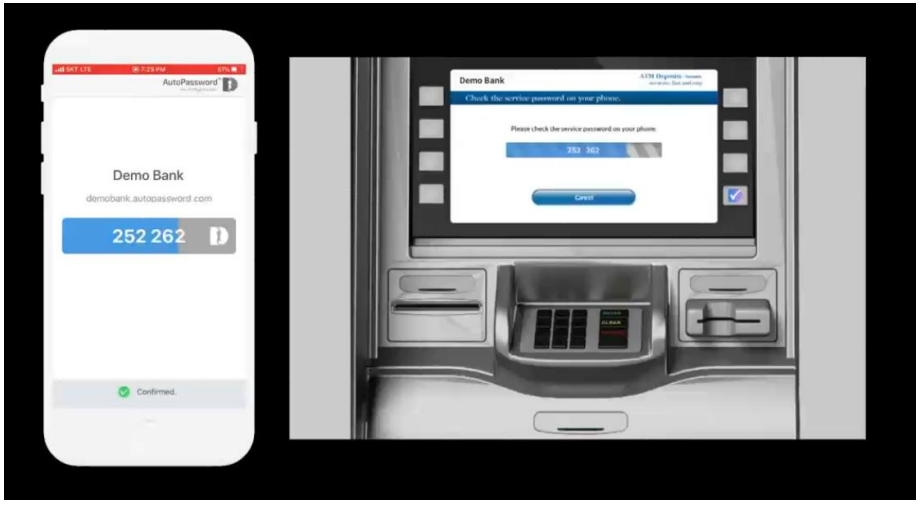
클라우드나 IoT 환경에서 생체인증을 적용하기 위해서는 해당 장치에 생체인증 센서가 장착되어 있어야 합니다. 그러나 많은 클라우드 장치나 IoT 장치는 생체인증 센서를 추가할 수 있는 USB 포트나 블루투스 기능이 없으며, 이 경우 결국 패스워드를 다시 사용해야 합니다.

AutoPassword는 대역외 생체인증 기술을 사용하여 이러한 한계를 해결합니다. 스크린을 갖춘 클라우드 또는 IoT 장치에서 자동패스워드를 먼저 제시하고, 사용자가 이를 스마트폰의 생체인증 센서로 승인함으로써 해당 장치에서도 안전한 인증을 수행할 수 있습니다. 이를 통해 생체인증 적용 범위를 데스크톱이나 노트북을 넘어, 클라우드 및 다양한 IoT 장치까지 확장할 수 있습니다.

대역외 생체인증으로 원격지 클라우드 PC 로그인



대역외 생체인증으로 ATM 거래 승인

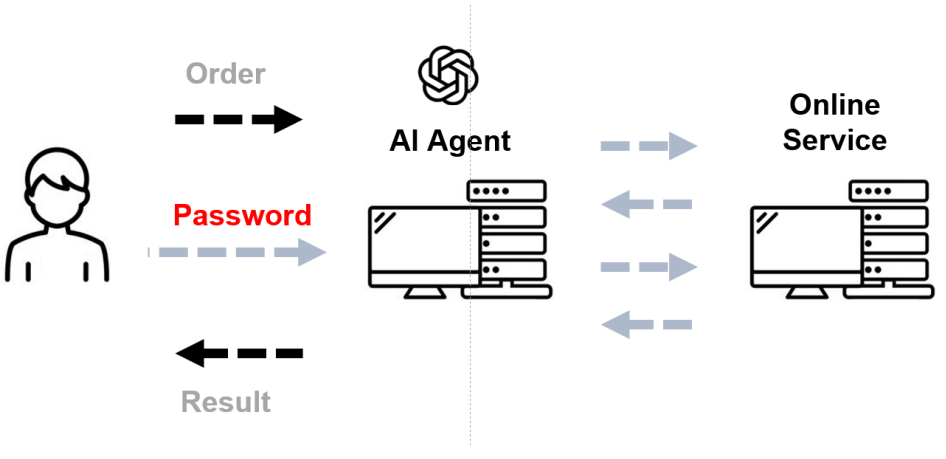


특징 5 – AI 에이전트까지 확장 가능한 대역외 생체인증 기술

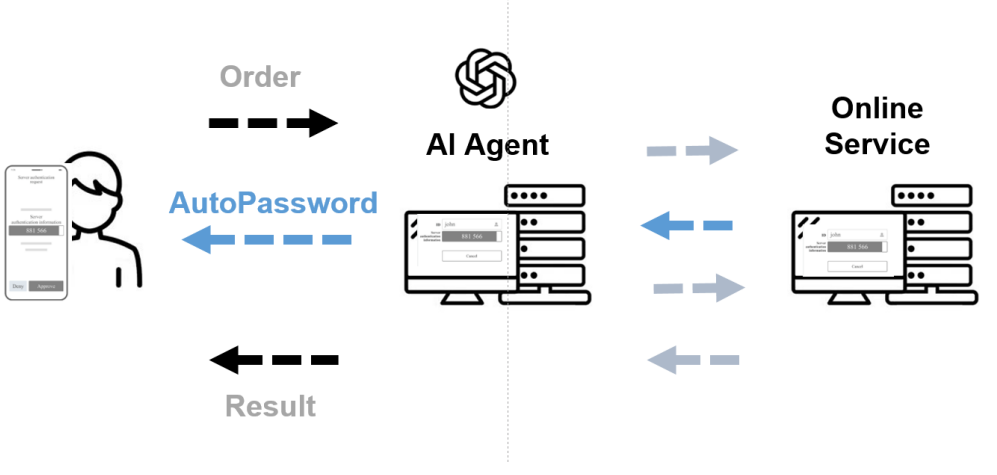
ChatGPT를 비롯한 생성형 AI 서비스의 활용이 확대되면서, 접속한 AI 서비스가 실제 서비스인지 위장된 서비스인지 확인하는 것은 중요합니다. AutoPassword는 사용자가 접속한 AI 서비스의 진위를 먼저 검증한 후 AI서비스를 사용할 수 있게 합니다.

또한 AI 에이전트를 활용할 때에도 AutoPassword는 효과적으로 사용됩니다. AI 에이전트를 사용하다 보면 사용자를 대신해 업무를 처리하는 과정에서 사용자의 패스워드를 제공해 주어야 합니다. AI 에이전트에게 패스워드를 알려주는 방식은 보안의 큰 문제입니다. 그러나 AutoPassword가 적용되어 있다면 AI 에이전트가 업무를 수행하는 과정에서 인증이 필요한 순간 사용자에게 자동패스워드를 제시할 수 있고, 사용자는 이를 스마트폰에서 승인하기 때문에 패스워드 공유에 따른 위험이 사라집니다. AutoPassword는 사용자가 AI 에이전트에게 패스워드를 입력하지 않고, AI에이전트가 인증이 필요한 경우에 사용자에게 자동패스워드를 제시하고 사용자가 이를 승인함으로서 안전한 AI 에이전트 활용이 가능하게 합니다.

사용자가 AI 에이전트에 패스워드를 입력하는 방식



AI에이전트가 사용자에게 자동패스워드를 제시하는 방식



DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

04

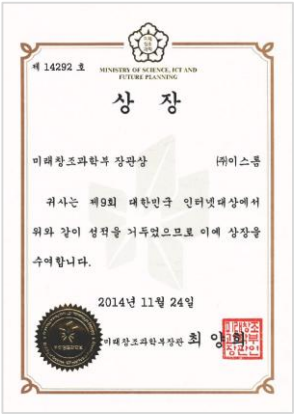
회사소개

03 레퍼런스

KB 국민은행	KB국민은행 – 제로트러스트 도입 시범사업을 통한 상호인증 기반의 강화된 사용자 인증 체계 구축 및 적용
우리은행	우리은행 – 우리은행 임직원 대상 패스워드리스 기반 PC 접근관리 및 애플리케이션 접근관리
유안타증권	유안타증권 – 유안타증권 임직원 대상 패스워드리스 기반 PC 접근관리 및 애플리케이션 접근관리
통계청	국회도서관 – 통계청에서 도입하여 도서관내에 설치된 통계정보 열람 PC에 대한 로그인 권한 제어
KORAIL	한국철도공사 – 차세대 나라장터 시스템 사용자 단말 인증 보안 강화를 위한 패스워드리스 인증 구축
KOMSA 한국해양교통안전공단	한국해양교통안전공단 – 외부 웹메일 로그인 시 패스워드리스를 이용한 사용자 로그인 보안강화
한국관광공사	한국관광공사 – 대한민국구석구석 시스템 개발 운영을 위한 관리자 및 협력사 인증 보안 강화
KIAT	한국산업기술진흥원 – 임직원용 내부 업무시스템에 도입하여 내부망과 외부망 에서의 개별적인 접근제어 운영
구리시	구리시청– 중요 서버 접근 시 로그인 보안 및 패스워드 자동변경을 통한 보안 컴플라이언스 대응
CWA 건설근로자공제회	건설근로자공제회 – 내부 시스템 운영 개선을 위한 서버 시스템의 로그인 보안 강화

03 레퍼런스

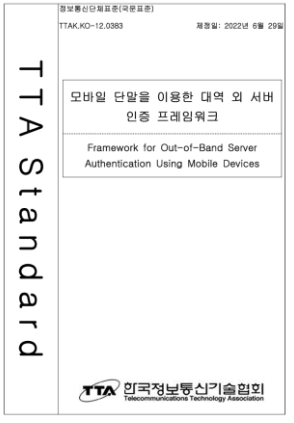
주요 시상



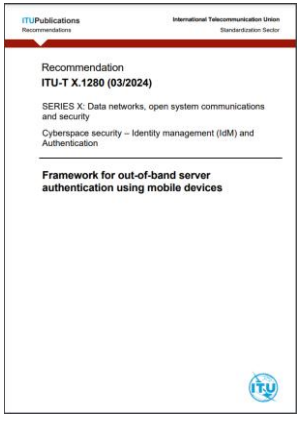
대한민국 인터넷대상

특허청장상

표준 기술



TTAK.KO-12.0383



ITU X.1280

주요 발표

FINOVATE FALL2016 ALUMNI
NEW YORK
FinovateFall 2016
Presenter

https://youtu.be/w2NtbPVaHSk

https://youtu.be/rBUK45fdBtY?t=838

FINOVATE FALL2018 ALUMNI
NEW YORK
FinovateFall 2018
Presenter

https://youtu.be/-DG-LYmRVfk

TRUSTECH
Payments | Identification | Security

https://youtu.be/nF72E24BCec

주요 인증

fido CERTIFIED UAF

GOOD Software

ISO/IEC 25023, 25051, 25041

oath
initiative for open authentication

IBM Security

DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

04

회사소개

패스워드리스 기반 신원인증 및 접근관리 전문회사

듀얼오스는 패스워드리스 기반 신원인증 및 접근관리 솔루션을 제공하는 기술회사입니다. 듀얼오스의 주요 솔루션으로는 패스워드리스 솔루션, 통합ID 및 접근관리 솔루션, 모바일 신분증 솔루션, 물리시설 접근관리 솔루션 등이 있습니다. 이 기술들은 UN산하 국제표준화기구인 ITU에서 X.1280와 X.oob-pacs로 제정될 만큼 뛰어난 사용성과 보안성을 갖추고 있으며, 제로트러스트 시대에 핵심 기술로 주목받고 있습니다. 듀얼오스는 ESG 실현을 위하여 전세계 B2C 온라인 서비스의 패스워드 문제를 해결할 수 있는 무료 Passwordless X1280 솔루션을 스위스 제네바에 위치한 패스워드리스 얼라이언스를 통하여 보급하고 있습니다.

제로트러스트 구축을 위한 패스워드리스 기반 신원인증 및 접근관리

패스워드리스 인증기술	통합ID 및 접근관리 기술	모바일 신분증 기술	물리시설 접근관리 기술
AutoOTP	AutoPassword	AutoPassword ID Card	AutoPassword ID Card
AutoPassword	AutoPassword Access Manager	AutoPassword ID Card Reader	AutoPassword IoT Controller

DualAuth

- 회 사 명 : ㈜듀얼오스
- 홈페이지 : www.dualauth.com
- 문의메일 : support@dualauth.com

도입 문의

- 주소 : (08589) 서울특별시 금천구 디지털로 130 남성프라자 13층
- 전화번호 : +82-2-6925-1305
- 사업문의 : sales@dualauth.com

DualAuth

감사합니다.