DualAuth

Passwordless and keyless mobile ID

AutoPassword ID Card Product Introduction

DualAuth

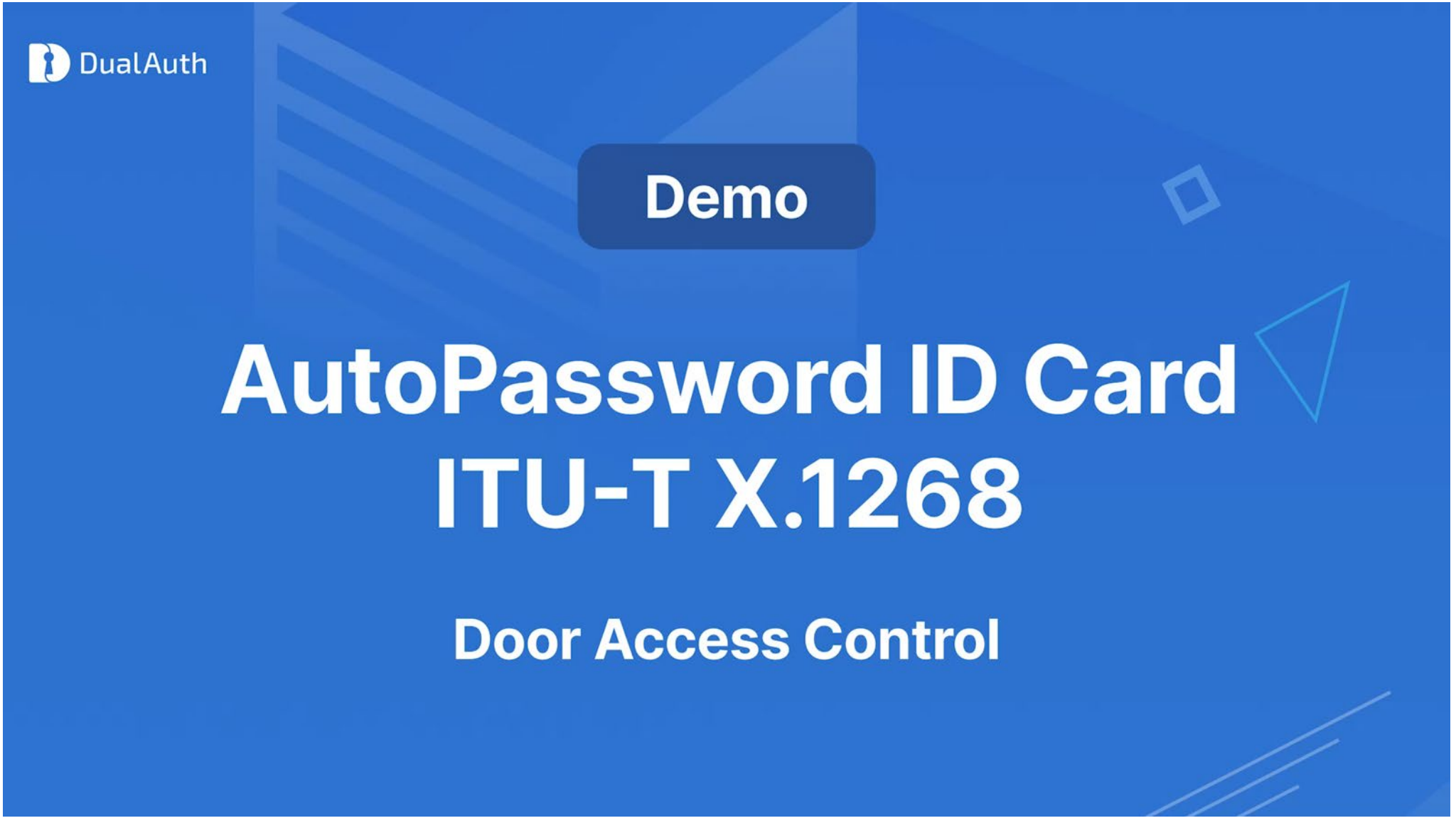
Passwordless and Keyless Mobile ID Card

AutoPassword ID Card

AutoPassword ID Card is a mobile ID supporting Passwordless and Keyless authentication. Through smartphone biometric authentication, users can securely perform mutual authentication with online systems and offline facilities.

Furthermore, when combined with a VDS (Visible Digital Seal)–based BioIDCard containing biometric data, the AutoPassword ID Card enhances security by granting access to online systems and offline facilities only after confirming that the biometric data captured during BioIDCard issuance matches that of the current mobile ID user.

AutoPassword ID Card technology is developed based on the international standards ITU-T X.1280 (Passwordless), ITU-T X.1268 (Keyless), and ISO 22378 (VDS).

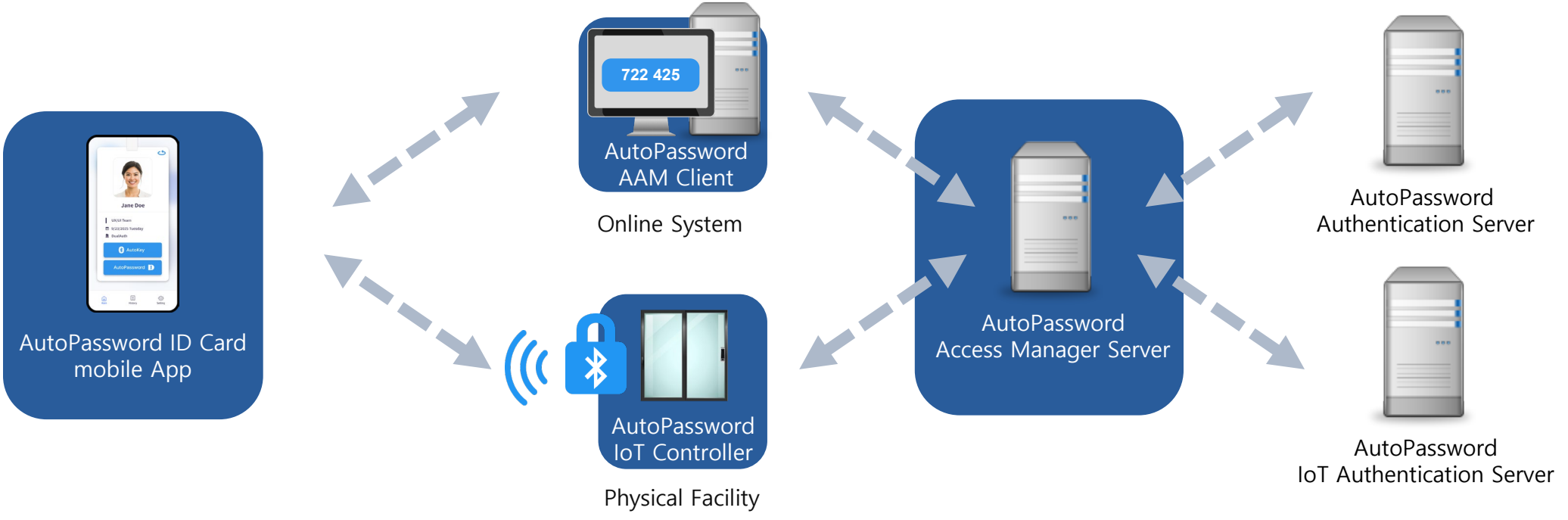


https://youtu.be/S3favCBySLY

AutoPassword ID Card Architecture

To use the AutoPassword ID Card, an enterprise or institution must integrate its online systems and physical facilities with the AutoPassword Access Manager and then distribute the AutoPassword ID Card to users.

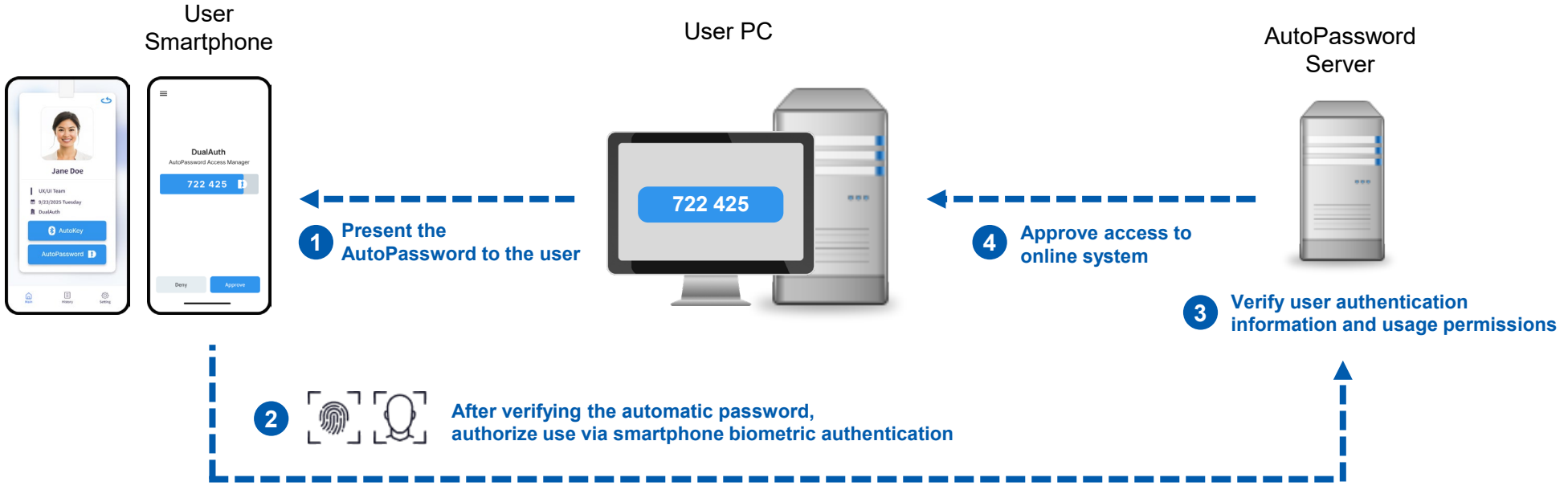
Users install the AutoPassword ID Card on their smartphone and activate it by completing an initial identity verification process (such as registering a password, confirming an email code, or registering a BioIDCard). After activation, users can securely access online and offline services using only their smartphone's biometric authentication, without needing separate passwords or physical keys when using online systems or offline facilities.



DualAuth

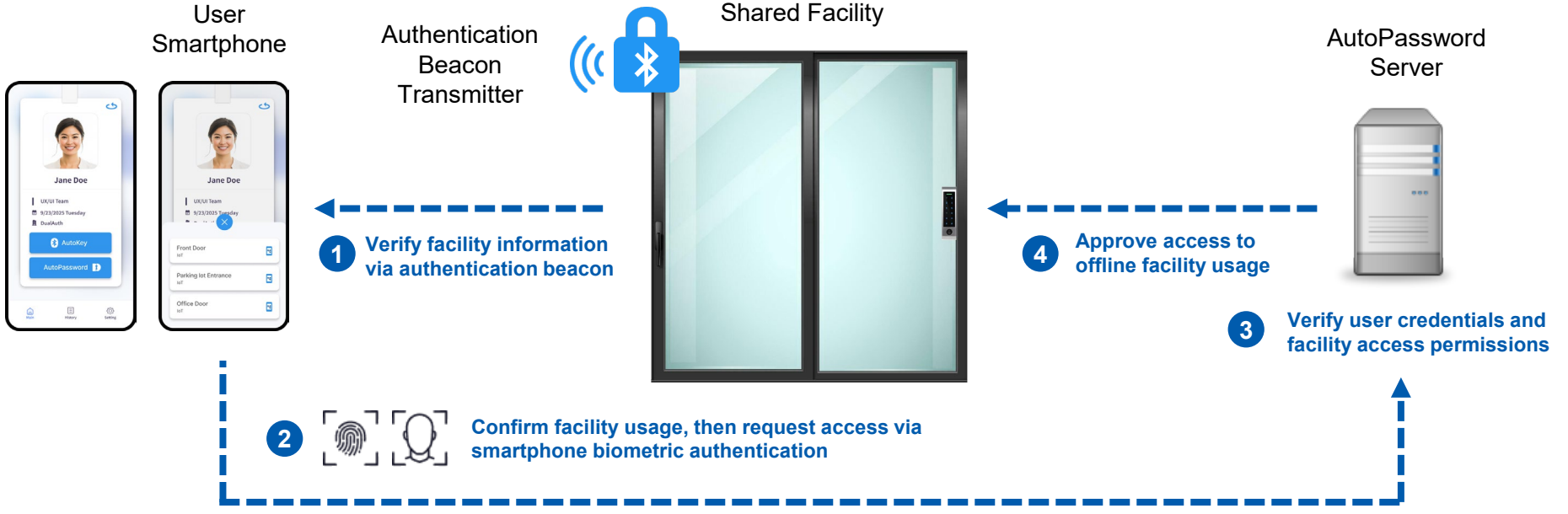
Feature 1 – Mobile ID Card Supporting Passwordless Authentication for Online Systems

The AutoPassword ID Card incorporates AutoPassword, a passwordless technology. AutoPassword is a mutual authentication technology where, instead of the user entering a password into an online system, the online system presents an auto-generated password to the user. The user then verifies this auto-generated password submitted by the online system via their smartphone and approves it. AutoPassword does not input or store passwords or authentication values on the user's device during the authentication process. Consequently, attempts to steal authentication information through existing attack methods such as phishing, pharming, and man-in-the-middle attacks are fundamentally neutralized. (ITU-T X.1280 international standard)



Feature 2 – Mobile ID for Offline Facility Access Without Cards or Keys

AutoPassword ID Card incorporates AutoKey, a keyless technology. AutoKey is a mutual authentication technology where, instead of the user inputting passwords, RFID cards, or biometric data at offline physical facilities, the facility transmits an authentication beacon. The user then verifies the facility via their smartphone and approves access using smartphone biometric authentication.
AutoKey utilizes the smartphone's biometric authentication, eliminating the need for physical facilities to separately register or store biometric data. It operates identically on both iPhone and Android devices, providing a standardized user experience. Furthermore, it eliminates the need to expose separate readers on exterior walls, enabling convenient use in offices and shared facilities. (Based on the international standard ITU-T X.1268)



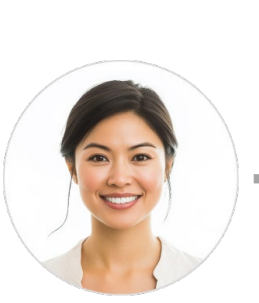
Feature 3 – Mobile ID Authentication Based on Issuer-Verified Biometric Information

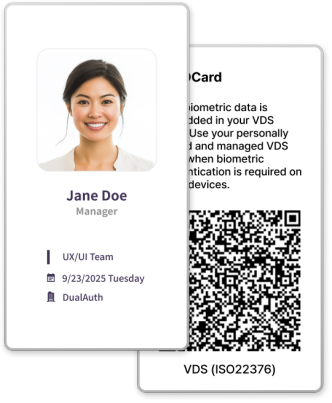
Existing smartphone-based mobile IDs had a structural limitation: if someone else's biometric information was added to the smartphone after the mobile ID was installed, unauthorized use by an unapproved user could occur.

In contrast, AutoPassword ID Card additionally supports a VDS (Visible Digital Seal)-based biometric verification mechanism beyond smartphone-based biometric authentication. Activating AutoPassword ID Card with a **VDS-based BioIDCard** containing biometric data enables enhanced security. Access to online systems and offline facilities is permitted only when the biometric data of the current AutoPassword ID Card user matches the biometric data verified during BioIDCard issuance.

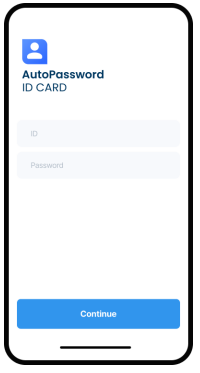
Generate VDS code from photo

Generate BioIDCard ID with attached VDS code

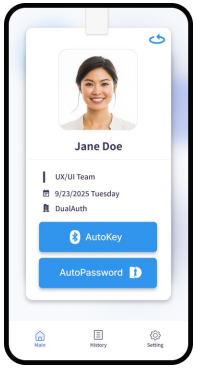




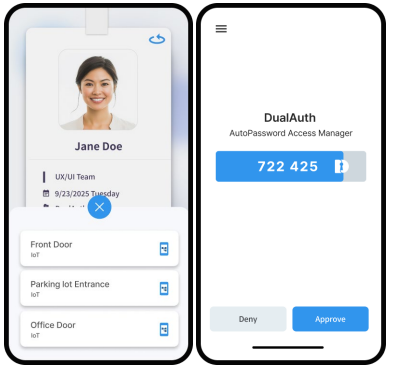
Install AutoPassword ID Card app



Activate AutoPassword ID Card



Use AutoPassword ID Card with biometric information verified by issuer



Activate AutoPassword ID Card when biometric data in VDS matches current user

Verify match between biometric data verified by issuer and current user when accessing online systems or physical facilities

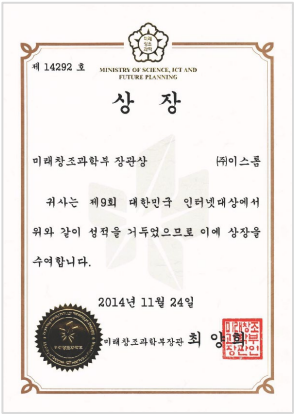
DualAuth

03 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

03 References

Awards


제 14292 호 MINISTRY OF SCIENCE, ICT AND FUTURE PLANNING

상 장

미래창조과학부 장관상 (주)이스룸

귀사는 제9회 대한민국 인터넷대상에서 위와 같이 성적을 거두었으므로 이에 상장을 수여합니다.

2014년 11월 24일

미래창조과학부장관 최 양희

The Korea Internet Awards


제17511호

상 장

-표준특허 창출지원 우수 참여기관-

(주)이스룸

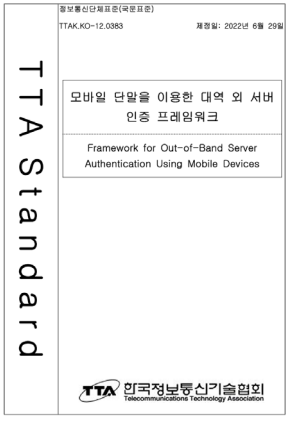
귀 기관은 표준특허 창출지원 사업을 통해 우수한 성과를 창출하여 표준특허 창출·활용 전략 확산에 기여한 바가 크므로 이 상장을 수여합니다.

2025년 6월 26일

특허청장 김

The Commissioner's Award

Standard Technologies


정보통신단체표준(국문표준)

TTAK.KO-12.0383 제정일: 2022년 6월 29일

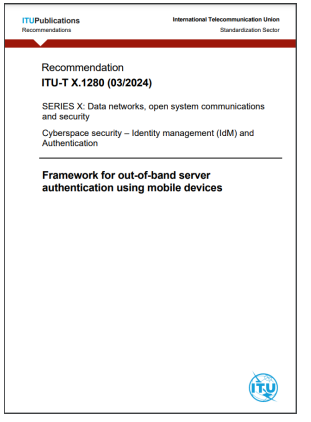
TTA Standard

모바일 단말을 이용한 대역 외 서버 인증 프레임워크

Framework for Out-of-Band Server Authentication Using Mobile Devices

TTA 한국정보통신기술협회 Telecommunications Technology Association

TTAK.KO-12.0383


ITUPublications Recommendations

International Telecommunication Union Standardization Sector

Recommendation

ITU-T X.1280 (03/2024)

SERIES X: Data networks, open system communications and security

Cyberspace security – Identity management (IdM) and Authentication

Framework for out-of-band server authentication using mobile devices

ITU X.1280

Presentations

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

Certificates

fido CERTIFIED UAF

GOOD Software

ISO/IEC 25023, 25051, 25041

oath initiative for open authentication

IBM Security

NEP 신제품인증 NEW EXCELLENT PRODUCT

DualAuth

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.oob-pacs 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
AutoOTP	AutoPassword	AutoPassword ID Card	AutoPassword ID Card
AutoPassword	AutoPassword Access Manager	AutoPassword ID Card Reader	AutoPassword IoT Controller

04 Contact

DualAuth

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

Request Implementation

- Address : 130 Digital-ro, Suite 1311,Gumchon-gu Seoul 08589
- Telephone : +82-2-6925-1305
- Business Inquiry : sales@dualauth.com

DualAuth

Thank you