DualAuth

제로트러스트를 위한 통합 ID 및 접근제어

AutoPassword Access Manager 제품소개서

DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

04

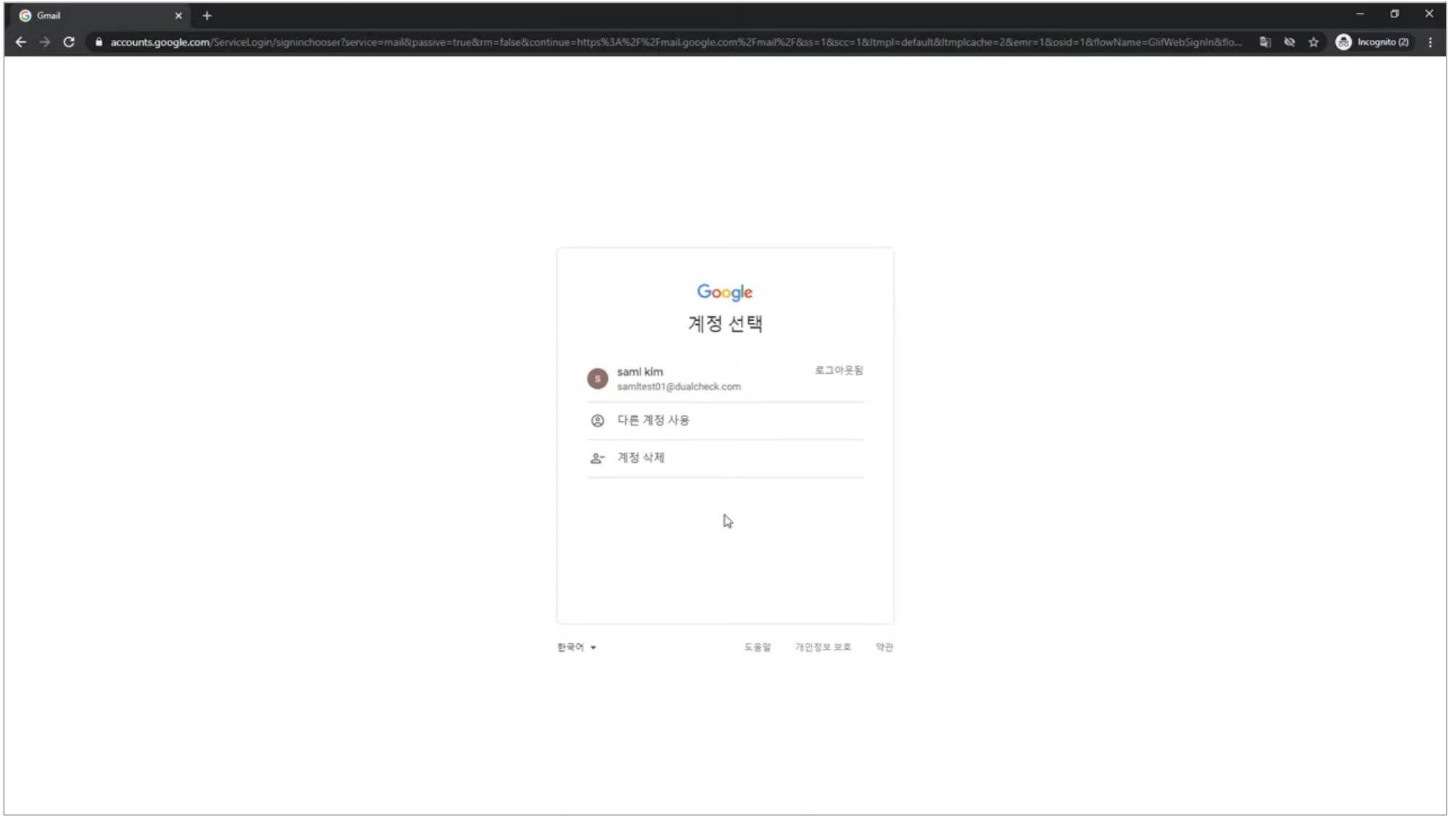
회사소개

통합 ID 및 접근관리

AutoPassword Access Manager

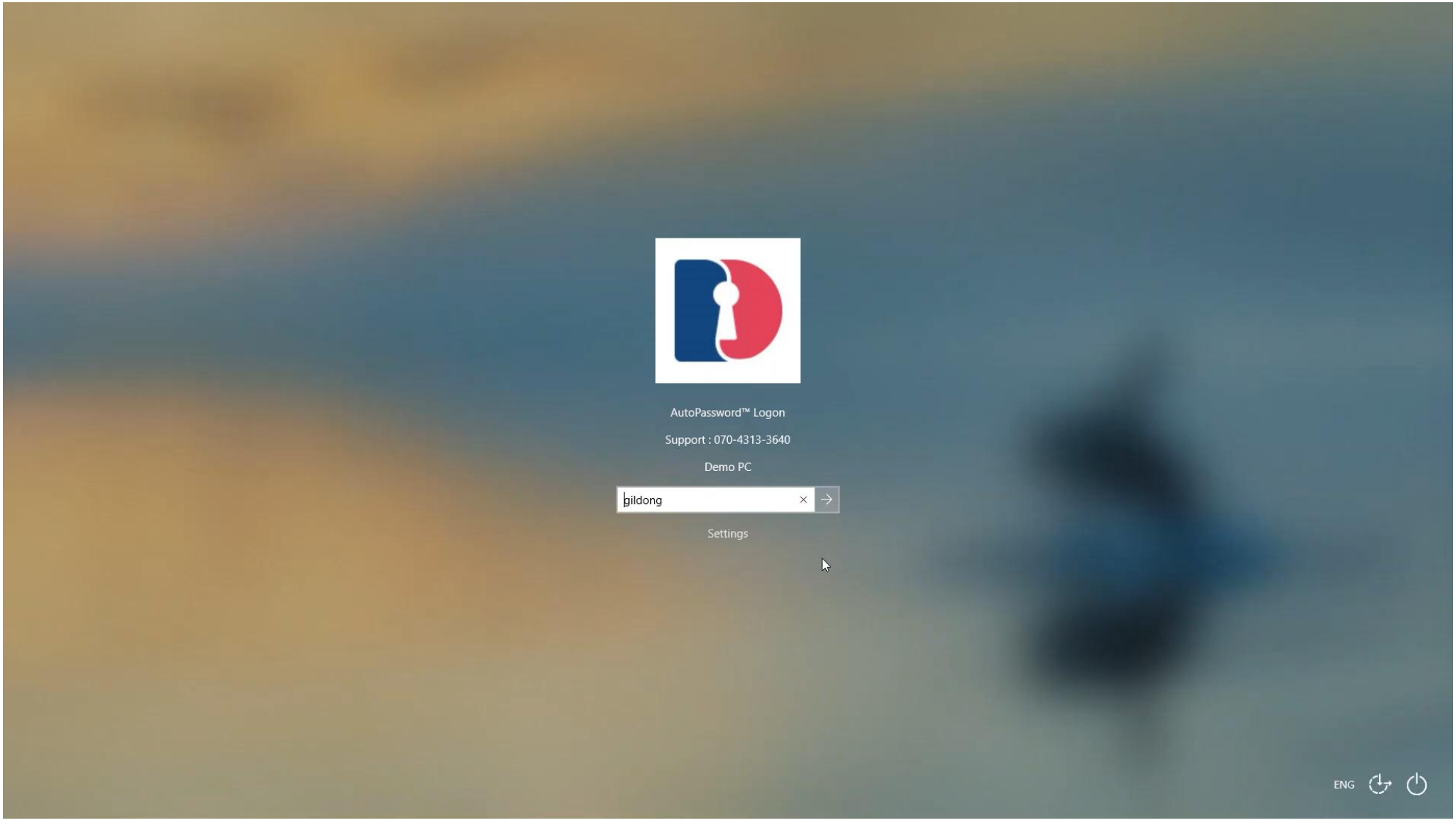
AutoPassword Access Manager는 AutoPassword를 지원하는 통합 ID 및 접근 관리 솔루션입니다. 이메일·그룹웨어 등 웹 애플리케이션 계정 관리뿐 아니라, 업무용 Windows PC, Linux 서버, 무선 네트워크 계정관리까지 지원하며, 중앙에서 계정 발급과 접근 정책을 일괄적으로 설정·관리할 수 있습니다.

01 제품 개요

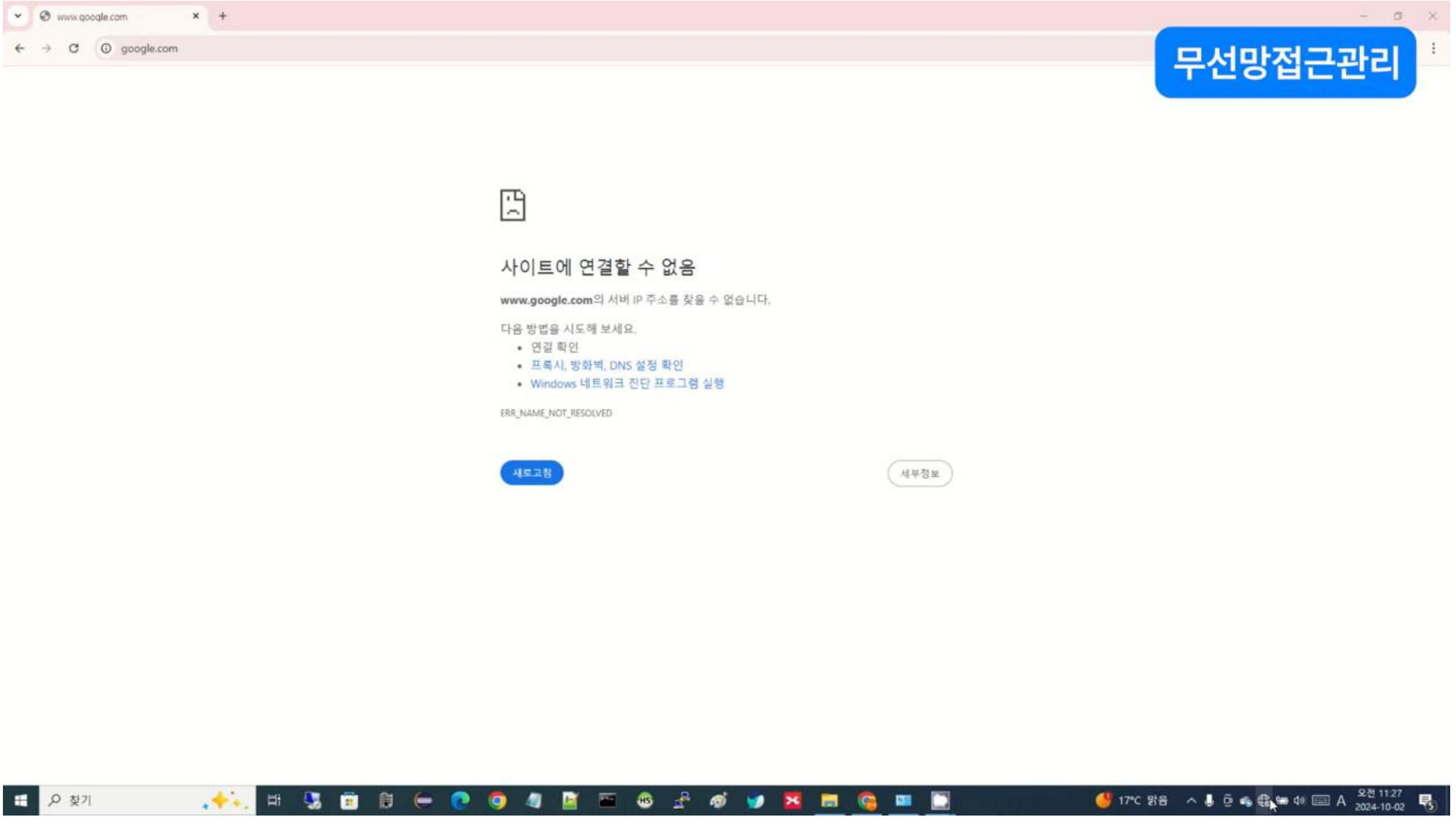


https://youtu.be/l5H1C9gz7tg

01 제품 개요



https://youtu.be/cjmjBDwgw00



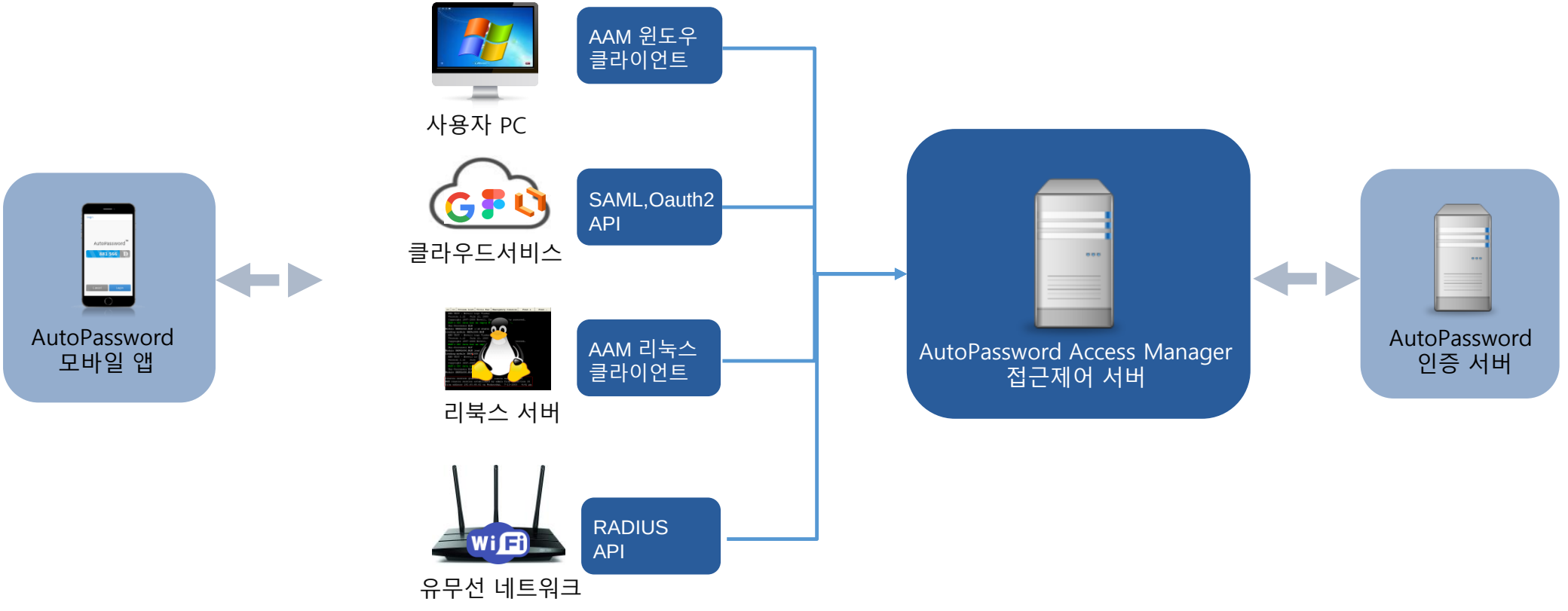
https://youtu.be/SMnv_WHhNe4

https://youtu.be/FDt0i06otUI

AutoPassword Access Manager 아키텍처

AutoPassword Access Manager로 전환하려면 기존 업무 시스템에 Access Manager 서버와 클라이언트를 설치하고, AutoPassword 인증서버와 모바일 앱을 추가하면 됩니다. 이 과정은 기존 시스템 구조를 크게 변경하지 않으면서도 안전하고 편리한 인증 환경을 구현합니다.

관리자는 먼저 Access Manager 서버를 설치한 뒤, 업무 시스템과 서버 간 통신이 가능하도록 클라이언트 프로그램을 설치하거나 API를 연동합니다. 또한 Access Manager는 SAML, OAuth2, OpenID Connect 등 표준 인증 프로토콜을 지원해 다양한 클라우드 서비스와 손쉽게 연동할 수 있습니다.



DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

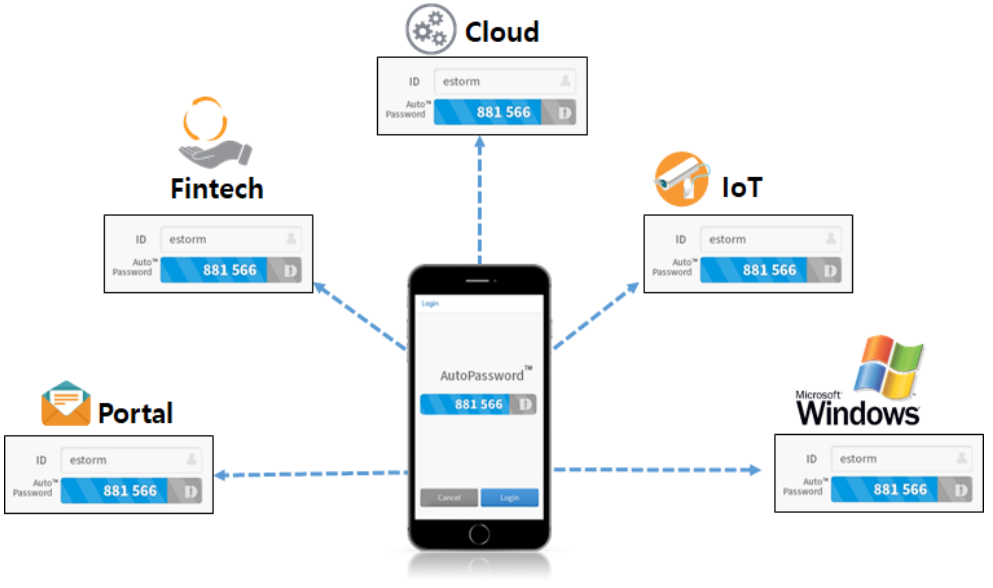
04

회사소개

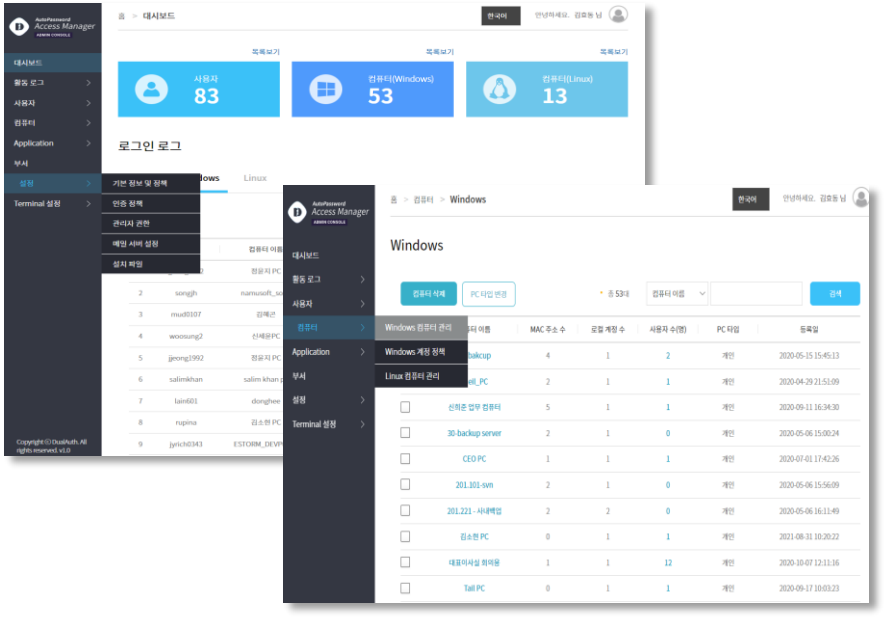
특징 1 – 하나의 통합 ID로 모든 업무 시스템을 로그인하고 사용 이력을 관리

AutoPassword Access Manager는 사용자가 하나의 ID와 인증 방식으로 PC, 이메일, 클라우드 서비스, 리눅스 서버, 유·무선 네트워크 등 다양한 업무 시스템에 접근할 수 있는 통합 환경을 제공합니다. 이를 위해 윈도우 AD 계정, 로컬 계정, 802.1X·RADIUS 기반 무선망, SAML·OAuth2·OpenID Connect, 리눅스 PAM 등 다양한 계정 관리 및 인증 방식을 연동합니다. 관리자는 단일 관리 콘솔에서 사용자 또는 조직별 접근 정책을 유연하게 설정하고, 사용 이력을 체계적으로 관리할 수 있습니다.

하나의 통합 ID와 AutoPassword로 모든 업무시스템 로그인



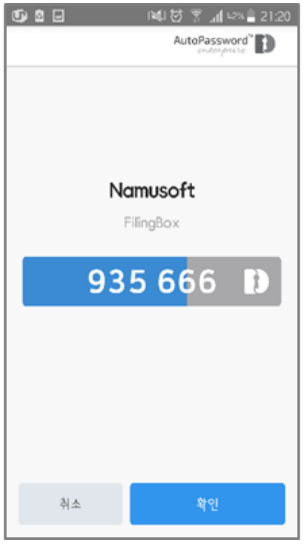
통합 ID별 업무 시스템 로그인 이력 조회

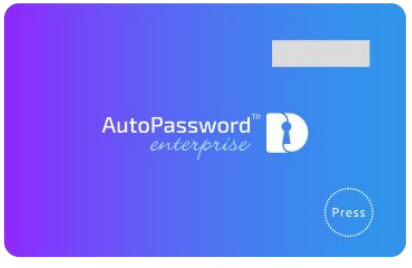


특징 2 – AutoPassword을 포함한 다양한 인증 수단 지원

AutoPassword Access Manager는 AutoPassword를 기본 인증 수단으로 제공하여, 생체인증 센서가 없는 단말기에서도 대역외 생체인증을 사용할 수 있습니다. 이를 통해 사용자는 업무용 클라우드나 리눅스 서버에 접속할 때, 인증값을 직접 입력하지 않고 업무 시스템이 제시하는 자동 패스워드를 스마트폰에서 검증하여 안전하게 로그인할 수 있습니다. 또한 스마트폰 분실 상황을 대비해 FIDO, OTP, 당일 임시 패스워드, AAM 패스워드 등 다양한 대체 인증 수단을 지원합니다.

AutoPassword 이외에 스마트폰 분실시 사용할 수 있는 OTP, FIDO 지문인증기, 당일 임시 패스워드 등을 지원

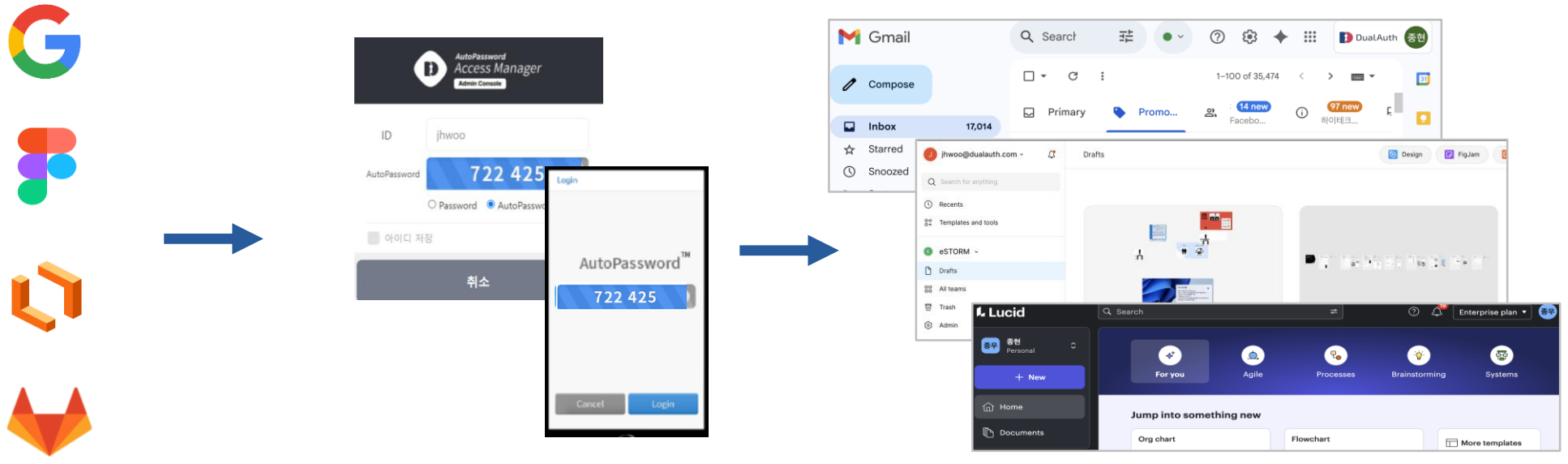




특징 3 – 클라우드 서비스나 업무 애플리케이션을 통합 로그인

AutoPassword Access Manager는 SAML, OAuth2, OpenIDConnect 등 표준 인증 프로토콜을 지원하여 주요 클라우드 서비스나 업무용 웹 어플리케이션에 AutoPassword를 이용한 통합 로그인이 가능합니다. 이미 Googlw Workspace, Figam, LucidCart, Dropbox, Github, WordPress 등 20여개의 주요 클라우드 서비스가 연결되어 있으며, 업무상 운영중인 각종 애플리케이션을 표준 프로토콜을 이용하여 추가로 연동할 수 있습니다. 표준 인증 프로토콜에 AutoPassword가 적용되어 가장 안전한 연합 인증이 가능해 집니다.

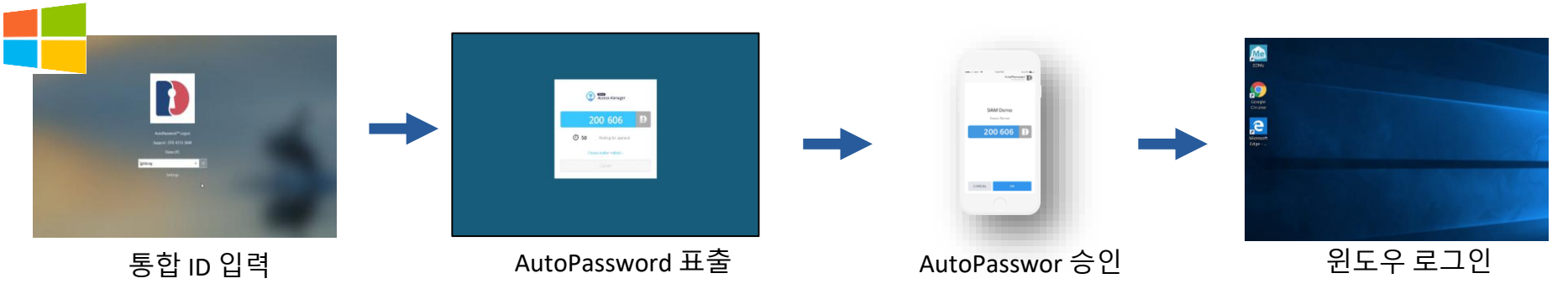
다양한 클라우드 서비스에서 통합ID와 AutoPassword로 로그인



특징 4 – Windows PC나 Linux 서버 통합 로그인

AutoPassword Access Manager는 Windows PC와 Linux 서버에서 AutoPassword를 이용한 로그인을 지원합니다. 생체인증 센서가 없는 PC나 리눅스 서버에서 대역외 생체인증을 통해 사용자가 안전하게 PC나 리눅스 서버에 접속 확인할 수 있습니다. 사용자는 업무용 장치에 패스워드나 기타 인증값을 직접 입력하지 않고, 윈도우나 리눅스 시스템이 제시하는 자동 패스워드를 스마트폰에서 검증하여 로그인할 수 있어, 보안성과 편의성을 모두 확보할 수 있습니다. 또한 로그인할때 마다 운영체제의 패스워드가 자동으로 갱신되어 사용자자는 패스워드 변경관리에서 해방됩니다. (Windows 경우 Local Account와 AD Account 둘 다 지원)

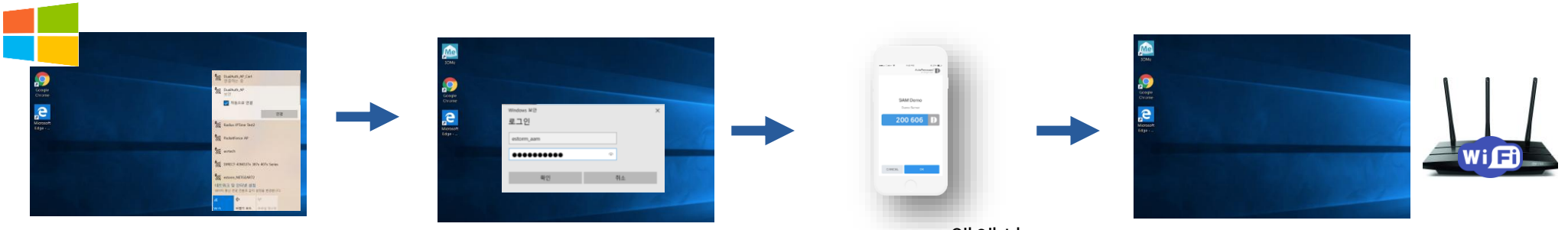
윈도우PC 와 리눅스 터미널에서 AutoPassword로 로그인



특징 5 – 유무선 네트워크 통합 로그인

AutoPassword Access Manager는 유·무선 네트워크 장치에서 RADIUS 인증과 AutoPassword 앱을 이용한 로그인을 지원합니다. 일반적으로 네트워크 접속 인증창은 변경이 어렵지만, AAM은 앱 내 SelfPassword 기능으로 이를 해결합니다. 사용자는 ID 칸에 통합 ID를, 패스워드 칸에 임의의 셀프 패스워드를 입력하면 됩니다. 이후 스마트폰에 동일한 셀프 패스워드가 표시되면, 이를 스마트폰 생체인증으로 승인하여 접속을 완료합니다. 이를 통해 인증창 변경이 불가능하고 생체인증 센서가 없는 PC에서도 스마트폰을 이용해 안전하게 유·무선 네트워크에 연결할 수 있습니다.

인증창 변경이 불가능한 유무선 네트워크에 SelfPassword로 로그인



무선 네트워크 선택 → 통합 ID와 SelfPassword 입력 → AutoPasswor 앱에서 SelfPassword 승인 → 무선망 연결

DualAuth

01

제품 개요

02

주요 특징

03

레퍼런스

04

회사소개

03 레퍼런스

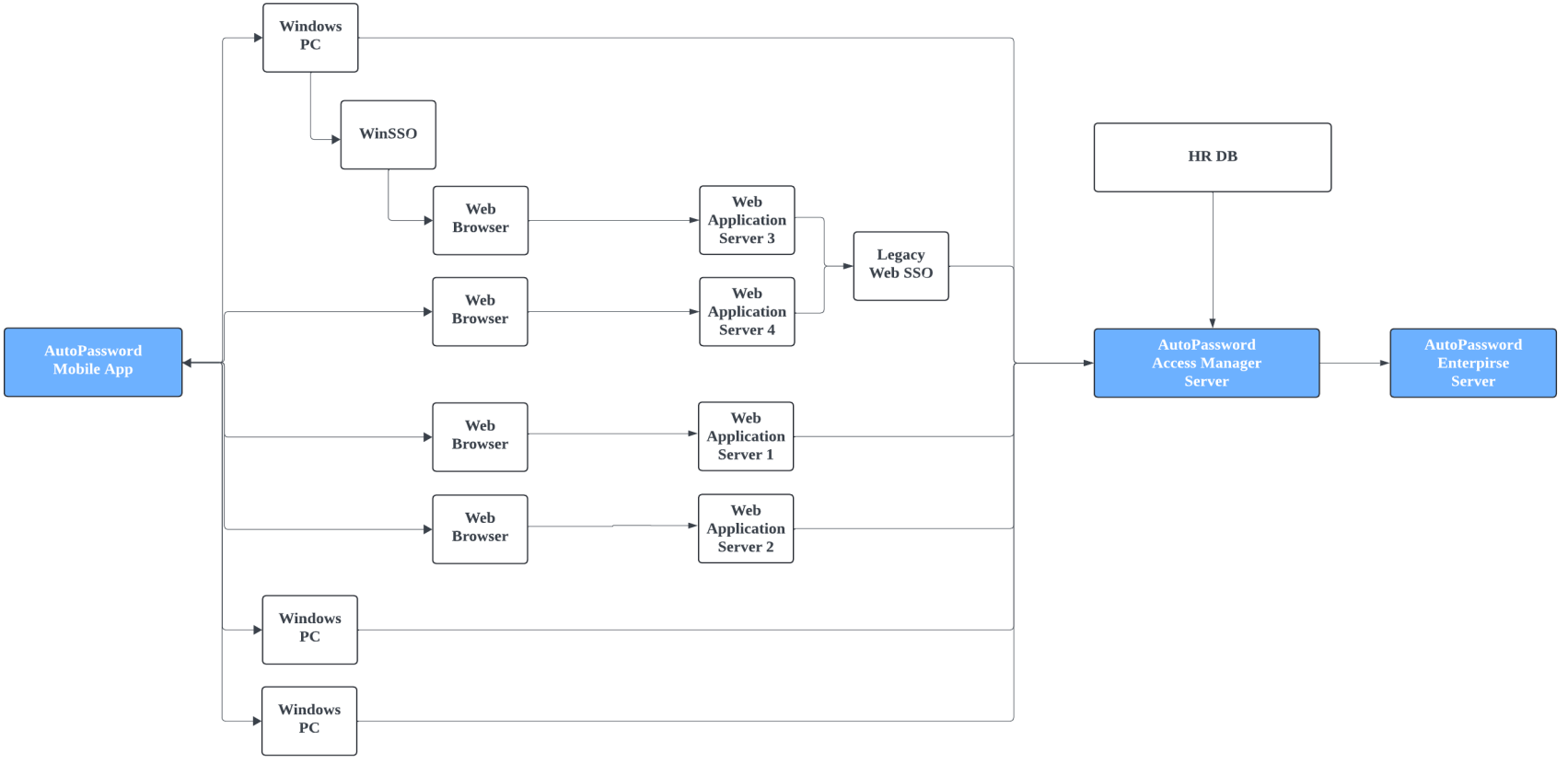
KB 국민은행	KB국민은행 – 제로트러스트 도입 시범사업을 통한 상호인증 기반의 강화된 사용자 인증 체계 구축 및 적용
우리은행	우리은행 – 우리은행 임직원 대상 패스워드리스 기반 PC 접근관리 및 애플리케이션 접근관리
유안타증권	유안타증권 – 유안타증권 임직원 대상 패스워드리스 기반 PC 접근관리 및 애플리케이션 접근관리
통계청	국회도서관 – 통계청에서 도입하여 도서관내에 설치된 통계정보 열람 PC에 대한 로그인 권한 제어
KORAIL	한국철도공사 – 차세대 나라장터 시스템 사용자 단말 인증 보안 강화를 위한 패스워드리스 인증 구축
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 AutoPassword Access Manager 소개

Case 1. 임직원을 위한 통합 ID 인증 및 접근 제어

- **도입배경** : 임직원의 윈도우PC 및 7개의 업무용 어플리케이션에 대한 3개 이상의 ID/PW 관리의 불편함 해결, 부분적인 2FA 적용 및 관리에 대한 통합인증 체계 마련
- **사업범위** : 윈도우 PC O만대, 기존 SSO 서버, 웹 애플리케이션 10여개 연동
- **도입효과**

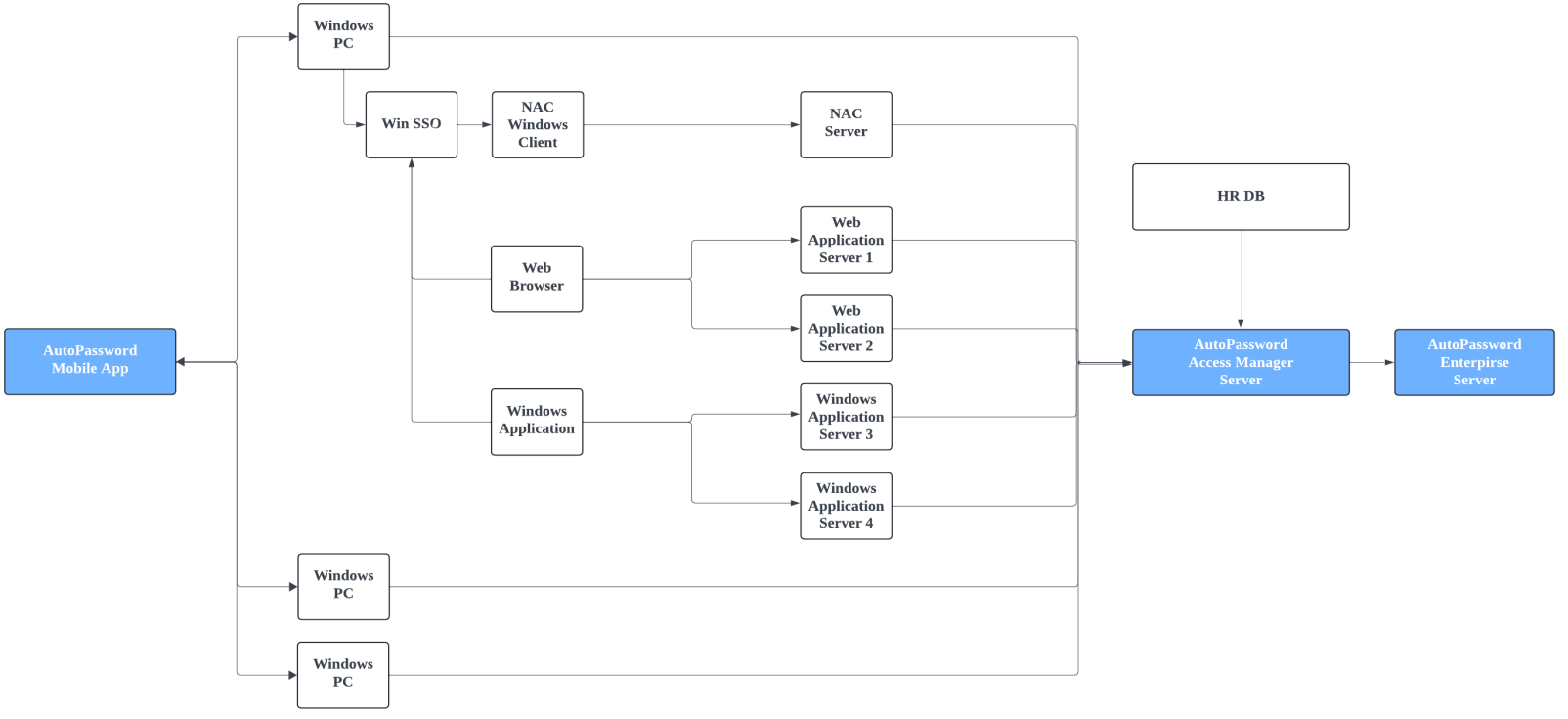
  - 사용중인 웹포털의 SSO에 대한 PW 및 2FA를 패스워드리스로 통합하여 인증의 복잡성을 낮춤으로써 사용자 업무편의성 향상
  - 여러 지점에 배치된 수많은 윈도우 PC와 사용자별 업무용 어플리케이션에 대한 통합적인 접근관리 체계를 구축



Case 2. 임직원을 위한 통합 ID 인증 및 접근제어 관리

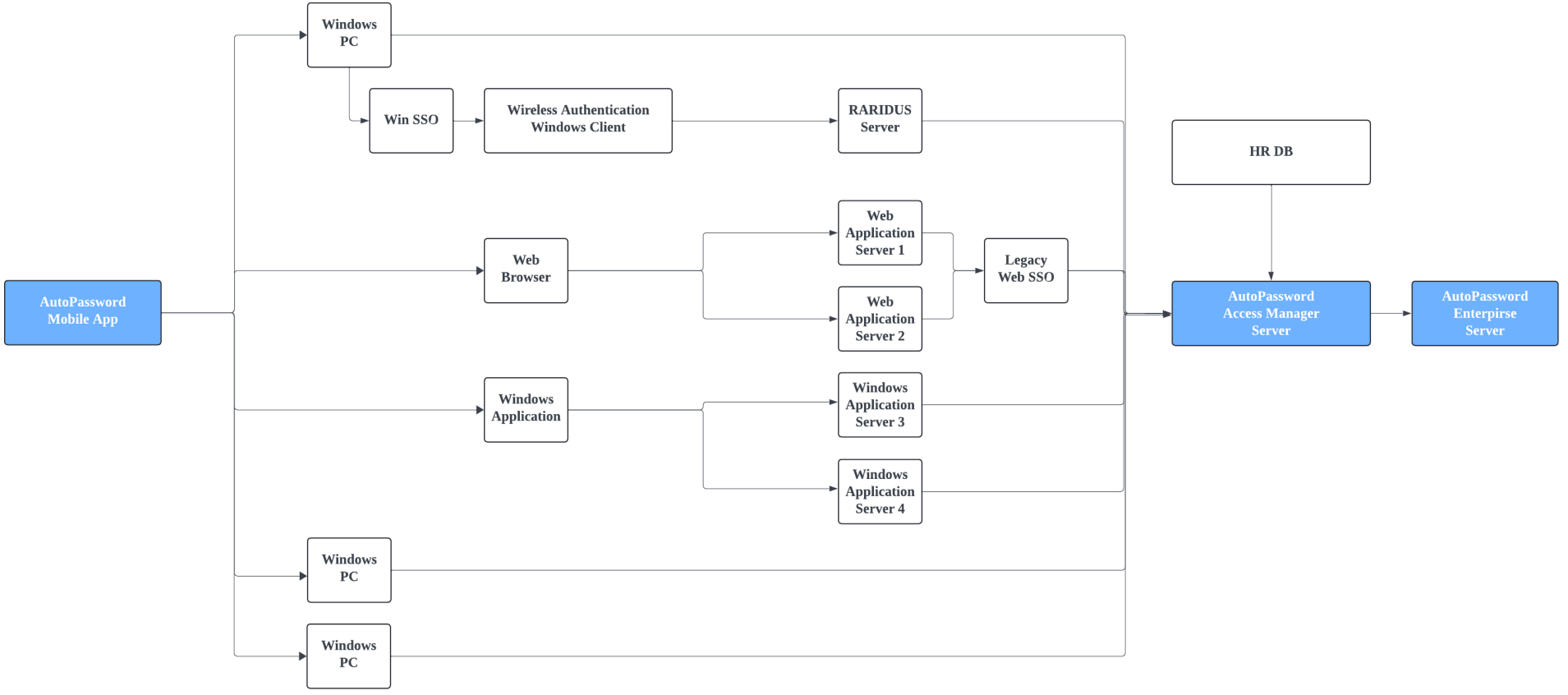
- **도입배경** : 윈도우PC 및 10여개의 업무용 어플리케이션에 대하여 2개 이상의 ID 및 PW 관리에 대한 불편함을 해소하기 위하여 통합ID 및 패스워드리스 기반의 인증체계로 전환하여 PC 및 업무용 어플리케이션에 대한 사용자 인증 환경 개선이 필요
- **사업범위** : 윈도우 PC O천대, 유선망 사용자 인증, 10여개의 윈도우/웹 애플리케이션
- **도입효과**

  - 윈도우 인증 이후 연속 인증 체계를 구축하여 유효시간 내 NAC 및 업무용 애플리케이션, 개별 웹 애플리케이션에 대한 연속 인증을 통한 현업 사용자의 윈도우 로그인 및 업무 애플리케이션에 대한 접근성 개선
  - 보안 수준을 구분하여 출근 시 PC 최초 접근에는 생체인증을 수행하고 이후 업무 중 화면이 잠기는 경우는 스마트폰 간편 인증으로 업무 진행에 대한 보안을 유지하도록 차등 인증프로세스를 구현



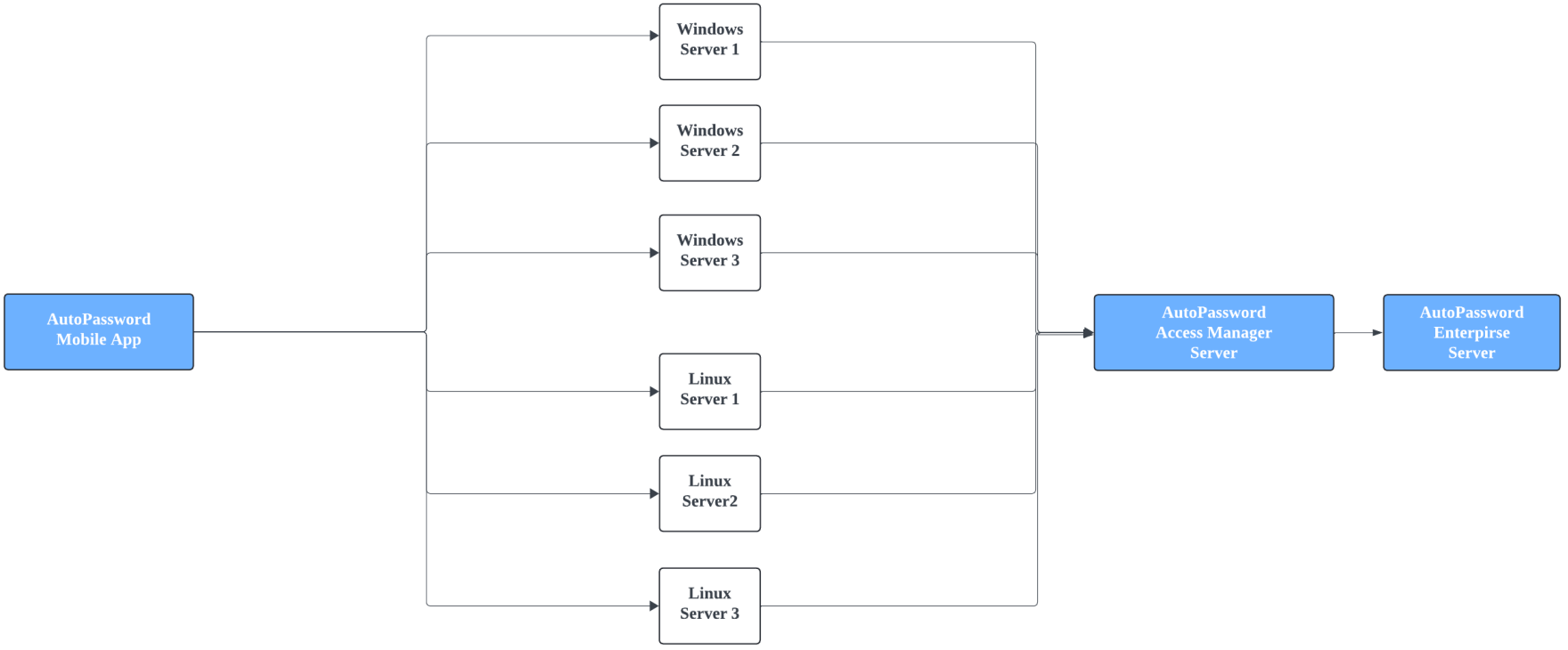
Case 3. 임직원을 위한 통합 ID 인증 및 접근제어

- **도입배경** : 임직원의 윈도우PC 및 2개 이상의 ID/PW 관리의 불편함 해소 및 사내 무선망 인증 환경에 대한 PC 사용 접근성 개선
- **사업범위** : 윈도우 PC, 무선망, 기존 Web SSO서버, 웹 애플리케이션 10+대
- **도입효과**
  - 통합 ID 및 패스워드리스 방식으로 윈도우 PC뿐만 아니라 업무용 어플리케이션까지 한번에 인증하는 체계로 전환
  - 윈도우 인증 이후 연속 인증을 통하여 유효시간 내 무선망 연속 인증을 진행하여 사용자의 노트북 사용에 대한 접근성을 크게 개선
  - 기존 웹 SSO에 대한 인증 방식을 패스워드리스 방식으로 연결하여 기존 PC와 웹 포털SSO의 사용성을 크게 개선



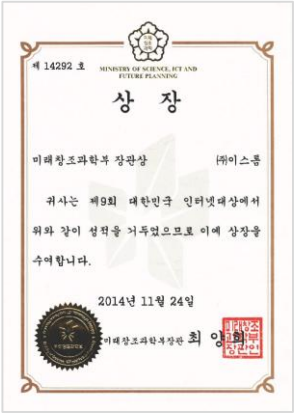
Case 4. 전산팀과 외주사의 통합 ID 인증 및 접근제어

- **도입배경** : 소규모 전산팀에서 수십여대의 서버에 대한 계정 및 패스워드 관리 업무에 대한 효율성 제고 필요
- **사업범위** : 범위 : OO여대의 윈도우 서버 및 OO여대 리눅스 서버
- **도입효과**
  - 서버시스템에 대한 체계적인 통합 계정 및 접근관리 환경을 구축
  - 외주사별 서버 접근에 대한 인증을 패스워드리스로 전환함으로서 외주인력에 대한 접근 제어 강화 및 업무효율성 제고
  - 운영관리 중인 OO여대 서버에 대한 패스워드 변경관리를 자동화함으로써 관리자 업무 효율성 향상



03 레퍼런스

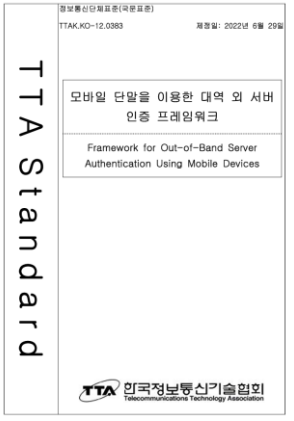
주요 시상



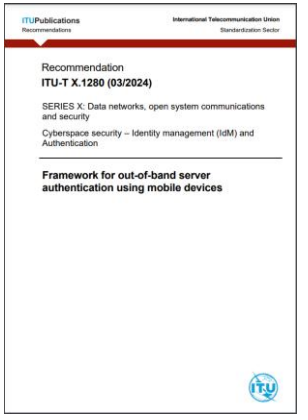
대한민국 인터넷대상

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.