DualAuth

Passwordless Identity Authentication
and Access Management

DualAuth Company Profile

DualAuth

01

Company Overview

02

Product Introduction

03

Achievements & References

04

Contact

Specialists in passwordless identity and access management

DualAuth is a technology company providing passwordless identity authentication and access management solutions. Its primary solutions include passwordless authentication solutions, integrated ID and access management, mobile ID solutions, and physical facility access management. These technologies possess outstanding usability and security, as evidenced by their adoption as ITU standards X.1280 and X.1268 under the UN's International Telecommunication Union. They are gaining attention as core technologies in the Zero Trust era. DualAuth is promoting its free Passwordless X1280 solution globally through the Passwordless Alliance based in Geneva, Switzerland, to solve password problems for B2C online services worldwide and advance ESG implementation.

Passwordless Identity Authentication and Access Management for Zero Trust Implementation

Passwordless Authentication Technology	Integrated ID and Access Management Technology	Mobile ID Technology	Physical Facility Access Management Technology
Passwordless X1280	AutoPassword	AutoPassword ID Card	AutoPassword ID Card
AutoPassword	AutoPassword Access Manager	AutoPassword ID Card Reader	AutoPassword IoT Controller

DualAuth

01

Company Overview

02

Product Introduction

03

Achievements & References

04

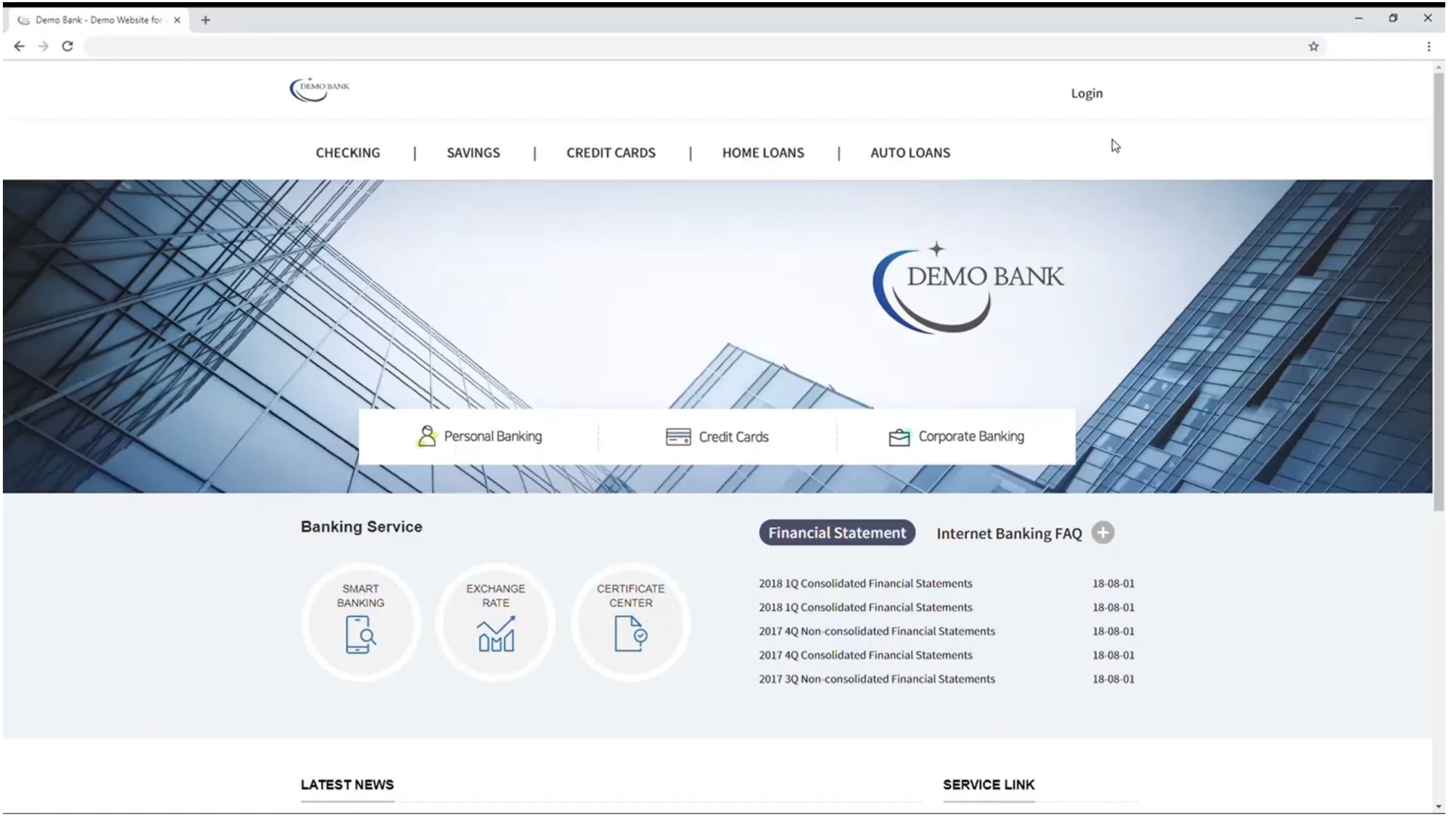
Contact

Passwordless Authentication Technology

AutoPassword

AutoPassword is a passwordless solution that employs mutual authentication technology. Instead of users entering passwords, the online system presents an auto-generated password to the user, who then verifies this password via their smartphone. (International Standard X.1280)

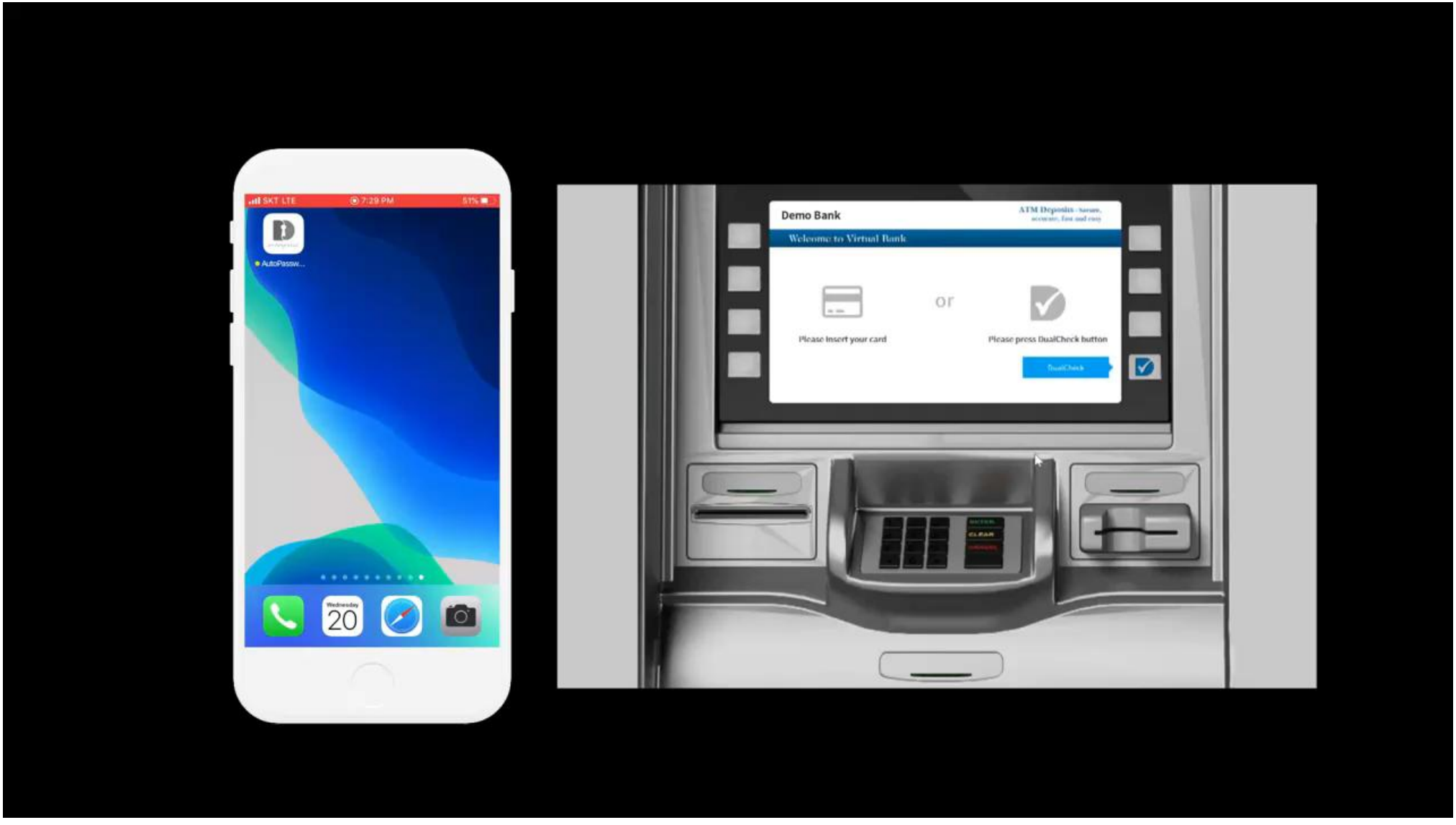
02 Product Information – Passwordless Authentication Technology



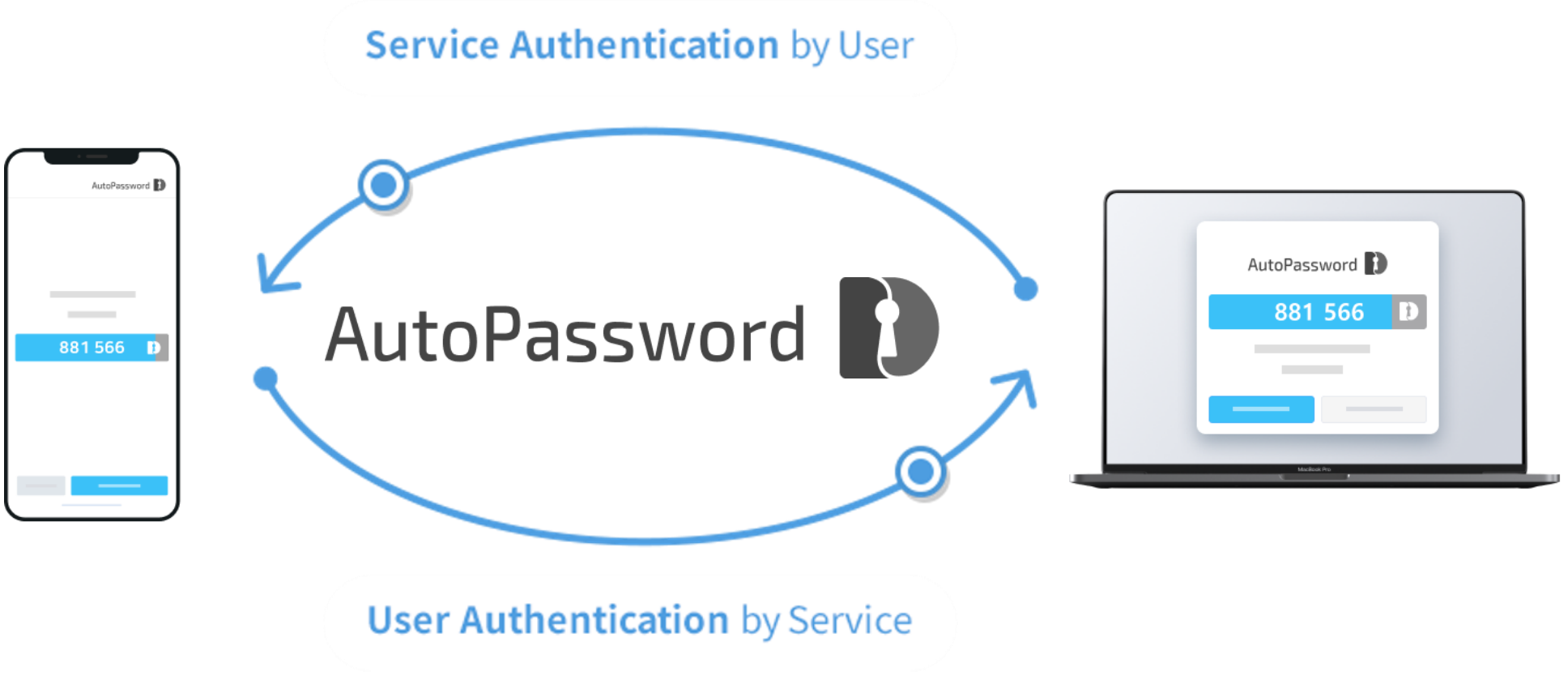
https://youtu.be/IpUyan0o4_A

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 Features

Existing user authentication technologies (passwords, OTP, certificates, biometrics, etc.) are methods where the user inputs an authentication value into an online system, proving to the system that they are the legitimate user. Therefore, the user bears the burden of proof for authentication.

However, AutoPassword is a mutual authentication technology where the accessed online system submits an auto-generated password to the user. The user then verifies this auto-generated password on their smartphone and approves it via a biometric sensor. This shifts the burden of proof for authentication to the online system.

AutoPassword Benefits

1. Shifting the user's burden of proof to the online system makes it more convenient for users. (Convenience)

2. Users can verify the authenticity of the online service they are accessing, preventing exposure to cyber attacks like phishing or pharming. (Security)

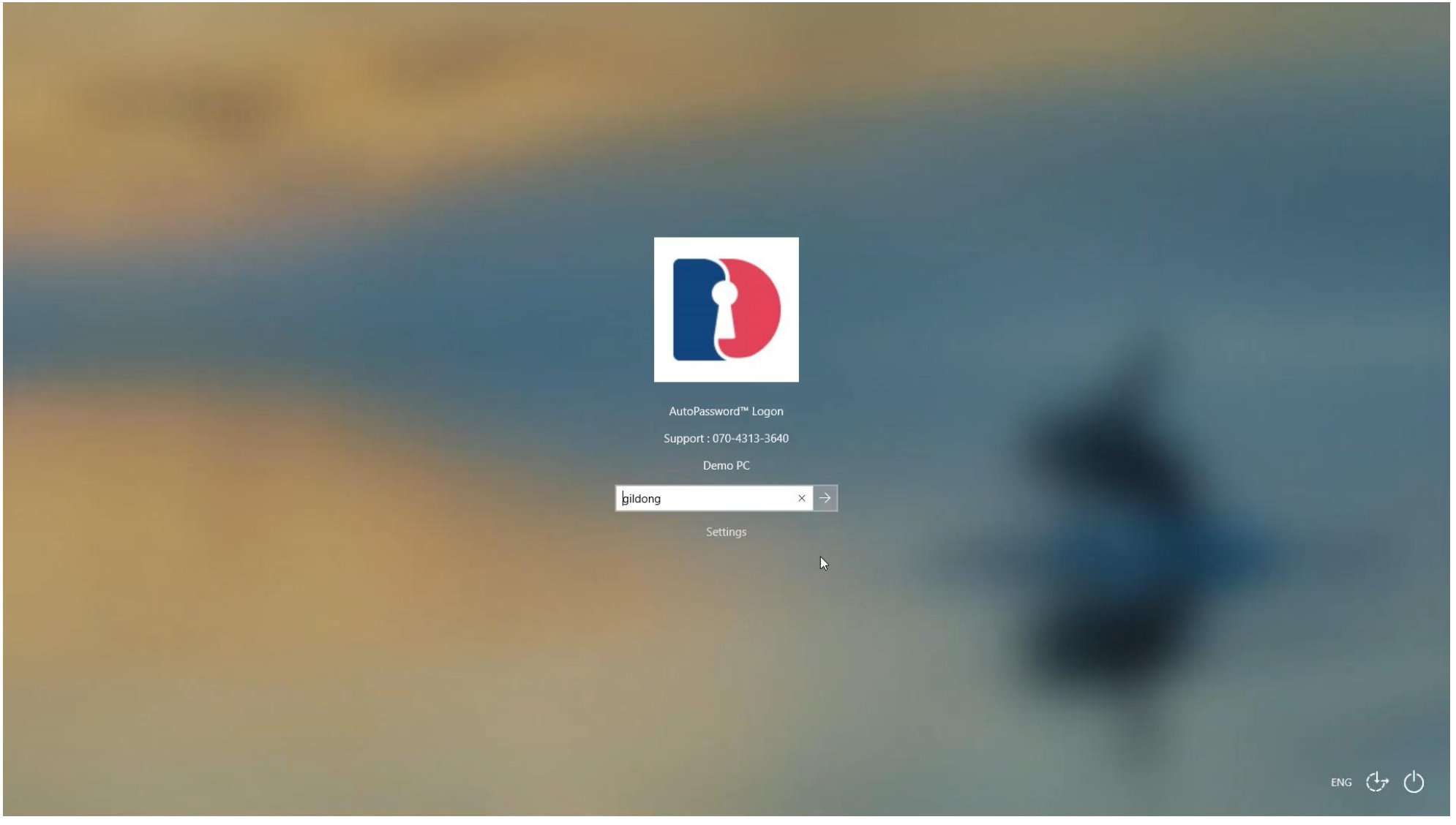
3. It enables biometric authentication on devices without dedicated biometric sensors using just the smartphone's biometric sensor. (Existing in-band biometric technologies require individual sensors per user device, whereas this technology verifies the requesting device before performing out-of-band authentication, making it the most cost-effective biometric solution available - Cost-effectiveness)

Integrated ID and Access Management Technology

AutoPassword Access Manager

AutoPassword Access Manager, an integrated ID and access management solution, is an access control technology that not only manages integrated accounts for web applications such as email and groupware, but also encompasses business Windows PCs, Linux servers, and wireless networks to establish account issuance and access policies.

Windows Demo

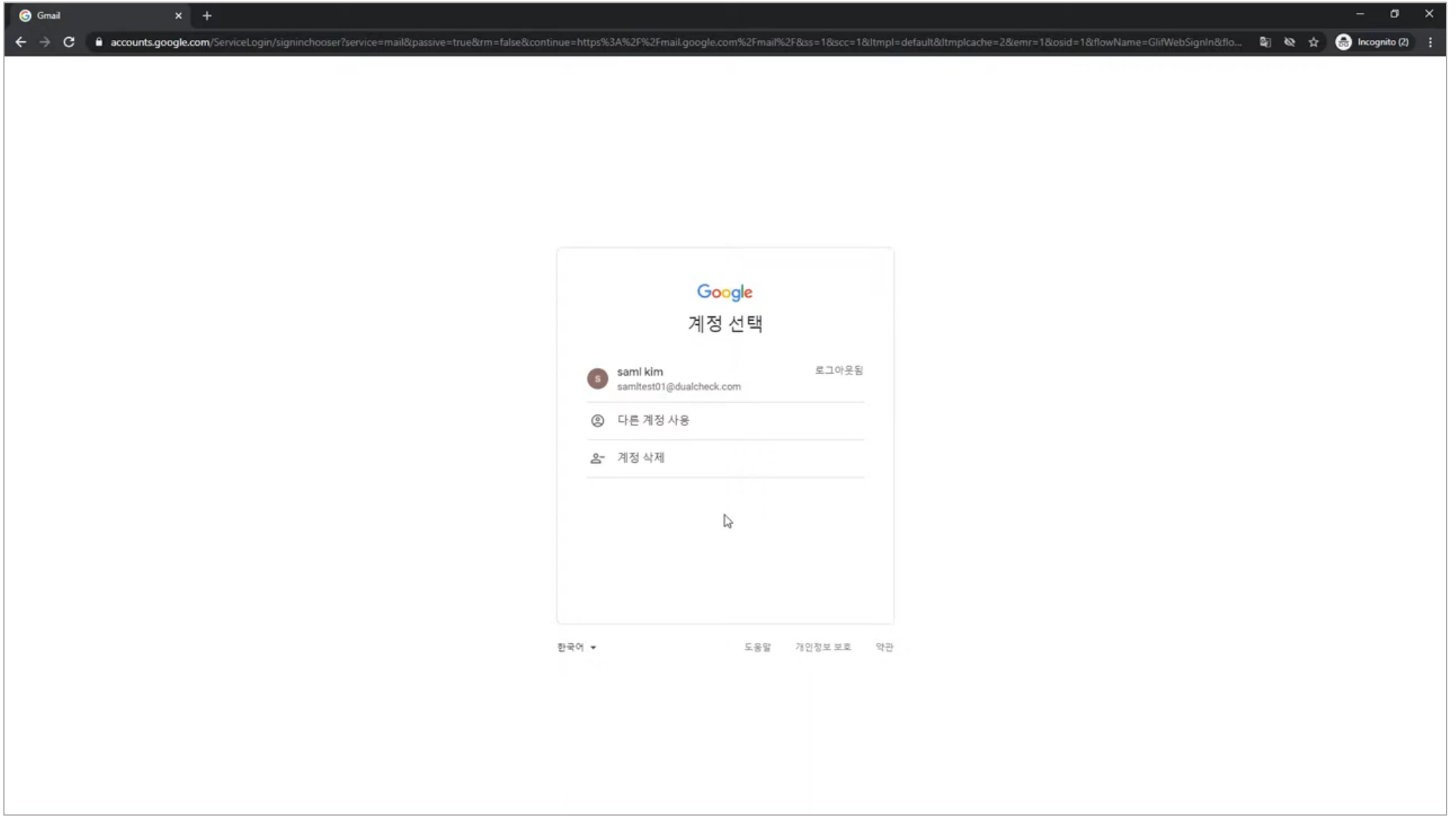


https://youtu.be/cjmjBDwgw00

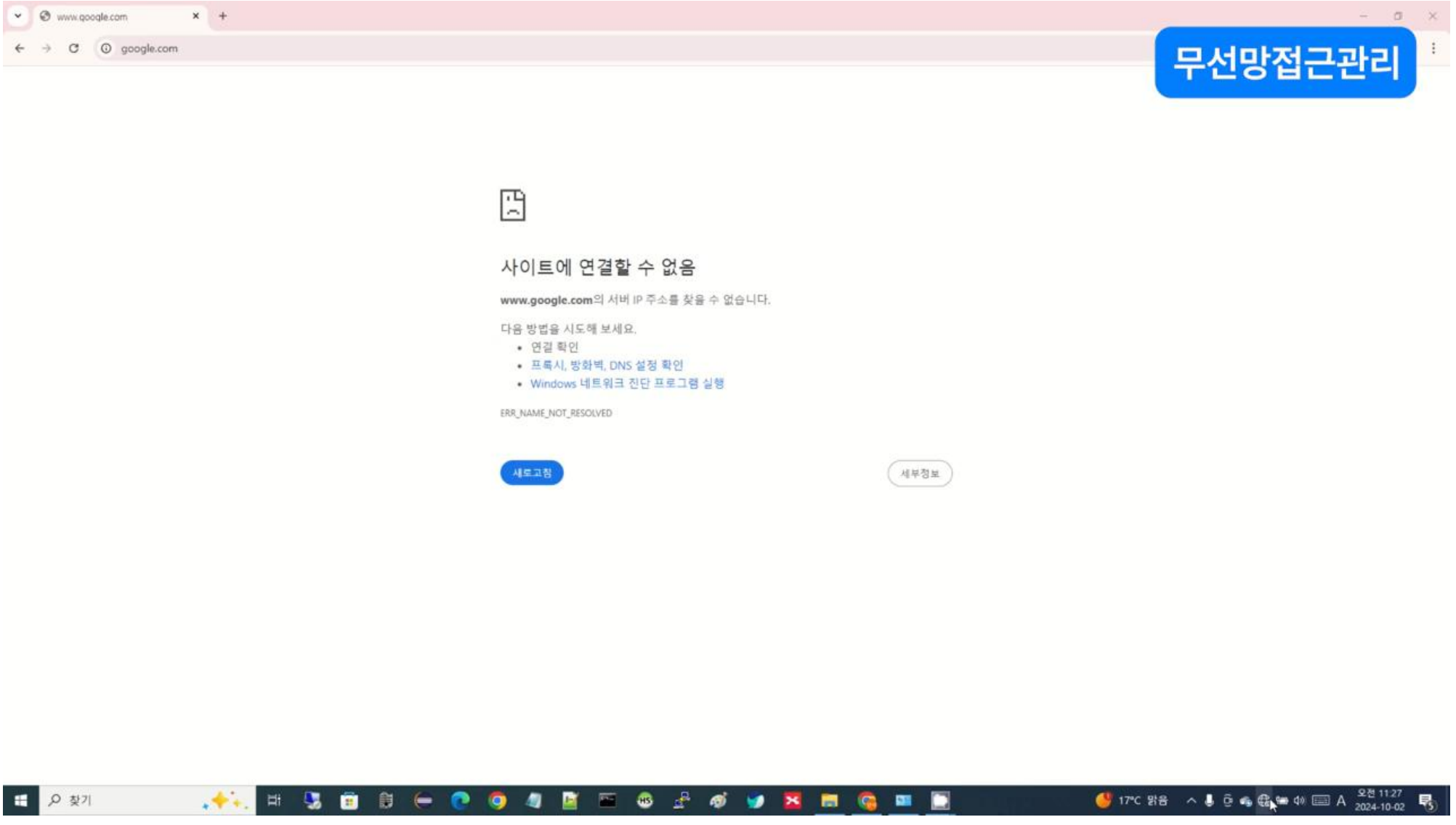
Linux Demo

https://youtu.be/FDt0i06otUI

02 Product Information – Integrated ID and Access Management Technology



https://youtu.be/l5H1C9gz7tg



https://youtu.be/3Es3Ru9OcLQ

AutoPassword Access Manager Features

Previously, the IDs and passwords used for email, Windows PCs, accessing Linux servers, and wireless networks were all separate. This made it difficult for users and administrators to manage user identification and access to resources in an integrated manner.

However, AutoPassword Access Manager is an integrated ID and access management product that enables users to be identified with a single user ID across applications used within the company, such as work PCs, Linux servers, groupware, and email, as well as wired/wireless networks. It also configures which systems that ID can access.

AutoPassword Access Manager Benefits

1. Employees can access all business systems (Windows PCs, Linux servers, email and groupware, wired/wireless networks, etc.) using a single unified ID and authentication method, simplifying the previously cumbersome management of accounts and passwords.

2. Administrators can set the scope of access to business systems per employee or organization, enabling company-wide permission management and history tracking from a single management screen.

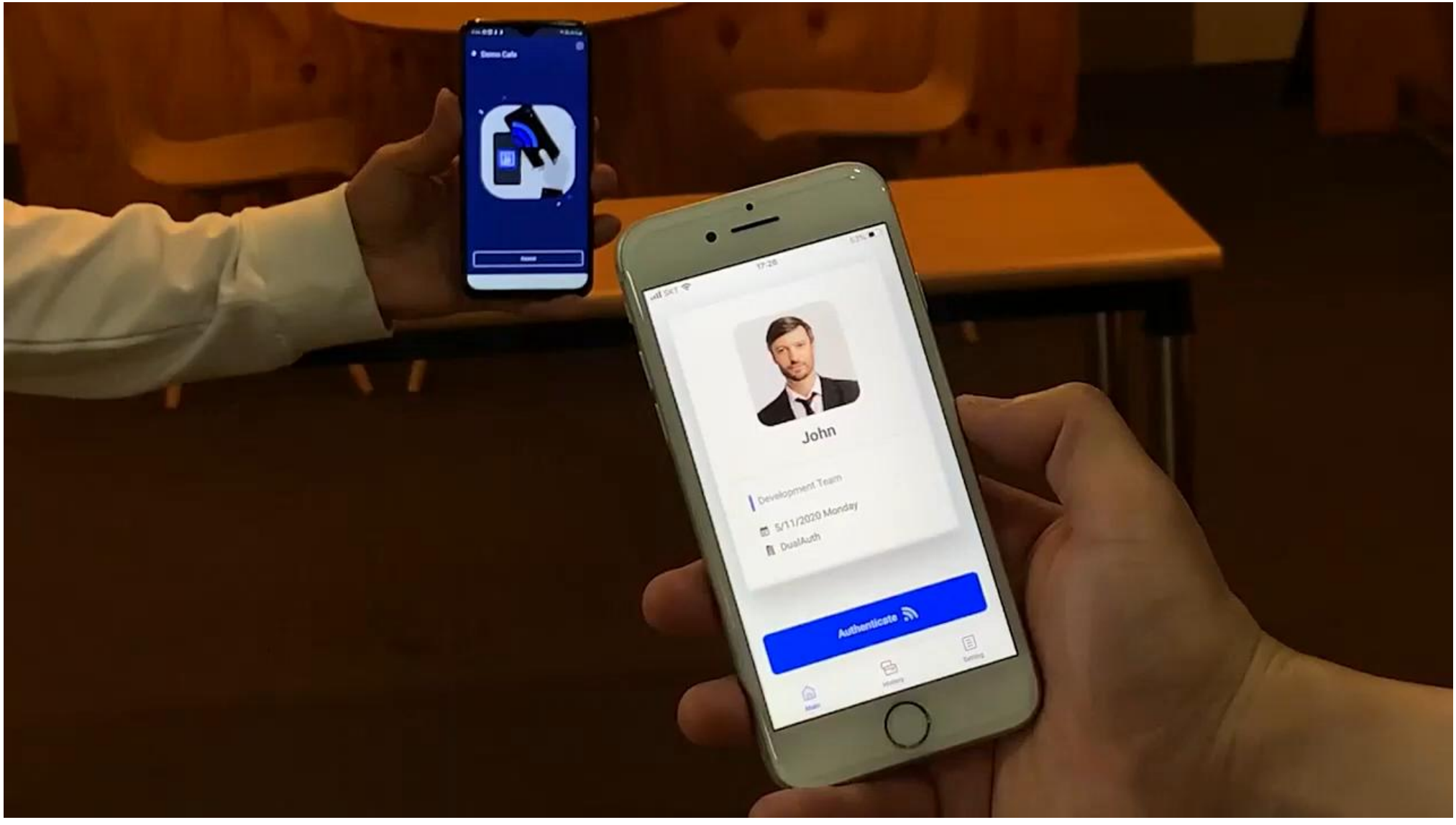
3. When the automatic OS password change feature is enabled within AutoPassword Access Manager, the OS password is automatically renewed each time a user logs into a Windows PC or Linux server, eliminating the need for users to manage their OS passwords.

모바일 신분증 기술

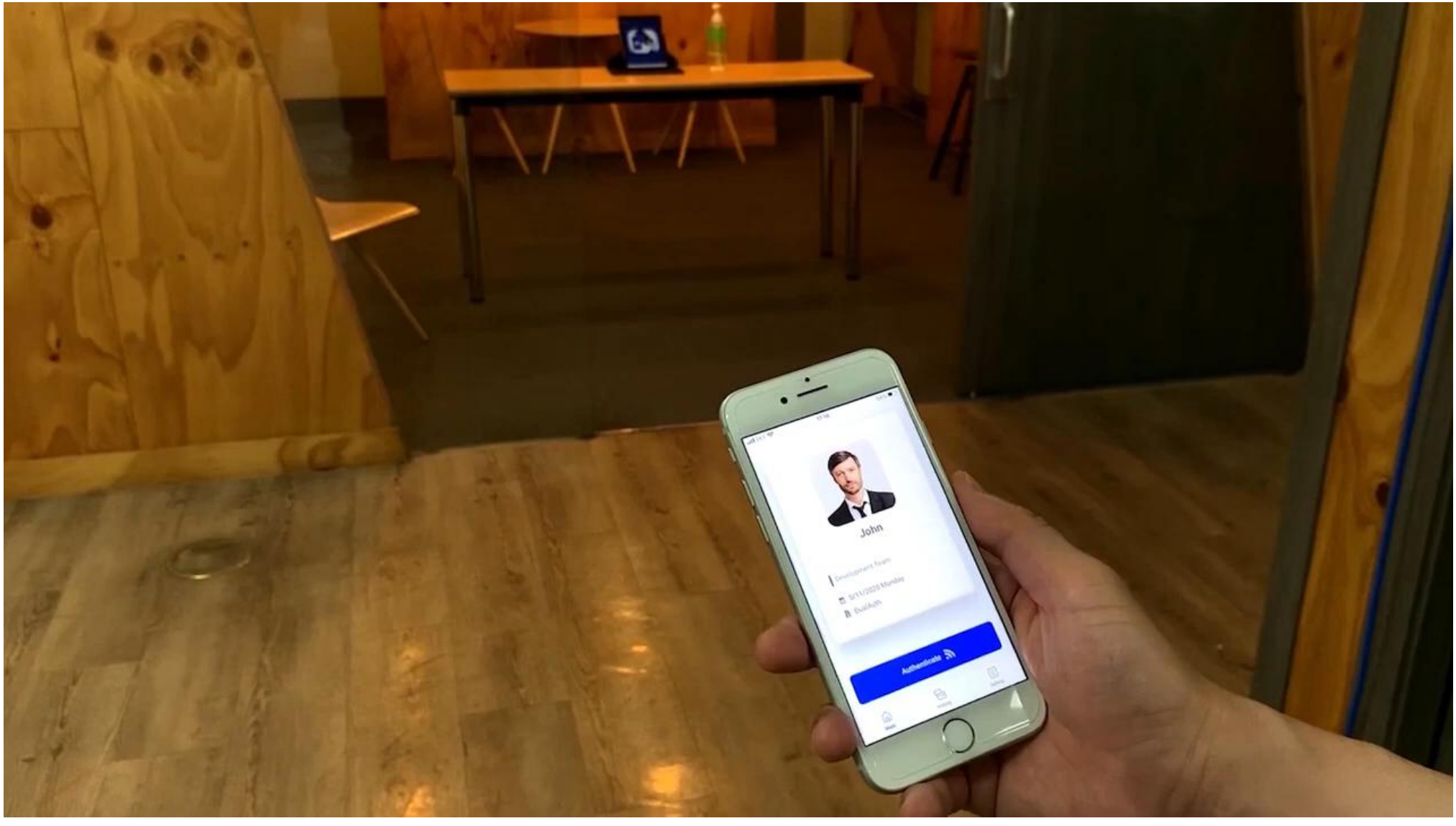
AutoPassword ID Card Reader

AutoPassword ID Card

AutoPassword ID Card, a mobile ID solution, is an out-of-band biometric authentication technology that operates based on the biometric information of company-approved users. It does not utilize the biometric authentication of smartphone manufacturers unrelated to the company at the time of mobile ID issuance. (International Standard X.1268)



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



https://youtu.be/80axVwQQbeM

02 Product Information – Mobile ID Technology

AutoPassword ID Card Features

Existing mobile ID cards only verify the holder's identity at the initial issuance stage. Subsequent uses of the mobile ID card do not require separate identity verification; instead, the smartphone OS's biometric authentication is used to confirm the ID card holder. Consequently, service providers receiving mobile ID cards have no way to verify whether the person presenting the mobile ID card is the same individual verified during the initial ID card issuance.

In contrast, AutoPassword ID Card allows users to request administrators to register a photo taken with their smartphone camera as their identity verification image. Once approved by the administrator, the mobile ID performs biometric authentication only using that approved photo. This prevents anyone other than the original user from misusing the mobile ID.

AutoPassword ID Card Benefits

1. The camera capturing the user's photo and the camera recognizing the user are the same, resulting in a high biometric authentication success rate. (Convenience)

2. Every time a user uses the mobile ID card, it verifies if they are the person approved by the administrator. All users' biometric data is stored only on the user's smartphone. (Security)

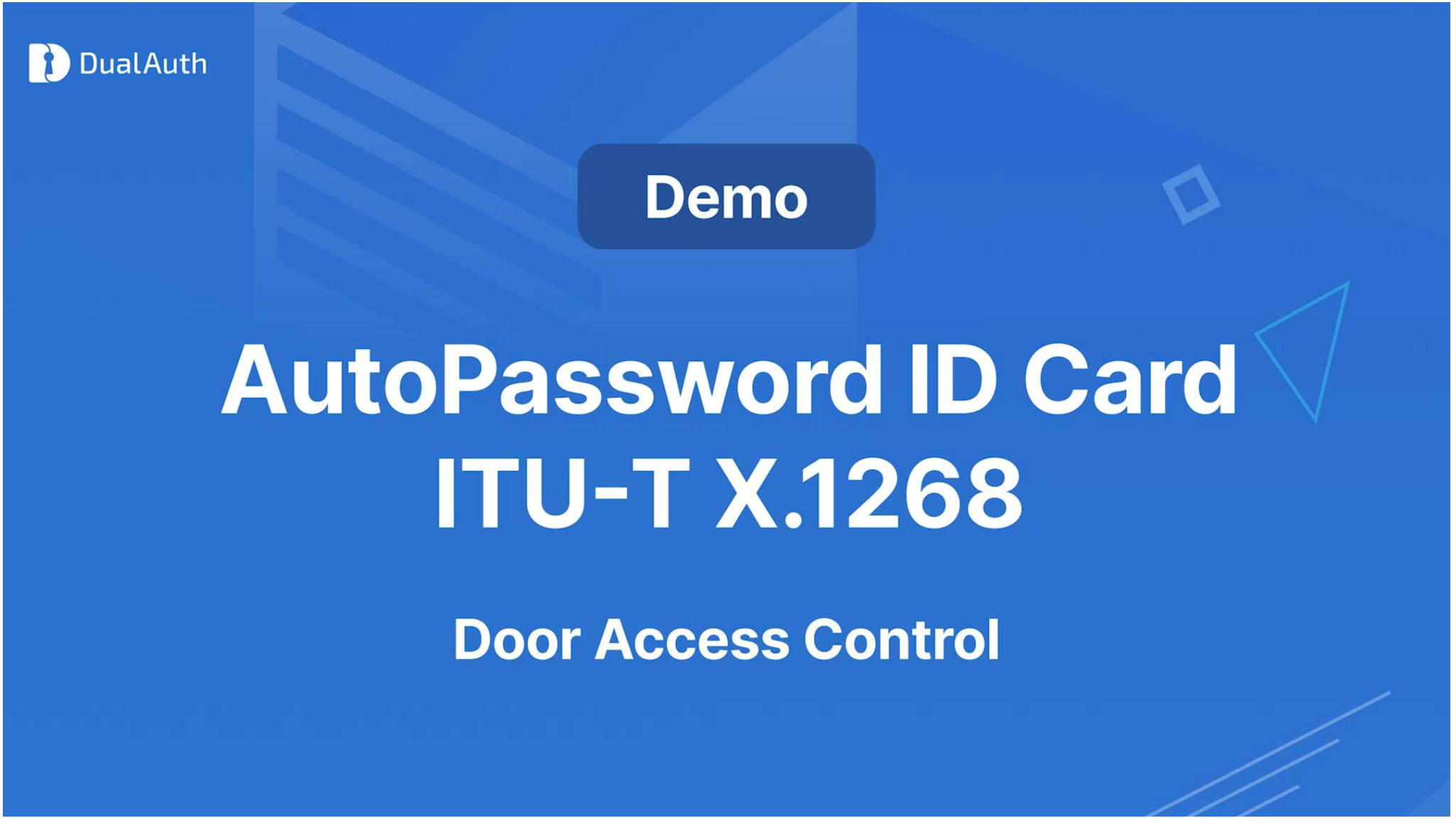
3. Biometric authentication can be performed using the biometric template stored within the mobile ID card, without requiring separate biometric sensors on other devices like PCs or tablets. (Cost-effectiveness)

Physical Facility Access Management Technology

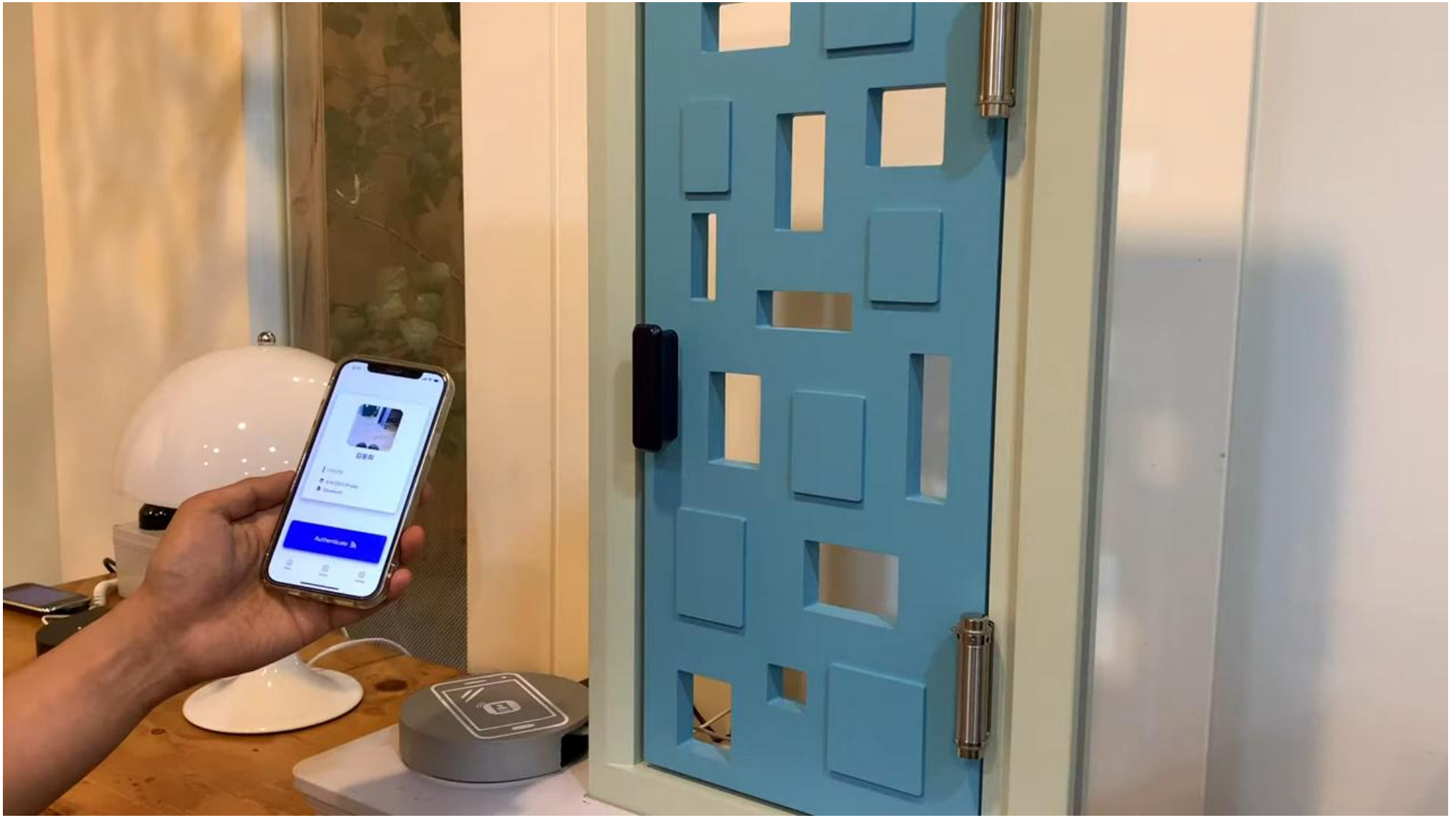
AutoPassword IoT Controller

AutoPassword ID Card

AutoPassword IoT Controller, a physical facility access management solution, is an out-of-band physical facility access management technology that performs access control to physical facilities using biometric authentication registered on the user's smartphone, without collecting the user's biometric data at unmanned facilities. (International standard X.oob-pacs currently being established)



https://youtu.be/S3favCBySLY



https://youtu.be/gdfakJZ-igI

https://youtu.be/uwKGa_ejF1M

02 Product Information – Mobile ID Technology

AutoPassword IoT Controller Features

Existing in-band authentication methods for mobile IDs require direct contact with a reader. However, communication protocols vary by smartphone manufacturer, making standardization difficult. From the user's perspective, NFC settings differ per smartphone, and QR code methods require scanning at a reader with both a camera and display—a cumbersome process. Furthermore, current readers verify only the user's authentication value without confirming the legitimacy of the device, creating potential security vulnerabilities.

The AutoPassword IoT Controller solves these problems. This device transmits an authentication beacon value to the user's AutoPassword ID Card app. The app verifies this value and then authorizes the smartphone to access the physical facility. Through this out-of-band mutual authentication method, any smartphone can safely control physical facilities using the mobile ID card via the same procedure.

AutoPassword IoT Controller Benefits

1. Users can utilize their mobile credentials not only at close range but also at short distances. (Convenience)

2. Users can first verify the physical facility and then choose whether to use their ID. Since it utilizes biometric information stored within the smartphone, there is no need to store biometric data separately at the physical facility. (Security)

3. Since the authentication beacon information for the physical facility is verified out-of-band on the smartphone, no external devices such as separate biometric sensors, NFC readers, or QR code scanners are required beyond Bluetooth. (Cost-effectiveness)

DualAuth

01

Company Overview

02

Product Introduction

03

Achievements & References

04

Contact

03 Achievements & References

Major Awards

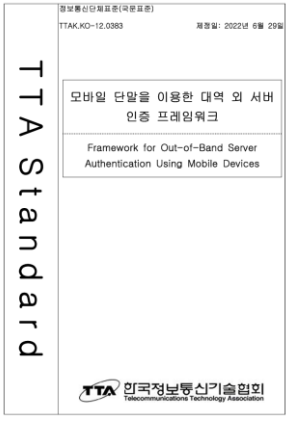
LONDON

FinTech Innovation Awards
2016 Finalist

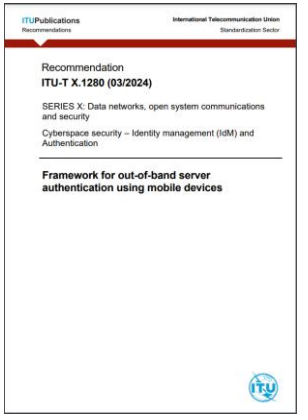
SEOUL

Korea Internet Grand Prize
Winner

Standard Technologies



TTAK.KO-12.0383



ITU X.1280

Key Announcements

NEW YORK
FinovateFall 2016
Presenter
https://youtu.be/w2NtbPVaHSk

HONG KONG
FinovateAsia 2016
Presenter
https://youtu.be/bRigHk2rkOc

NEW YORK
FinovateFall 2018
Presenter
https://youtu.be/-DG-LYmRVfk

https://youtu.be/nF72E24BCec

Major Certifications

ISO/IEC 25023, 25051, 25041

03 Achievements & References

KB국민은행	KB Kookmin Bank - Establishing and applying a mutual authentication-based enhanced user authentication system through the Zero Trust Adoption Pilot Project
우리은행	Woori Bank - Passwordless PC access management and application access management for Woori Bank employees
유안타증권	Yuanta Securities - Passwordless PC access management and application access management for Yuanta Securities employees
통계청	National Library of Korea - Controlling login rights for statistical information viewing PCs installed in the library introduced by Statistics Korea
KORAIL	Korea Railroad Corporation - Implemented passwordless authentication to strengthen user terminal authentication security for the next-generation Nara Market System
KOMSA 한국해양교통안전공단	Korea Maritime Transportation Safety Authority - Enhanced user login security using passwordless authentication for external webmail login
한국관광공사	Korea Tourism Organization - Enhanced authentication security for managers and partners for system development operations in every corner of Korea
KIAT	Korea Advanced Institute of Industrial Technology - Introduced to internal work system for employees to control individual access to internal and external networks
구리시	Guri City Hall - Responding to security compliance through login security and automatic password change when accessing important servers
CWA 건설근로자공제회	Construction Workers' Mutual Aid Society - Strengthened login security of server system to improve internal system operation

DualAuth

01

Company Overview

02

Product Introduction

03

Achievements & References

04

Contact

DualAuth

- Company : DualAuth
- Web : www.dualauth.com
- General Inquiry : support@dualauth.com

Headquarter

- Address : 130 Digtal-ro,Suite 1311,Gumchon-gu Seoul 08589
- Telephone : +82-2-6925-1305
- Business Inquiry : Kim Wonjin Director kwj@dualauth.com
  010-3438-8085 (Mobile)

DualAuth

Thank you