DualAuth

패스워드리스 기반 신원인증 및 접근관리

(주)듀얼오스 회사 소개서

DualAuth

01

회사 개요

02

제품 소개

03

성과 및 레퍼런스

04

연락처

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.1268로 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

01

회사 개요

02

제품 소개

03

성과 및 레퍼런스

04

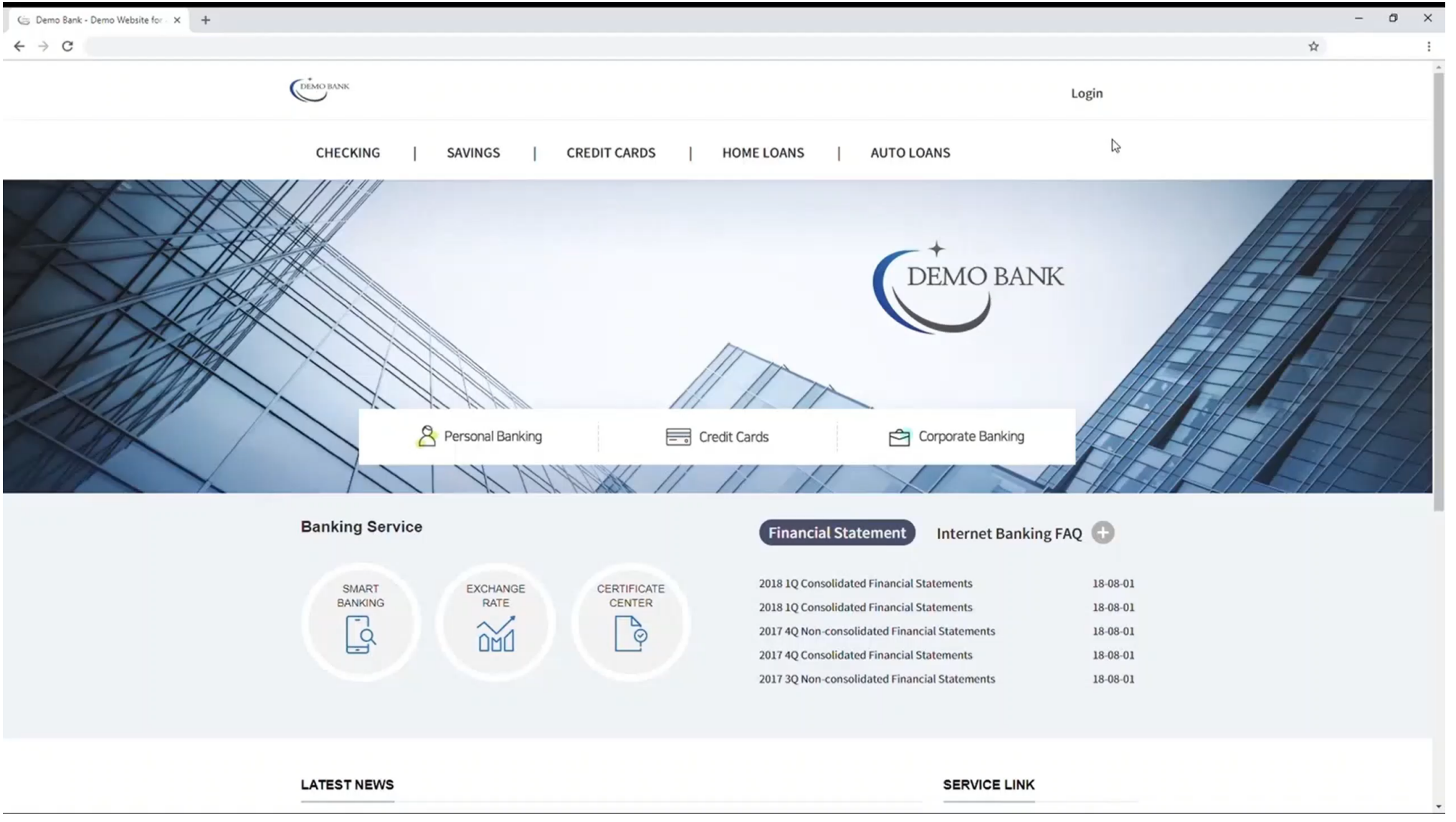
연락처

패스워드리스 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)

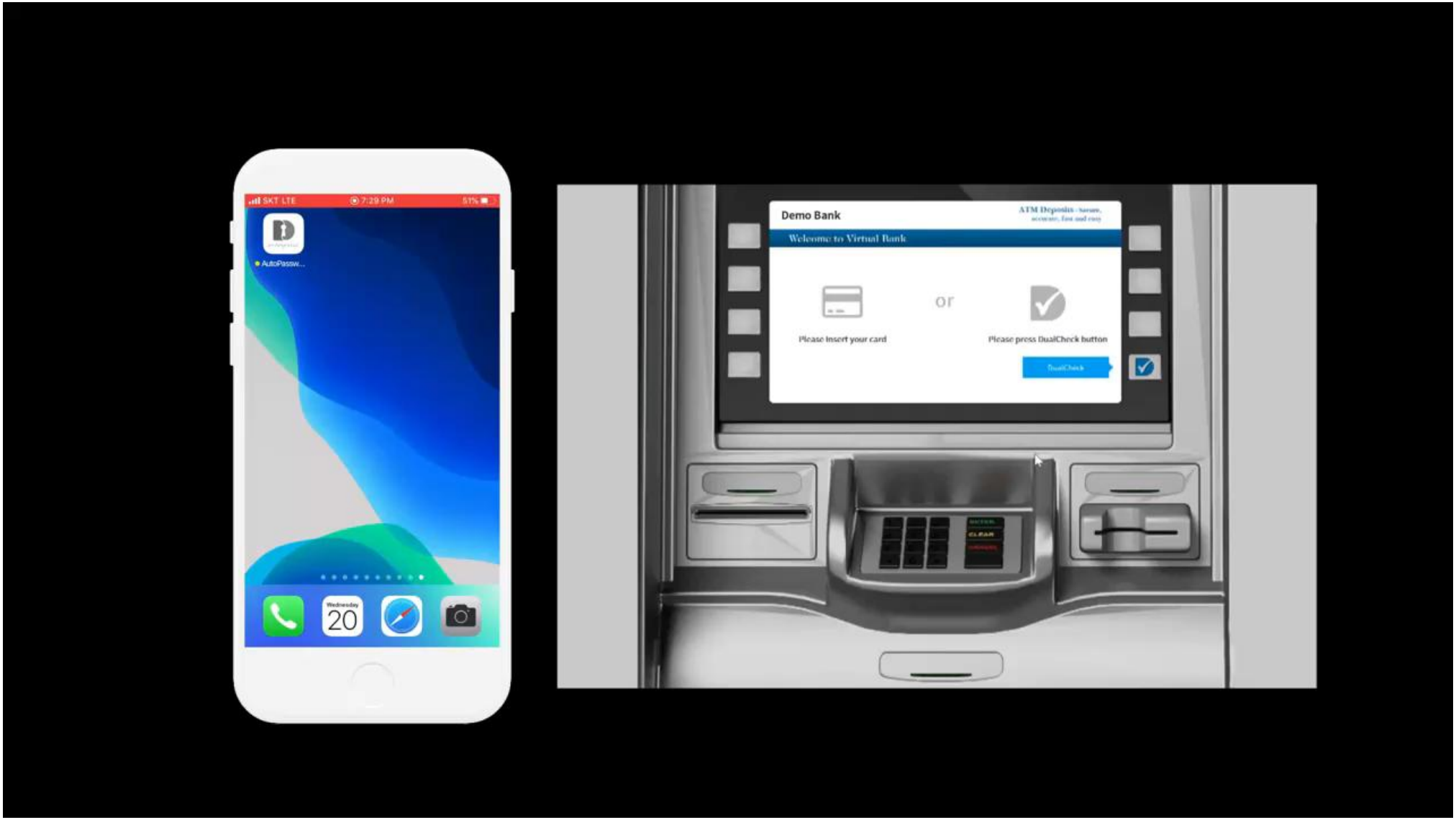
02 제품 소개 – 패스워드리스 인증기술



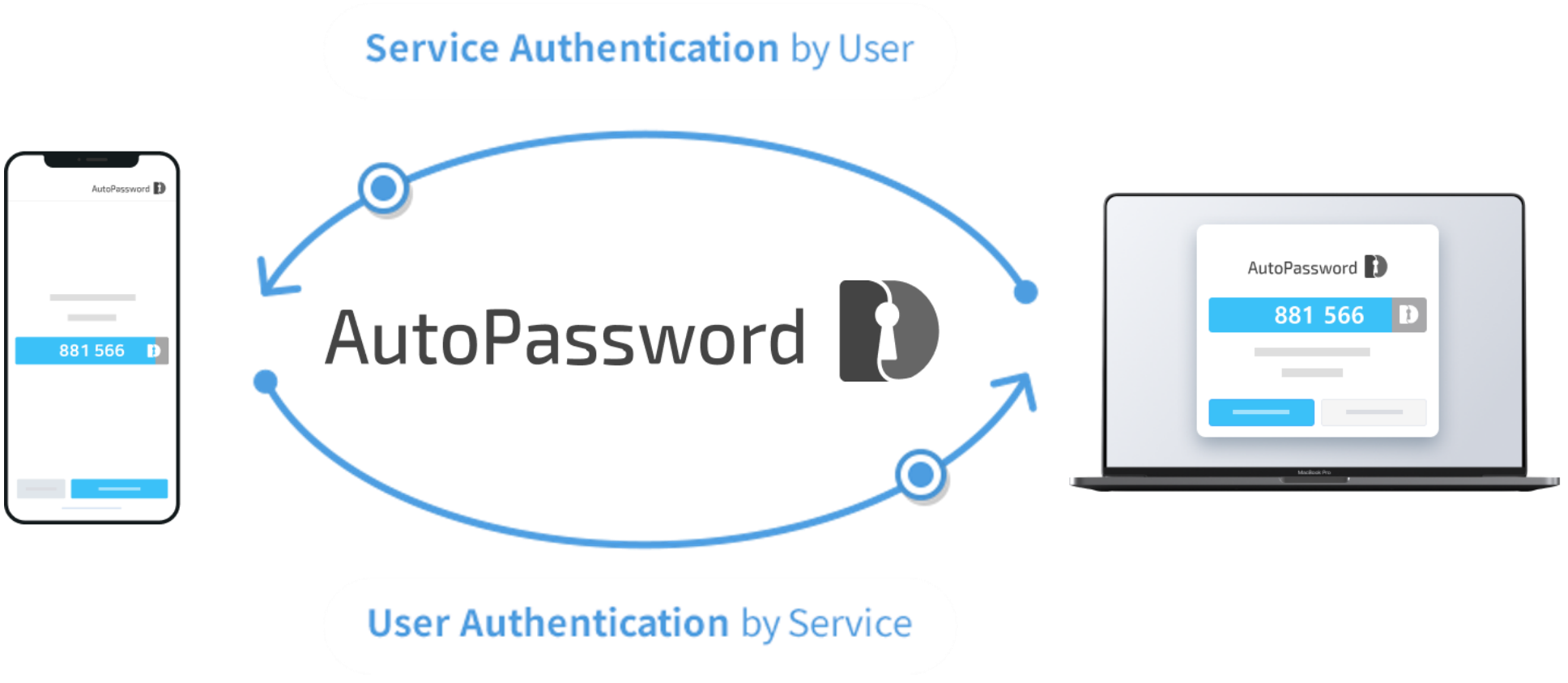
https://youtu.be/IpUyan0o4_A

Mobile Application Login

https://youtu.be/ebN2kTGZIRE



https://youtu.be/ytJvOE3f-8k


Service Authentication by User
AutoPassword
881 566
AutoPassword
AutoPassword
881 566
User Authentication by Service

AutoPassword 특징

기존의 사용자 인증기술(패스워드, OTP, 인증서, 생체인증 등)은 사용자가 온라인 시스템에 인증값을 입력하는 기술로, 사용자가 정당한 사용자 인지를 온라인 시스템에 입증하는 기술입니다. 따라서 사용자가 인증에 대한 입증 책임을 져야 합니다.

하지만 AutoPassword는 접속한 온라인 시스템이 사용자에게 자동패스워드를 제출하고, 사용자는 온라인 시스템이 제출한 자동패스워드를 사용자 스마트 폰에서 검증 후 생체센서로 승인하는 상호 인증 기술로 인증에 대한 입증책임을 온라인 시스템이 맡도록 하였습니다.

AutoPassword 효과

1. 사용자 입증책임을 온라인 시스템 입증책임으로 전환하여 사용자가 편해집니다.(편리성)

2. 사용자가 접속한 온라인 서비스에 대한 진위여부를 확인할 수 있어 피싱이나 파밍과 같은 사이버 공격에 노출되지 않습니다. (보안성)

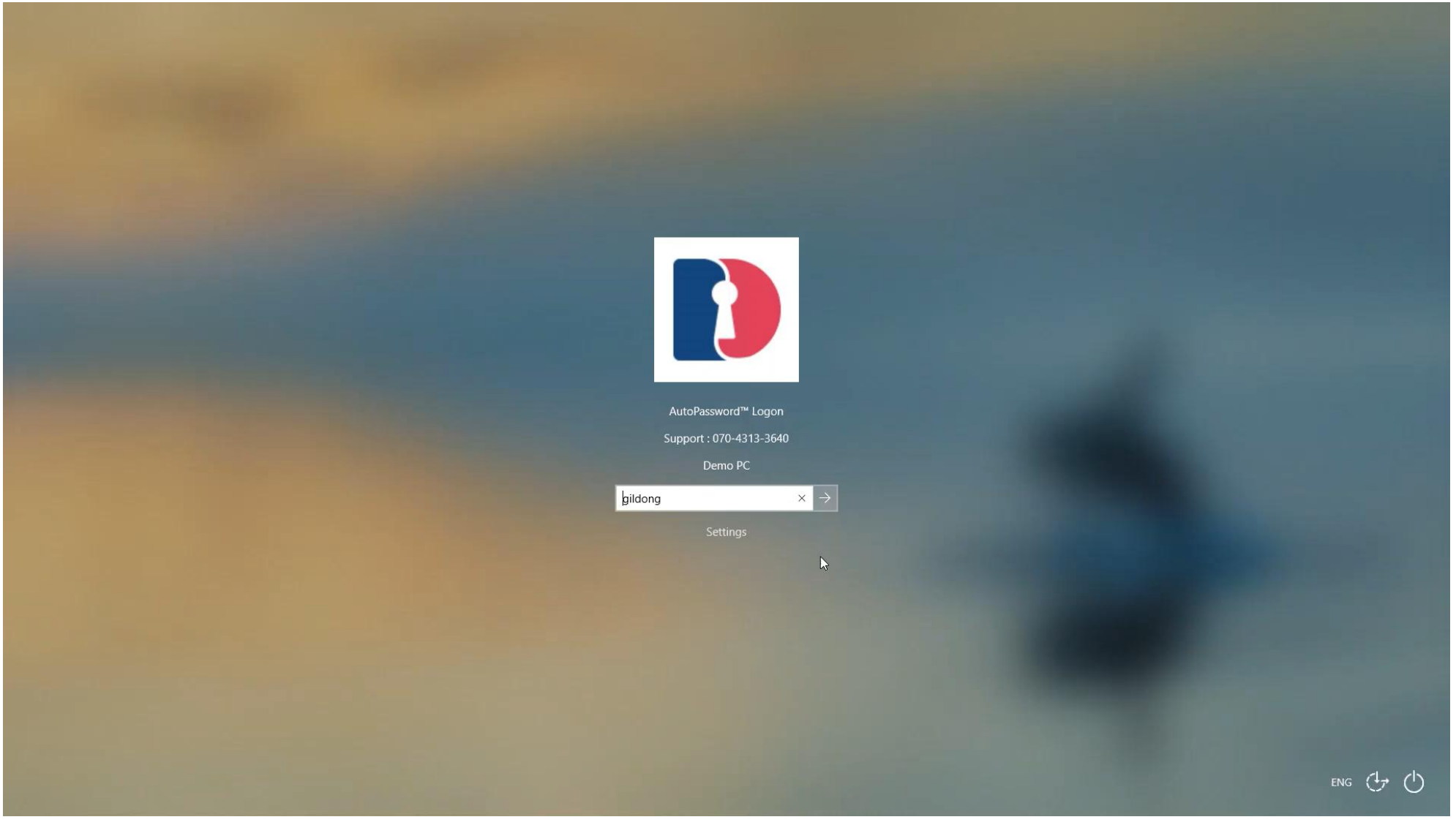
3. 스마트폰의 생체인증 센서 하나로 생체인증 센서가 부착되지 않는 단말기에서 생체인증을 진행할 수 있습니다. (기존 생체인증 기술은 사용자 단말기마다 개별 생체인증 센서가 필요한 대역내 생체인증 기술이나 본 기술은 어떤 사용자 단말기에서 스마트폰의 생체인증을 요청하는지 확인한 후 대역외로 생체인증을 진행하기 때문에 현존하는 가장 경제적인 생체인증 기술 - 경제성)

통합 ID 및 접근관리 기술

AutoPassword Access Manager

통합 ID 및 접근관리 솔루션인 AutoPassword Access Manager는 이메일, 그룹웨어와 같은 웹 어플리케이션 통합 계정관리 뿐만 아니라 업무용 Windows PC, Linux 서버, 무선 네트워크까지 포괄하여 계정 발급 및 접근 정책을 설정하는 접근제어 기술입니다.

Windows Demo

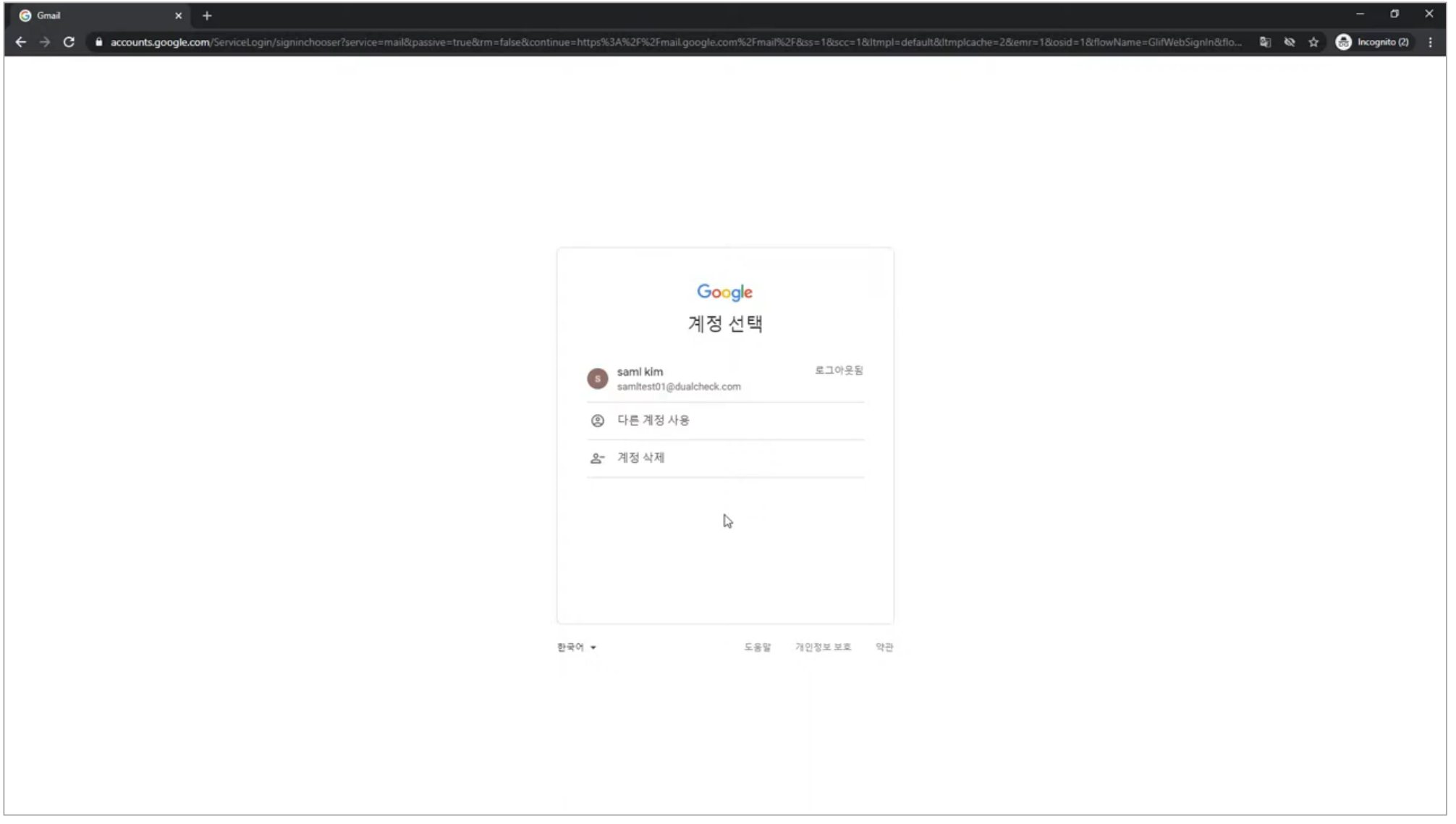


https://youtu.be/cjmjBDwgw00

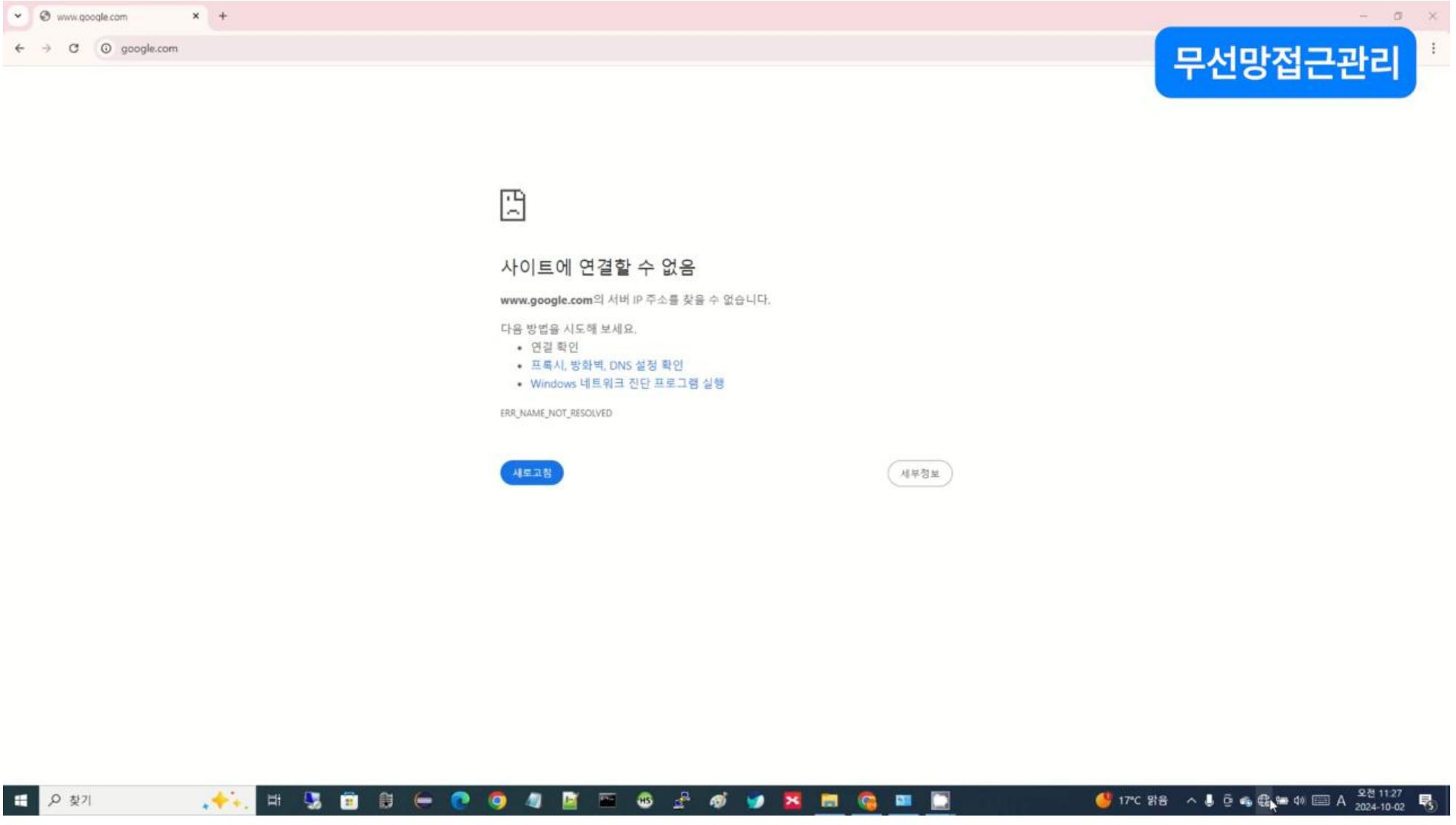
Linux Demo

https://youtu.be/FDt0i06otUI

02 제품 소개 – 통합 ID 및 접근관리 기술



https://youtu.be/l5H1C9gz7tg



https://youtu.be/SMnv_WHhNe4

AutoPassword Access Manager 특징

기존에는 이메일에 사용하는 ID와 패스워드, 윈도우즈 PC에서 사용하는 ID와 패스워드, 리눅스 서버에 접근하는 ID와 패스워드, 무선망에 사용하는 ID와 패스워드가 제각각이어서 사용자나 관리자 관점에서 통합적인 사용자 식별과 자원에 대한 접근 관리가 어려웠다.

하지만 AutoPassword Access Manager는 회사에서 사용하고 있는 업무용 PC, 리눅스 서버, 그룹웨어, 이메일과 같은 애플리케이션과 유/무선 네트워크 등에서 하나의 사용자 ID로 사용자가 식별될 수 있고, 해당 ID가 어떤 시스템에 접근할 수 있도록 설정하는 통합 ID 및 접근관리 제품입니다.

AutoPassword Access Manager 효과

1. 임직원이 업무상 사용하는 업무 시스템(윈도우 PC, 리눅스 서버, 이메일 및 그룹웨어, 유/무선네트워크 등)을 하나의 통합ID와 인증수단으로 접근할 수 있어 번잡했던 계정과 패스워드 관리가 단순해 집니다.

2. 관리자가 임직원별, 조직별로 업무 시스템 접근 범위를 설정할 수 있어 하나의 관리 화면에서 전사적인 권한관리와 이력조회가 가능해집니다.

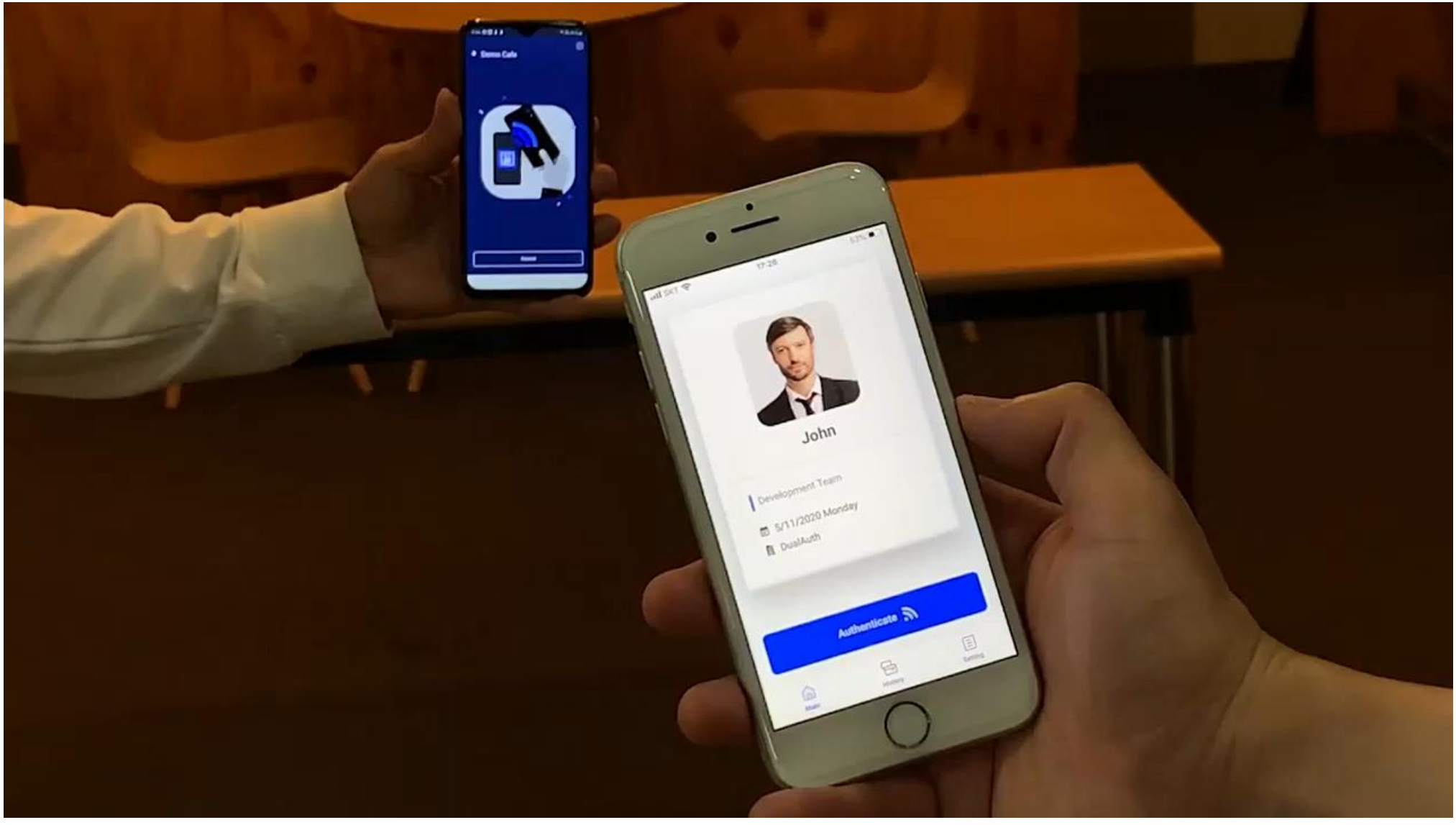
3. AutoPassword Access Manager내 OS 패스워드 자동 변경을 설정하면 윈도우 PC, 리눅스 서버에 사용자가 로그인 할때 마다 OS 패스워드를 자동으로 갱신하여 사용자가 OS 패스워드 관리를 하지 않아도 됩니다.

모바일 신분증 기술

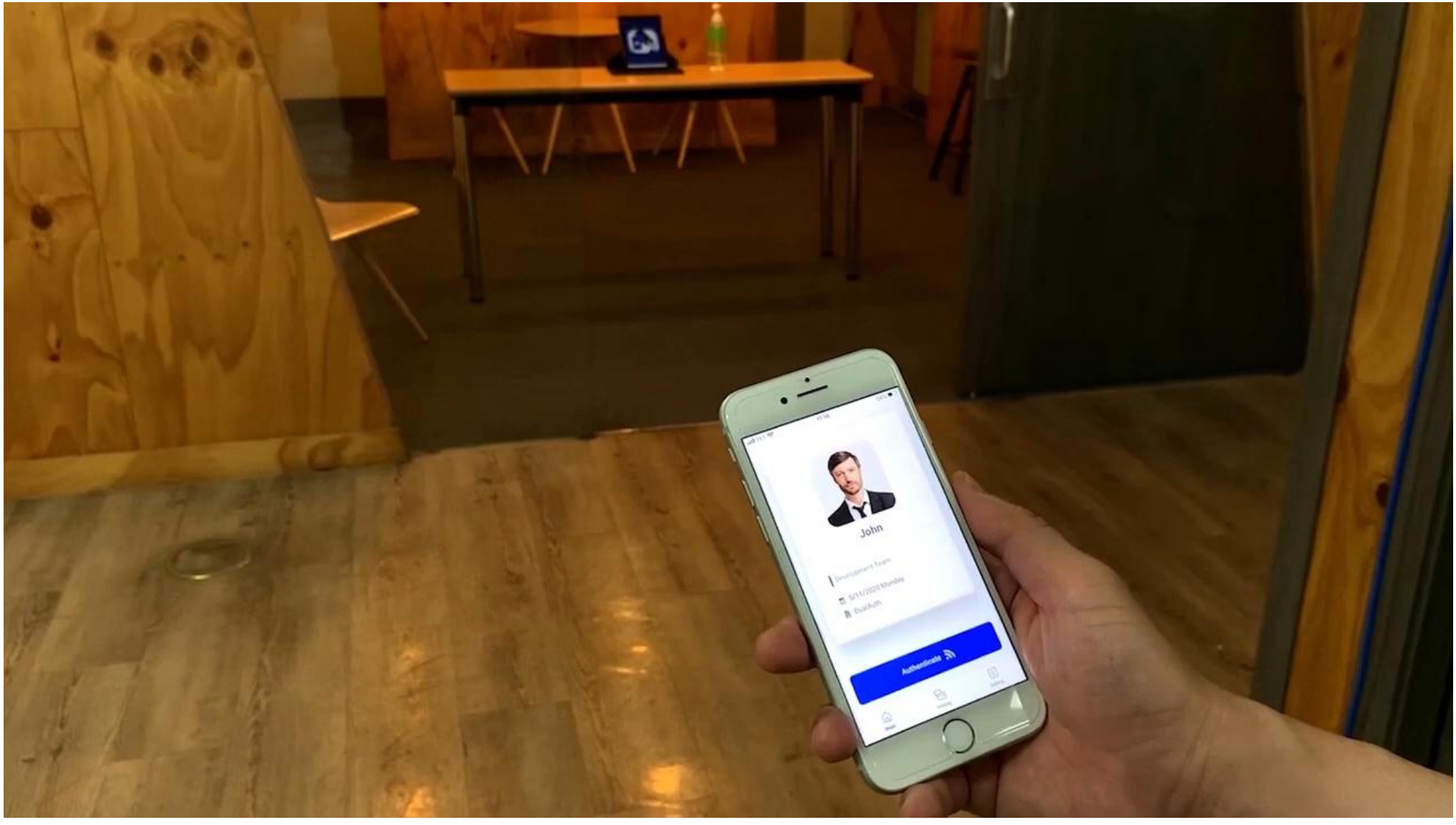
AutoPassword ID Card Reader

AutoPassword ID Card

모바일 신분증 솔루션인 AutoPassword ID Card는 모바일 신분증 발급 당시 회사와 관계없는 스마트폰 제조사의 생체인증을 이용하는 것이 아니라 회사 승인한 사용자의 생체정보를 기반으로 동작하는 대역외 생체인증 기술입니다.



https://youtu.be/9Vy-ajCjnYg



https://youtu.be/80axVwQQbeM

02 제품 소개 – 패스워드리스 인증기술

AutoPassword ID Card 특징

기존 모바일 신분증은 최초 발급 시점에만 처음 본인 여부를 확인합니다. 이후 모바일 신분증 사용 시에는 별도의 본인 확인 없이, 스마트폰 OS에서 제공하는 생체인증을 통해 신분증 소지자를 확인합니다. 이 때문에 모바일 신분증을 제출받는 서비스 제공자 입장에서는, 모바일 신분증을 제시하는 사람이 최초 신분증 발급 시 확인 받은 사람과 동일인인지 확인할 방법이 없습니다.

반면, AutoPassword ID Card는 스마트폰 카메라로 촬영한 사진을 신원 확인 이미지로 등록하도록 관리자에게 신청할 수 있습니다. 관리자가 이를 승인하면, 모바일 신분증은 해당 승인된 사진으로만 생체인증을 수행합니다. 이를 통해, 최초 발급 받은 사용자 이외의 다른 사람이 모바일 신분증을 도용하는 것을 차단합니다.

AutoPassword ID Card 효과

1. 사용자의 사진을 촬영한 카메라와 사용자를 인식하는 카메라가 같아서 생체인증 성공률이 높습니다. (편리성)

2. 사용자가 모바일 신분증을 사용할 때마다 관리자가 승인한 사람인지 확인할 수 있으며, 모든 사용자의 생체데이터는 사용자 스마트폰에만 저장됩니다. (보안성)

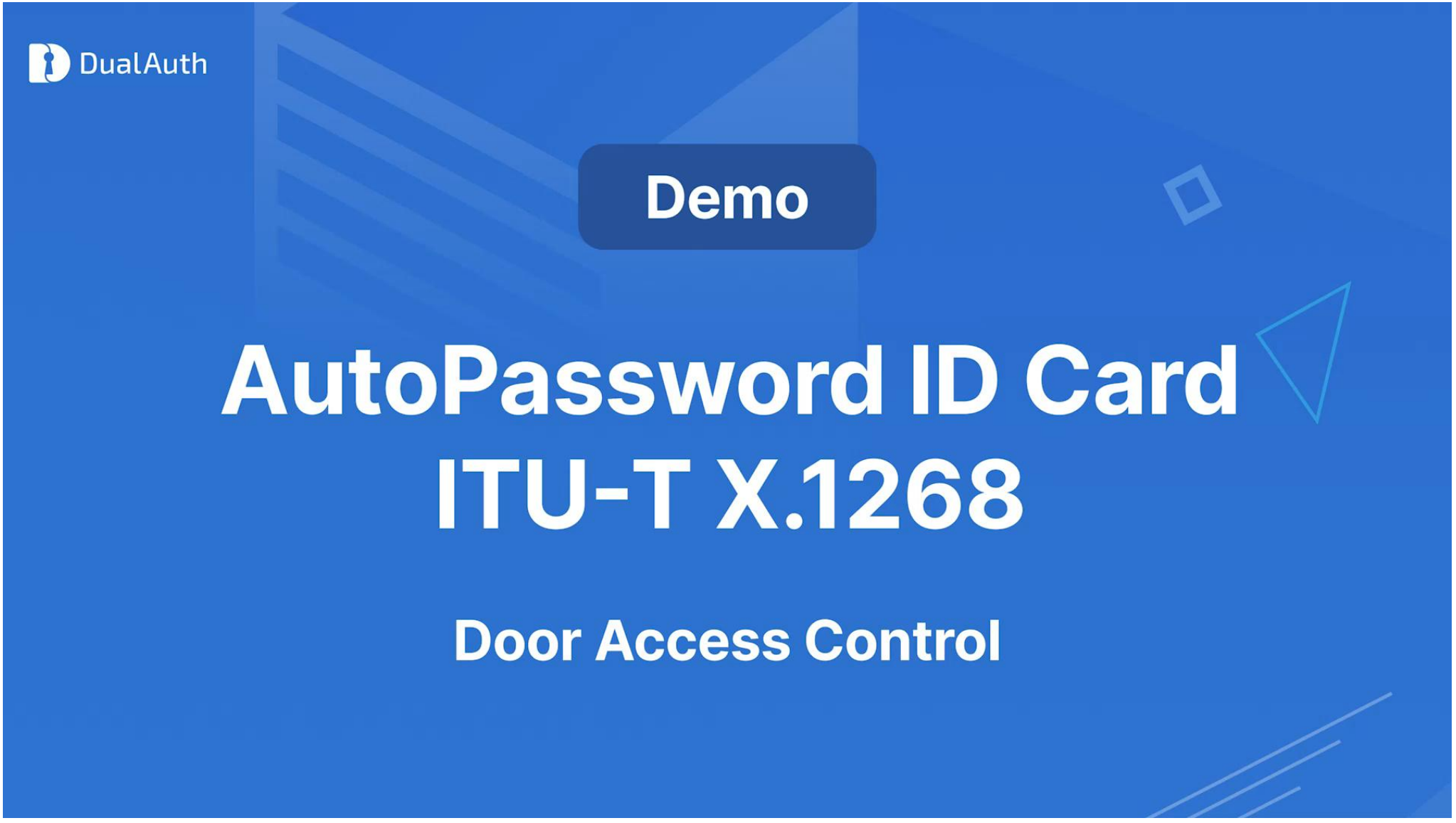
3. PC나 태블릿 등 다른 기기에서 별도의 생체인증 센서를 부착하지 않고도, 모바일 신분증내 생체템플릿을 이용하여 생체인증을 진행 할 수 있습니다. (경제성)

물리시설 접근관리 기술

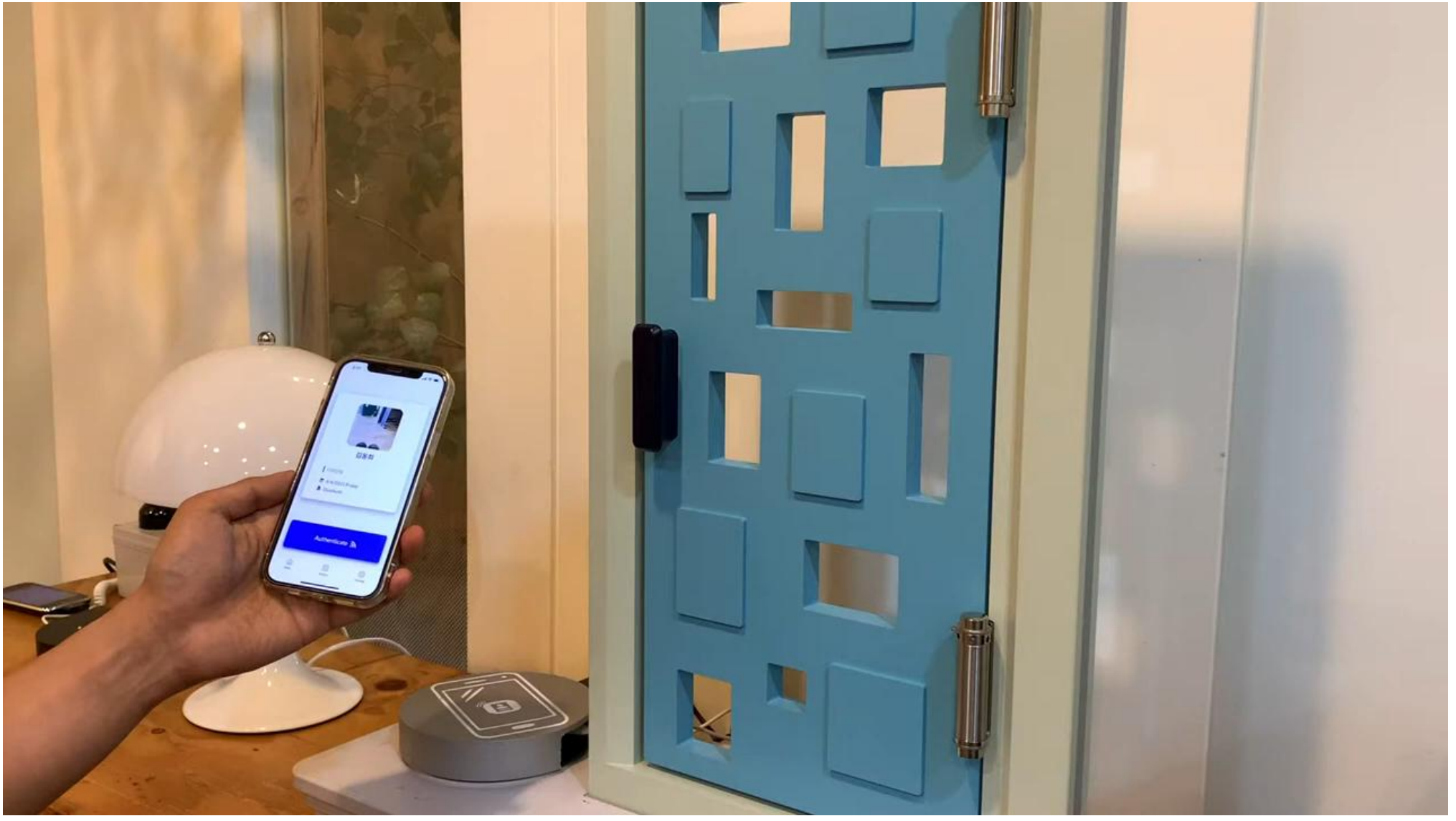
AutoPassword IoT Controller

AutoPassword ID Card

물리시설 접근관리 솔루션인 AutoPassword IoT Contoller는 무인시설에서 사용자의 생체데이터를 수집하지 않고, 사용자의 스마트폰에 등록된 생체인증을 통해서 물리시설에 대한 접근관리를 수행하는 대역외 물리시설 접근관리 기술입니다. (국제표준 X.1268)



https://youtu.be/S3favCBySLY



https://youtu.be/gdfakJZ-igI

https://youtu.be/uwKGa_ejF1M

02 제품 소개 – 모바일 신분증 기술

AutoPassword IoT Controller 특징

기존 모바일 신분증의 대역내 인증 방식은 리더기에 직접 접촉하여 인증합니다. 그러나 스마트폰 제조사마다 통신 방식이 달라, 하나의 방식으로 표준화하기 어렵습니다. 사용자 입장에서도 스마트폰별로 NFC 설정 방법이 다르고, QR코드 방식은 카메라와 화면이 함께 있는 리더기에 스캔해야 하는 번거로움이 있습니다. 더욱이, 현재 리더기는 정당한 장치인지 확인하지 못한 채 사용자만 인증값을 제출하기 때문에 보안 취약점이 발생할 수 있습니다.

AutoPassword IoT Controller는 이러한 문제를 해결합니다. 이 장치는 사용자의 AutoPassword ID Card 앱에 인증 비컨 값을 송출하고, 앱은 이를 검증한 뒤 스마트폰 내에서 물리 시설 사용 여부를 승인합니다. 이와 같은 대역외 상호 인증 방식을 통해, 어떤 스마트폰이든 동일한 절차로 모바일 신분증을 사용하여 물리 시설을 안전하게 제어할 수 있습니다.

AutoPassword IoT Controller 효과

1. 사용자가 근접거리 뿐만 아니라 근거리에서도 모바일 신분증을 사용할 수 있습니다. (편리성)

2. 사용자가 물리 시설을 먼저 확인 한 후 신분증을 사용 여부를 선택할 수 있으며, 스마트폰내 생체정보를 이용하기 때문에 물리시설에 별도의 생체정보 보관할 필요가 없습니다. (보안성)

3. 물리시설의 인증 비컨 정보를 스마트폰에서 대역외로 검증하기 때문에 블루투스 이외에 별도의 생체인증센서, NFC 리더, QR 인식 스캐너 같은 외부 기기가 필요가 없습니다. (경제성)

DualAuth

01

회사 개요

02

제품 소개

03

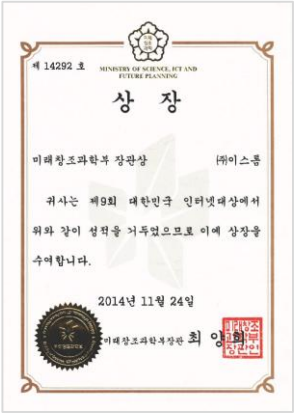
성과 및 레퍼런스

04

연락처

03 성과 및 레퍼런스

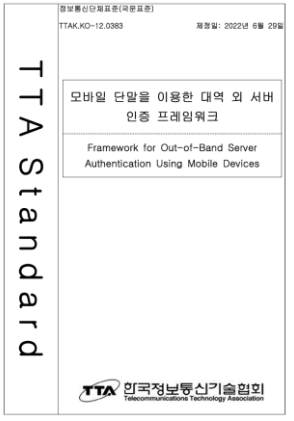
주요 시상



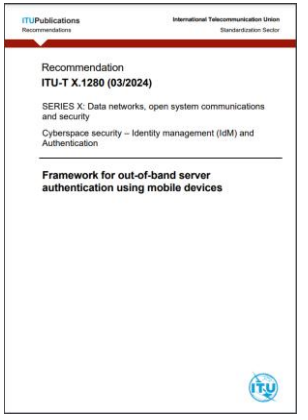
대한민국 인터넷대상

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

NeP 신제품인증 NEW EXCELLENT PRODUCT

03 성과 및 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
CW 건설근로자공제회	건설근로자공제회 – 내부 시스템 운영 개선을 위한 서버 시스템의 로그인 보안 강화

DualAuth

01

회사 개요

02

제품 소개

03

성과 및 레퍼런스

04

연락처

DualAuth

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

한국오피스

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

DualAuth

감사합니다.